Realization of Integrated Mobility Management Protocol for Ad-Hoc Networks

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

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

Abstract—

A multi-layer mobility management architecture has been designed to take care of real-time and non-real-time traffic for intra-domain and inter-domain mobility in a survivable network. It consists of three components based on functionality. SIP based mobility management is used for real-time communication, and MIP-LR is used for non-real-time communication when nodes move between two different domains while MMP takes care of movement within a domain. A testbed has been implemented using the features of each mobility management approach in an integrated manner. In this paper we present our implementation and integration experience of these three mobility management protocols and evaulate their performance under simulated military environment while interacting with Dynamic DNS, DRCP/DCDP and coordinating among themselves based on the application type and domain being served.

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 without affecting the ongoing multi-media session.

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], [6] while providing support for personal, terminal and session mobility. [5] provides a performance evaluation of IP Micro-Mobility Management using host based routing scheme. 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 associated 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 as 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], [10] 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 [11]. Although a new transport protocol called SCTP [14], can be used with SIP to take care of traffic due to mobility when IP address changes.

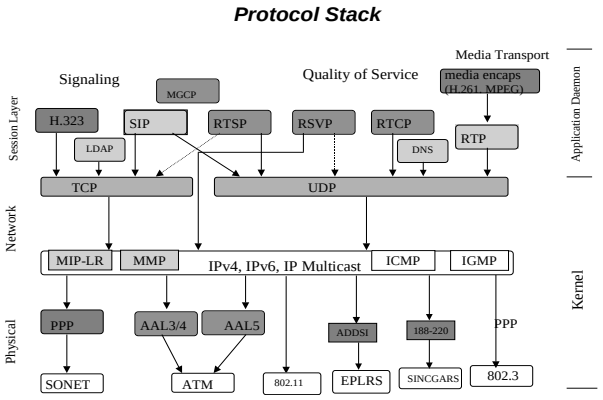

Fig. 1. Mobility Management Protocol Stack

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.

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

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 from simulation and experiments. Section III briefly describes the mobility management architecture for a typical military environment and how these mobility protocols fit together. Section IV cites some related work, and section V concludes the paper with some open issues.

II. Mobility components

The sections below provide some simulation and experimental results carried out for each of these mobility management techniques. In each case, results were compared with

that of traditional Mobile IP approach. A new architecture has been designed, where all three mobility management components can function simultaneously on the same terminal while taking care of its own individual function. MMP takes care of movement of the clients within a micro-mobility domain, SIP takes care of real-time communication such as RTP/UDP, and MIP-LR takes care of non-real-time communication such as TCP based application for inter-domain mobility. In an integrated demonstration it has been shown that, MMP, SIPMM and MIP-LR can co-exist without affecting each other.

A. Application Layer Component - SIP based approach

Application layer mobility management is based on Session Initiation Protocol which has been proposed standard as an RFC 2543 in IETF [16]. [3] provides a good background about the application layer mobility management using SIP.

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 [19] 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. 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 [17]. 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.

B. SIP Performance

Using SIP for mobility management of real-time traffic provides 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 show the relative performance difference between SIP and Mobile IP

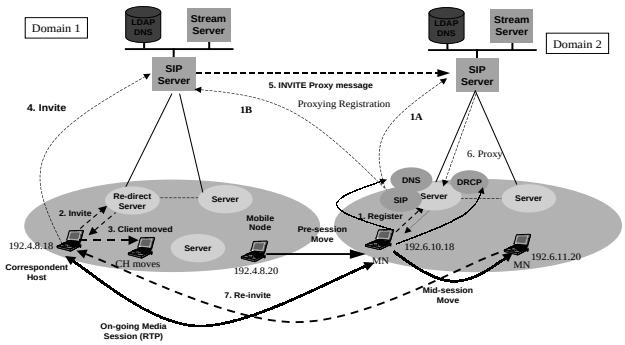

Fig. 2. SIP Mobility for a Survivable Network

under different network conditions obtained both from simulations and experimentation. Experiments were 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.

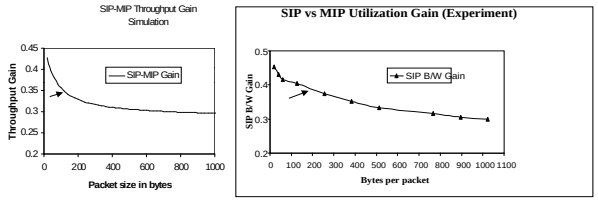

Fig. 3. SIP/MIP Signaling and Transport Overhead

As part of the experiment, SIP based terminal mobility for real-time traffic was tried using a modified and customized version of Columbia University's sipc (SIP client) and sipd (SIP server). Following section provides some performance measurement during subnet mobility. A Multimedia SIP session for real-time traffic was established between two clients in a IEEE 802.11 environment. The mobile host moves away from the CH while the session is in progress. As soon as the mobile host discovers that it is in a new subnet it gets a new IP address using DRCP [13] a light-weight version of DHCP, sends a Re-Invite to the corressponding host and sends a new registration message to the registrar. Packet sizes for different messages are also noted. For initial call set up a typical INVITE message was 455 UDP bytes, ringing was 223

bytes, OK was 381 bytes, ACK was 216 bytes, REGISTER and its OK messages were about 370 bytes and 412 bytes. Subsequent de-registration and re-registration messages were of 372 and 425 bytes respectively followed by OK messages which were of size 510 and 410 bytes.A typical Re-Invite after subnet change and respective OK messages were 450 and 380 UDP bytes respectively. It takes about 100 msec for the processing time on Linux based MH between consecutive messages (e.g., between receiving an OK and sending the ACK which is strongly OS dependent). It took about 5 msec to forward the INVITE packet to traverse between MH and CH when MH is at home. As the MH moves away to a foreign network with more network routers in between, Re-INVITE takes about 70 msec because of the queueing delay at the routers enroute. The SIP registrar was placed in the middle of the network between the two domains, it took about 150 msec to complete the whole re-registration process, however it takes more processing time to delete the old registration than updating a new one at the registrar. These figures would vary depending upon the operating system, and network topology. It would be desirable to reduce the Re-Invite time, re-registration time in a wireless roaming environment for faster handoff and avoiding loss of data.

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 takes care of many of the issues associated with a survivable network such as location of the home agent, home agent vulnerability, triangular oruting and tunneling associated with Mobile IP.

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 by using Linux's new libipq and iptables utility. In addition, the database mapping of 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.

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 4 shows the use of MIP-LR in an adhoc networking environment where some of the nodes may be actually airborne.

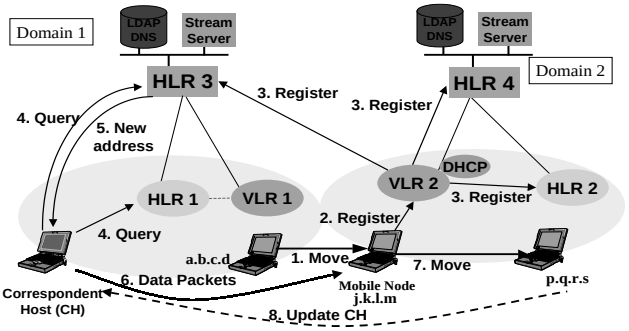

Fig. 4. MIP-LR for a Survivable Network

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 5 provides an anlaytical and experimental comparison between MIP and MIP-LR.

MIPLR registration request is about 52 bytes, where as registration reply is about 50 bytes UDP packets. MIP-LR query

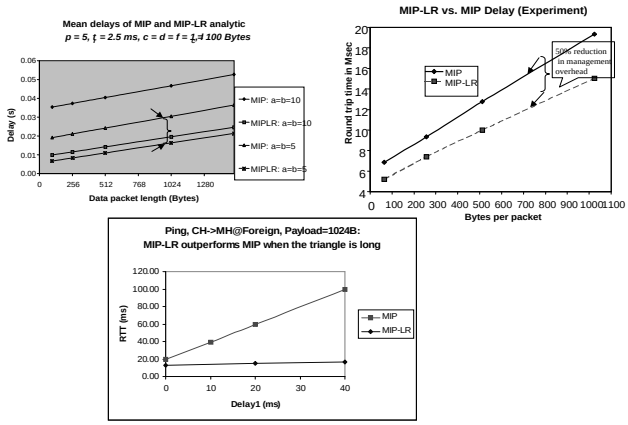

Fig. 5. Cost comparison MIP vs. MIP-LR

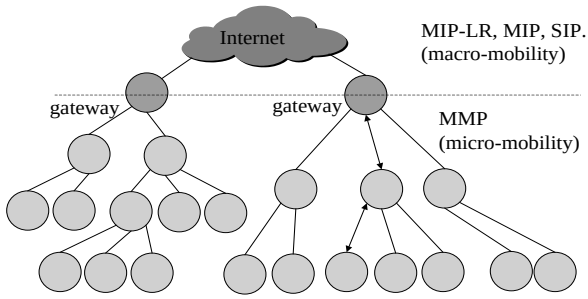

Fig. 6. An abstraction of MMP

made by CH is about 24 bytes. LR notifies the CH about the MH location using a 28 byte response packet. As the MH gets a new address it notifies the CH and LR using a binding update message which is about 28 byte. An additional 28 byte header(20 byte IP and 8 byte UDP)

E. Micro Mobility Management Component - MMP

MMP is a derivative of the Cellular IP/HAWAII family of micro-mobility schemes [6], [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 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. 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.

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 both simulation and experimental results obtained from the testbed.

III. Integrated Mobility Management Testbed

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.

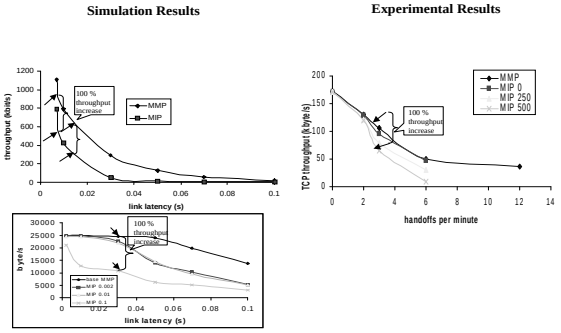

Fig. 7. MMP throughput with varying latency

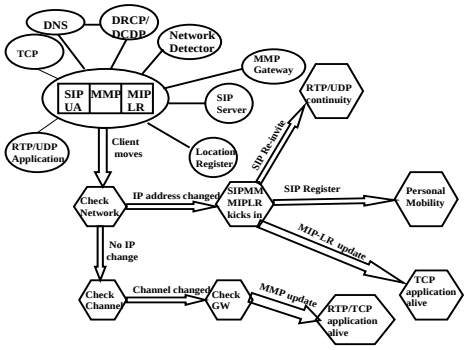

Fig. 9. IMM logical flow

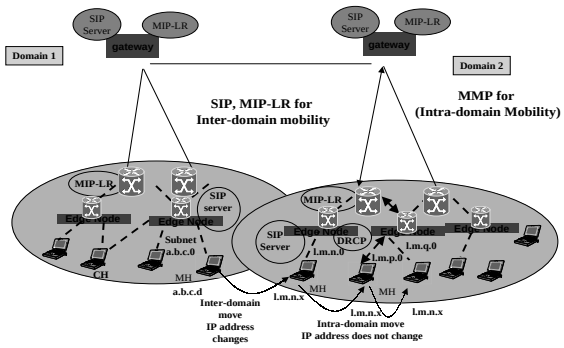

Fig. 8. Integrated Mobility Management

Proposed mobility management architecture mostly relies on server based approach. Figure 8 shows the mobility architecture taking into account all three mobility management approaches. This mobility architecture assumes that the end hosts are smart and IP addresseable, 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 becomes active depending on if the client is communicating via real-time traffic (RTP/UDP) or 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 for pre-session mobility.

IP address management is made possible by using DRCP/DCDP servers. DRCP (Dynamic Rapid Configuration Protocol) is faster version of DHCP. DRCP server configures a node's interface with an IP address, and provides the addresses of DNS server, SIP server etc. DCDP (Dynamic Configuration and Distribution Protocl) server provides a pool of IP addresses to the node so that it can behave like a DRCP server. In the integrated mobility management scheme 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 nodes and MMP-GW, where the gateway would act like a DRCP/DCDP server, and one of the MMP nodes acts like a DRCP server.

Figure 9 shows a logical view of how all the components interact with each other while providing an Integrated Mobility Management solution for both Real-time and Non-real-time traffic.

Each MMP node has two interfaces. One of the interfaces

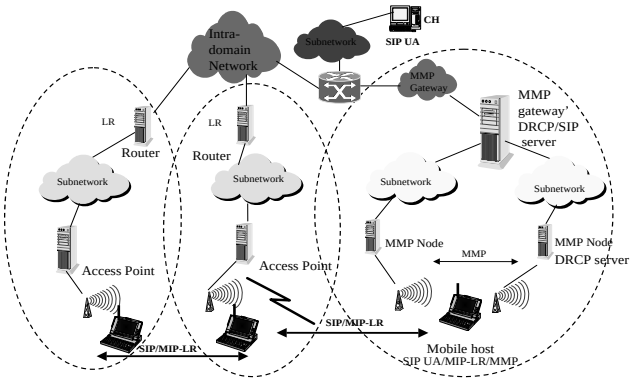

Fig. 10. Integrated Mobility Management Testbed

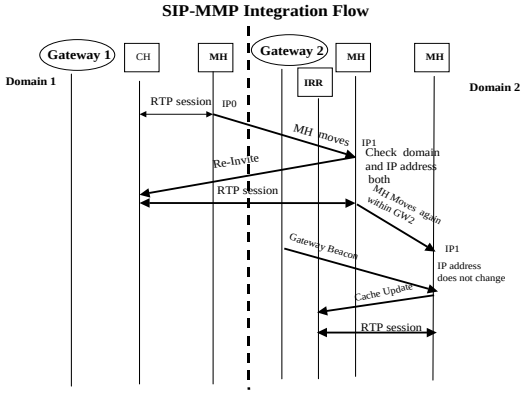

Fig. 11. SIP-MMP Integration

of each MMP node gets configured using DRCP server on the gateway upstream. Second interface of one of the MMP node gets a DCDP pool from the MMP-GW and acts like a DRCP server for the mobile. Since dynamic DNS [9] has been implemented in the testbed. This way DNS database gets updated when IP address changes in any of the MMP elements providing a dynamic name to IP address association. Thus manual change in the configuration files in the MMP elements is not needed any more. This mode of operation is very similar to FAs running in co-located care of addess mode. Since RIP (Routing Information Protocol) is configured in the testbed there is no need for installing static routes to forward the traffic from CH to MH even when the MH is within the MMP domain.

Figure 10 shows the testbed where the Integrated Mobility Management prototypes have been experimented and results were taken. Although the goal was to operate all three mobility management techniques at the same time on the single terminal while each doing its own function each mobility management prototype was tested pairwise also such as SIP and MMP, SIP and MIP-LR. Figures 11, 12 and 13 provide protocol flows of how each pair of protocols interact with each other.

Figure 11 provides a protocol flow for SIP and MMP integration. It shows a typical scenario limited to a case when the mobile makes a movement from one gatway's domain to a second one and in the process changes its IP address. A SIP session has been established between the CH and MH, when MH is under one gateway within an MMP domain, but CH is connected somewhere else. As the mobile moves under the second gateway and attaches itself to an MMP node within that gateway domain, it changes its IP address in the process and sends a Re-INVITE to the CH. CH sends thus redirects this traffic to the new location of the MH. As the mobile makes further movement from one MMP node to another one within the second domain, it does not change the IP address but binds to the new MMP node in the second domain. Routing cache within the MMP nodes take care of forwarding the traffic to the correct place within the domain.

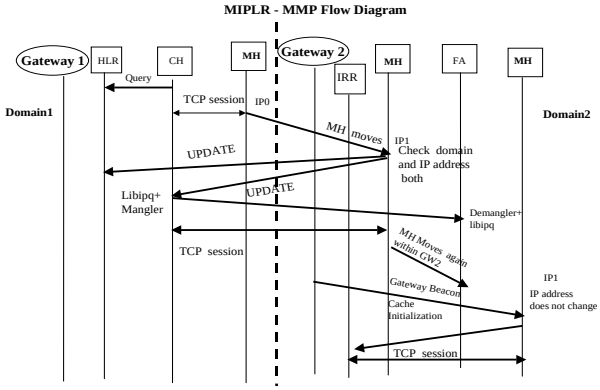

Fig. 12. MIPLR-MMP Integration

Figure 12 shows protocol flow for MIPLR-MMP integration. In this case MIP-LR works in a co-located mode while interacting with DRCP server, thus FA actually co-exists with the mobile host. This particular scenario shows a transition of MH between two gateways. Each gateway has two MMP nodes under its domain. One of the MMP nodes in either domain acts like a DRCP server while dispensing the IP address. CH starts a TCP session with the permanent address of MH (called MHpip) and queries the real address of the MH from the Location Register. By virtue of the IPtables and Mangler the TCP traffic actually gets directed to the new COA of the MH. As the mobile makes another move to a new MMP domain, it listens to a different DRCP server advertisement from one of the MMP nodes within the second domain and gets itself configured with a new IP address, at the same time it also listens to the beacon from the second gateway with a new beacon ID. This helps updating the routing cache within the MMP nodes for movement within the domain. After getting configured with the new IP address, mobile sends an update message (binding update) to the correspondnet host and

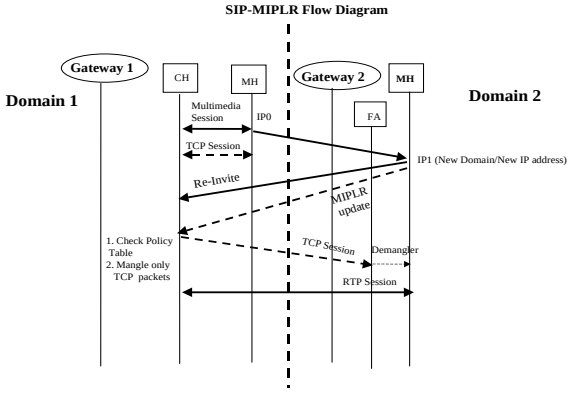

Fig. 13. SIP-MIPLR Integration

Location register. As the mobile makes further move within the second domain by connecting to a separate MMP node it does not change its IP address but sends the cache update to the intermediate nodes, thus traffic gets routed without getting broken.

Figure 13 shows a typical protocol flow integrating both SIP and MIP-LR. Since this is an Inter-domain movement, IP address gets changed on the mobile that is making a move from one domain to another one. As the mobile gets configured by the DRCP server running on the MMP node, it obtains a new IP address. As part of the SIP mobility scheme it sends a Re-Invite to the CH to keep the real-time traffic continuous, similarly MIP-LR sends an update message to the CH. As a result of a port based scheme instituted within MIP-LR, ports 5060 (SIP signaling port), RTP media ports (port 10000 and 20000 in this case) are not affected by MIP-LR mangling. Thus TCP based traffic is taken care of by MIP-LR and RTP based traffic is taken care of by SIP.

IV. Related Work

There have been some related work to support mobility in military environment [18]. 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 describes how these can work together in a military environment. A testbed implementation shows that these three mobility management protocols can co-exist on the same terminal operating at the same time while interacting with DRCP/DCDP, My-SQL based configuration database, and dynamic DNS. Intra-domain and Inter-domain mobility management is achieved for both real-time and Non-real-time application. Integration with quality of service and self managed virtual networks are the next steps which are being investigated.

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] K. Daniel Wong, Hong-Yu Wei, A. Dutta, K. Young, H. Schulzrinne, "Performance of IP Micro-Mobility Management Scehemes using Host Based Routing", *Proc. WPMC 2001*, Denmark, October 2001

[6] 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.

[7] E. Gustafsson, A. Jonsson and C. Perkins, "Mobile IP regional registration", draft-ietf-mobileip-reg-tunnel-03.txt, IETF, July 2000, Work in Progress.

[8] M. Handley, H. Schulzrinne, E. Schooler and J. Rosenberg, "SIP: Session Initiation Protocol", RFC 2543, IETF, March 1999.

[9] S. Thomson, Y. Rekhter, J. Bound, "Dynamic Updates in the Domain Name System", RFC 2136, IETF, March 1997

[10] 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.

[11] 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.

[12] R. Droms, "Dynamic Host Configuration Protocol (DHCP)", RFC 2131, IETF, March 1997.

[13] A.J. Mcauley, S. Das et al, "Dynamic Registration and Configuration Protocol" IETF Draft, work in progress.

[14] Stream Control Transport Protocol, http://www.ietf.org/rfc/rfc2960.txt

[15] 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.

[16] M. Handley, Eve Schooler, H. Schulzrinne, Jonathan Rosenberg " Session Initiation Protocol" RFC 2543.

[17] H. Schulzrinne " SIP registration draft" draft-schulzrinne-sip-register-00.txt, IETF work in progress.

[18] Subir Das, Archan Misra, Anthony Mcauley "A Comparison of Mobility protocols for Quasi-Dynamic networks" submitted for ATIRP conference

[19] Ashutosh Dutta, Faramak Vakil, Henning Schulzrinne et al. "Application Layer Mobility Management Scheme for Mobile Wireless Internet"