

Secure Universal Mobility for Wireless Internet

Ashutosh Dutta

Tao Zhang

Sunil Madhani

Telcordia Technologies,

Piscataway, New Jersey

Kenichi Taniuchi

Kensaku Fujimoto

Yasuhiro Katsube

Yoshihiro Ohba

Toshiba America Research Inc., Piscataway,
New Jersey

Henning Schulzrinne

Computer Science Department,

Columbia University, New York

Abstract

The advent of the mobile wireless Internet has created the need for seamless and secure communication over heterogeneous access networks such as IEEE 802.11, WCDMA, cdma2000, and GPRS. An enterprise user desires to be reachable while outside one's enterprise networks and requires minimum interruption while ensuring that the signaling and data traffic is not compromised during one's movement within the enterprise and between enterprise and external networks. We describe the design, implementation and performance of a Secure Universal Mobility (SUM) architecture. It uses standard protocols, such as SIP and Mobile IP, to support mobility and uses standard virtual private network (VPN) technologies (e.g., IPsec) to support security (authentication and encryption). It uses pre-processing and make-before-break handoff techniques to achieve seamless mobility across heterogeneous radio systems. It separates the handlings of initial mobility management and user application signaling messages from user application traffic so that VPNs can be established only when needed, thus reducing the interruptions to users.

I. Introduction

A user should be able to roam seamlessly between heterogeneous radio systems, such as public cellular networks (e.g., GPRS, cdma2000, WCDMA networks), public wire-line networks, enterprise (private) wireless local area networks (LANs) and public wireless LAN hotspot networks that may use IEEE 802.11, Bluetooth, or other short-range radio technologies such as DSRC (Dedicated Short Range Communications) commonly used along highways. A user should be able to communicate and to access network services in a seamless and secure manner over any type of access network. A user should also be

able to maintain on-going secure application sessions when moving across different access networks.

An enterprise user on an external network is typically required by one's enterprise to use a virtual private network (VPN) to connect to the enterprise network so that the enterprise network can authenticate the user and determine whether traffic from the user should be allowed to enter the enterprise network. The VPN also provides security protections to the user's traffic over an external and often un-trusted network (e.g., any public network, the Internet, an Internet Service Provider's network, a corporate network other than the user's own corporate network). Such security protection may include both integrity protection and confidentiality protection. Therefore, a key issue in supporting seamless and secure roaming across heterogeneous radio systems is how to meet the security requirements while a mobile is moving across enterprise networks and external networks and between different types of external networks.

Today's leading VPN technologies, such as IPsec [6], is a set of protocols defined by the Internet Engineering Task Force (IETF) to provide security protections such as authentication, privacy protection, and data integrity protection, do not have sufficient capabilities to support seamless mobility. For example,

- An IPsec tunnel will break when the mobile terminal changes its IP address as a result of moving from one network to another, unless proper measures in addition to the current standard IPsec is implemented. A new version of IKE (Internet Key Exchange), IKEv2 [7], is supplemented with the mobility extension that may solve this mobility problem, but it is still in the early stages of development.

- VPN establishment may require user manual intervention when the user has to use a time-variant password to establish the VPN. This suggests that careful consideration needs to be given to when a VPN should be set up.
 - A VPN should be set up only when the user or a user application has a need for it. This suggests that user manual intervention will be incurred only when a user or a user application has a need for the VPN.
 - VPN setup should occur as infrequently as possible to reduce the frequency of user manual intervention and level of interruptions to user applications. This suggests that once a VPN is set up, it should be kept alive as long as allowed by the enterprise security policy. Since different enterprises will likely have different security policies, the VPN lifetime should be a flexible parameter.
- VPNs may introduce significant overhead. Many applications, e.g., non-confidential short messages from intranet to a mobile, may not need to be transported over a VPN. This suggests that on certain occasions the mobile should be allowed to receive non-confidential packets from the intranet without a VPN. Thus there is a need to have an architecture that can provide flexible VPN setup as on need basis.

In this paper, we propose a new architecture, named Secure Universal Mobility or SUM. It supports secure seamless mobility without requiring a mobile to maintain an always-on VPN. It does so by introducing another external home agent in the DMZ network of an enterprise in addition to the internal home agent. It can also incorporate more advanced mobility management techniques, such as MOBIKE, to reduce mobility management overhead. Alternatively it can allow application-layer protocols, such as SIP [12], to be used to support mobility. In addition it is independent of radio access technologies such as IEEE 802.11 and CDMA.

The rest of the paper is organized as follows. Section II discusses related work in this area. Section III describes the SUM architecture, provides an overview of handoff analysis and describes its various associated functional components. Section IV describes handoff performance measurements for both video and voice applications that represent VBR (Variable Bit Rate) and CBR (Constant Bit Rate) traffic respectively, obtained from our testbed. We conclude the paper in Section V.

II. Related Work

Over the past few years there have been several efforts to support seamless and secured mobility covering multiple administrative domains. Miu et al [13] describe architecture and systems that supports secured mobility between public and private networks. However it is limited to movement between similar kinds of networks e.g., (802.11b). Rodriguez et al [12] introduce the concept of mobile router where the end clients with different access technologies connect to the mobile router's internal interface. In this case, clients do not change their IP addresses. Instead, the mobile router keeps on changing the external IP addresses as the clients move around and connect to different access networks such as GPRS, CDMA and 802.11b. Although it has addressed technology diversity, network diversity and channel diversity, and supports a variety of traffic, it has not discussed how to support security along with mobility. Snoeren et al [14] discuss fine-grained failover using connection migration mechanism. It achieves fine-grained, connection-level failover across multiple servers during an active session. However it does so by proposing changes in the TCP stack of the end clients without changing the application. References [15], [16], describe the integration of Mobile IP and IPsec in an 802.11b environment but have not illustrated the use of heterogeneous access. Cheng et al [3] describe a novel approach that achieves smooth handoff, but it assumes foreign agents in the visited network and does not involve heterogeneous access technologies.

Recently, there has been much activity within the Internet Engineering Task Force (IETF) to develop solutions to maintain VPN connectivity while a mobile device changes its IP address. Adrangi et al [5] describe several scenarios of how a combination of Mobile IP (MIP) and VPN can support continuous security binding as a mobile device changes its IP address. However, it does not address how to support seamless handoff while preserving a VPN and also does not address heterogeneous access technologies. Luo et al [1] describe a secure mobility gateway that maintains mobility and security association between a mobile and a VPN gateway, but it does not offer flexible tunnel management techniques to allow the VPN tunnel to be turned ON and OFF dynamically and has not explored mechanisms to provide smooth handoff. Birdstep (www.birdstep.com) proposes an approach that uses two instances of MIP to support seamless and secure mobility between an enterprise network and external networks. When a mobile moves to an external network, one instance of MIP is used to ensure that the VPN to the mobile does not break when the mobile changes its IP address. Another instance of MIP is used to ensure that packets sent to

the mobile's enterprise network can be forwarded to the mobile through the VPN. A key advantage of the Birdstep approach is that it is based completely on existing IETF protocols. It, however, requires that a mobile keeps its VPN always on while the mobile is outside its enterprise network. Furthermore, it is limited to using MIP for mobility management. MOBIKE [2] provides an alternative approach to seamless mobility using the mobility extension of IKEv2 to support continuous VPN when a mobile changes its IP address. It is however limited to use between external networks and needs other mobility protocols to support seamless mobility from internal network to external network.

The proposed SUM architecture overcomes the limitations of the Birdstep approach when Mobile IP is used to support mobility. SUM uses the existing standard-based protocols such as IPsec, Mobile IP, and SIP over transport layer mechanism (TCP, RTP/UDP) without modifying these protocols. It uses make-before-break mechanism to enable seamless mobility over heterogeneous access technologies.

III. The SUM Architecture

Figure 1 shows a reference architecture. An enterprise network is typically divided into intranets and demilitarized zones (DMZ). An intranet is a trusted portion of an enterprise network. A DMZ is a portion of an enterprise network that can be accessed from external networks under looser access control than the intranets.

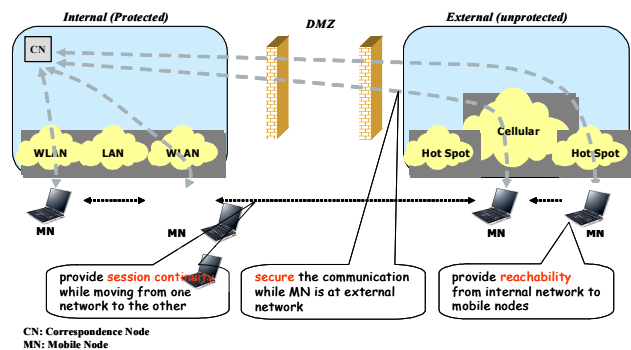


Figure 1: Mobility scenario in DMZ-equipped enterprise network

There can be several modes of communication with a mobile. A mobile can move between internal protected network and external networks or between external networks while in session with a correspondent node that can either be within an enterprise or located in an external network. The initial communication could have been started while the mobile is within the enterprise or in the external network.

SUM seeks to achieve the following main capabilities while supporting different mobility scenarios:

- Maintain *reachability* from the intranet to a mobile user outside one's enterprise network in a secure manner with minimum interruption to the user and user applications.

Reachability can be achieved using either network-layer or application-layer mobility management techniques. At the network layer, a mobile can have a permanent IP address for correspondent hosts to address their packets to the mobile regardless whether the mobile is inside or outside its enterprise network. This can be accomplished using, for example, MIP. In this case, a mobile relies on a MIP home agent (HA) in the enterprise network to maintain the association between the mobile's home address and its current care-of address (a process commonly referred to as binding). When the mobile changes its local IP address, it registers the new local IP address with its home agent and the home agent will forward future packets to the mobile's new location. When a mobile moves onto an external network, a dual-HA approach can be used to maintain reachability from the intranet to the mobile. This will be discussed in more detail in Section III.1.

Application-layer protocols such as SIP may also be used to maintain reachability to mobiles on external networks. In this case, mobile's home SIP proxy inside the mobile's enterprise network keeps up-to-date mapping between the mobile's application-layer address (e.g., SIP URI) and its current contact address. This will be discussed in more detail in Section III.B.

- Provide a *secure* environment to mobile users that is comparable to the security level the users get inside their enterprise network, regardless of where they are.

Signaling messages and user application traffic can be protected using security mechanisms at different protocol layers. For example, IPsec [6] provides IP-layer encryption and authentication. Using IPsec-based VPNs to access an enterprise network, a user first establishes an IPsec tunnel to an IPsec gateway which typically resides in the enterprise's DMZ. The user end of the IPsec tunnel is identified by the mobile's current care-of IP address that the user obtained from the visited network to send and receive IP packets over the visited network. This means that the IPsec tunnel will break when the mobile changes its care-of address as a result of moving from one network to another. Establishing a new IPsec tunnel requires several message (e.g., IKE messages) exchanges between the mobile and the IPsec gateway and can

add excessive delay to the handoff. This can give rise to transient data loss when the mobile changes its IP address rapidly.

- Maintain *session continuity* as the mobile is on the move.

A mobile can have various scopes of mobility such as micro mobility where only layer-2 network association may change, macro mobility where IP-layer network association changes, and domain mobility where a mobile moves from one network domain to another that may be operated by a different network provider. We have experimented with Mobile-IP and SIP-based approaches to support session continuity for the later two cases, as IP address does not change for micro-mobility case.

To support seamless mobility, it is important to reduce handoff delay and transient data loss during handoff. Setting up VPN tunnels or establishing connectivity to a cellular data network (e.g., GPRS, WCDMA, or cdma2000) could introduce excessive delays that are intolerable to real-time applications. We will describe handoff processing and make-before-break handoff mechanisms that can significantly reduce handoff delay and data loss during handoff.

III.A. Handoff Delay Components

When a mobile moves from one network to another, handoff delays may be incurred at each protocol layer as illustrated in Figure 2. While packet loss is often attributed to handoff delay, end-to-end delay consists of a number of components including transmission delay, propagation delay, and queuing delay in the intermediary servers.

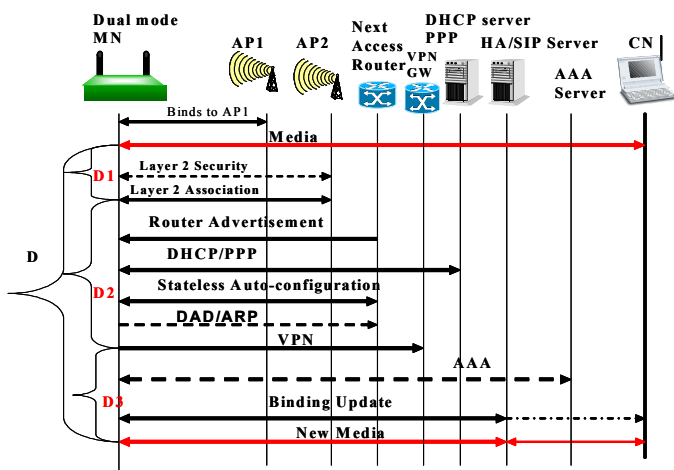


Figure 2. Handoff delay components

Handoff delay consists of the following main components: time to perform layer-2 association, to obtain a local IP address, to perform binding update, to perform authorization, to establish security association (e.g., VPN connection), and to perform media re-direction. When handoff procedures at different protocol layers are performed sequentially from the lower layer up as is typically done using today's handoff techniques, the total handoff delay D_L is as follows:

$$D_L = D_1 + D_2 + D_3$$

As demonstrated in the Figure 2, D_1 is attributed due to delay in layer-2 binding, D_2 consists of delays due to layer-3 handoff operations such as IP address acquisition, duplicate address detection, layer-3 security association with the VPN gateway, D_3 is due to application layer authorization, binding update and media redirection. Values of D_1 and D_2 will depend upon the type of access network (e.g., WLAN, GPRS, CDMA) the mobile is moving to where as D_3 will depend upon the distance between mobile and correspondent node. If T is the propagation delay for packets to travel from the correspondent host to the mobile, the packets transmitted by the correspondent host during $T + D_L$ will be lost during a handoff. Reference [20] provides an analysis of SIP-based handoff delay and confirms that handoff delay while moving to a 3G network is unacceptable for streaming multimedia. Make-before-break mechanism introduced in the SUM architecture involving multiple interfaces can reduce packet loss by making a step-wise transition to the new network while still in communication with the primary interface. Step-wise transition allows the mobile to perform several steps of handoff at different Signal-to-Noise ratio.

Thus probability of a successful make-before-break handoff depends upon several factors such as the mobile's velocity, SNR (Signal-to-Noise) ratio threshold at which a mobile makes the decision to switch, overlapping coverage area, link speed of the access network etc.

In Section IV we provide experimental results of regular handoff and the handoff that uses make-before-break algorithm.

III.B. Mobile IP-based SUM Architecture

Figure 3 illustrates a MIP-based SUM architecture. It uses two MIP home agents. An internal home agent (denoted by i-HA) inside the intranet supports mobility inside the intranet. The external home agent (denoted by x-HA) in the DMZ handles a mobile's mobility outside the enterprise and ensures that a VPN to the mobile does not break when the mobile changes its IP address. The i-HA and x-HA collectively ensure

that packets received by the i-HA can be forwarded to the mobile currently on an external network.

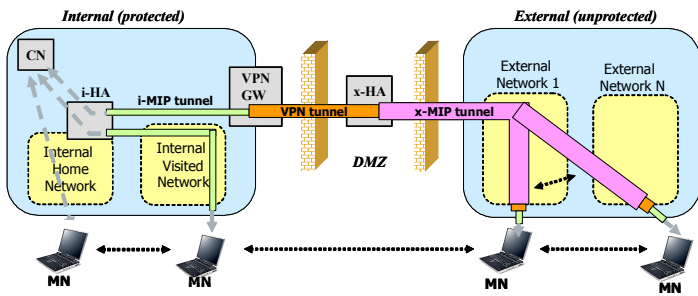


Figure 3: Secure mobility using MIP-based approach

A mobile has two MIP home addresses: an internal home address i-HoA in the mobile's internal home agent and an external home address x-HoA in the external home agent. The mobile's care-of address registered with its i-HA is referred to as its internal care-of address and will be denoted by i-CoA. The mobile's care-of address registered with the x-HA is referred to as its external care-of address and will be denoted by x-CoA. The instance of MIP running between the mobile and its i-HA is referred to as internal MIP or i-MIP. The instance of MIP running between a mobile and the x-HA will be referred to as external MIP or x-MIP. After a successful VPN establishment the mobile obtains an address from the VPN gateway (VPN-GW) that is denoted as TIA (Tunnel Inner Address)

When the mobile is within the intranet, standard MIP [8] or SIP mobility [9] can be used to support its mobility. In the rest of the paper, we focus on how to support mobility between enterprise network and external networks and mobility between external networks.

When a mobile moves into a cellular network, setting up the connection to a cellular network can take a long time. For example, we routinely experienced 10-15 second delays in setting up PPP connections to a commercial cdma2000 1xRTT network. In addition, establishing a VPN to the mobile's enterprise network could also lead to excessive delay. To enable seamless handoff, handoff delays need to be significantly reduced.

Therefore, we apply handoff pre-processing and make-before-break techniques to reduce handoff delay. In particular, a mobile anticipates the needs to move out of a currently used network, based on, for example, the signal qualities of the networks. When the mobile believes that it will soon need or want to switch to a new network, it will start to prepare the connectivity to the target network while it still has good radio

connectivity to the current network and the user traffic is still going over the current network. Such preparation may include, for example,

- Activating the target interface if the interface is not already on (e.g., a mobile may not keep its cellular interface always on if it is charged by connection time),
- Obtaining IP address and other IP-layer configuration information (e.g., default router address) from the target network,
- Performing required authentication with the target network, and
- Establishing the network connections needed to communicate over the target network (e.g., PPP connection over a cdma2000 network).

Although both the interfaces are on at any specific point of time, the decision to switch over from one interface to another will depend upon a local policy that can be client-controlled or server-controlled. In this case the handover anticipation is purely based on signal-to-noise ratio (SNR) of the 802.11 interface. But this handoff decision could be based on any other specific cost factor.

When the mobile decides that it is time to switch its application traffic to the target interface, it takes the following main steps:

- Registers its new care-of address acquired from the target network with the x-HA.
- Establishes a VPN tunnel between its x-HoA and the VPN gateway inside the DMZ of its enterprise network.
- Registers the gateway end of the VPN tunnel address as its care-of address with the i-HA. This will cause the i-HA to tunnel packets sent to the mobile's home address to the VPN gateway, which will then tunnel the packets through VPN tunnel and the x-MIP tunnel to the mobile.
- When the mobile moves back to the enterprise network, the VPN and the MIP tunnels will be torn down. Dismantling the VPN tunnel may take up to a few seconds, thus some transit packets may get lost or may arrive at a later time leading to out-of-order packets. Most of today's applications are capable of reordering of the out-of-sequence packets (e.g., out-of-sequence RTP packets).

When the mobile moves to another external network and acquires a new local care-of address (x-CoA), the mobile's x-HoA remains the same. Therefore, the

mobile's VPN does not break. The mobile only needs to register its new local care-of address with the x-HA so that the x-HA will tunnel the VPN packets to the mobile's new location.

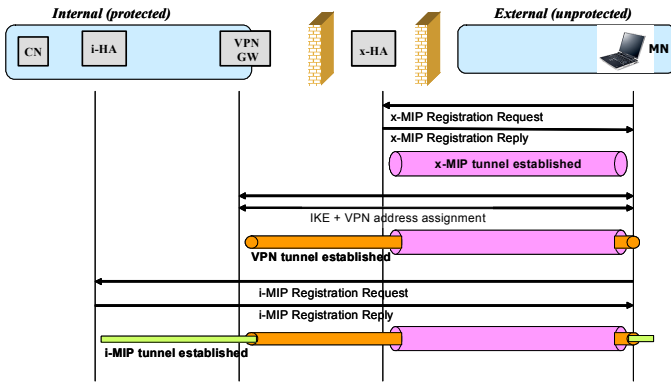


Figure 4: Interaction of protocols for SUM using Mobile IP-based architecture

Figure 4 illustrates how the MIP and VPN tunnels are set up during the mobile's movement from an enterprise network to an external network. If the mobile uses reverse tunneling, the data from the mobile will flow to the correspondent host in the reverse direction of the path shown in Figure 4.

III.C. Dynamic VPN establishment

Existing approach to secure mobility typically requires a mobile to maintain an always-on VPN when the mobile is outside its enterprise network regardless of whether the mobile has user traffic or not. This adds additional overhead on the mobile because of the tunnel keep-alive messages and may also introduce extra security risks (e.g., when the mobile device is lost). The proposed SUM solution employs a dynamic VPN establishment mechanism so that a mobile outside the enterprise network no longer needs to maintain a VPN to its enterprise network all the time. Instead, it establishes a VPN only when it needs to communicate with a correspondent host inside the enterprise network or to communicate through the enterprise network with a correspondent host on external networks.

Dynamic VPN establishment can be implemented using pre-condition features of SIP signaling when the correspondent host and the mobile are SIP-enabled. When the mobile is outside the enterprise network and has no user traffic to send into the enterprise network, it sets up only the two Mobile IP (MIP) tunnels: one from the i-HA to the x-HA and another from the x-HA to the mobile. This ensures that the SIP signaling from the correspondent host can reach the mobile and vice-versa. At this stage, no VPN is established, thus initial signaling between the intranet and the mobile is not protected by a VPN. Other security measures can be

used to secure these initial signaling messages. For example, S/MIME [10] or TLS [11] (Transport Layer Security) could be used to secure the initial SIP signaling messages.

When a correspondent host (CH) wants to initiate communication with the mobile, it sends a SIP INVITE message to the mobile. This INVITE message can be sent in two ways. If the SIP proxy only has the home address of the mobile in the database, it will reply with a 302 redirect message in response to INVITE from the CH. CH will then send the INVITE to the internal home address of the mobile. The i-HA intercepts that packet, tunnels the packet to the x-HA which further tunnels the packet to the mobile. Alternatively the SIP proxy may keep a direct mapping between care-of-address and its home address. The SIP INVITE message notifies the mobile about an impending call. To answer this call, the mobile first checks to see if there is already an existing VPN. In the absence of a VPN, the mobile uses IKE to establish a new VPN. Then, the mobile uses the VPN to register the VPN gateway end of the VPN tunnel address with the i-HA so that the i-HA will forward future packets to the VPN gateway. At this point, the traffic between the mobile and the corresponding will travel through the VPN. Thus SIP OK from the mobile is carried within the VPN tunnel. This delays the SIP signaling a little bit in the beginning but ensures that further communication is protected.

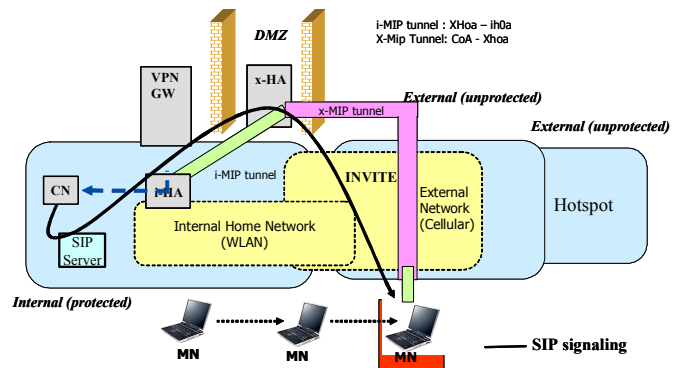


Figure 5: Dynamic tunnel management with SIP

There is no need to set up the initial double MIP tunnels if the SIP proxy at home has prior knowledge of the mobile's CoA. In that case initial INVITE from CN does not need to be carried over a double tunnel.

Figure 6 shows the protocol flows associated with the dynamic tunneling mechanism using SIP's INVITE mechanism. Initially when the mobile is away it just sets up a double MIP tunnel, but the i-MIP tunnel is set up with a different care-of-address (x-HoA). After receiving INVITE from the correspondent host, the triple tunnels (x-MIP, VPN, i-MIP with TIA as the

care of address) are set up so that the rest of the signaling and data traffic can flow over a secured link.

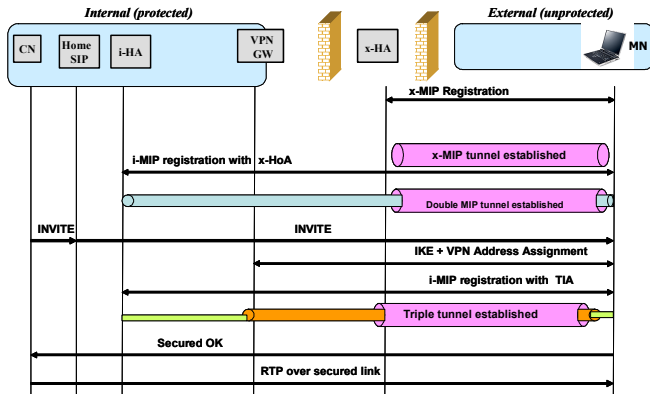


Figure 6: Protocol flow for dynamic tunnel management

In this specific scenario, home SIP server keeps an association between the mobile’s URI and the home address. Both the SIP server and MIP home agents are used in this scenario. A complete SIP-based scenario will be described later on.

III.D. MOBIKE-based architecture

Using two instances of MIP and IPsec to support secure roaming introduces heavy tunneling overhead due to triple encapsulation (i-MIP, IPsec, and x-MIP) and may not be appropriate for bandwidth-constrained wireless networks. Techniques such as robust header compression (ROHC) [17] or IP-layer compression can reduce overhead. Most recently, mobility binding has been included as part of IKEv2 [7], where the mobile does not need to tear down its existing security association and re-establish it as it changes its IP address. Instead, it can modify the existing security association to update its IP address. This work is being discussed within IETF and we present the preliminary results of MOBIKE-based approach in Section IV.

As illustrated in Figure 7, using IKEv2, MOBIKE can modify the existing security association without re-establishing the IPsec tunnel when the mobile changes its IP address. This reduces header overhead by eliminating the need to use MIP (or another separate mobility management protocol) to maintain continuous VPN while moving between two external networks. MOBIKE by itself however cannot provide seamless mobility when the mobile moves from internal networks to external networks. But, MOBIKE can work with both SIP and MIP-based mobility, where the mobile uses its VPN tunnel inner address (TIA) to register with the home proxy and sends the binding update first time it moves out of the internal network.

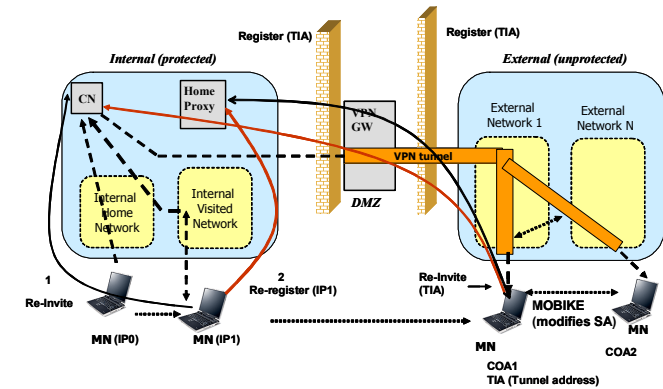


Figure 7: SIP and MOBIKE-based SUM architecture

IV. Testbed Implementation and Performance Evaluation

We have implemented the SUM framework in a multimedia test-bed as illustrated in Figure 8. It consists of an enterprise wireless LAN using IEEE 802.11b, cdma2000 1xRTT cellular network service from Verizon, and a public hotspot network using IEEE 802.11b with NTT/Verios’s T-1 line as backhaul into the Internet. This section shows performance measurements for roaming between enterprise network and cdma2000 1XRTT access network.

We have realized both secure seamless mobility and dynamic VPN establishment techniques described earlier. MIP was used for mobility support and SIP was used to support dynamic VPN establishment. We have experimented with MIP HAs from SUN and Cisco. Nortel’s VPN gateway is used to provide IPsec tunnels between a mobile on an external network and the enterprise network. A Microsoft Windows version of MIP client was used in the experiment.

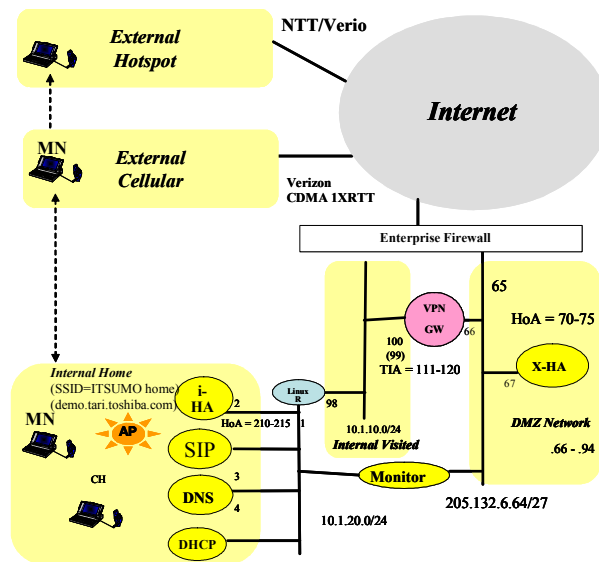


Figure 8: SUM experimental testbed

The mobile uses Sierra's Air Card 555 PCMCIA card to access the cellular network. We have used both audio and video-based streaming applications using RAT and VIC tools respectively. These represent CBR (Constant Bit Rate) and VBR (Variable Bit Rate) traffic respectively.

Table 1 shows the IP addresses associated with most of the functional components of the testbed.

Table 1: IP address parameters

Network Element	IP Address
CN	10.1.20.100
MN (i-CoA)	10.1.20.110 (DHCP)
MN (x-CoA)	166.157.173.122-(PPP assigned)
i-HoA	10.1.20.212
x-HoA	205.132.6.71
i-HA	10.1.20.2
x-HA	205.132.6.67
TIA (MN)	10.1.10.120
VPN-GW	205.132.6.66 10.1.10.100
SIP Server	10.1.20.3
DHCP Server	10.1.20.4

In this experiment the enterprise network is using private address space and thus we needed to install a Linux router that provides the NAT functionality. But in reality things are simpler when the enterprise network also has globally routable IP address range. Both the internal home agent and external home agent are configured with a range of i-HoA and x-HoA addresses. These addresses are mapped to the corresponding i-CoA and x-CoA respectively. VPN gateway is configured with a set of TIA addresses. During the VPN setup with IKE, mobile node gets configured with a specific TIA address from this range. During the triple encapsulation process, TIA address of the mobile is sent as the care-of-address for setting up the i-MIP tunneling.

Figures 9, 10 and 11 describe the protocol flow sequences for roaming from the enterprise to the wide area network and then back. Figure 9 shows the signaling flows for gradual movement of the mobile from the enterprise to the wide area network.

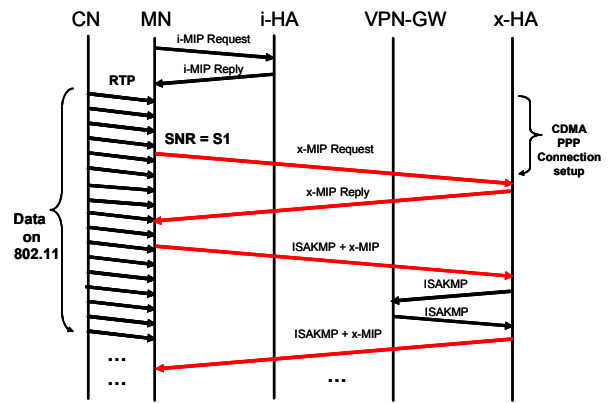


Fig 9: PPP setup over CDMA at SNR (S1)

Initially when the mobile is in the enterprise it receives the traffic sent by the CN using its only active 802.11b interface. As the mobile starts moving away, at a specific threshold of Signal-to-Noise ratio (SNR = S1), PPP connection to the cellular network is set up in the background while the mobile is still receiving traffic over 802.11b.

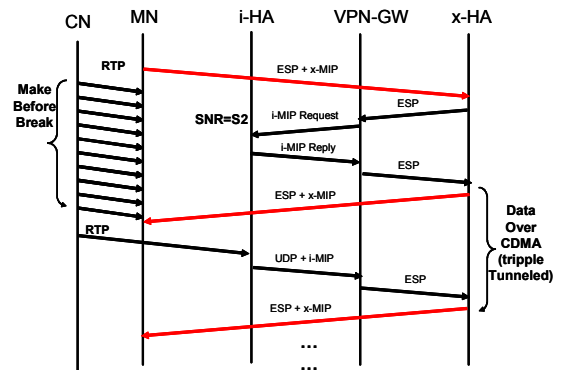


Fig 10: Make-before-break scenario at SNR = S2

Figure 10 shows the make-before-break situation as the mobile moves away further and loses connection with the 802.11 network. Make-before-break mechanism ensures that the PPP connection and all the associated tunnels are set up before the mobile loses contact with the 802.11 network. Figure 11 shows the scenario as the mobile returns home. VPN tunnel tear-down and CDMA disconnection take place in the background when the mobile still receives voice and video traffic via its 802.11 interface. As shown there are some out-of-order transient packets received.

We conducted several experiments using the mechanisms described in this paper for the SUM testbed described in figure 8. We used *ethereal* and *tcpdump* measuring tool to capture the data on the mobile's network interfaces. These tools capture the packets, the timing and their sequence numbers.

the 802.11 interface and first packet received on cellular interface.

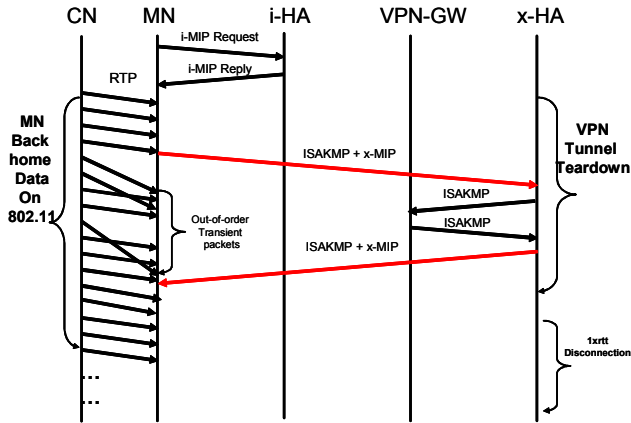


Fig 11: Mobile returning home (cellular-802.11)

Analysis of these results generate the performance parameters such as delay, packet loss, out of order packets etc. To realize the benefit of the make-before-break mechanism used in SUM, we compare these results with no-make-before-break mechanism. Figure 12 shows the results of handoff without make-before-break mechanism during mobile’s movement from 802.11 to cellular and back. Here, we observe packet loss due to layer 3 binding and other configuration steps as described in Section III.A.

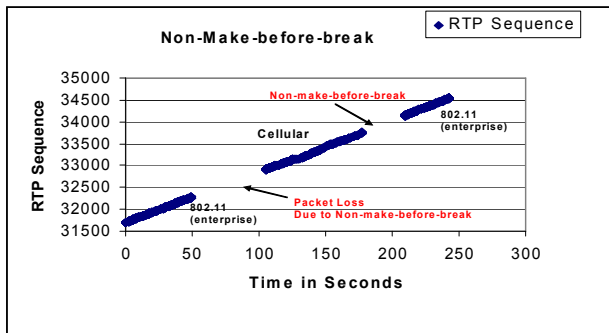


Figure 12: Hand-off with no-make-before break

Figure 13 shows the relative sequence of protocol flow during a mobile’s handoff from an 802.11b network to cellular and then back while using make-before-break mechanism. We show three types of protocols here in the diagram, protocol 1 denotes the RTP packets received on the mobile, protocol 2 denotes multiple instances of IPsec setup and teardown, and protocol 3 denotes the Mobile IP signaling between the mobile, i-HA and x-HA.

From several experiments, we observed that no packet was dropped during the mobile’s movement from 802.11 networks to the cellular network, thanks to the handoff pre-processing and make-before-break handoff techniques. However there is at least one gap of about 500 ms between the last packet received on

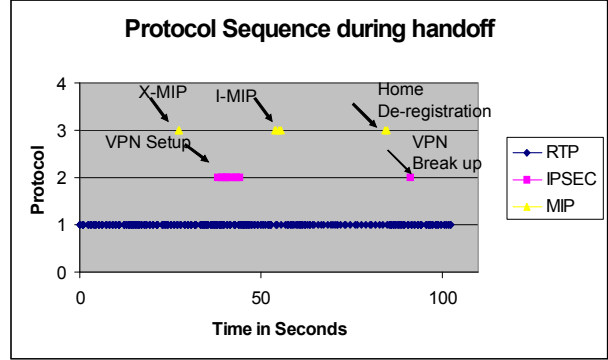


Figure 13: Protocol sequence during Handoff

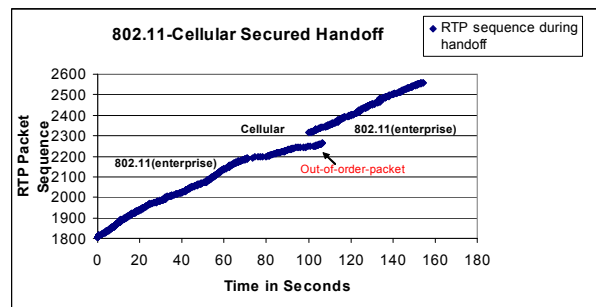


Figure 14: RTP sequence during handoff (internal-external) with make-before-break

This delay is due to the i-MIP registration over the dual tunnel (x-MIP and VPN tunnel). The cellular network provided a lower data rate than the wireless LANs thus there is the low gradient.

As the mobile moves on to the next external network such as hotspot, it simply updates the x-HA with its new local CoA and does not need to re-establish the VPN. When the mobile returns to its enterprise home network, it received several out-of-sequence packets. This is because the mobile already began to receive traffic from the enterprise network using its 802.11b interface while the VPN and MIP tunnels are being dismantled on the CDMA interface. According to the implementation it takes up to 5 seconds before the cellular interface is taken down after the mobile has registered its 802.11b interface with the internal home agent. During this time, the mobile continues to receive the transit traffic on its cellular interface, allowing the mobile to recover the transit packets which are already in the flight.

Figure 14 shows RTP sequence numbers received on the mobile as it performs handoff between 802.11b network and cellular network. As explained earlier, we observe that the packets are received out of sequence for about five seconds after the mobile has come back to the 802.11 network. While in cellular network

“Low Gradient” of the curve in Figure 12 is due to the low bandwidth in the cellular network.

Figure 15 shows extended results when the mobile makes two transition in the external network such as handoff between enterprise (802.11) to cellular (CDMA) and then to another hotspot (802.11). It shows that there is no packet loss during each of the handoff. However during mobile’s handoff from cellular to hotspot, transient out-of-order ESP packets may be discarded if the anti-replay option is on for a specific VPN connection.

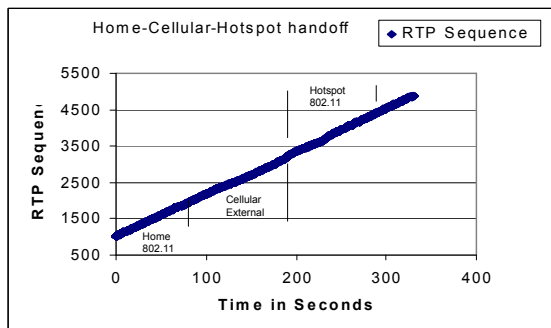


Figure 15: RTP packets at mobile (home-external-external handoff)

Figure 16 shows a time-flow analysis of Mobike-based handoff as described in Figure 7 of Section III. It shows an instance where the mobile moves from visited cellular network to hotspot and then back to cellular. Mobike signaling takes less time during handoff to hotspot than during handoff to cellular. Mobike-based handoff although does not need triple encapsulation, it still suffers from packet loss if there is no make-before-break mechanism deployed during transition. Signaling timeline is shown along MN.

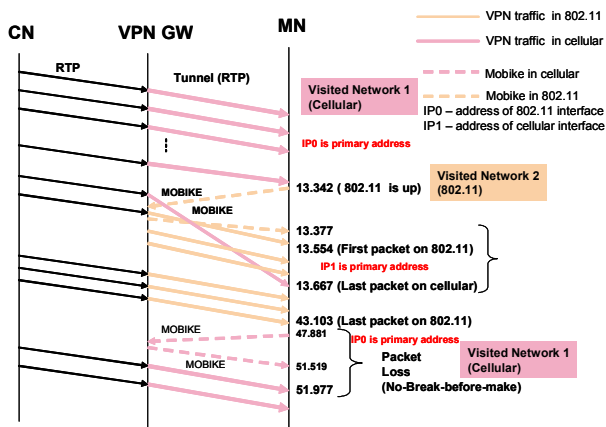


Figure 16: Mobike-based handoff (cellular-hotspot-cellular)

We set up an NTP server and synchronized the correspondent host and mobile node to measure the timing associated with each operation. From the measurements taken on the mobile, we observed that it takes about 10 seconds for the PPP negotiation to

complete, about 300 ms for the x-MIP registration to complete, about 6 sec for VPN tunnel setup, 400 ms for the i-MIP registration, and 200 ms for mobile IP de-registration when the mobile is back.

As observed in the last set of experiments packet loss during all three types of movements (i.e., enterprise (802.11b) to the cellular network, cellular network to hotspot (802.11b), and hotspot (802.11b) to hotspot (802.11b)) are avoided using proactive movement detection handoff scheme. Because of the limited bandwidth on the cellular network (60 kbps throughput) voice quality gets affected if proper codec was not chosen. We however plan to try this experiment on a high speed cellular network such as CDMA1XEVDO.

Figure 16 (a) and (b) show the transmission delay in logarithmic scale for the RTP packet from a streaming video being sent using VIC, and variation between inter-packet departure gap at CH and inter-packet arrival gap at MH.

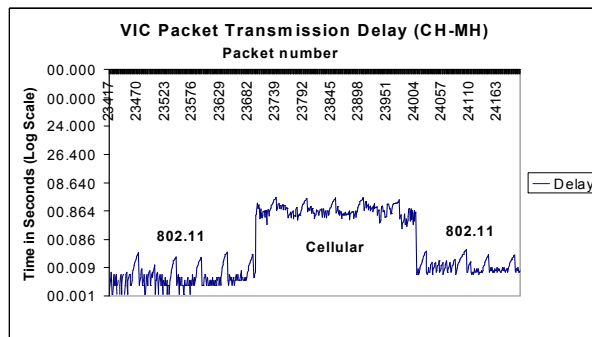


Figure 16 (a) Packet transmission delay (Viedo)

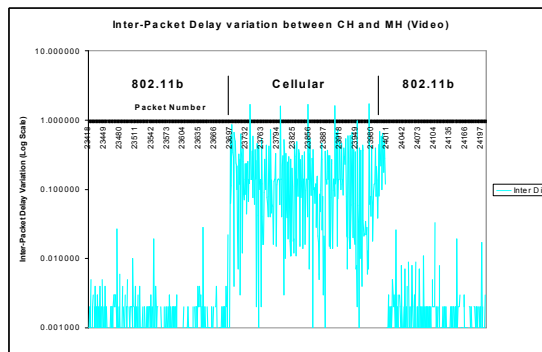


Figure 16 (b) Inter-packet departure and arrival variation delay for VBR (Video)

This variation delay seems to be more prominent in cellular network than 802.11b and thus will give rise to more jitter in the cellular network. It is interesting to note that video streaming is bit bursty in nature and thus has larger gap between bursts of packets (~1.5 s – 2.6 s) than the delay between consecutive packets within a burst (2 ms- 5 ms) both at the sending side and receiving side.

As is observed in Figure 17 (a), the transmission delay for RTP packet is almost 5 ms when the mobile is in 802.11b network but transmission delay for the packet increases in a random fashion as it moves to the cellular network and then saturates. This could be attributed to the queuing delay in the network.

Figure 17 (b) shows variation delay between inter-packet departure gap at CH and inter-packet arrival gap at MH. This variation seems to be more prominent in cellular than in 802.11b network for voice traffic also and may affect the audio quality in the cellular network.

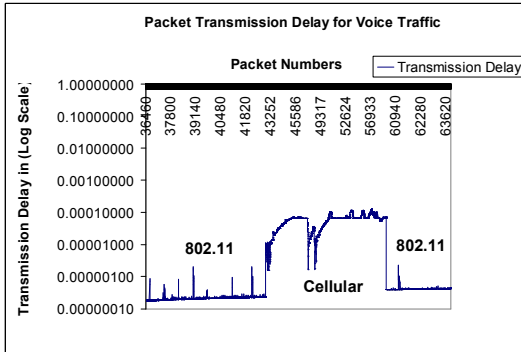


Figure 17 (a) Packet transmission delay (Voice)

Extent of burstiness of video traffic is affected by the frame rate of the video at the sending host. Figures 17 (a) and (b) show the results from the VoIP application using Robust Audio Tool (RAT). In the specific experiment we have used GSM encoding with a payload of 33 bytes. Compared to VIC-based video streaming, VoIP application is CBR (Constant Bit Rate) traffic and there is no burstiness. Transmission delays in Figure 17 (a) and 17 (b) are in logarithmic scale.

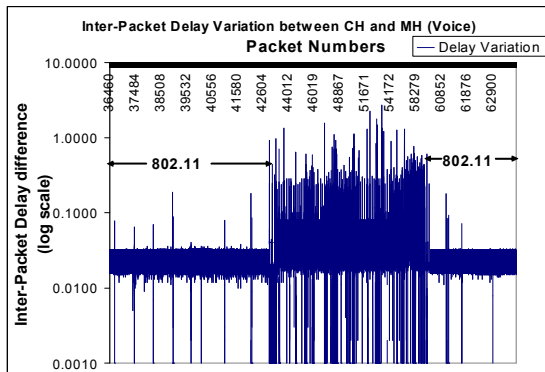


Figure 17 (b) Inter-packet departure and arrival delay variation for CBR (Voice)

Inter packet delay at the sender will depend partly upon the codec type and unit of transmission packet. We also observed that home agent could not encapsulate many of VoIP packets during its movement to cellular network and while within cellular. However we did not

lose any packet for VBR traffic such as video streaming traffic. Table 2 shows the timings associated with PPP setup, packet transmission delay, inter-packet arrival delay both at sender and receiver, MIP registration, DHCP and VPN setup in this experiment.

An overall analysis of the results from the above prototype experiment shows that a make-before technique adopted here help achieve smooth handoff while preserving the security of the data and signaling during the mobile's handoff. VBR-based video traffic is bursty in nature and thus gave a different set of values for inter-packet gap and transmission delay compared to a CBR based voice traffic. Transmission delay in 802.11b network does not show that much variation as compared to the cellular network. This could be attributed to the fact that cellular medium is a shared one and is subject to bandwidth fluctuation and interference more than the 802.11 network which is under more controlled environment.

In this specific experiment, we have not included the interaction with AAA server during its movement from enterprise to cellular environment. In reality hotspot and cellular networks may belong to two different administrative domains and the user may have separate subscription profile. Thus the mobile will need to contact the AAA server to perform profile verification before being able to continue the communication with the correspondent host. As part of our future work we plan to build a Secure Mobility Gateway (SMG) that will have the prior arrangement with the AAA servers in each of the roaming domains and will work as a broker agent between the domains. By having a dual functionality (e.g., AAA broker and external home agent) the mobile does not need to communicate with two different AAA servers belonging to two different domains. Recently there has been proposal in the "Core Networks" working group of 3GPP2 [18] that suggest that AAA profile verification and Mobile IP authentication can also take place in parallel. This mechanism will make the handoff between administrative domains bit faster as the AAA profile verification can take place in parallel while Mobile IP authentication can take place using other access authentication protocols such as PANA [19] (Protocol for carrying Authentication to Network Access).

V. Conclusions

We have presented an architecture and test-bed realization of secured universal mobility across heterogeneous radio systems including 802.11b and CDMA-based networks. Both Mobile IP and SIP-based architecture were discussed. Security, mobility, reachability, and dynamic VPN tunnel management are some of the highlights of the architecture. Test-bed experiments show that make-before-break mechanism allows seamless mobility during mobile's movement

between heterogeneous networks but out-of-order packet sequence was observed during the transition from external network to internal network. Although packet loss was eliminated there was additional packet transmission delay during transition from 802.11 network to another cellular network and while in cellular network. VoIP and video streaming traffic were used as CBR and VBR application respectively. Both of these applications showed different characteristics in terms of packet transmission delay, burstiness, jitter and packet loss for both the types of access networks during the handoff experiment. SIP and Mobike-based approaches seem to provide alternatives to MIP-based approaches and could reduce tunnel overheads and can interwork.

Table 2: Signaling Timing and CODEC Details

Type of operation	Timing
PPP setup	10 sec
X-MIP	300 ms
VPN Tunnel setup	6 sec
I-MIP	400 ms
I-MIP at home	200 ms
IPsec processing (end host)	60 ms
MOBIKE Update	30 ms in 802.11, 4 sec in cellular
DHCP (address acquisition)	~ 3 sec in 802.11b
One way Transmission Delay	Video – (a) ~5 ms (802.11b), (b) 500 ms - 2.5 sec (CDMA) Audio - (a) ~ 4 ms (802.11b), (b) gradual increase and then saturates in (CDMA)
Inter-packet gap	VIC (VBR)– variable (intra-burst, Inter-burst) RAT (CBR)– 16 ms – 32 ms
CODEC	RAT–GSM, Silence suppression Off VIC - H.263, 50 kbps, 5 fps

VI. References

[1] Hui Luo, Zhimei Jiang; Byoung-Jo Kim, N.K, Shankaranarayanan, P. Henry, “ Internet Computing, IEEE Volume 7, Issue 2, March-April 2003 Page(s):25 - 33

[2] T. Kivinen, “MOBIKE protocol”, draft-kivinen-mobike-protocol-00.txt, Internet Engineering Task Force, Work in progress

[3] Ann-Tzung Cheng, et al , “Secure Transparent Mobile IP for Intelligent Transport System” ICNSC 2004, Taipei

[4] www.birdstep.com

[5] F. Adrangi, H. Levkowitz, Mobile IPv4 Traversal of VPN Gateways, <draft-ietf-mip4-vpn-problem-statement 03.txt>, Work in progress, IETF

[6] C. Kaufman (Ed.), Internet Key Exchange (IKEv2) Protocol, draft-ietf-ipsec-ikev2-17.txt, IETF , work in progress

[7] C. Perkins (Ed.), IP Mobility Support for IPv4, RFC 3344

[8] H. Schulzrinne, Elin Wedlund, “Application Layer Mobility using SIP” ACM Mobile Computing and communications Review, vol 4 no 3, p47-57, July

[9] P. Hoffman (Ed.), “S/MIME Version 3 Message Specification for S/MIME”, RFC 2634, IETF

[10] T. Dierks, C. Allen “Transport Layer Protocol Version 1.0”, RFC 2246, IETF

[11] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, “Session Initiation Protocol” RFC 3261, Internet Engineering Task Force

[12] P. Rodriguez, R.Chakravorty, I. Pratt, S. Banerjee, “MARS: A commuter router Infrastructure for the Mobile Internet”, Mobisys 2004

[13] A. K. Miu, P. Bahl, “Dynamic Host configuration for Managing between Public and Private Networks”, USITS, 2001, San Francisco

[14] A. Snoeren, D. Andersen, H. Balakrishnan, “ Fine-grained Failover Using Connection Migration”, USITS, 2001, San Francisco

[15] M. Barton, D. Atkins, J. Lee, S. Narain, D. Ritcherson, K.E. Tepe, K.D Wong, “Integration of IP mobility and security for secure wireless communications”, Proceeding of ICC 2002

[16] A.Dutta, S. Das, A. McAuley, S. Baba, Y. Ohba, H. Schulzrinne, “Secured Mobile Multimedia Communication for Wireless Internet”, ICNSC 2004, Taipei

[17] C. Bormann (Ed.), “Robust Header Compression”, RFC 3095, IETF

[18] 3rd Generation Partnership Project 2, www.3gpp2.org

[19] A. Yegin (Ed.), “Protocol for Carrying Authentication for Network Access Requirements”, work in progress, IETF PANA working group

[20] N. Banerjee, W. Wu, K. Basu, S.K Das , “Analysis of SIP-based mobility management in 4G wireless networks”, Elsevier Special Issue of Computer Communication Journals, May 2004