

Mobility Testbed for 3GPP2-Based Multimedia Domain Networks

Ashutosh Dutta, Kyriakos Manousakis, Subir Das, and Fuchun J. Lin, Telcordia Technologies
Tsunehiko Chiba, Hidetoshi Yokota, and Akira Idoue, KDDI R&D Laboratories, Japan
Henning Schulzrinne, Columbia University

ABSTRACT

Wireless service providers strive to preserve the quality of service and user experience for mobile users. Several standards bodies are defining architectures that can be used as a platform to provide secure and seamless services to these mobile users. These architectures aim to provide several required functions such as signaling, configuration, security association, encryption, and billing. However, the placement of several functional components and their interaction at several layers contributes to the operational complexity and thus affects the optimal results. Testbed realization of any standardized architecture can help investigate the underlying networking issues. In this article, we describe a mobility test bed implementation based on one of the architecture alternatives of 3GPP2, where the outbound signaling servers are distributed around the edges of the network. We experiment with three different hand-off techniques and analyze the associated experimental results. Analysis of these experimental results and experiences obtained from the testbed implementation can be helpful to any service provider that plans to deploy a version of the MMD (multimedia domain) architecture with distributed signaling servers.

INTRODUCTION

Mobile users require secure and seamless mobility access as they move across heterogeneous access networks such as IEEE 802.11, code division multiple access (CDMA2000), worldwide interoperability for microwave access (WiMAX), and general packet radio service (GPRS). However, additional complexity of the underlying networks and the variety of security and bandwidth requirements for each of these types of networks make it difficult to achieve the desired quality of service. In an effort to provide cellular-like dependable but more flexible service to mobile users over an IP network, several standards bodies such as 3GPP, 3GPP2, ITU-T, IEEE, and IETF are working together to define a set of protocols and architectures that can be used by service providers. The 3rd Generation Partnership Project (3GPP) focuses on defining

the architecture and associated functional elements called IMS (IP multimedia subsystem), designed for wideband code division multiple access (WCDMA) networks [1]. Similarly, 3GPP2 has defined an IMS-equivalent architecture called multimedia domain (MMD) that can be used over CDMA2000 networks [2]. However, there has not been any wide-scale deployment based on these architectures. Thus, it is useful to build pilot testbeds based on these architectures, analyze the performance, and recommend modifications that may be required to optimize these systems. The results of the experience gained during implementation and performance analysis also can be useful to the wireless service providers who plan to build these networks based on IMS/MMD architecture. We highlight our experience while building a 3GPP2-based architecture. We describe the basic functional components of the testbed and the results of the implementation but focus our discussion on security and mobility optimization issues.

The rest of the article is organized as follows. The next section provides an overview of the IMS/MMD testbed architecture at a functional level. Then we highlight several issues that might affect the optimization of MMD networks. The following section describes the MMD testbed and analyzes three different types of handoff scenarios and associated performance results. Finally, we conclude the article.

MOBILITY MANAGEMENT IN THE MMD ARCHITECTURE

In this section we discuss several physical and functional components of the MMD architecture that form the mobility framework. In a regular CDMA2000 environment, mobility is handled at each level of the network stack. In a data-oriented cellular environment, the mobile node (MN) usually initiates a data call via the base transceiver station (BTS). The base station controller (BSC) responsible for this BTS forwards the call to the associated packet control function (PCF). The PCF selects a packet data serving node (PDSN) based on certain unique characteristics of the MN and establishes a generic routing

Dynamic Host Configuration Protocol servers are configuration agents and help the mobiles with the configuration of network layer identifiers such as IP address, address of P-CSCF, and domain name service (DNS) servers. Each visited network may be equipped with a DHCP server.

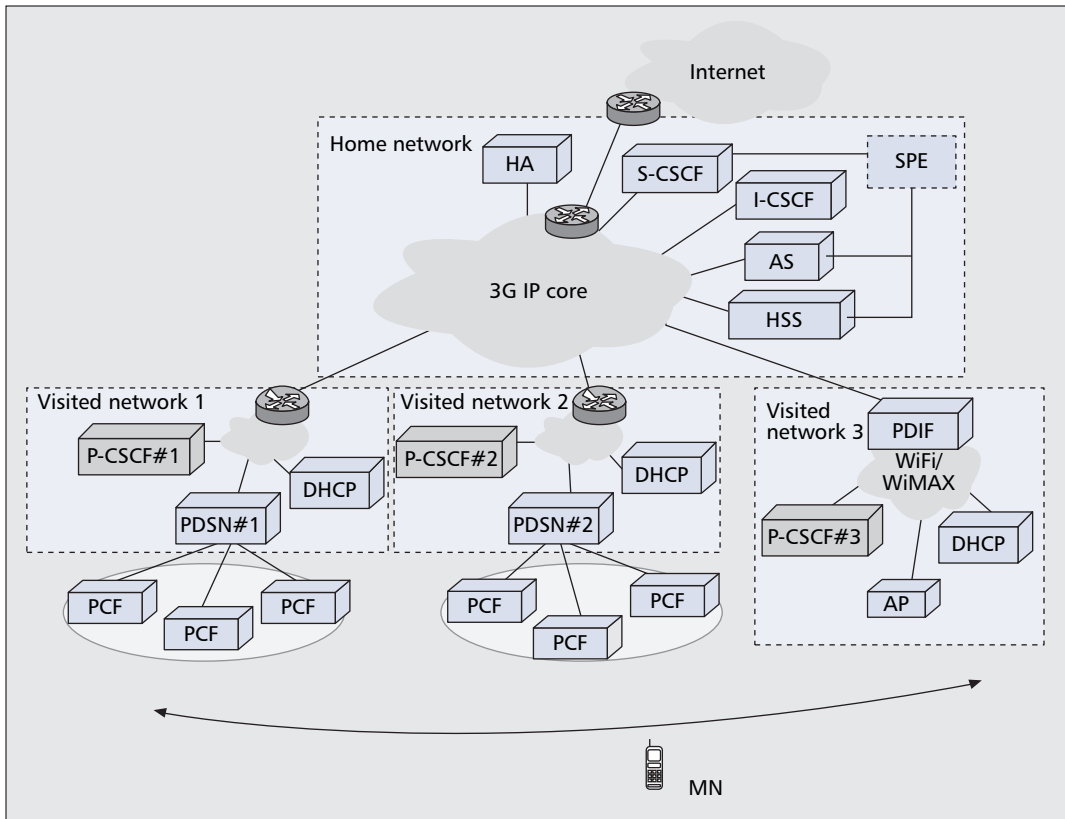


Figure 1. Functional elements of IMS/MMD distributed architecture.

encapsulation (GRE) tunnel with the PDSN [3]. When the mobile moves between two BTS with in one PDSN, a new Point-to-Point Protocol (PPP) session is not warranted. However, if the mobile moves between two BTS that are controlled by two different PCF, each PCF may choose a new PDSN in the hierarchy to terminate the PPP session. Besides these core network elements, MMD architecture uses other functional elements at the network layer and the application layer that handle mobility binding, signaling, security, and quality of service. Mobility at the PDSN layer is handled by network layer mobility such as mobile IP [4, 5], but application layer mobility [6] can be used, as well, without a requirement to install a mobility component in the PDSN. However, we have used Mobile Internet Protocol Version 4 (MIPv4) during the realization of this specific testbed, as many carriers plan to deploy MMD architecture in their already installed MIPv4 networks.

At a functional level, an MMD architecture primarily consists of several signaling entities such as proxy-call session control function (P-CSCF), interrogating-CSCF (I-CSCF), serving-CSCF (S-CSCF), and home subscriber server (HSS) [2]. However, 3GPP2 does not mandate the placement of P-CSCF in any specific part of the network. Thus, an access network provider can place the P-CSCF based on its specific requirement and ease of management. However, placement of P-CSCF may affect the operation of the network in terms of scalability and hand-over optimization. The authors provide a gap analysis of alternate architecture based on placement of P-CSCF in [7].

Here we focus our discussion on an implementation of the 3GPP2 architecture where a P-CSCF is located in each visited sub-network.

Figure 1 shows one such functional architecture where P-CSCF are distributed across the visited networks. In this specific architecture, there are four networks labeled home network, visited network 1, visited network 2, and visited network 3. Two of the networks have CDMA2000 access, and the third network supports either wireless fidelity (WiFi) or WiMAX. A mobile terminal can access its IMS services in any of the visited networks. Roaming service and mobility are supported by a combination of Session Initiation Protocol (SIP) components such as P-CSCF, S-CSCF, I-CSCF, and mobile IP components such as home agent (HA) and foreign agent (FA). We provide a description of some of the functional components.

MN: MN is the mobile node that moves across the networks.

DHCP servers: Dynamic Host Configuration Protocol servers are configuration agents and help the mobiles with the configuration of network layer identifiers such as IP address, address of P-CSCF, and domain name service (DNS) servers. Each visited network may be equipped with a DHCP server.

HA: An HA serves as the anchor point for a mobile in a mobile IP environment and maintains the mapping between the mobile's home address and the new care-of address that the mobile obtains in each network. This care-of address is obtained either from a stateful DHCP server or from a foreign agent or by means of stateless auto-configuration. In a normal case, the signaling and media traverse the HA that

If the mobile performs frequent handoff and changes its P-CSCF at every move, it must re-register and perform MIP update during each move and that may lead to transient data loss. In such situations, it may be advisable to have the P-CSCF closer to the mobile and to perform the discovery quickly.

contributes to the additional delay because of the associated redundant routing path.

S-CSCF: The S-CSCF is the central node of the signaling plane. It is a SIP server, and performs session control functions. It is always located in the home network. It can either query the HSS or the DNS server to locate the appropriate P-CSCF for outgoing intra-domain calls and the appropriate I-CSCF for interdomain calls. The S-CSCF in the testbed is implemented as a back-to-back user agent (B2BUA), with one UA receiving incoming calls and a second UA sending the invitation to the terminating end.

P-CSCF: The P-CSCF behaves as a SIP proxy and is the first outbound proxy for a mobile in the visited network. The P-CSCF routes REGISTER requests to the I-CSCF and caches the S-CSCF address so that it can route the rest of SIP signals directly to the S-CSCF. IMS/MMD architecture mandates that there should be security association between the mobile and P-CSCF.

I-CSCF: The I-CSCF is another SIP proxy that provides forwarding of messages to the correct S-CSCF, through HSS or DNS look-ups. I-CSCF also acts as an entity that hides information for interdomain calls.

HSS: The HSS stores information about the subscribers, their addresses, and their services, such as user account, contact URI of the user, address of P-CSCF for each mobile, E.164 number. The HSS is located in the home network and communicates with the S-CSCF.

Service provisioning environment (SPE): The SPE is collocated with the HSS, but logically it is a separate component. It provides a mechanism to view the services that are deployed on the application server (AS), and system administrators can use it to provision services automatically for each user.

Application server (AS): The AS sends messages to the HSS defining the applications deployed on the AS, along with the parameters required to configure an instance of the service. This description is used by the SPE to generate the system administrators' screens for service configuration and provisioning. The AS also accepts messages from the SPE to configure applications, on a per user basis.

OPTIMIZATION ISSUES FOR MMD NETWORKS

We briefly describe some of the key issues and metrics that must be considered for an optimized operation of the MMD network.

Context transfer and security association: As the first signaling entity, each P-CSCF keeps the state of certain aspects of an ongoing call. This call state includes certain metrics of the ongoing call, such as quality of service (QoS), bandwidth information, and calling data record. However, to maintain the same quality of call in the new network when roaming occurs, the existing call state must be transferred as quickly as possible to the new P-CSCF. Similarly, establishing a security association between the mobile and the new P-CSCF is also required before media can pass. Thus, it is important to devise methodologies that can transfer the call state between the P-CSCF and expedite the security association proactively.

An expedited P-CSCF discovery mechanism can help achieve some of these optimizations.

Number of signaling messages over the air: As the wireless bandwidth is scarce, it is good design practice to use protocols that use the minimum number of message exchanges during the IP address assignment and server discovery. A smaller amount of round-trip time during these message exchanges also helps to reduce the time for server discovery and IP address acquisition.

Number of cache entries per P-CSCF: The number of simultaneous registrations a server can handle depends on the CPU and processing power of the server. The mobility rate affects the number of registrations and caching. Caching also directly relates to the number of call states that a P-CSCF must maintain.

Distance between mobile and HA: When the mobile is using MIPv4 to handle mobility binding, the distance between the mobile and the HA plays an important role. During the normal MIP registration and binding update, transient packets are lost in the absence of any fast-handoff mechanism. In addition, in some cases, an HA being used to discover the P-CSCF address also delays the P-CSCF discovery.

Number of IPsec tunnels for signaling and media traffic: Secure Internet Protocol (IPsec) is one possible way of providing security association for signaling and media traffic. If the authentication and encryption are provided on a hop-by-hop basis, then a new security association must be established every time there is a change in the end-point identifier upon the movement.

Distance between mobile and P-CSCF: Every SIP signaling message to and from the mobile must traverse the P-CSCF, and there is also a security association between the mobile and the P-CSCF. Thus, there is a trade-off between having a P-CSCF closer to the mobile and the number of P-CSCF the mobile must change during its movement.

Interdomain roaming: During interdomain movement, authentication, authorization, and access (AAA) domains may change; and additional signaling between different entities in both the domains may be involved. Thus, additional operations and handoff delays may be included. Optimization issues for interdomain roaming may be required to consider optimized security association, authentication, and context transfer between the P-CSCF. However, we have not implemented interdomain roaming in the current testbed.

Packet-to-mobility ratio: The packet-to-mobility ratio depends upon the number of packets communicated during each movement, mobility rate, and so on. If the mobile performs frequent handoff and changes its P-CSCF at every move, it must re-register and perform MIP update during each move and that may lead to transient data loss. In such situations, it may be advisable to place the P-CSCF closer to the mobile, and to perform the discovery quickly.

TESTBED IMPLEMENTATION AND RESULTS

In this section we describe the testbed that we prototyped according to the target architecture mentioned in Fig. 1. We also present experimen-

The experimental measurement in this specific, realistic test bed highlights the performance bottlenecks of the system and indicates the hand-off actions that may require improvement to provide optimization.

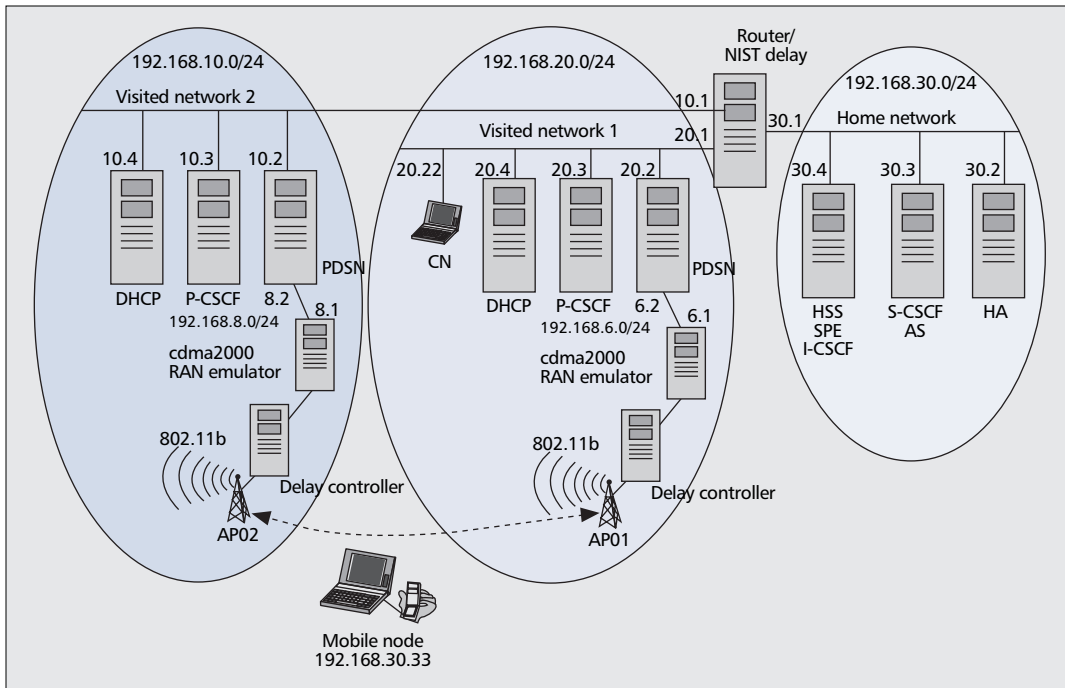


Figure 2. Prototype testbed architecture.

tal results involving three different handoff scenarios. Figure 2 shows the experimental MMD testbed that emulates an MMD architecture.

The current version of the testbed has three networks assumed to be within the carrier domain. The home network emulates the components owned and controlled by the carrier; under the current assumption, users do not roam to their home network during intra-domain movement. In addition, there are also two visited networks that emulate the movement areas of the mobile nodes. The components in these areas may or may not be owned by the same IMS carrier, and could apply to interdomain also.

The home network hosts the HSS, S-CSCF, I-CSCF, and HA. Each of the visited networks hosts the P-CSCF. Furthermore, each visiting network is equipped with a DHCP server that provides the P-CSCF address to the mobile nodes in the corresponding network via the use of a DHCP INFORM message. In the absence of cellular CDMA radio-access network (RAN), we emulated CDMA2000 access over 802.11 networks. The 802.11 access point (AP) in each visited network is connected to a CDMA2000 RAN emulator, and this emulator is connected to a PDSN. The traffic generated from the users of the visiting network goes through the RAN emulator and the PDSN before reaching any of the destinations.

We focus on the measurements and behavior of the IMS system during a mobile handoff. This study provides the required information to understand the details of the system behavior during the users' handoff. This behavior can be characterized by the various functional operations that occur during the handoff and the relative time it takes for each of these operations. The experimental measurement in this specific, realistic testbed highlights the performance bottlenecks of the system and indicates the handoff actions that may require improvement to provide optimization.

The following sections provide the details of the handoff experiments conducted in the testbed.

HANDOFF EXPERIMENTS

User mobility contributes to handoff that results in performance degradation of the communication. We provide our analysis of handoff experiments in the IMS testbed that shows the effect of handoff. We illustrate various functions that occur during handoff and measure the corresponding amount of time it takes for each of these operations. For completeness of the handoff analysis, we implemented three representative handoff modes of operation:

- The non-optimized
- The reactive
- The proactive

Details of each of these mechanisms are provided in subsequent sections. Initially we provide a brief overview of some of the functions that occur during the handoff operation.

Operations during Handoff — Following is a list of operations that are executed during a handoff.

Layer 2 Configuration — Whenever the mobile node connects to a new RAN, it goes through the process of re-establishing its Point-to-Point Protocol over Ethernet (PPPoE) credentials and obtaining its PPP address. Since the current PPPoE access is provided over IEEE 802.11, it also is subject to additional 802.11-related handoff delay due to scanning, authentication, and association.

After the layer 2 association is established, the MN initiates the PPPoE active discovery (PADI). Upon the reception of the PPPoE active-discovery offer (PADO), the MN responds with a PPPoE active-discovery request (PADR) to start the process of selecting the network. This request is acknowledged with a PPPoE active-discovery

The faster re-establishment of security association in the new network and the faster context transfer or context creation helps to open the gate more quickly at PDSN. Faster gate opening at the new PDSN results in reduced hand-off delay and less transient data loss between MN and CN.

session confirmation (PADS). After the discovery of the new network, the MN goes through the user authentication process by using Link Control Protocol (LCP) and Challenge Handshake Authentication Protocol (CHAP) before an access is granted on the PPP link.

Layer 3 Configuration — Part of the MN handoff process is the configuration of several layer 3 parameters, such as a new care-of address, default gateway, and P-CSCF server address. Although the care-of address could be provided by the FA, the DHCP server, or in a stateless manner for IPv6, SIP server configuration parameters are obtained by the corresponding DHCP server in the MN's new network [8]. In the current testbed, the MN broadcasts a DHCP INFORM message to obtain new configuration information, and the DHCP server of the corresponding IMS network responds with a DHCP ACK message that contains the requested information (e.g., P-CSCF IP address).

Mobility Binding — After establishing a new PPPoE access, the MN can either listen to the FA advertisements or can solicit a Mobile IP advertisement for faster detection. Based on MIP advertisements, the MN determines that it is in a different network and registers its new care-of address to the HA. In the current prototype, we are operating in foreign agent-care-of address (FA-CoA) mode, so the IP address of the node does not change, and the traffic will be directed to the MN through the FA.

Session Registration — After the mobility binding and configuration operations have completed, the mobile registers with the S-CSCF by sending a SIP REGISTER request via the newly configured P-CSCF. This message is intercepted by the FA, is encapsulated, and is tunneled to the HA. The HA sends this to the P-CSCF, which handles registering the mobile with S-CSCF via I-CSCF. Trombone routing caused by Mobile IP adds to the additional delay for the completion of the mobile's re-registration. Reverse tunneling between FA and HA forces the SIP signaling destined to P-CSCF to traverse all the way to HA even if the mobile is closer to P-CSCF. In addition, additional encapsulation and decapsulation at HA and FA also contributes to the delay.

Security Association — According to MMD, security association must be established between MN and P-CSCF before any media can pass through the PDSN. Authentication and key agreement (AKA) is a challenge-response-based mechanism that uses symmetric cryptography. By means of AKA, both MN and P-CSCF can establish security association between themselves. However, in the current version of the testbed, we use SIP REGISTER and an out-of-bound protocol to implement an emulation of AKA. This out-of-bound protocol operates between P-CSCF and S-CSCF and obtains the required security key similar to AKA operation.

Session Maintenance — If the MN moves during an active session, maintenance of this session is required. In particular, after the re-registration is complete, the MN retransmits a re-INVITE

message to the correspondent node (CN). The re-INVITE message contains the Session Description Protocol (SDP) description of the active session. In case of mobile IP as the mobility protocol, the INVITE will carry the home IP address in the SDP. However, SDP parameters associated with re-INVITE can be used to create new context. This re-INVITE message also is subject to trombone-routing delay. However, the INVITE operation does not add delay to the media handoff in case of proactive and reactive handoff, because context generation is handled by means of context transfer. Only non-optimized handoff is affected due to re-INVITE operation. We define each of these handoff methods in the following sections.

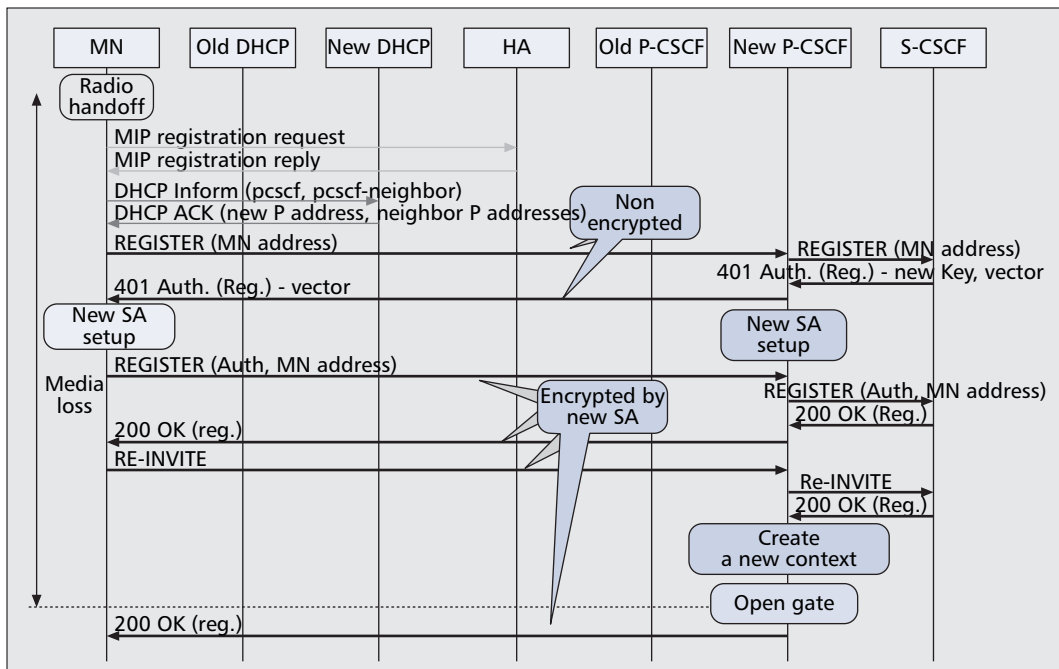
Media Control on PDSN — Establishing a security association between P-CSCF and MN, and context generation by means of new context creation or context transfer from previous P-CSCF are preconditions before the PDSN can allow the media traffic. After the new P-CSCF has a new context and the required security association with the mobile, it opens the firewall gate at the PDSN to allow the media traffic by interacting with the policy and charging rules function (PCRF).

The faster re-establishment of security association in the new network and the faster context transfer or context creation helps to open the gate more quickly at the PDSN. Faster gate opening at the new PDSN results in reduced handoff delay and less transient data loss between MN and CN. We describe the details of three different modes of operation that could be possible in a real deployment scenario.

Non-Optimized Handoff Mode — The most basic handoff mode is the non-optimized mode. This mode incurs the maximum amount of handoff delay. In this mode of operation, a new call context is created every time the mobile moves to the new network. The message flow for the non-optimized operational mode is provided in Fig. 3.

The MN completes all the handoff functions at layer 2 and layer 3 (L2 and L3), as described earlier. Specifically, after the MN establishes PPP access to the new network, it performs the MIP binding functions, and it obtains the new network configuration information via DHCP. Then the SIP-related handoff functions are performed, starting with the SIP re-registration and the security association establishment, using emulated AKA. If the MN moves during an active session, session maintenance is carried out with the transmission of an encrypted SIP re-INVITE message that carries the SDP description of the ongoing session. Upon receipt of this message, P-CSCF creates a new context for the same mobile and instructs the gate at PDSN to open. This results in the resumption of the media in the new access network.

Reactive Handoff Mode — In the reactive mode of operation, all the L2 and L3 operations take place as in the non-optimized mode. The detailed message flow is provided in Fig. 4. By comparing with Fig. 3 (non-optimized mode), the difference between the two handoff operational modes is evident. In particular, the session maintenance information message (e.g., re-INVITE) that carries the SDP description of the active ses-



■ Figure 3. Detailed message flow for the non-optimized handoff mode.

The most optimized hand-off operational mode is the proactive mode. As its name implies, the context creation in the new IMS network and security association with the new P-CSCF occur while the MN is still in the old network.

sion does not play any role in context creation and thus does not affect the media handoff delay. The context created in the P-CSCF in the new visited network is transferred from P-CSCF in the old visited network. The objective of this approach is to reduce the handoff delay by eliminating the dependence on the session maintenance messages (INVITE and 200 OK).

After the radio handoff and the establishment of the PPP access in the new network, MN performs the regular MIP binding and obtains the required configuration information using DHCP. MN initiates a SIP REGISTER message via the new P-CSCF. When this message reaches the S-CSCF, the S-CSCF informs the old P-CSCF to transfer the context of the active session to the new P-CSCF. At this point, the old P-CSCF transfers the context to the new P-CSCF, and the context is created in the new network. After the completion of the SA setup (e.g., AKA) between MN and new P-CSCF, the gate opens at PDSN, and the session resumes.

Proactive Handoff Mode — The most optimized handoff operational mode is the proactive mode. As its name implies, the context creation in the new IMS network and security association with the new P-CSCF occur while the MN is still in the old network. Even though this specific handoff mode provides the smallest media delay, it depends heavily upon the discovery of neighboring P-CSCF ahead of time and the accuracy of its movement profile. The carriers could use information service discovery methods such as IEEE 802.21 [9] or IEEE 802.11u [12] to obtain the information about the neighboring networks. Various techniques, such as signal strength threshold, can be used to determine the precise movement pattern of the mobile.

Figure 5 provides the detailed message flows of proactive handoff. Prior to the MN radio handoff, some of the handoff functions are done proac-

tively in the old network. Specifically, the MN, utilizing the DHCP INFORM, acquires the addresses of P-CSCF from the neighboring IMS networks. In this case, a DHCP server is equipped with the information about the servers in the neighboring domains [8]. After the MN identifies the new neighboring network it is likely to move, it informs its current P-CSCF about the address of its new P-CSCF. The current P-CSCF transfers the context of the active session (e.g., SDP, CDR information) to the new P-CSCF. Similarly, a new security association is established between new P-CSCF and the mobile after the mobile sends a “MoveNotify” message to S-CSCF when the movement is imminent. This proprietary protocol, in some manner performs a proactive AKA operation by transferring the security context from the current P-CSCF to the new P-CSCF ahead of time. The mobile performs regular AKA after it moves to the new network. Thus, the new PDSN opens its gate for this specific mobile’s media even before the mobile has moved. After the mobile re-establishes its connection in the new network, and completes the MIP operation, media starts flowing. The mobile’s SIP-related signaling such as re-REGISTER or re-INVITE do not affect the media handoff delay here.

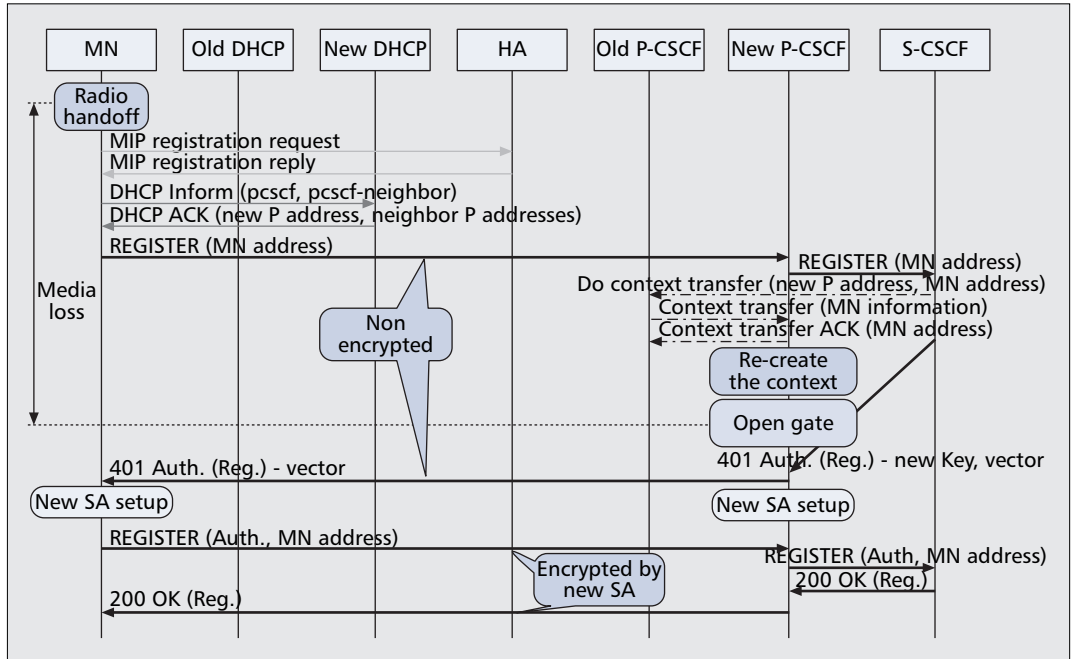
Based on the message flow description, it is obvious that the proactive handoff operational mode is very promising. We compare the results of each handoff operation in the following section.

Performance Results — The focus of this performance analysis is to highlight the relative effectiveness of proactive handoff compared to the other two handoff techniques. In Fig. 6, we plot the delays associated with the different handoff functions that contribute to the overall handoff delay for three different handoff scenarios. On the average, the mobile was subjected to a 3666-ms delay for proactive handoff, a 9685-ms delay for reactive handoff, and a 12,526-ms delay

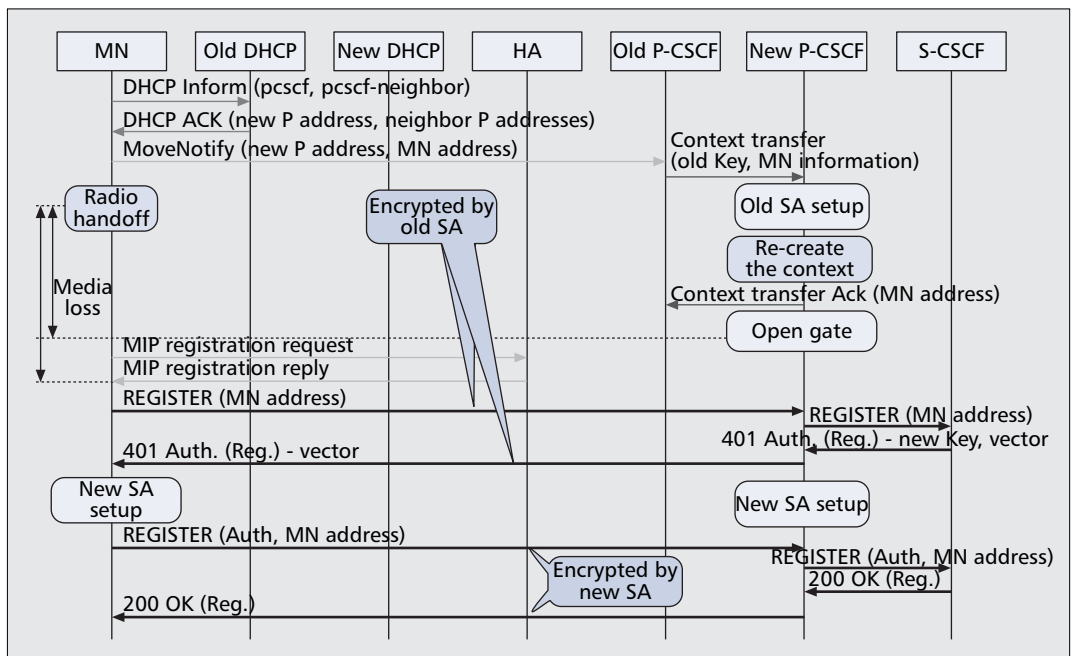
The SIP-related signaling required for context transfer and security association contributes to additional hand-off time for a non-optimized case compared to a reactive case, because it must create the context with an additional re-INVITE signaling.

for non-optimized handoff. The number of packets lost is proportional to the handoff delay and depends on the packet generation rate. The overall handoff delay consists of delays due to different operations such as layer 2 configuration, layer 3 configuration, binding update, registration, security association, and media redirection. As is evident, proactive handoff does not contribute to any delay due to DHCP, context transfer, and SIP-based security association compared to a reactive or non-optimized case. On the other hand, a non-optimized case is subjected to maximum delay due to additional signaling messages during SIP-based security association and the context-creation phase. Layer 2 delay, PPPoE

delay, and MIP binding delay remain more or less the same for all three handoff scenarios. Similarly, in the case of reactive handoff, in addition to layer 2 delay, a major component of the delay came from SIP registration, security association, and context transfer. As we used Mobile IP, these results are inclusive of inherent trombone-routing delays and can further be reduced when the mitigation techniques are applied [11]. A different mobility protocol such as MIPv6 [5] or SIP-based mobility [6] may result in a smaller binding-update delay. The SIP-related signaling required for context transfer and security association contributes to additional handoff time for a non-optimized case compared to a reactive case,



■ Figure 4. Detailed message flow for the reactive handoff mode.



■ Figure 5. Detailed message flow for the proactive handoff mode.

because it must create the context with an additional re-INVITE signaling.

To gain an insight into the role of these optimization techniques in a real deployment scenario, we obtained some additional results. We used a National Institute of Standards & Technology (NIST) delay simulator and varied the emulated distance between the home network and the visited network by introducing delays of 0 ms through 500 ms, with an increment of 50 ms. We provide additional handoff results in Table 1. These results show only the components of the handoff delay that are affected due to additional delay introduced between the home network and the visited network. Since the experimental results indicate a basic trend, we show the second order approximation of the values by taking the values of the trend line. From the analysis, it appears that delays related to layer 2 and layer 3 configuration are not affected because these operations do not involve a home network. Delay due to mobile-IP-binding update increases for all three cases as the emulated distance is increased, but there is an appreciable increase in delay for SIP-security association in the cases of non-optimized and reactive handoff. In the proactive case, the additional series of network delay did not have any effect on the handoff delay component related to SIP, AKA, and context transfer. The additional handoff delay in the proactive case was contributed by the increased MIP-update delay only.

We observed that the MIP-update delay was increased by a round-trip delay. It also is noteworthy to mention that these results were obtained without any trombone-routing mitigation technique. These techniques when applied to reactive

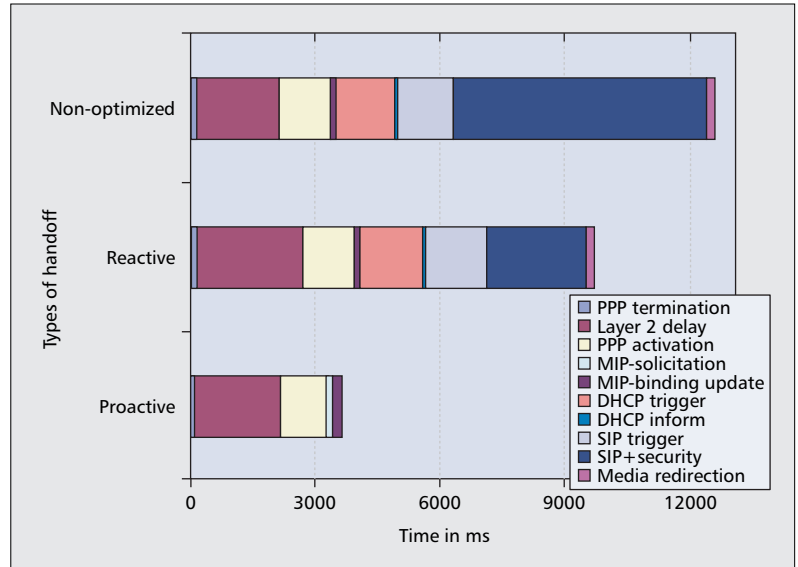


Figure 6. Handoff result analysis for three types of handoff.

and non-optimized handoff methods reduce the handoff delay as well. The authors describe the details of mitigation techniques in [11].

Ideally, an interactive application such as voice-over-IP (VoIP) has a threshold value of one-way delay of up to 150 ms, and a streaming application can withstand a delay of up to 400 ms. The effect of handoff delay could be mitigated by the addition of buffers in the networks, but the buffer value should be designed with the threshold of the one-way delay in mind. Although

Types of handoff	Proactive handoff			Reactive handoff			Non-optimized handoff		
	SIP, AKA, context transfer delay (ms)	MIP update delay (ms)	L2 PPP delay (ms)	SIP, AKA, context transfer delay (ms)	MIP update delay (ms)	L2 PPP delay (ms)	SIP, AKA, context transfer delay (ms)	MIP update delay (ms)	L2 PPP delay (ms)
0	0	51	2736	1010	62	1523	3999	41	2239
50	0	152	2693	1375	161	1744	4584	145	2217
100	0	252	2650	1741	261	1964	5170	248	2194
150	0	352	2607	2107	360	2184	5756	352	2172
200	0	453	2563	2472	459	2405	6342	455	2150
250	0	553	2520	2838	558	2625	6927	559	2128
300	0	654	2477	3203	658	2845	7513	663	2106
350	0	755	2434	3569	757	3066	8099	766	2084
400	0	855	2391	3935	856	3286	8685	870	2061
450	0	956	2347	4300	955	3506	9270	973	2039
500	0	1057	2304	4666	1055	3726	9856	1077	2017

Table 1. Effect of distance between home network and visited network on handoff components.

There are important and complicated issues that should be investigated in terms of how the protocols and functional components interact with each other in an MMD architecture. These are best realized by way of a testbed prototype.

proactive handoff takes the least amount of time, it can be reduced still further by optimizing some of the functional components, such as layer 2 association and PPP activation [3, 10].

Thus, an efficient AKA protocol, faster context transfer, and mitigation of trombone routing can help optimize the handoff operation related to SIP registration and security association. As part of future work, we plan to reduce the proactive handoff delay further by applying optimization techniques to layer 2 and layer 3 configurations.

CONCLUSIONS

Most vendors focus on providing a platform for flexible services but pay little attention to the underlying networking issues. However, there are important and complicated issues that should be investigated in terms of how the protocols and functional components interact with each other in an MMD architecture. These are best realized by way of a testbed prototype. We discussed a specific target architecture for the testbed prototype according to the 3GPP2 MMD specification. In addition to building an MMD-compliant mobility testbed, our contribution includes analysis of different handoff mechanisms and associated functional modules that contribute to the handoff delays. Our testbed can be used as an optimized realistic platform that can provide useful insights into the deployment and evaluation of roaming services. We believe that the details of the implementation and analysis of the handoff results can be beneficial to CDMA2000 wireless service providers and useful to the design and evolution of 3GPP2 networks.

REFERENCES

- [1] 3GPP TS 23.218, "Technical Specification Group Core Network; IP Multimedia Session Handling; IM Call Model."
- [2] 3GPP2 X.S0013-004-0 v2.0, "All-IP Core Network Multimedia Domain: IP Multimedia Call Control Based on SIP and SDP."
- [3] Kagalkar *et al.*, "PPP Migration: A Technique for Low-Latency Handoff in CDMA2000 Networks," *ACM Mobiquitous '05*, San Jose, CA.
- [4] C. Perkins *et al.*, "IP Mobility Support in IPv4," IETF RFC 3344, Aug. 2002.
- [5] D. Johnson *et al.*, "Mobility Support in IPv6," IETF RFC 3775, June 2004.
- [6] E. Wedlund and H. Schulzrinne, "Mobility Support Using SIP," *IEEE/ACM Multimedia Conf.*, Seattle, WA, 1999.
- [7] T. Chiba *et al.*, "Gap Analysis and Architecture Alternatives for 3GPP2 Networks," *IEEE Vehic. Tech.*, Feb. 2007.
- [8] H. Schulzrinne, "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol," IETF RFC 3361, Aug. 2002.
- [9] IEEE P802.21/D05.00, "Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services," contrib. to IEEE 802.21 WG.
- [10] Arunesh Mishra *et al.*, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," *ACM SIGCOMM Comp. Commun. Rev.*, vol. 33, no. 2, Apr. 2003.
- [11] T. Chiba *et al.*, "Trombone Routing Mitigation Techniques for IMS/MMD Networks," *IEEE WCNC '07*, Hong Kong, Mar. 2007.
- [12] IEEE 802.11u Task Group, Interworking with External Networks: <http://grouper.ieee.org/groups/802/11>

BIOGRAPHIES

ASHUTOSH DUTTA [SM] (adutta@research.telcordia.com) received a B.S. in electrical engineering in 1985 in India, an M.S. in computer science in 1989 from the New Jersey Institute of Technology, and is currently pursuing his Ph.D. part-time at Columbia University. He is a senior scientist in the

Telcordia Technologies Internet Network Research Laboratory. Prior to joining Telcordia Technologies, he was the director of Central Research Facilities at Columbia University from 1989 to 1997 and worked as a computer engineer with TaTa from 1985 to 1987. His research interests include session control protocols, streaming multimedia, wireless multicast, and mobile wireless Internet. He serves as Vice-Chair of the IEEE Princeton and Central Jersey section.

KYRIAKOS MANOUSAKIS [M] received with honors his Diploma in electronics and computer engineering from the Technical University of Crete, Chania, Greece in 1998, and his M.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park in 2002 and 2006, respectively. He is currently a senior research scientist in the Mobile Networking Research group of Telcordia Technologies, Piscataway, New Jersey. His research interests include wireless communications, network management, self-configuration, next-generation networks, and routing and security in ad hoc networks. He is the recipient of the Award of Excellence in Telecommunications from Ericsson. Also, he is a multiple-time recipient of the Greek National Scholarship Foundation (IKY) Award and Technical Chamber of Greece Award. He is a member of IEEE Communications, Computer, and Information Theory Societies.

SUBIR DAS [M] is a senior scientist in the Mobile Networking Department, Applied Research, Telcordia Technologies. Prior to joining Telcordia Technologies, he was a faculty member in the Electrical and Electronics Communications Engineering Department, Indian Institute of Technology, Kharagpur. His research interests include mobility management, network security, IP multimedia subsystems, and ad hoc networking. He has more than 40 publications and three U.S. patents to his credit. He is very active in standards organizations and is a leading contributor to various standards. He is a Technical Program Committee member and tutorial speaker for IEEE- and ACM-sponsored international conferences. He is a reviewer of IEEE and ACM journals and magazines.

FUCHUN JOSEPH LIN is a chief scientist in Applied Research, Telcordia Technologies. He received his B.S. and M.S. in computer science from National Chiao-Tung University, Hsinchu, Taiwan, and his Ph.D. in computer science from Ohio State University, Columbus. He has 19 years of experience at Bell Labs and Telcordia Technologies. His current focus at Telcordia is in the areas of service integration and next-generation fixed and mobile networks based on IMS/MMD.

TSUNEHICO CHIBA received his B.E. degree from Hokkaido University in 2000. He began working for KDDI Corporation, Japan, in 2000 and has worked for KDDI R&D Laboratories since 2004. He has four years of experience developing commercial CDMA2000 core networks at KDDI Corporation. He has been working in the field of CDMA2000 access and core networks, IMS/MMD networks, and protocol testing since he moved to KDDI R&D Laboratories. He is a member of IEICE.

HIDETOSHI YOKOTA [M] received B.E., M.E., and Ph.D. degrees from Waseda University, Tokyo, Japan, in 1990, 1992, and 2003, respectively. He joined KDDI R&D Laboratories in 1992. From 1995 to 1996 he was with SRI International, Menlo Park, California, as an international fellow. His current research interests include mobile communications and ad hoc networks. He is a member of IPSJ and IEICE.

AKIRA IDOUE received his B.E and M.E. degrees from Kobe University in 1984 and 1986, respectively, and his Ph.D. degree from the University of Electro-Communications in 2007. Since joining KDD (now KDDI) in 1986, he has worked in the field of network architecture and communication protocols. He is currently a senior manager of the Ubiquitous Networking Laboratory at KDDI R&D Laboratories, Inc. He is a member of IPSJ and IEICE.

HENNING SCHULZBINNE [F] received his Ph.D. from the University of Massachusetts, Amherst. He is currently chair of the Department of Computer Science at Columbia University, New York. His research interests include Internet multimedia systems, ubiquitous computing, mobile systems, quality of service, and performance evaluation. He was a member of the technical staff at AT&T Bell Laboratories, Murray Hill, New Jersey, and an associate department head at GMD-Fokus, Berlin, Germany, before joining the Computer Science and Electrical Engineering Departments at Columbia. He co-developed protocols, such as RTP, RTSP, and SIP, that are now Internet standards, used by almost all Internet telephony and multimedia applications.