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 (i.e., with little interruption to users and user applications) 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.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design

General Terms

Management, Measurement, Performance, Experimentation, Security

Keywords: Mobility, Mobile IP, Hot Spot, 802.11, Handoff, Security

1. 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). A user should be able to communicate and to access network services in a seamless and secure manner regardless of which type of access network one is using. A user should be able to maintain one's on-going secure application sessions when one moves 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 into 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 network, which is usually an 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 integrity protection (i.e., protecting the information from unauthorized change) and confidentiality protection (i.e., preventing attackers on an external network from interpreting the contents in the packets).

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, 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 also involves heterogeneous access technologies such as 802.11 and CDMA1XRTT respectively.

The rest of the paper is organized as follows. Section 2 discusses some of the related work in this area. Section 3 describes the SUM architecture and its various associated functional components. Section 4 describes the test-bed set up and performance measurement citing the specific handoff scenario for both video and voice traffic that represent VBR (Variable Bit Rate) and CBR (Constant Bit Rate) traffic respectively. We conclude the paper in section 5.

2. 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 the end clients do not change their IP addresses rather the mobile router keeps on changing the external IP addresses as they move around and connect to different access networks such as GPRS, CDMA and 802.11b. Although it has taken care of technology diversity, network diversity and channel diversity to support 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-gained, 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 during 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 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 thus avoids the need to use a separate mobility protocol, such as Mobile IP, to maintain continuous VPN and thus reduces the overheads needed to support secure mobility.

The proposed SUM architecture overcomes some of 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 any need to modify these. Make-before-break mechanism provides seamless mobility over heterogeneous access technologies.

3. The SUM Architecture

Figure 1 shows reference architecture without any related components that we will use to discuss SUM. An enterprise network is typically divided into intranets and de-militarized zones (DMZ). An intranet is the 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.

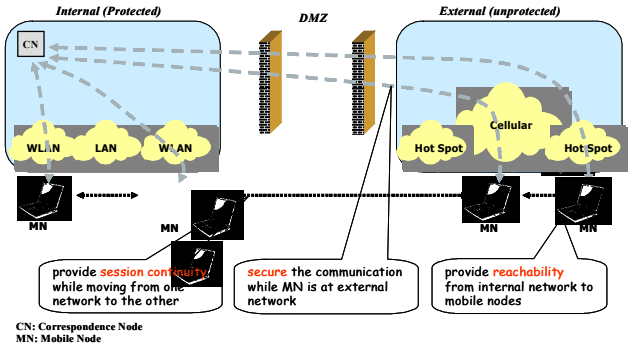

Figure 1: Mobility scenario in DMZ-equipped enterprise network

Several modes of communication can take place with the mobile.

- Both the mobile and its correspondent hosts are inside the same enterprise network.
- The mobile host moves between its enterprise network and wide-area-based cellular networks while communicating with the correspondent host inside the enterprise network.
- The mobile in a cellular network communicates with correspondent nodes on external networks.
- The correspondent host within an enterprise can initiate communication with the mobile which is already in the cellular network.
- The mobile can initiate communication with a correspondent host which is within an enterprise.

Although a mobile can always maintain multiple simultaneous network connections, each over a different type of network, this paper focuses on the case where a mobile uses one interface (network) at any given time even if both the interfaces are up.

SUM seeks to achieve the following main capabilities:

- 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 nodes to use 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 its mobility service provider's network (e.g., 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 IP address, it registers the new 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 3.1.

  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 the 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 3.2**.**

- Provide a *security* environment to a mobile that is comparable to the security level the user gets inside his/her enterprise network, regardless of where the mobile is.

  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.

3.1 Mobile IP Based SUM Architecture

Figure 2 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.

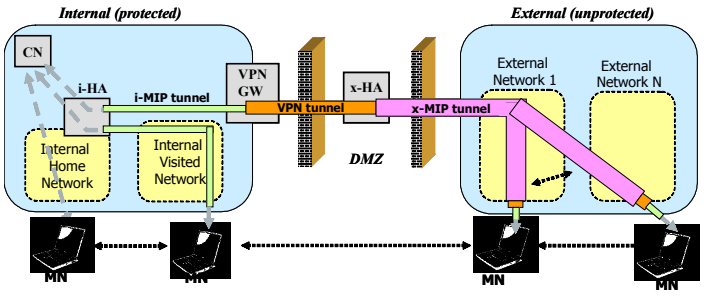

Figure 2: Secure mobility using MIP-based approach.

For clarity we define the following terms as these are used in the document.

- **i-HA-addr:** The IP address of the i-HA.
- **X-**HA-addr: The IP address of the x-HA.
- **i-MIP**: The instance of MIP used between a mobile and the mobile's i-HA.
- **x-MIP**: The instance of MIP used between a mobile and the x-HA.
- **i-CoA** (Internal Care-of Address): A mobile's care-of address registered with the mobile's i-HA.
- **x-CoA** (External Care-of Address): A mobile's care-of address registered with the mobile's x-HA.
- **VPN-GW**: VPN Gateway.
- **TIA**: Tunnel Inner address of the mobile

A mobile will have 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 will be 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 will be 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.

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 onto 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 keeps 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 few seconds, thus some of the packets which are already in the transit may get lost or may arrive at a later point. As a result, packets may arrive at the mobile out of order. 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 3 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 3.

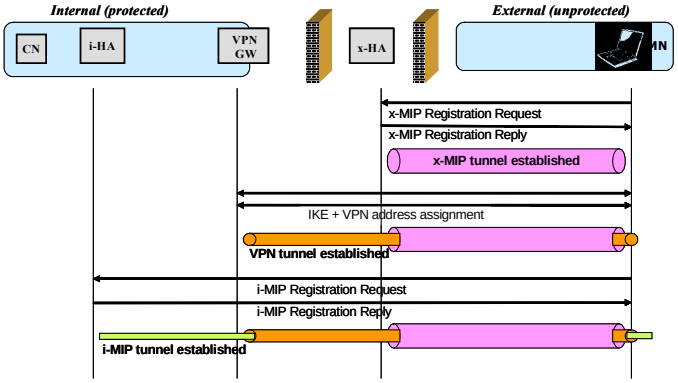

Figure 3: Interaction of Protocols for SUM using Mobile IP based architecture

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-based 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 to and from the mobile is not protected by a VPN tunnel. Other security measures can be used to secure the 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. 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 of course delays the SIP signaling little bit in the beginning but ensures that further communication is protected. There is no need to set up the initial double MIP tunnel if the SIP proxy at home has the prior knowledge of the mobile's COA. In that case initial INVITE from CN does not need to be carried over a double tunnel.

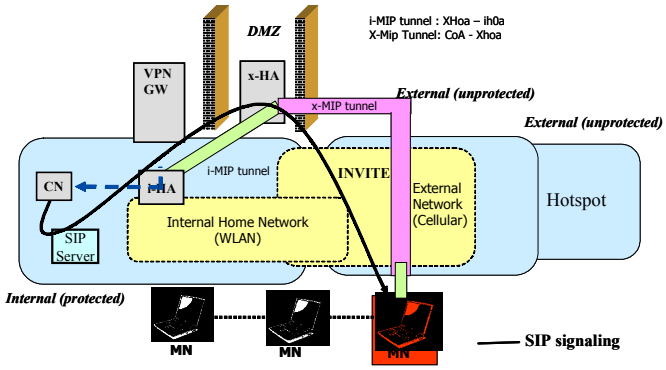

Figure 4: Dynamic tunnel management with SIP Signaling

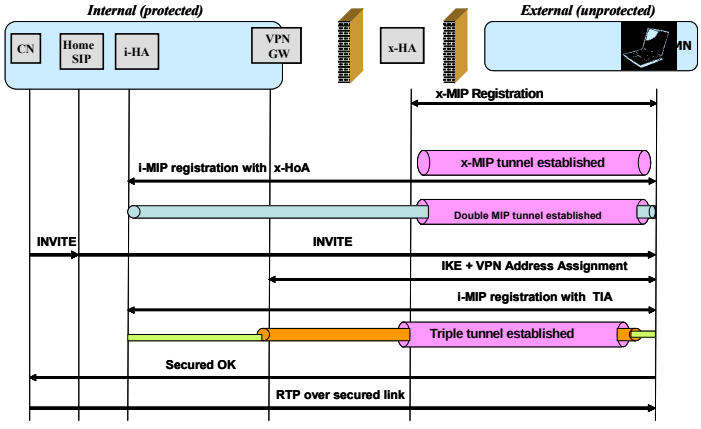

Figure 5: Protocol flow for dynamic tunnel management

Figure 5 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 getting INVITE from the correspondent node original 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. In this specific scenario home SIP server keeps an association between URI and the home address of the mobile. Thus both the SIP server and home agents are used in this specific scenario compared to a complete SIP-based scenario described later on.

3.2 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. Instead, it can modify the existing security association when it changes the IP address. This work is very recent within IETF and needs to be explored as part of future work.

As illustrated in Figure 6, 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. MOBIKE-based architecture can work using both SIP and MIP-based mobility, where the mobile uses its VPN tunnel address (TIA) to register with the home proxy.

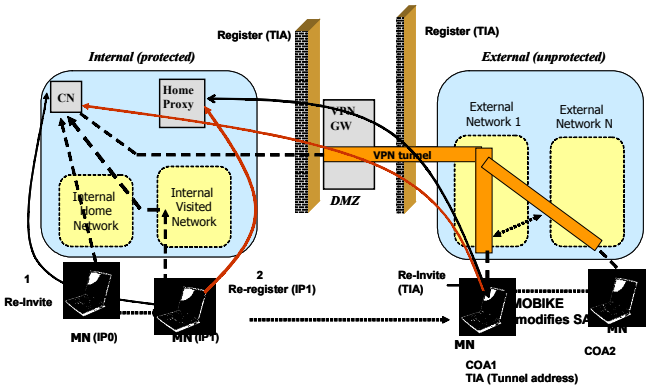

Figure 6: SUM architecture based on SIP and MOBIKE

4. Testbed Experimentation and Performance Evaluation

We have implemented the SUM framework in a multimedia test-bed as illustrated in Figure 7. It consists of an enterprise wireless LAN using IEEE 802.11b, CDMA1xRTT cellular network service from Verizon, and a public hotspot network using IEEE 802.11 with EarthLink's DSL as backhaul into the Internet. But the measurements shown here reflect only moving back and forth between enterprise network and CDMA1XRTT access network and does not include the Earthlink hotspot.

We have realized both secure seamless mobility and dynamic VPN establishment techniques described earlier to reduce handoff delay and data loss during the handoff in both directions. Mobile-IP 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.

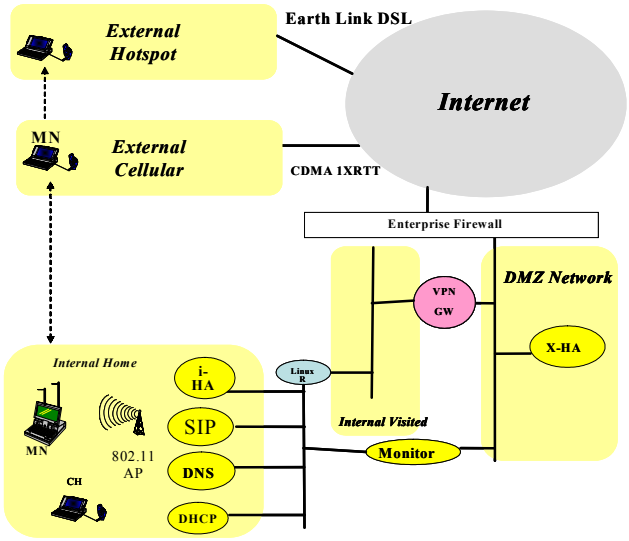

Figure 7: SUM Testbed

The mobile uses Sierra's PCMCIA card to access the cellular network. We have used both audio and video-based streaming applications using RAT and VIC tools respectively. The pre-processing and make-before-break handoff mechanisms establish the IPsec tunnel in the background while the communication is still going on through the 802.11 interface.

Table 1 shows the IP addresses associated with most of the functional components of the testbed. In this experiment the enterprise network is using private address space and thus we needed to install a Linux router in between that provides the NAT functionality. But in reality things would be simpler where 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 get mapped to the corresponding i-CoA and x-CoA respectively. VPN gateway is configured with a set of TIA addresses. During the VPN set up 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.

Table 1: IP address parameters

Entity	IP Address
CN	10.1.20.100
MN (i-CoA) MN (x-CoA)	10.1.20.110 (DHCP) 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

Figures 8, 9 and 10 describe the protocol flow sequences associated with the mobile's movement from the enterprise to the wide area network and then back.

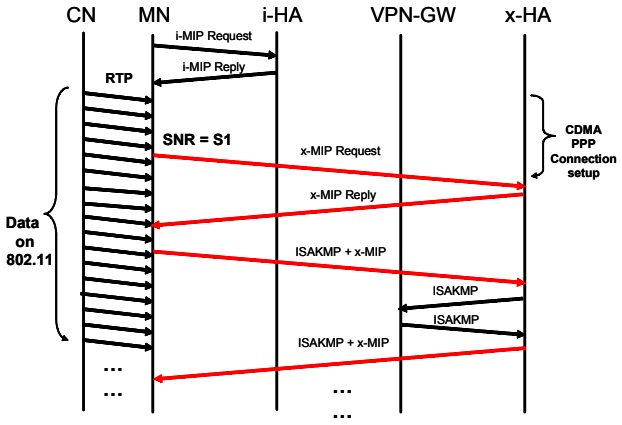

Figure 8: PPP setup over CDMA at SNR (S1)

Figure 8 shows the signal flows associated with the gradual movement of the mobile from the enterprise to the wide area network. Initially when the mobile is at the enterprise it receives the traffic sent by the CN (Correspondent Node) using standard ARP mechanism. Initially 802.11 is the only active interface and there is no PPP connection. As the mobile starts moving away, at a specific threshold value of Signal-to-Noise ratio (SNR = S1), PPP connection starts getting set up in the background while mobile is still receiving traffic on its 802.11 interface.

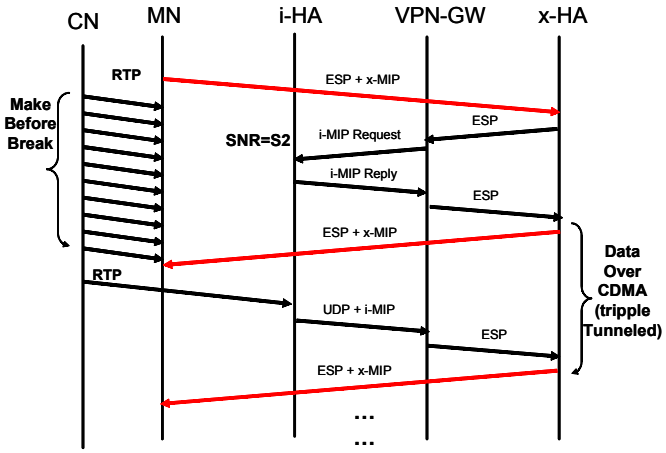

Figure 9: Make-before-break scenario at SNR = S2

Figure 9 shows the make-before-break situation as the mobile moves away further and loses connection with the 802.11 network. Make-before-break mechanism makes sure that the PPP connection and all the associated tunnels are set up before it loses the connection with the 802.11 network. Figure 10 shows the scenario as the mobile gets back home. VPN tunnel tear-down and CDMA disconnection take place in the background when the mobile still receives voice and video traffic in its 802.11 interface.

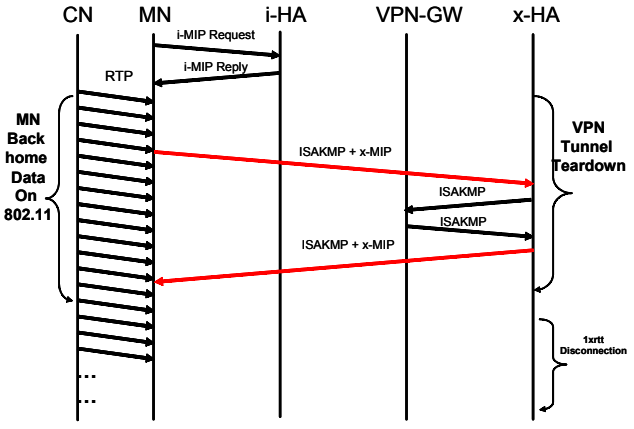

Figure 10: Mobile coming back home

We used ethereal and tcpdump measuring tool to capture the data on the mobile's multiple interfaces. These tools help capture the packets, the timing and their sequence numbers. Analysis from this log helps generate the performance parameters such as delay, packet loss, out of order packets etc. Figure 11 shows a set of measurements from the test-bed described in figure 7. It shows a sequence of the protocols executed on the mobile as it makes a transition from the enterprise network to the cellular network and then moves back. 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 the 802.11 interface and first packet received on cellular interface. 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, it will simply update the x-HA with its new local CoA and does not need to re-establish the VPN. When the mobile moves back to its home network inside the enterprise network, some packets received by the mobile were out of sequence. This was due to the fact that 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 11 shows the relative sequence of protocol flow during a mobile's handoff from an 802.11b network to cellular and then back. We are showing only three types of protocols here in the diagram, protocol 1 denotes the RTP packets received on the mobile, protocol 2 shows the IPSEC instances, and protocol 3 denotes the Mobile IP signaling between the mobile, i-HA and x-HA. We set up an NTP server and synchronized the correspondent host and mobile node to measure the timing associated with each operation.

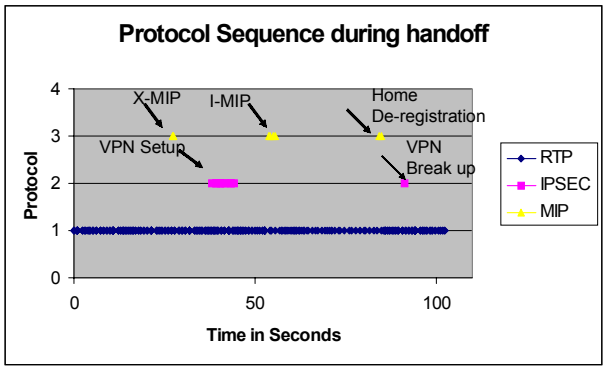

Figure 11: Protocol sequence during Handoff

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.

Thus 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.

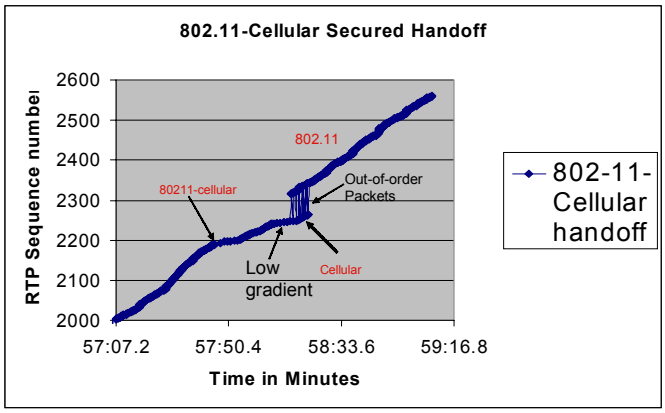

Figure 12: RTP packets at mobile during handoff

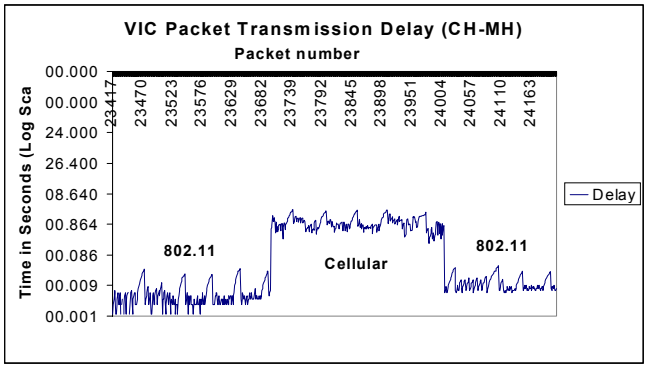

Figure 13 (a) Packet transmission delay

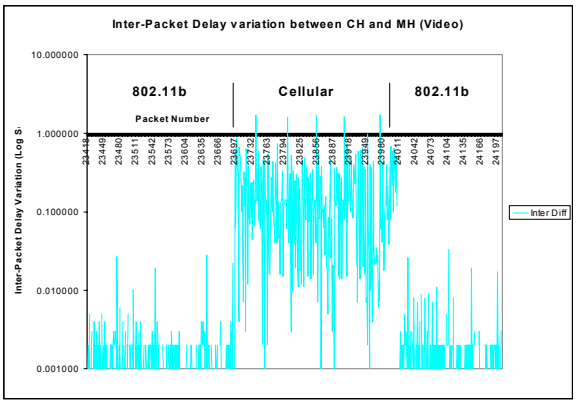

Figure 13 (b) Inter-packet departure and arrival variation delay for VBR (Video)

Figure 12 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 13 (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. 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

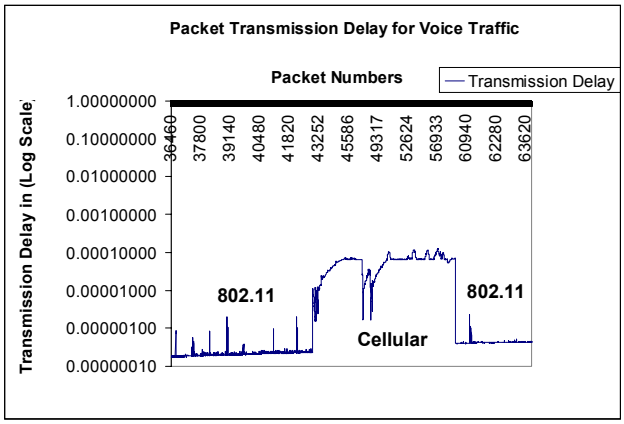

Figure 14 (a) Packet Transmission Delay

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. Extent of burstiness of video traffic is affected by the frame rate of the video at the sending host. Figure 14 (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 10 (a) are in logarithmic scale.

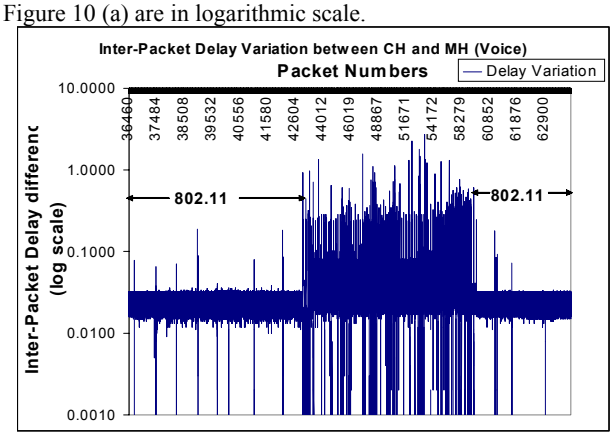

Figure 14 (b) Inter-packet departure and arrival delay variation for CBR (Voice)

As is observed in Figure 14, 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 14 (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.

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.

Table 2. 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
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

An overall analysis of the results from the above prototype experiment shows that a make-before break 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 controlled environment. In a real life scenario enterprise network is subjected to other traffic and may attribute to the signaling delay and packet loss.

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).

5. 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 smooth handoff is achieved during the movement between heterogeneous networks, but an additional delay was introduced during the 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.

6. References

[1] Hui Luo et al, "Integrating Wireless LAN and Cellular Data for the Enterprise", IEEE Internet Computing, April 2003

[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. Levkowetz, Mobile IPv4 Traversal of VPN Gateways, <draft-ietf-mip4-vpn-problem-statement 02.txt>, Work in progress, IETF

[6] C. Kaufman et al, Internet Key Exchange (IKEv2) Protocol, draft-ietf-ipsec-ikev2-14.txt, IETF , work in progress

[7] C. Perkins et al, 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 2000

[9] P. Hoffman et al, "S/MIME Version 3 Message Specification for S/MIME", RFC 2634, IETF

[10] T. Dierks et al, "Transport Layer Protocol Version 1.0", RFC 2246, IETF

[11] J. Rosenberg, H. Schulzrinne et al, "Session Initiation Protocol" RFC 3261, Internet Engineering Task Force

[12] P. Rodriguez, R.Chakravorty et al., "MAR: A commuter router Infrastructure for the Mobile Internet", Mobisys 2004

[13] A. 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 et al., "Integration of IP mobility and security for secure wireless communications", Proceeding of IEEE International Conference on Communications (ICC) 2002

[16] A.Dutta, S. Das et al, "Secured Mobile Multimedia Communication for Wireless Internet", ICNSC 2004, Taipei

[17] C. Bormann et al, "RObust Header Compression", RFC 3095, IETF

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

[19] A. Yegin et al, "Protocol for Carrying Authentication for Network Access Requirements", work in progress, IETF PANA working group