An Experimental Testbed for Wireless Internet Telephony and Streaming Multimedia

Telcordia Technologies Inc., 445 South Street, Morristown, NJ 07960

S. Baba, N. Nakajima, Y. Ohba
Toshiba America Research Inc., Morristown, NJ 07960

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

Abstract—In an effort to realize wireless Internet telephony and streaming multimedia in a highly mobile environment a testbed emulating a wireless Internet has been built. This would allow establishing multi-media calls between IP mobiles and integration between IP and PSTN end-points in a wireless environment. Different functionalities and components involved with the wireless Internet streaming multimedia have been prototyped and experimented in the testbed. These include signaling, registration, dynamic binding, location management while supporting the QoS features for the mobile users. This paper describes some of the components of the testbed and highlights the experiences while building this testbed which could be beneficial to some who plan to build a similar testbed to realize several features and capabilities of Mobile Wireless Internet, and evaluate the performance before wide scale deployment.

I. INTRODUCTION

Providing flexible and programmable multimedia services at a lower cost to the end users in a more efficient way has been main motivation behind transitioning to a packet based network from a traditional circuit switched network. Most of the effort underway now are limited to wired line network however. As personal communication and ubiquitous access becomes more prevalent, it is necessary to come up with some robust solution which can support multiple applications such as mobile IP-telephony, multimedia and other streaming application over wireless IP network. Supporting multimedia operation over wireless links would have to consider several factors such as signaling, quality of service, bandwidth management, mobility management and authentication among others.

With a view to realizing different protocols and components needed for supporting mobile streaming multimedia such as wireless IP telephony, broadcasting streaming content in a 3G wireless IP environment, a testbed has been designed and implemented where the proof of concept for different functional component of a 3G-IP network can be demonstrated.

Building Wireless Internet Telephony and Streaming Multimedia testbed is based on a framework discussed in [14] and [8]. This testbed provides a blue-print of a 3G-IP network [27] that would also involve providing support for roaming across different carrier domains (e.g., micro, macro, and dominant mobility), with a provision for billing and network management. It also touches upon the integration with 2G network by means of interaction with other signaling protocols such as MGCP [29] and other associated gateways based on SIP [1]. Localized streaming services for the mobile users have been demonstrated by exploiting wireless multicast in the local domain as described in [9]. Figure 1 provides a high-level view of the framework upon which this testbed is built.

This paper is organized as follows. Section II briefly discusses the testbed architecture and how different requirements for Wireless Internet are realized, in section III we define the different components associated with the testbed. Section IV describes the details of several functional modules implemented. A sequence of operation is described in section V. Some of the performance measurements are cited in section VI. Section VII concludes the paper with some open issues and future work.
II. TESTBED ARCHITECTURE

This testbed provides realization of several components which are part and parcel of Wireless Internet Telephony such as signaling, registration, configuration, binding, authentication, and QoS. Proposed testbed emulating a wireless Internet is built upon Linux, Windows and Solaris based platform. Software components used in the testbed are based on the standard IETF protocols such as SIP (Session Initiation Protocol), and SDP (Session Description Protocol) [20] for signaling and media description respectively, RTSP [23] (Real-Time Streaming Protocol) for multimedia streaming, Mobile IP or its variant for binding, DHCP [13] or its variant Dynamic Registration and Configuration Protocol [31] for configuring the client and DiffServ based protocols for QoS such as DSNP (Dynamic Service Level Specification Negotiation Protocol) [26] as the mobile moves from one subnet to another. IEEE 802.11 based wavelan base stations are being used as access points to the wired network. New protocols are developed or extensions are made to the existing ones to provide all the features of a 3G-IP network, such as faster registration, configuration, binding, mobility and QoS. Following subsections describe how different features are implemented. It is noteworthy to mention that this testbed has experimented both the kinds of mobility management i.e. network layer approach using Mobile IP and application layer approach using SIP. Following are some of the functional components needed for Wireless Internet Telephony.

A. Signaling

This architecture is built with a vision of 3G-IP network where the end-systems are assumed to be IP end-points, although a possible transition from 2G to 3G network has also been experimented with interaction between IP and non-IP end points via a soft switch. These IP addresses can be part of the global unique IP address space or can be privately owned in which case addressing can be resolved using NAT (Network Address Translation) or IP masquarading. Because of the distributed nature of this network, Session Initiation Protocol (SIP) has been used to demonstrate the signaling and initiation of multi-media call, and its tear down, between the clients. SIP server and SIP user agent are part of the signaling architecture, although SIP server functionality can easily be integrated into the Call Agent for demonstrating IP-PSTN call features. An end-to-end signaling architecture has been shown here. While SIP takes care of signaling of multimedia calls between multiple parties, there has been proposal to extend SIP so that it can take care of mobility for mid-session call. HMMP (Host Mobility Management Protocol) a framework [7] based on an extension of SIP has been submitted to IETF for consideration. This method provides an alternative approach to Mobile IP for binding issues for mid-session mobility and can also take care of pre-session mobility by means of unique URI registration as defined in [3].

B. Handoff

Hand-off, often known as hand-over is a process that allows an established call/session to continue when an MS moves from one cell to another without interruptions in the call/session. The hand-off process is built upon the registration, configuration, dynamic address binding, and location management functions. Hand-off process is transparent to users and should satisfy the following requirements so that it would ensure the integrity, privacy, and confidentiality of user’s location, perform the necessary requirements so that it maintains the QoS of the ongoing sessions through minimizing the loss of transient data during the hand-off, as well as satisfying the delay requirements of real-time applications.

In end-to-end wireless IP paradigm, three logical levels of hand-off procedure can be defined:

i. Cell Hand-off: It allows an MS to move from a cell to another in a subnet within an administrative domain. One subnet may consist of multiple cells. IP address of the mobile host remains same in this case.

ii. Subnet hand-off: It allows an MS to move from a cell within a subnet to an adjacent cell within another subnet that belongs to the same administrative domain.

iii. Domain hand-off: It allows an MS to move from one subnet within an administrative domain to another in a different administrative domain.

All the above levels of handoff have been prototyped in the testbed.

C. Dynamic Configuration

Registration and configuration involves registering with the network and configuring the end point itself. DHCP, PPP, and Mobile IP provide several standard ways of providing the registration facility to the end clients. However, Dynamic Rapid Configuration Protocol [17] is a lightweight version of DHCP that takes care of faster registration and configuration keeping in mind the efficient use of scarce wireless bandwidth. It does so by shrinking the message size, minimizing the messages in transaction and limiting the use of broadcast. As a sister protocol to DHCP, DRCP would have the mechanism to provide the DNS information, lease negotiation and would provide with client server authentication mechanism.

There are many ways subnet discovery can be taken care of: it can be done using detection of channel change in layer 2 or by server discovery method similar to router discovery mechanism in Mobile IP. This can be achieved by modifying the client code of DHCP so as to trigger either Mobile IP update or SIP re-invite upon detection of a new subnet. Similar changes are built-in features of DRCP, and it can be easily taken care of by server discovery method.

D. Registration

Registration is a process by which a network is made aware of the existence and location of an MS and its associated user.
When an MS becomes active or roams into a network for the first-time, it would register with the network. This process comprises sending a registration request from the MS to the network and performing an AAA (Authentication, Authorization, Accounting) process by the network, and sending appropriate responses to the MS as well as location management entities to ensure that the network is aware of MS’s current location. Depending upon the extent of registration, it can be categorized as complete or expedited/partial registration. Complete registration usually takes more time than the expedited registration. There are variants of AAA protocols to take care of security association between the mobile station and home AAA server when a client moves between the subnets within a domain. Home AAA server or an intermediate broker agent SIP Central Point of Contact[35] is contacted when the user moves into a new domain for the first time to establish the credentials. It is important to complete the registration process in a timely manner during the handoff process.

E. Binding

Binding allows continuous connectivity of TCP and UDP streams when the communicating end-nodes are moving around. Binding between the mobile host and correspondent host when the mobile host is moving is typically taken care of by Mobile IP [2] or by one of its many variants [11], [12] although it suffers from some drawbacks such as triangular routing and encapsulation. MosquitoNet’s [30] Mobile IP version without Foreign Agent is used as one of the alternatives in the testbed, to take care of the binding issues. In this case, care of address is typically provided by the DHCP server or DRCP server. Although there are other alternative solutions such as Cellular IP [10], HAWAII [12], TeleMIP [11] to provide mobility within a domain. While traditional Mobile IP based approach takes care of the binding problems we have used an application layer technique based on SIP based mobility management to take care of personal, and terminal mobility [3]. References [14] and [4] propose some extension of SIP where by mobility of multimedia calls (RTP/UDP based stream) and TCP application can be taken care of without using underlying Mobile IP and any network components in the middle of the network.

F. Authentication, Authorization and Accounting

Current testbed is using Diameter [33] as an AAA (Authentication, Authorization and Accounting) protocol running on NAS (Network Access Servers) and AAA servers to provide AAA services. In addition, we are developing a new protocol called BURP (Basic User Registration Protocol) [32] which is a light-weight protocol used between mobile hosts and NAS as a user front-end of Diameter. BURP is implemented as an application layer protocol to enable a flexible access control which works on any layer 2 technology, on both IPv4 and IPv6, and with any configuration protocol such as DHCP and DRCP.

III. Testbed Components

The proposed testbed consists of many hardware components and associated software and protocols. A picture of the current testbed is shown in Figure 2.

A. Mobile Station (Node) (MN)

Mobile stations are multi-media laptops and PDAs equipped with camera, and audio devices and have PCMCIA slots for 802.11B interface to communicate with the base station. Each of these Mobile Stations has multi-media application such as (wb, vic, rat) running in order to establish a multimedia (video, audio, data) calls.

B. Base Station (BS)

Base stations are Lucent’s IEEE 802.11B based access points operating at 2.4 Ghz frequency range. Each of these has an IP address which is addressable through SNMP agent. Each base station also operates on a separate 802.11 channel to avoid the possibility of interference. Yagi Array antennas are used to extend the lab to outside and provide external field coverage for up to 2 miles.

C. Radio Access Network

The Radio Access Network represents the wireless and back-haul infrastructure that provides MSs with wireless access to the wireline infrastructure. In IMT-2000, RANs use programmable software radios to provide the flexibility across frequency bands at the MS and across RAN.

D. Base Station Controller (BSC)

There is currently no hardware Base Station Controller (BSC) which would in practice can control several base stations. Alternatively the base stations are connected to the router directly through stationed network. Base Station Controller is assumed to be a multi-port switch (VLAN switch) which can control the respective base stations connected to each of its ports. It could be assumed to be a switch capable of controlling the Base Stations based on the MAC address, however these base stations and base station controllers are part of the same subnet. In some cases BSC can be an ether switch capable of filtering multicast packets, and being able to prioritize the traffic destined for a particular mobile host connected to a base station, providing proper QoS in terms of bandwidth. IEEE 802.1p scheme for providing class of service can be used also in the VLAN switch.

E. ERC (Edge Router and Controller)

An ERC is a routing and control system that connects a wireless access network to a regional wireline IP network. Each ERC may support several RANs. An ERC comprises two functional entities, an edge router (ER) and an edge control agent (ECA). The ER functions as an IP router, while the ECA is an intelligent agent that interacts with the Domain Control Agent (DCA) to control the RANs as well as support...
necessary network-wide control tasks. Control Agent functionality can be distributed within a domain.

In the testbed, ERCs are Linux PCs acting as routers with multiple ethernet interfaces. There are multiple base stations connected to the interface of each router via Cisco’s VLAN switches. Each interface of ERC is on a separate subnet. We assume each ERC to be part of the same domain here. In our experiment there are two main routers each dedicated to act as a domain router for each domain. In this architecture ERC provides more functionality than a router, since ERC also runs many of the server and client software such as BURP server daemon, Diameter client and local QoS node (QLN).

A separate interface has been dedicated for external network which is tested in the field outside the laboratory environment.

![Fig. 2. Basic testbed](image)

### F. Domain Control Agent

The domain control agent provides session management as well as the means of interaction between users and network control system and interaction among network control entities. DCA also supports 1) Mobility Management, 2) Authentication, Authorization and Accounting and 3) QoS management. It is assumed that each autonomous system would have components of domain control agent distributed within it.

Each domain control agent would interact with each other directly or via an Inter-Domain control agent using proper authentication mechanism. Following are some of the components of Domain Control Agent which are distributed within a domain.

### G. SIP server/SIP User Agent

SIP user agent runs on all the communicating nodes. Client version of SIP is a tcl/tk and C code, and provides a nice user interface for managing the multimedia calls. SIP server daemon (sipd) is run on a server, thus making it either a proxy/re-direct or registrar. SIP server is not used when the session is established using direct mode. When a call is established using a SIP server (non-direct mode), it can interact with location server, and can be used for services like registration, security and location updates. SIP User agent and servers have also been used for providing personal and terminal mobility support.

### H. DRCP server/client

As explained earlier DRCP is a lightweight version of DHCP suitable for wireless roaming. There is a DRCP server in each subnet. In some cases when there are multiple interfaces on a server, drcp daemon (drcpd) is started on each interface but with different configuration file. This is responsible for leasing IP addresses to the clients, when they request for IP addresses. DRCP client daemon runs in each terminal which gets the IP address from the server upon boot up or after entering a new subnet. This code has been modified to speed it up by interacting with IEEE 802.11 driver, Mobile IP and SIP user agent. As part of the built-in mechanism of DRCP the client would default to DHCP in the absence of DRCP servers.

### I. Mobile IP Server/Client

One of the alternative mobility management scheme implemented in the testbed follows Mobile IP approach. This approach is in accordance with some approaches adopted in the standard bodies such as 3GPP2 and MWIF. However in this testbed this approach is used for non-real-time traffic such as TCP/IP.

As part of providing layer 3 mobility management solution for non-real-time application, MosquitoNet’s Mobile IP is implemented in the testbed. It can operate without foreign which usually provides the care of address, rather DRCP server dispenses it to the client upon a DISCOVER message from the client. Mobile IP server daemon runs in the home agent and client daemon runs in the mobile client. Mobile IP client daemon is started before it makes a move, and it is restarted each time after the mobile node gets a new address on moving to a new subnet. There are many configuration files which need to be maintained in the server and client for different modes of operation such reverse tunneling, policy table.

### J. Application Server

The application server is a Pentium PC running Linux and run multiple daemons for variety of application such as streaming, web access and IMT2000 emulation. So logically application server consists of a Real Stream server, Apache HTTP server, and IMT 2000 emulation server. Practically all these application can co-exist in the same server or stay distributed.

In the absence of a CDMA 2000 based infrastructure, IMT 2000 functionality has been emulated to take advantage of some of the features such as assigning priority of services for a particular kind of application (signaling, data transfer, ftp, http) for a certain host pair, variable speed (e.g., 14.4 kbps, 384 kbps, 2Mb/s), variable state (active,dormant).

This emulation software provides the flexibility to the client to request a certain kind of service (e.g., prioritized bandwidth) for a certain kind of application. For example,
signaling traffic may be assigned one particular type of priority than the actual data traffic. Even for data traffic, http may get better priority than the ftp traffic, which can be done based on port pair being used based on the application. IMT 2000 emulation software has been developed using tcl/tk and C. This QoS feature is being replaced by a diffserv based approach in order to provide QoS guarantee either in the network layer or application layer.

### IV. FUNCTIONAL FEATURES

Some of the current features that can be demonstrated in the testbed are listed below.

1. Multimedia call setup and teardown using SIP signaling
2. Seamless mid-Session mobility (micro, macro, and domain) using both Mobile IP and SIP based re-invite mechanism
3. Fast-handoff and registration using light weight version of DHCP (e.g., DRCP)
4. IMT2000 emulation (Priority of traffic assigned based on application and source-destination pair)
5. QoS features for mobile clients
6. Authentication, Authorization, Accounting (Interdomain and Intradomain)
7. Wireless Multicast support
8. IP-PSTN integration in wireless environment

Following sections provide methods of operation for some of the features

#### A. Session Establishment

Both the correspondent host and mobile host which run Linux operating system obtain their IP address from a DRCP server upon boot-up.

Once the clients are up and running, SIP User Agent (sipc) is started up in both the clients. The correspondent host (CH) establishes a call to the mobile client (which may be present in the same subnet) with proper media description by using SDP. This multimedia call can be direct or additionally a SIP proxy server can also be used while the call is being set up, so that security and authentication can be demonstrated. The callee answers the call with its proper media preference. Once both the clients agree on a set of media preferences, the call is established. This call may involve voice, video and data all together. SIP helps to set up the call, but after that actual media flows as RTP/UDP stream between two end-points using the standard routing mechanism. We are using white board (wb) application to demonstrate data sharing, (rat) to demonstrate voice exchange, and (vic) to demonstrate video communication. All these three media streams use different port numbers for each application. An emulation software such as IMT 2000 can potentially be used to assign priority to each of these application based on their port number, and also a different priority can be assigned to actual SIP signaling since it uses a separate port number (5060) to be specific. At any point of time either caller or callee can send BYE so that the call terminates.

#### B. Mobility of Multimedia stream

Mobility can be categorized broadly into two kinds: pre-session mobility and mid-session mobility. Pre-session mobility can be taken care of by proper pre-registration. Current Mobile IP and DHCP/DRCP protocols provide traditional ways to take care of pre-session mobility using layer three technology. However SIP can be used to address pre-session mobility by means of registration and re-direction using unique URI scheme, an application layer technique. However mid-session mobility is something which is more important and can be sub-divided into three different categories such as, micro, macro, and domain. Mid-session mobility can be taken care of by using standard Mobile IP approach or application layer approach such as SIF.

DRCP/DHCP daemon runs on the designated servers in the respective subnets. After the SIP multimedia call is established and the RTP media streams flow in duplex mode, mid-session mobility can be demonstrated.

Micro mobility is demonstrated when the client moves between two cells, but the base stations involved are part of the same subnets. In this case the client does not change its address however, thus neither mobile IP is triggered nor SIP re-invite is sent to maintain the mobility intact. Handoff is taken care of based on layer two signal strength of the cells.

Macro mobility is demonstrated when the mobile client moves further away to a different cell, and in this case this new cell is part of a different subnet. As soon as it moves to a new subnet domain, the client discovers (via server advertisement message or sensing a different 802.11 channel number) that it is in a new subnet domain and triggers a DRCP DISCOVER message. The designated DRCP server in the second subnet responds with a new IP address. The mobile client now gets configured with a new IP address. As soon as it obtains the new IP address, mobile IP client daemon is updated on the client and home agent knows the whereabouts (new IP address) of the mobile host. So the RTP stream destined for the mobile client gets tunneled through the home agent, which gets decapsulated at the mobile client. By using application layer mobility scheme a re-invite is sent to the corresponding host so as to redirect the traffic.

Domain mobility has been demonstrated by extending the mobility to outside of the lab space and configuring a separate DNS domain. There is one host acting as primary DNS server which keeps the database for both the DNS domains. By means of Yagi Array antenna, coverage of wavelan testbed has been extended to the field. Experiments show that several multimedia application (audio, video, and data) do not have any discontinuity problems even if the cars are moving at a speed of 45 mph. Dynamic DNS is implemented to provide the update as the IP address of the mobile changes. Seamless mobility can be obtained even in the case of domain handoff.

Fast handoff is associated with each type of mobility. Fast handoff of multimedia stream is typically dependent upon quick detection, faster reconfiguration, and registration with the new subnet/domain and re-direction of the stream after
detection of the new subnet. Standard version of DHCP takes about 10-15 sec without ARP checking [19], it offers 5 sec latency (with ARP checking suppressed), and it is about 100 msec with DRCP. DRCP offers the lowest time for latency because of the factors mentioned in the earlier section.

C. SIP-AAA Interaction

We implemented the following SIP-AAA interaction model. In this model when the SIP server receives a SIP Register message from the MH, it consults with the home AAA server for authentication and authorization by using Diameter, where the database of the SIP user accounts is located in the home AAA server, not in the SIP server. This model is in accordance with the signaling scheme mentioned in the MWIF (Mobile Wireless Internet Forum). Note that although our SIP-AAA interaction implementation covers only the limited cases in which local SIP server or SIP proxy is not involved, several methods have been proposed such as [34] and [35] in order to cover the entire scenario of SIP-AAA interaction, and discussion is ongoing.

BURP offers user registration/authentication at the application level with AAA(Diameter) framework. Initial authorization is taken care of by BURP by instituting firewall even before any signal is passed onto the network. This offers local authentication for quick handoff as the client moves between the subnets. In this model SIP registration is authenticated only after consulting with AAA.

In usual case SIP registration is done in the SIP server, after the client obtains a new address. Interaction between the SIP server and AAA server is meant to provide a mechanism so that a communicating user’s activities are monitored securely for accounting and auditing purpose. Besides authentication via home SIP server and home AAA server, a user is also authenticated via interaction between local AAA server and home AAA server using Diameter. Figure 3 shows SIP-AAA interaction.

D. BURP-AAA interaction

When the MH moves into a new domain, it performs a BURP registration to the BURP server in the domain. Since the BURP server has no pre-established security association with the MH at the time of BURP registration, the BURP server consults with the home AAA server directly or indirectly through a local AAA server by using Diameter to authenticate the user on the MH. Once the BURP registration is successful, an LSA (Local Security Association) is established between the MH and BURP server so that further authentication required for intra-domain hand-off is performed locally and quickly at the BURP server without contacting the home AAA server. In addition to the case of intra-domain hand-off, the local authentication is also performed periodically in order to detect the event that the user silently disappears from the domain due to e.g., battery exhaustion or bad radio conditions.

The ERC in which the BURP server resides maintains an association between the user identity such as an NAI (Network Access Identifier) and lower-layer identity such as an IP address for each user. The ERC also has a firewall functionality so that only the packets sent from/to the MH belonging to the authorized users can pass through the firewall. Since the association between the user identity and lower-layer identity dynamically changes as a result of hand-off, the ERC updates the access control list of the firewall if and only if there is a change in the association and the resulting BURP registration or a local authentication is successful. This means that SIP Register or Re-invite messages will not pass through the firewall until the access control list is updated.

An example message sequence for BURP/Diameter is illustrated in Figure 4. Note that we designed SIP-AAA and BURP-AAA to be performed separately because the complete architecture including SIP-AAA and BURP-AAA is still under discussion. Our testbed will be adjusted according to the future discussion.

E. Quality of Service

Dynamic SLS negotiation protocol [DSNP] is based on diffserv approach but uses two levels of hierarchical servers within a domain (subnet level and domain level) to provide the required quality of service to the mobile clients roaming between subnets and domains. The higher (Domain) level server keeps track of the QoS requirement of the mobile client and distributes this information to other routers in the domain.
where the traffic is shaped accordingly as the client moves in there. Details of this can be found in [26]. Both incoming and outgoing traffic can be shaped at the edge router (ERC) before being delivered. For real-time (RTP/UDP) traffic RTCP feedback [36] can be used to provide QoS requirement to the domain level server. How RTCP feedback approach can be used with diffserv approach is for further study.

F. Wireless IPMulticast

In order to achieve better bandwidth efficiency, make the group communication (many-to-many) and broadcasting content (e.g., audio/video streaming from a single source) more effective and make use of localized stream services, IP Multicast has been deployed in this testbed. There are many issues related to multicast mobility (e.g., continue to be part of the same group while changing cells, subnets domains), use of a smart base station controller to restrict the multicast stream to one cell after the listener has moved, are being looked into by using IGMP snooping or CGMP.

A standard multicast stream flow has been shown in figure 5.

G. Wireless Call Agent/SIP-PSTN integration

Previous sections illustrate the interaction between all IP end-points. In addition to providing mobile multimedia support between the IP end-points, this test-bed also provides a way of integrating the PSTN components by using Call-Agent (Media Gateway Controller) [29] and SIP server. Call Agent is based on Media Gateway Control Protocol, where Media Gateway Controller is resident on a server, and would control the non-IP devices connected to the gateway. This gateway is usually a media gateway, whose interface is connected to the IP cloud. The other interface usually connects to a standard analog phone, or a PBX. Media gateway converts the analog signal to IP stream, and has a MGCP slave agent which is controlled by the Media Gateway Controller. In this testbed the gateway is nothing but a Cisco router with an FX board which connects to a standard analog phone. The call agent maintains a database of the PSTN end-points, and would have access to intelligent database which would provide some AIN (Advanced Intelligent Networking) functionality. In order to provide scalability or domain connectivity there can be multiple call-agents. The protocol between the call-agents can be SIP-T, an open standard protocol in IETF.

A standard Call-Agent and SIP server configuration has been shown in figure 6. There is another way of using MGCP without using the standard residential gateway. In this case a mini residential gateway has been implemented as a software on the mobile terminal itself and the voice can be generated from the terminal itself. This way MGCP can be used on a mobile terminal. Mobility in this case has been tried using standard Mobile IP in windows environment although application layer mobility is not ruled out, where SIP based mobility management can be used.

SIP-PSTN integration has been realized by using a pair of mediatrix gateway [25], analog cordless phones and windows based SIP server which keeps a mapping between the end-points. In this scenario each mediatrix box has SIP User Agent installed in it, which generates and terminates the SIP signal.

A call flow showing the interaction between the end-points (SIP UA and Analog phone) using Call Agent (Media Gateway Controller) is shown in figure 7.
formation from each of these inter-acting protocols. Seamless mobility for a multimedia session with registration, network configuration, and dynamic binding for different sets of mobility such as Micro, Macro and Domain has been described in the following steps.

Mobile station in the home network tries to make a SIP call before the user is authorized by the BURP server, and it fails. This demonstrates that the client needs to be authenticated at the nearest ERC before the SIP signaling goes through.

Then MS invokes BURP for user registration using to open the firewall controlled by ERC. Then CH makes a SIP call to MS using SIP proxy server which is in the same domain. MS starts to move towards another domain and experiences a domain handoff first (Domains are segregated as AAA domains not DNS domains in this case such as tari.toshiba.com and research.telcordia.com) and then a micro and a macro handoff respectively once it is present in the new domain. As soon as it moves to a new domain (which is also a new subnet), it listens to the DRCP server advertisement and gets a new IP address to get it quickly configured. Session mobility is taken care of by SIP mobility, while user authentication is taken care of by BURP within a domain and interaction between the AAA entities is done when MH moves between domains. Personal mobility is achieved by terminating the existing call between CH and MH, then re-inviting the MH with its unique URI. Terminal mobility is achieved by re-inviting the CH everytime MH moves to a new subnet, and thus getting the media re-directed to the correct IP address. Time taken for media delivery (redirection) is not affected by SIP’s re-registration mechanism, but the local authentication mechanism by BURP would probably delay the media delivery to some extent because of the firewall in there. Re-registration is mostly done for any new incoming multimedia calls. A complete flow diagram showing the interaction of several protocols as the mobile moves from domain to domain and cell(subnet) to cell(subnet) is shown in the figure 8.

Experiments were carried out in this testbed to validate different functionalities meant for the wireless Internet. The mobile host moved from one domain to another and then performed micro and macro mobility within that domain. Measurements were taken to find out how much time each atomic operation took. Tepdump output were taken on the mobile host and correspondent hosts, for specific signal messages to determine the timing for each of the operation, such as moving between cells, triggering to obtain an IP address using DRCP, sending the BURP messages for BURP-AAA interaction, interaction between the Diameter server and SIP server, interaction between two AAA servers during the domain handoff etc. Figure 9 shows a typical hand-off sequence as the mobile host moves from one domain to another and in the process changes between subnets.

This handoff delay would constitute several components such as delay due to 802.11B channel change (mostly termed as micro-mobility), subnet discovery, IP address acquisition, local authentication by means of BURP, and delay due to SIP Re-invite. These delay figures would depend heavily upon the processing speed of the end hosts, number of routers in the path, and background traffic. A complete Re-invite, OK and ACK sequence took about 500 msec including the processing time for media redirection by about 350 msec. Address acquisition because of DRCP is within 100 msec, which does not include the extra time needed to check the channel change periodically. SIP re-registration does not affect the media re-direction to the new address, since it is independet of the Re-Invite process and is used mostly for location management. A typical complete registration process so that the client’s new IP address gets updated in the SIP server is about 150 msec.

From the experimental results it was observed that it takes almost 1 sec from the time it lost connectivity with the old access point until the host gets configured with the new channel number after setting up connection with the new access point, at which point DRCP Discover kicks in by the client. According to [?] beacon interval from an access point is about 100
msec. It is assumed that rest of the time is used to process the beacon and set up the channel number in the application.

In the experiment, RTP packet interruption due to DRCP, BURP and SIP amounts to about 1 sec. SIP Re-INVITE re-transmission takes place during the domain handoff, if the BURP registration has not taken place yet during the domain handoff, but this can be reduced also if the BURP registration takes place before SIP re-invite is issued. As it turns out the bulk of the time is consumed for SIP signaling (Re-INVITE, ACK, OK) which is about 600 msec. With proper optimization this can be reduced to 200 msec, including the processing time on the end hosts.

These values would be different if the correspondent host is also moving. The figures listed in the table are in msec. As evident domain hand-off takes more time than subnet handoff because of extra time taken due to interaction with the AAA server.

In optimized mode, the total interruption due to subnet and domain handoff would be limited to 400 msec, with domain handoff taking slightly more time because of AAA interaction.

![Diagram](Fig. 9. Handoff Sequence)

VII. CONCLUSIONS AND OPEN ISSUES

This paper described different techniques associated with building a wireless Internet testbed. It touches upon the implementation details of several components associated with the testbed. These would include all IP wireless multimedia calls over a mobile environment, authorization, accounting, QoS, multicast and IP-PSTN interaction. A performance measurement was carried out to determine the time taken for each associated atomic operation, and means were determined to optimize each of these operations.

VIII. ACKNOWLEDGEMENT

Authors would like to acknowledge the effort of other ITSUMO team members David Famolari, Faramak Vakil, Moncef Elaoud of Telcordia, T. Maeda, Yasuto Sobatake of Toshiba America Research and Prof. Parmesh Ramanathan of University of Wisconsin towards the realization of different components of the testbed. Help from Xiaotao Wu and Jonathan Lennox of Columbia University towards sipc and sipd are also appreciated.

REFERENCES

[27] www.mwif.org
[30] mosquitonet.stanford.edu
[37] www.wavelan.com
[38] Ramon Caceres, Venkat Padmanavan “Fast and Scalable Wireless Handoffs in Support of Mobile Internet Audio ” Baltzer Journals