Secured Mobile Multimedia Communication for Wireless Internet

Ashutosh Dutta, Subir Das, Peter Li, Anthony McAuley
Telcordia Technologies Inc., 445 South Street, Morristown, NJ 07960

Yoshihiro Ohba, Shinichi Baba
Toshiba America Research Inc., Morristown, NJ 07960

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

Abstract- *Wireless Internet roaming may include several radio access networks involving different layer 2 technologies such as 802.11b, CDMA and GPRS. As a mobile user moves around and switches between wireless cells, subnets and domains, it needs to maintain the session continuity. At the same time security of signaling and transport media should not be compromised. A multi-layer security framework involving user authentication, packet based encryption and access control mechanism can provide the desired level of security to the mobile users. Architecture, implementation and performance of a similar framework in a mobile environment is presented here. Results and performance analysis of the implementation will be of immense value for wireless Internet service providers, before it is actually deployed in a wide scale manner.*

Key Words: Wireless Internet, Secured Mobility, Handoff

1 Introduction

Multimedia streaming traffic is gaining momentum as one of the killer application for the next generation Internet. Streaming media includes interactive traffic such as IP telephony and broadcast or multicast content delivery. Supporting streaming traffic in a mobile wireless Internet is faced with several challenges due to continuous handoff experienced by a mobile user. These challenges include dynamic binding, location management, quality of sevice and end-to-end security for signaling and transport. Mobile users will use heterogeneous radio access networking technologies such as 802.11b, CDMA, and GPRS specific to LAN (Local Area Network) and WAN (Wide Area Network) respectively. Mobility support in this environment can be provided by variety of mobility management techniques such as Mobile IP [1] and its variants such as IDMP [2], MIP-LR [3] and micro-mobility management techniques such as HAWAII [4], Cellular IP [5], application layer mobility management techniques such as SIP-MM [6]. It is imperative that both signaling and transport media sessions are secured, the user is authenticated as it moves around between cells, subnets and domains. Thus it is desirable to develop a multi-layer security framework for the mobile users that is independent of layer 2 access technologies.

As the mobile moves, it is subjected to potential attack at different parts of the access and core network. A multilayer security scheme can provide a comprehensive solution that can possibly reduce any such attack and can support a dependable and secured multimedia application. Building a wireless Internet telephony and streaming multimedia testbed is based on a basic framework discussed in [7]. A comprehensive testbed has been designed and implemented where the proof-of-concept for different functional components of a next generation wireless network including security can be demonstrated. Some of the important features of the multimedia testbed include mechanism to provide support for roaming across different carrier domains (e.g., micro, macro,and domain mobility) with a provision for billing and network management, quality of service, security, authentication and support for IPv6. Here we focuss on a multi-layer-security framework, its implementation and performance evaluation in the mobile wireless testbed.

This paper is organized as follows. Section 2 provides a snapshot of the related work and existing solutions that offer security in a mobile wireless Internet. Section 3 elaborates several functional components of the multimedia testbed. Section 4 describes the architectural framework and operational procedure of the multi-layer security features proposed. Implementation overview and performance details are presented in section 5. Finally we conclude the paper in section 6.

2 Related Work

Recently there have been flurry of activities in the area of security for mobile networking in wireless environment. Most of the previous work focus on encryption mechanism and key distribution methodology. Reference [8], [9] explain different ways of how Mobile IP and IPSec [10] can work together. [11] explains some of the insecurity associated with 802.11. Reference [12] provides an IPSec based solution in mobile IP environment by instituting an IPSec gateway next to home agent. However these proposals do not provide a comprehensive solution for end-to-end security across provider domains involving AAA (Accounting, Authorization and Authentication) entities. Most recently Mobile IP working group is looking into supporting IPSec based VPN (Virtual Private Network) for mobile networks by instituting dual home agents. But overhead and encapsulation associated with this triple encapsulation may not be suitable for real-time communication.

This paper provides end-to-end security solution involving multiple provider domains and compares the performance results with two different types of mobility binding approaches such as network layer based Mobile IP and application layer SIP based mobility.

3 Mobile Multimedia Components

Current multimedia testbed is shown in Figure 1. This testbed emulates a wireless Internet with multiple carrier domains. Mobile stations are multi-media laptops and PDAs equipped with cameras, and audio devices and have either built-in feature or PCMCIA slots for 802.11b and CDMA1XRTT interface for communication.

Base stations provide the last-hop connectivity to the mobile users over different types of radio access network such as 802.11b, Bluetooth and CDMA/GPRS. An ERC (Edge Routing and Controller) in the testbed is a routing and control system that connects a wireless access network to a regional wireline IP network. Each ERC may support several RANs. An ERC comprises two functional entities, an edge router (ER) and an Edge Control Agent (ECA). The ER functions as an IP router , while the ECA is an intelligent agent that interacts with the Domain Control Agent (DCA) to control the RANs as well as support necessary network-wide control tasks. ERC's control entity provides many of the server and client software such as PANA (Protocol for carrying Authentication to Network Access) server daemon, Diameter client, IPSEC server, DRCP (Dynamic Rapid Configuration Protocol) server.

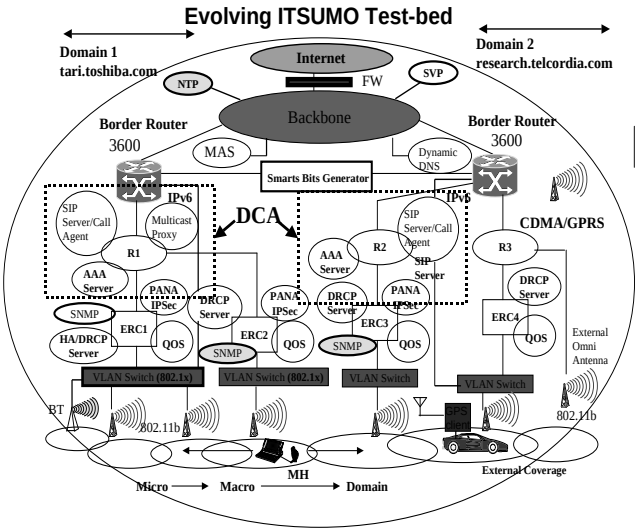

Figure 1: Experimental testbed

The domain control agent (DCA) provides session management as well as the means of interaction between users and among network control entities. DCA also supports 1) mobility management, 2) authentication, authorization and accounting and 3) QoS management. It is assumed that each autonomous system has several components of domain control agent distributed within its entity.

Location management and application layer mobility (personal and terminal) are taken care of by SIP [13]. SIP user agent runs on all the communicating nodes that helps set up and tear down the multi-media calls. A SIP server can act in proxy/re-direct mode and can also behave as a registrar. When a call is established using a SIP server (non-direct mode), it can interact with location server such as finger server or rwho server, and can provide services such as registration, secured key exchange and location updates.

Address acquisition is taken care of by DRCP [14]. DRCP is a light-weight version of DHCP suitable for wireless roaming that dispenses IP addresses to the roaming clients. DRCP client code interacts with IEEE 802.11 driver, mobile IP and SIP user agent during the handoff process. As part of the built-in mechanism of DRCP, the client defaults to DHCP in the absence of DRCP servers.

In addition to application layer mobility provided by SIP for real-time traffic, current testbed implements Mobile IP as one of the alternate mobility management scheme. Mobile-IP based approach is mostly used for non-real-time application such as TCP based traffic. As part of providing layer 3 mobility management solution for non-real-time application, SUN Micro System's Mobile IP [15] is implemented in the testbed. It operates in co-located care-of-address mode where a DRCP server dispenses IP address to the client.

4 Multilayer Security Framework

Several levels of security mechanism have been designed to support multi-media calls across multiple carrier domains. These provide user based access control, packet based encryption and end-to-end security for both signaling and media. Two types of mobility approaches have been illustrated in this paper; network layer mobility binding using SUN's mobile IP and application layer mobility using SIP mobility. SUN mobile IP was used in conjunction with DRCP so that the client obtains a new care-of IP address and does not need any foreign agent in the visited domain. Unlike Mobile IP, SIP based mobility provides an end-to-end mobility solution without depending upon underlying home agent or foreign agent.

A specific carrier domain is designated to be an AAA domain. The mobile multimedia testbed is using Diameter [16] as an AAA (Authentication, Authorization and Accounting) protocol running on NAS (Network Access Servers) and AAA servers to provide profile based verification services. In addition, a new protocol is being developed called PANA [17] that provides user-to-network access control. PANA provides access control mechanism to the mobile client and can work as front end to an AAA server running Diameter. It acts as a user front-end for Diameter server. PANA is implemented as a user level protocol to enable a flexible access control that works independent of any layer 2 technology, on both IPv4 and IPv6. It can work with any configuration protocol such as DHCP and DRCP. An access control mechanism involving SIP, PANA and AAA has been developed that will protect the intruders from hijacking an established session. AAA functionality has been added by instituting Diameter servers in each domain (visited and foreign) that help provide profile verification for the mobile users. The AAA framework acts as a backend entity to PANA server or SIP server and helps in setting up the access control at the edge router.

Following lists several of the access control mechanism using SIP, AAA, PANA and IPSEC functionality. SIP and AAA based security model provides access control on SIP registration and SIP signaling. PANA and AAA based security model helps access control on the edge routers and interacts with IPSec to provide packet encryption.

4.1 SIP-AAA Model

We have implemented the following SIP-AAA interaction model in order to realize how SIP signaling can interact with AAA infrastructure in a mobile environment. In this model when the SIP server receives a SIP Register message from the MH, it consults with the home AAA server for authentication and authorization by using Diameter protocol. SIP user's profile verification database is located in the home AAA server, not in the SIP server. It is to be noted that although our SIP-AAA interaction implementation covers only the limited cases in which local SIP server or SIP proxy is not involved, several methods have been proposed such as [18] and [19] in order to cover the entire scenario of SIP-AAA interaction.

PANA offers user registration/authentication at the application level with AAA (Diameter) framework. Initial authorization is taken care of by PANA protocol that helps setting up the firewalls within ERC and thus controls any signal or data traffic that is passed onto the network. This offers local authentication for quick handoff as the client moves between the subnets within a domain. In this model SIP registration is authenticated only after consulting with AAA server. In usual case, SIP registration is done in the SIP server, after the client obtains a new address. Interaction between the SIP server and AAA server is meant to provide a mechanism so that a communicating user's activities are monitored securely for accounting and auditing purposes. Besides authentication via home SIP server and home AAA server, a user is also authenticated via interaction between local AAA server and home AAA server using Diameter. Figure 2 shows SIP-AAA interaction that has been implemented in the testbed.

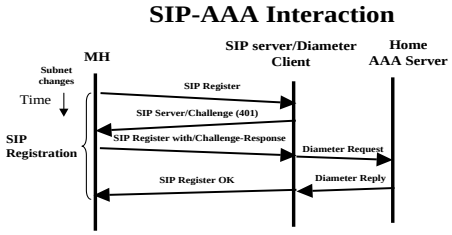

Figure 2: SIP-AAA Interaction

4.2 IPSec-PANA-AAA model

The proposed multi-layered security scheme provides packet based encryption and an application layer authentication based on user NAI. When the MH moves into a new domain, it performs a PANA (Protocol for carrying Authentication for Network Access) registration with the PANA server in the domain. Since the PANA server has no pre-established security association with the MH at the time of PANA registration, the PANA server consults with the home AAA server directly or indirectly through a local AAA server by using Diameter protocol to authenticate the user on the MH. Once the PANA registration is successful, an LSA (Local Security Association) is established between the MH and PANA server so that any further authentication that is required for intra-domain hand-off is performed locally and quickly at the PANA server without contacting the home AAA server. In addition to intra-domain hand-off case during movement, the local authentication is also performed periodically in order to detect the event that the user silently disappears from the domain due to, e.g., battery exhaustion or bad radio conditions.

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

It is possible to combine PANA with various kinds of access control mechanism. In the testbed, PANA is used to provide dynamic control of a router with firewall functionalities so that full network access is authorized for only hosts associated with authenticated PANA clients. The firewall which was once opened for an authorized hosts is closed immediately when periodical PANA re-authentication fails. An example message sequence for PANA Diameter is illustrated in Figure 3.

4.3 Packet encryption

Although 802.11b access provides WEP (Wired Equivalent Privacy) based encryption scheme for the last-mile wireless hop, we have used an IPSEC based encryption mechanism to secure the packets on the last hop wireless networks so that it can be layer 2 agnostic. An IPSEC tunnel is established between the mobile client and the edge router by distributing the key using IKE (Internet Key Exchange) mechanism. We use PANA for distributing IKE credentials to an authorized host. When the host is authorized as a result of PANA based authentication, the IKE credentials are carried in a PANA message and are transferred from the PANA authentication agent to the host. The credentials are then used for establishing an IPsec tunnel between a host and an access router, that provides a secure unicast communication channel in the access network including a wireless LAN segment. The dynamic distribution of the IKE credentials enables hosts to roam among different administrative domains since there is no need for a host to pre-configure the credentials. As the mobile moves to a different subnet and attaches to a new subnet, another IPSec tunnel is established between the mobile host and the edge router. It is to be noted that this IPSec tunnel

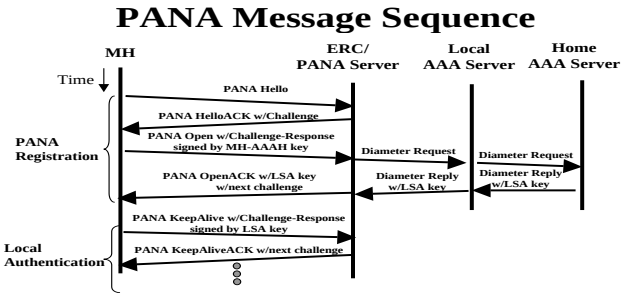

Figure 3: PANA-AAA Interaction

secures the signaling and data only on the last hop wireless access in each domain.

4.4 End-to-end security

While an IPSEC based encryption mechanism helps secure the last hop wireless channel, it is essential to provide end-to-end security to both the data and signaling. A combination of Mobile IP and IP-Sec based solution can provide one such architecture but it suffers from the overhead associatd with triple-encapsulation. Since the Real-time traffic is RTP/UDP based, secured RTP (SRTP) [20] is used to provide encryption to different types of multimedia traffic such as audio, video and data. Setting up a secured RTP session involves exchanging separate RTP key between the mobile host and correspondent host for a specific real-time media type as audio, video or data. SIP clients use PGP based authentication scheme while registering with the SIP servers. RTP key exchange takes place by means of INVITE-exchange method using SIP signaling at the time of setting up calls. Since RTP key is part of SDP parameters it is protected using S/MIME (Secured MIME) [21] mechanism. This methodology ensures that both signaling and data can be secured end-to-end and does not suffer from extra overhead associated. Figure 4 shows a snapshot of the components involving DRCP, SIP, IPSec, PANA, Diameter and Mobile IP.

4.5 Sequence of operation

In order to demonstrate seamless mobility, different suite of protocols have to interwork at several layers to provide desired functionality. Figure 5 shows a protocol flow where Mobile IP based mobility binding is used and figure 6 shows a protocol flow for SIP based mobility with Secured RTP for end-to-end security.

Mobile station in the home network tries to make a SIP call before the user is authorized by the PANA server, and it fails. This demonstrates that the client needs to be authenticated at the nearest ERC before the SIP signaling goes through. Then the MS activates PANA agent for user registration to open the firewall rules controlled by ERC by providing the correct NAI (Network Access Identifier). Then CH makes a SIP call to MS using SIP proxy server which is in the same domain. During this time the SRTP key is exchanged as part of INVITE exchange mechanism. MS starts to move towards another domain and experiences a domain handoff first (Domains are segregated as AAA domains not DNS domains in this case) and then a micro and a macro handoff respectively once it is present in the new domain. As soon as it moves to a new domain (which is also a new subnet), it listens to the DRCP server advertisement and gets a new IP address to get it quickly configured. Session continuity is taken care of by SIP Re-INVITE or Mobile IP binding update, while user authentication is taken care of by PANA within a domain. Interaction between the AAA servers is performed only when MH moves between domains. In case of SIP based terminal mobility, continuity is achieved by re-inviting the Correspondent Host (CH) everytime MH moves to a new subnet, and thus getting the media re-directed to the correct IP address. Time taken for media delivery (redirection) is not affected by SIP's re-registration mechanism, but the local authentication mechanism by PANA will probably delay the media delivery to some extent because of the established firewall. Re-registration is mostly done for any new incoming multimedia calls as the mobile host moves away. While PANA provides a user based authentication, IP-Sec from [10] has been implemented between the client and the first hop router to provide packet based security. In the testbed IPSec tunnels are set up between the client and ERC1. These get de-tunneled beyond ERC1 and tunneling takes places again between ERC2 and MH after the handover. However in case of Mobile IP binding, mobile node can interface with IPsec and firewall triggered by PANA agent. In order to work with firewall mobile node has to create reverse IP tunneling from mobile's care-of-address back to home agent.

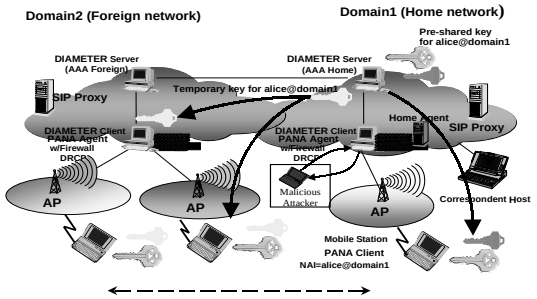

Figure 4: DRCP-SIP-IPSec-AAA-PANA Interaction

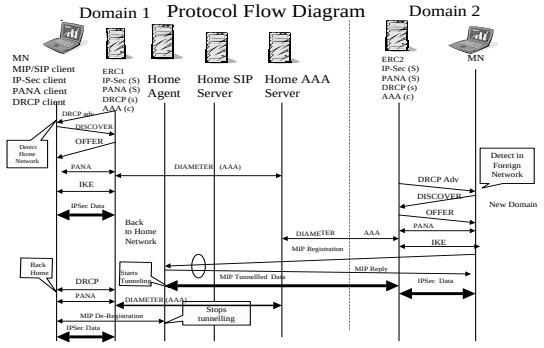

Figure 5: Protocol flow with Mobile-IP

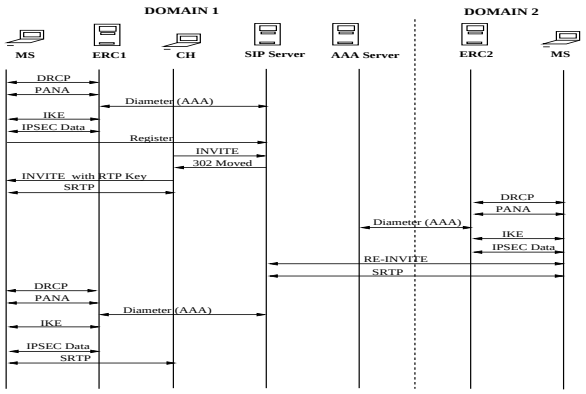

Figure 6: SIP mobility and Secured RTP Flow

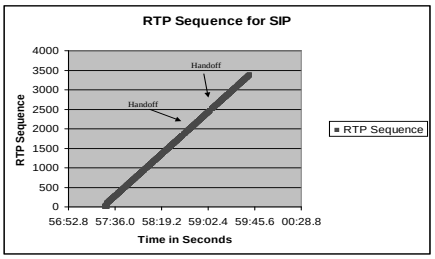

Figure 7: RTP packet loss with SIP mobility

5 Performance Analysis

Experiments were carried out in the multimedia testbed to validate the features of secured inter-domain mobility. Measurements were taken for both Mobile IP and SIP based terminal mobility as they interacted with DRCP, PANA and IPSec. We took measurements to figure out the timing associated with each atomic operation during the process. This measurement process allowed us to determine the timing for each of the operation associated with signaling, time for moving between cells, triggering to obtain an IP address using DRCP, sending the PANA messages for PANA-AAA interaction, interaction between the Diameter server and SIP server, interaction between two AAA servers during the domain handoff, Mobile IP registration with IP-Sec tunnels.

It is noteworthy to mention that, these parameters strongly depend on media used, number of hops, authentication mechanism used, background traffic, processing speed of the correspondent and mobile hosts. A complete Re-invite, OK and ACK sequence associated with SIP took about 500 ms including the processing time at the end hosts. As an optimization technique CH could start forwarding the data to the MH as soon as it receives the Re-Invite message (without waiting for ACK and OK message) thus helping to reduce the time for media redirection by about 350 ms. Address acquisition because of DRCP is within 100 msec, but that does not include the extra time needed to detect the channel change at layer 2 or DRCP server advertisement periodically. SIP re-registration does not affect the media re-direction to the new address, since it is independent of the Re-Invite process and is used mostly for location management. A typical complete registration process so that the client's new IP address gets updated in the SIP server is about 150 ms. From the experimental results it was observed that it takes almost 1 sec from the time it lost connectivity with the old access point until the host gets configured with the new channel number under the new access point. As it binds to the new access point and listens to the server advertisement, DRCP Discover process sets in by the client. Beacon interval from an 802.11b access point is about 100 msec (this value is however variable) that contributes to the L2 delay. It is assumed that rest of the time is used to process the beacon and set up the channel number in the application before a layer 2 association is established.

Secured mobile communication has been demonstrated by integrating both Mobile IP and SIP based mobility with IPSec, PANA and AAA. IP-Sec tunnel between the client and

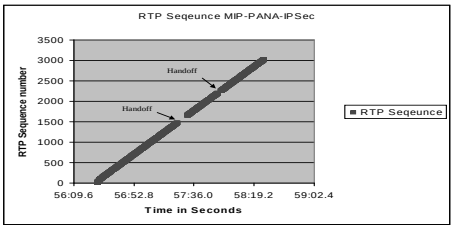

Figure 8: RTP packet loss with Mobile IP

ERC1 and ERC2 adds an overhead of about 53 bytes for UDP packets that comprise the IP headers, SPI, Sequence number and authentication header. Sun's Mobile IP code has been modified so that it can work with DRCP while enabling reverse IP tunneling over IPSec. In the secured mobility experiment it was found that overall timing for RTP packet interruption due to DRCP, PANA and SIP amounts to be under 2 sec. SIP Re-INVITE retransmission takes place during the domain handoff, if the PANA registration has not completed during the domain handoff. But this can also be reduced if the PANA registration takes place before SIP re-invite is issued. As it turns out, the bulk of the time is consumed for SIP signaling (Re-Invite, ACK, OK) which is about 600 ms. As evident, domain hand-off takes more time than subnet handoff because of extra time taken due to interaction with the AAA server. In optimized mode, the total interruption due to subnet and domain handoff is limited to 400 msec, with domain handoff taking slightly more time because of AAA interaction.

Table 1 shows the timing associated with different functional components for subnet and domain handoff measured in seconds. As is evident domain handoff takes more time than subnet handoff because of associated AAA interaction. Figure 7 shows the loss of RTP packets as the mobile is subjected to inter-domain handoff using application layer SIP based mobility approach. Figure 8 shows similar results when the mobile is subjected to inter-domain handoff but uses network layer mobile IP based approach. It is interesting to note that SIP based mobility approach offers less gap in RTP packets during the mobile's handoff between subnets belonging to two different domains compared to Mobile IP based

Table 1: Handoff Values in Seconds

Handoff	RTP1	RTP2	DRCP	PANA	SIP
Ave(S)	0.322	1.81	0.079	0.002	0.227
SDV(S)	0.07	0.492	0.033	0.0005	0.255
Ave(D)	0.241	1.89	0.08	0.045	0.289
SDV(D)	0.061	0.306	0.014	0.002	0.254

approach. Although in both the cases, IPSEC tunnel setup and tear down contributes to most of the delay during domain handoff.

6 Conclusions

This paper provides an architectural and implementation perspective of secured mobile multimedia communication supporting wireless Internet telephony and streaming multimedia. It has realized several functional components needed to provide a seamless operation over the wireless Internet across multiple service provider domains. In addition to describing the functional components of the architecture, and sequence of operation, it has highlighted some of the performance measurement to determine the time taken for supporting secured inter-domain mobility. Two primary mobility binding approaches were investigated to realize these atomic operations. Results and analysis of the secured multimedia communication in an emulated Internet will prove beneficial for the mobile wireless operators.

References

[1] C. Perkins, "IP mobility support for IPv4," RFC 3344, Internet Engineering Task Force, Aug. 2002.

[2] S. Das, A. Misra, P. Agrawal, and S. K. Das, "Telemip: Telecommunications-enhanced mobile IP architecture for fast intradomain mobility," *IEEE Personal Communications Magazine*, vol. 7, pp. 50–58, Aug. 2000.

[3] R. Jain, T. Raleigh, D. Yang, L. F. Chang, C. J. Graff, M. Bereschinsky, and M. Patel, "Enhancing survivability of mobile Internet access using mobile IP with location registers," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (New York), Mar. 1999.

[4] R. Ramjee, T. F. LaPorta, L. Salgarelli, S. Thuel, K. Varadhan, and L. Li, "IP-based access network infrastructure for next-generation wireless networks," *IEEE Personal Communications Magazine*, vol. 7, pp. 34–41, Aug. 2000.

[5] A. Campbell, J. Gomez, S. Kim, A. G. Valk, C.-Y. Wan, and Z. R. Turnyi, "Design, implementation, and evaluation of cellular IP," *IEEE Personal Communications Magazine*, vol. 7, pp. 42–49, Aug. 2000.

[6] E. Wedlund and H. Schulzrinne, "Mobility support using SIP," in *2nd ACM/IEEE International Conference on Wireless and Mobile Multimedia (WoWMoM)*, (Seattle, Washington), Aug. 1999.

[7] A. Dutta, J. Chen, S. Madhani, A. McAuley, N. Nakajima, and H. Schulzrinne, "Implementing a testbed for mobile multimedia," in *Proceedings of the IEEE Conference on Global Communications (GLOBECOM)*, (San Antonio, Texas), Nov. 2001.

[8] J. Binkley, "An integrated IPsec and mobile IP for FreeBSD," Technical Report 01-10, Portland State University, Oct. 2001.

[9] J. Zao, J. Gahm, G. D. Troxel, M. Condell, P. Helinek, N. Yuan, I. M. Castineyra, and S. T. Kent, "A public-key based secure mobile IP," *Wireless Networks*, vol. 5, no. 5, 1999.

[10] Freeswan. www.freeswan.org.

[11] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, (Rome, Italy), pp. 180–189, July 2001.

[12] M. Barton, D. L. Atkins, J. F. Lee, S. Narain, D. Ritcherson, K. E. Tepe, and K. Wong, "Integration of IP mobility and security for secure wireless communications," in *Conference Record of the International Conference on Communications (ICC)*, (New York, NY, USA), pp. 1045–1049, Apr. 2002.

[13] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. R. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: session initiation protocol," RFC 3261, Internet Engineering Task Force, June 2002.

[14] A. McAuley, S. Das, S. Madhani, S. Baba, and Y. Shobatake, "Dynamic registration and configuration protocol (DRCP)," internet draft, Internet Engineering Task Force, July 2000.

[15] "Sun mobile ip." playground.sun.com/pub/mobile-ip.

[16] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter base protocol," RFC 3588, Internet Engineering Task Force, Sept. 2003.

[17] Y. Ohba *et al.*, "Problem statement and usage scenarios for PANA," internet draft, Internet Engineering Task Force, Apr. 2003. Work in progress.

[18] H. Schulzrinne, "SIP registration," internet draft, Internet Engineering Task Force, Apr. 2001. Work in progress.

[19] H. Basilier, P. Calhoun, M. Holdrege, T. Johansson, J. Kempf, and J. Rajaniemi, "AAA requirements for IP telephony/multimedia," internet draft, Internet Engineering Task Force, Mar. 2002. Work in progress.

[20] M. Baugher *et al.*, "The secure real-time transport protocol," internet draft, Internet Engineering Task Force, July 2003. Work in progress.

[21] S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, and L. Repka, "S/MIME version 2 message specification," RFC 2311, Internet Engineering Task Force, Mar. 1998.