An Enhanced Mobility Management Approach for Wireless IP Networks

Jeng-Yueng Chen[1,3], Wen-Shiung Chen[2], Chun-Chuan Yang[1], Yi-Hung Huang[3] and Heng-Te Chu[2,3]
[1]Dept. of Computer Science and Information Engineering, National Chi Nan University, Puli, Nantou, Taiwan
[2]VIPCCL, Dept. of Electrical Engineering, National Chi Nan University, Puli, Nantou, Taiwan
[3]Dept. of Information Networking Technology, Hsiuping Institute of Technology, Dali, Taichung, Taiwan
E-mail: {s2321902, wschen, ccyang}@ncnu.edu.tw

***Abstract*-Mobile IP (MIP) and Mobile IP Route Optimization (MIP-RO) have been proposed to provide mobility management in the Internet. However, the MIP protocol suffers from triangular routing problem. MIP-RO adopts binding cache to avoid the triangular routing problem and provides smoother handoff. It is very difficult to enforce a binding cache upon each node in the entire Internet. Instead, we developed a more efficient handoff scheme, called Mobile Routing Table (MRT) to enable the edge routers to take over the address binding. Nevertheless, we cannot demand all the edge routers to support MRT in the Internet. Therefore, this paper introduces five different schemes which relieve the limitation of the original MRT approach and cut down the triangular routing problem as much as possible. We analyze and compare both the standard MIP and the proposed approaches. The performance results are reported.**

Keywords: Mobile IP, mobility management, handoff

I. INTRODUCTION

Due to the rapid growth of mobile devices, mobile subscribers have outnumbered wired subscribers over recent years. Meanwhile, mobile devices have been becoming more and more powerful, too. Therefore, people widely expect to use wireless devices to easily access Internet, including rich multimedia resources. Such access relies increasingly on IP-based techniques. These trends interest people greatly in seamless connectivity while mobile nodes are accessing Internet and moving around different IP-based networks and systems.

Regarding the mobile networks, the most critical point is to keep track of the locations of mobile devices which may move around different points of attachment. IP mobility works on OSI layer 3 and intends to provide mobile hosts with continuous Internet connectivity when hosts move from their home network to visiting networks. The Mobile IP (MIP) technique is the most common solution for mobile devices to seamlessly hand off over the Internet [1]. Nevertheless, there are still many problems about the MIP, such as triangular routing, tunneling management, the need for a home IP address and a temporary unfixed address, called Care-of-Address (CoA), for each host, and etc.

In the original MIP mechanism, the triangular routing introduces extra transmission delay, packet loss and signaling overhead [2]. Route optimization was proposed by means of using binding update to inform the correspondent node (CN) of the mobile node's current IP address [3]. However, it is very difficult to enforce a binding cache on every node in the entire Internet. Instead, a more efficient handoff scheme, called Mobile Routing Table (MRT) was proposed to avoid the triangular routing problem, which ran on edge routers, e.g., home agent and foreign agent, to optimize the routing path [4]. Similarly, we cannot demand that all the routers in the Internet really support MRT. Therefore, we need a method that can find the appropriate routers that do support MRT. Hence, this paper introduces five new schemes that cooperate with MRT for optimizing routing path, such that triangular routing problem can be cut down as much as possible.

Following the introduction in Section I, the remaining of this article is organized as follows. Section II gives a brief description about MRT scheme. The proposed schemes are described in Section III. Section IV shows problems about the proposed schemes and their enhancement. Section V evaluates the performance about the proposed scheme. Finally, a conclusion is presented in Section VI.

II. THE MRT APPROACH

In the standard MIP, the home agent (HA) maintains an IP address-mapping table that records the mapping relationship between the home addresses of all mobile nodes (MNs and the associated CoAs. In MIP with route optimization, except the table in the HA, each node, which may be either the CN or the MN, must maintain a binding cache in itself that is also used to record the CoA associated with the MN communicating with the node. With this scheme of binding cache, the CN may send the packets directly to the MN, rather than forwarding via the HA.

However, it is impossible to implement a binding cache in all of the nodes within the entire Internet. If we construct an MRT in each mobile agent (including the HA, FA, and router) only, the binding cache in each node may be removed. As a result, any MN may link to any network on the Internet even without a binding cache.

The MRT is actually an extension of the traditional address-mapping table used in the standard MIP for recording the CoAs of the MNs, and maintained by the HA, FA and routers in order to tunnel the packets from the CN to the MN, regardless of how stationary or mobile the CN is. Figure 1 shows the structure of the records in the MRT. Each MRT record consists of four fields: field 1 records the home IP address of the MN, field 2 records the current CoA of the MN, field 3 is the V-Flag, and field 4 records the so-called Last

1-4244-0270-0/06/$20.00 (c)2006 IEEE

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2006 proceedings.

Elapsed Time (LET). The V-Flag is a 1-bit flag that records whether an MN is now in its home network or not. V-Flag="0" indicates that the MN is in home network, while "1" indicates the MN in foreign network. The LET field records the time instant that the last packet past through the agent during a transmission session between the MN and the CN.

Home Address	CoA	V-Flag	LET
163.22.24.210	163.17.78.118	1	2828
163.22.24.172	163.22.24.172	0	2837

Figure. 1. Structure and examples of record in the MRT.

When each upstream packet is going to be sent out through its agent (possibly the HA, FA, or Router), the agent first searches its MRT to learn whether the destination's IP address exists or not. If not, the node with the destination's IP address may be a fixed node or a mobile node newly connected with the node, and thus the packets will be sent via an optimal path by using the IP routing protocol. On the other hand, the packets are sent out to the current CoA of the node, stored in field 2 of the associated record.

The MRT is also useful as the packets are transmitted into the network from the Internet. Intercepting a packet from the Internet, the HA first searches its MRT to learn whether the destination's IP address exists or not. If not, the HA will discard this packet since it judges the IP address wrong. If the destination's address exists in the first field of the HA's MRT, then the HA checks the V-Flag field again. If the V-Flag value is equal to "0," the MN is now in the home network, and the packet is going to send to the MN directly. If the V-Flag value is "1," the MN is in the foreign network now and the HA tunnels the packet to the MN's CoA, and then send an "MRT Update" message to the FA/router to update its MRT.

III. The Proposed Enhanced MRT Schemes

There are two limitations in the original MRT approach: each edge router in the Internet has to support MRT and each HA needs to know all the MRT routers in the networks where CNs are located. We cannot claim that each CN does implement binding cache. Similarly, we also cannot demand that all the routers in the Internet support MRT. Therefore we need a method that can find the appropriate routers that support MRT.

To remove those limitations, we introduce five different schemes that will cooperate with MRT for optimizing routing path. Originally, when HA tunnel packets, received from CN, to MN. If HA can find appropriate MRT routers along the path between HA and CN, HA can use MRT binding update messages to insert the binding information, such that MRT routers can forward the follow-up packets to MN directly. Hence, the triangular routing problem can be resolved. The proposed schemes can aid MRT routers finding. In the following, we describe the five schemes in detail.

A. Scheme 1: Directed Broadcast

The first scheme combines ICMP address mask query and directed broadcast mechanism to find the routers that support MRT [5]. After transmitting the first packet to MN by tunneling, HA sends an ICMP address mask query message to find the network mask of CN. The address mask query is sent to CN network by using the directed broadcast, and will get the configured network mask from the replied message. HA then sends MRT binding message to the subnet of CN via directed broadcast, too. If there is no MRT acknowledgement received within limited time, there is no any MRT router within the network. The broadcast boundary has to enlarge. HA repeatedly extends netmask and sends MRT binding message again till reaches the IP classful default netmask. This approach can find the possible routers that support MRT within network boundary of CN. If there is no MRT router in this region, the process may fail and the packets are still transmitted by tunneling at HA.

B. Scheme 2: Router Discovery

Instead of ICMP address mask query, this scheme uses the ICMP router discovery message to find the routers that may support MRT. The ICMP router discovery messages are called "Router Advertisements" and "Router Solicitations." Each router periodically multicasts router advertisements via each of its multicast interfaces, to announce the IP address(es) of that interface. HA first sends the ICMP router solicitation message to the CN network. After receiving ICMP router advertisement message, HA can find the default router of CN. HA then sends MRT binding message to the router. If there is no MRT acknowledgement received within limited time, HA uses SNMP query messages and combines with Reverse Path Forwarding (RPF) mechanism to find related routers that connected with default router of CN. HA then sends MRT binding messages to the possible routers. This approach can find the possible routers that support MRT in the path from CN to HA. If there is no MRT router located on this path, the process may fail and the packets are still transmitted by tunneling at HA.

C. Scheme 3: MRT Tracking

The third scheme uses the tracking mechanism, similar to traceroute, to find all the MRT routers on the path from HA to CN. This scheme can find the most appropriate MRT router which can provide optimal delivery path. Traceroute utilities work by sending packets with low time-to-live (TTL) fields in the IP packet. The TTL value specifies how many hops the packet is allowed before it is returned. When a packet can't reach its destination because the TTL value is too low, the last router returns the ICMP time exceeded message and identifies itself. By sending a series of packets and incrementing the TTL value with each successive packet, it finds out all the intermediate routers. In this approach, HA sends MRT binding update message to CN with TTL=1. If HA receives an ICMP Time exceeded message, the message must come from an intermediate router. HA then sends MRT binding update message destined to intermediate router. If HA receives an MRT acknowledgement, the message must come from the intermediate router that supports MRT, and the packet transmitted from CN will be transferred to MN directly at the MRT router. HA then sends MRT binding update message to CN and increases the TTL by 1. The iteration will stop when MRT binding update reach the CN. Finally, All the MRT routers in the path from HA to CN update the MRT tables. All of the

MRT routers can forward the follow-up packets to MN directly. Hence, the triangular routing problem can be resolved.

D. *Scheme 4: ICMP Echo*

In the ICMP echo mechanism, the sender can issue a request packet which can carry any information in the payload. The receiver just sends back a reply packet with the same payload. Therefore, we may put MRT binding information into the payload of an echo request packet. The MRT-aware routers will check the payload of ICMP echo reply message and update its binding table. The MRT-aware router forwards the echo reply packet back to the MN directly and the same packet to the HA. Figure 2 shows the operation flow of this scheme.

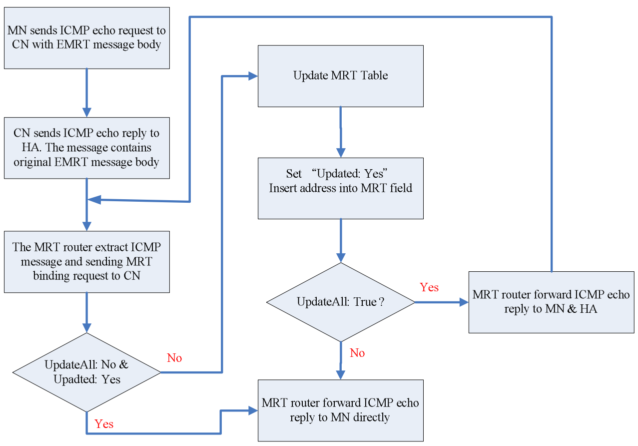

Figure 2. Flowchart of the ICMP echo-based scheme.

In this scheme, signaling for mobility management is accomplished by the exchanges of ICMP echo messages between the MNs and the MRT-aware routers. The payload of ICMP echo request and reply messages are specified by means of text-based message similar to SIP [6]. Figure 3 (a) shows an example of playload of ICMP echo request.

MRTBinding MRT/1.0 IPversion: 4 From: 163.17.2.1 To: 140.134.3.1 CoA: 163.22.24.22 FAA: 163.22.24.1 MRT: 0.0.0.0 UpdateAll: Yes Updated: 0	200 OK MRT/1.0 IPversion: 4 From: 163.17.2.1 To: 140.134.3.1 CoA: 163.22.24.22 FAA: 163.22.24.1 MRT: 140.128.247.254 UpdateAll: Yes Updated: 2
(a) Echo request	(b) Echo reply

Figure 3. An example of payload of echo request/reply messages.

It starts with "MRTBinding" used for the MRT-aware router to quickly identify the packet. The protocol is named as MRT with the current version being 1.0. The second line in the example shows that the address binding is IP version 4 address. "From" and "To" headers show the addresses of MN and CN, respectively. The "CoA" header keeps the current CoA of MN and the FAA keeps the current address of FA which the MN is using. The most important header is "MRT" that the MRT-aware router will insert its address into this header. The optional "UpdateAll" header is used when the MN tries to update all the MRT-aware routers along the path. When the value of "UpdateAll" of the header is "Yes," the MRT-aware router has to send the same echo reply packet to the HA as well as to the MN. Otherwise, it just sends the echo reply packet back to the MN. The "Updated" field of the header is used to store the number of MRT-aware routers found. Each MRT-aware router will increase the value by 1 before forwarding. Figure 3 (b) shows an example of playload of ICMP echo reply. It starts with "200 OK," and "MRT" and "Updated" headers have been modified by the MRT-aware routers.

E. *Scheme 5: Destinatiion Unreachable*

When a host or router can not deliver a datagram, the datagram is discarded, and the host or router sends a destination unreachable message back to the source host. The code field for this message specifies the reason for discarding the datagram. In this scheme, the MN first sends a MRT binding packet to CN with a special unused port number. CN will issue an ICMP destination unreachable message back to MN with the code equal to 3 since CN does not listen to that port number. When the MRT-aware routers receive ICMP destination unreachable message with the code equal to 3, they will issue an MRT binding request to MN and update their binding tables.

Figure 4 illustrates the transmission flow of the proposed scheme 1-3 approaches:

❶ Since CN only knows the home address of MN, it will send all the packets to HA.
❷ HA checks its binding information and tunnels those packets to MN.
❸ After transmits the first packet to MN by tunneling, HA uses one of the proposed schemes to find the appropriate MRT routers. HA uses MRT update message to insert the binding record to MRT table of the router.
❹ MRT router then can forward the follow-up packets to MN directly.

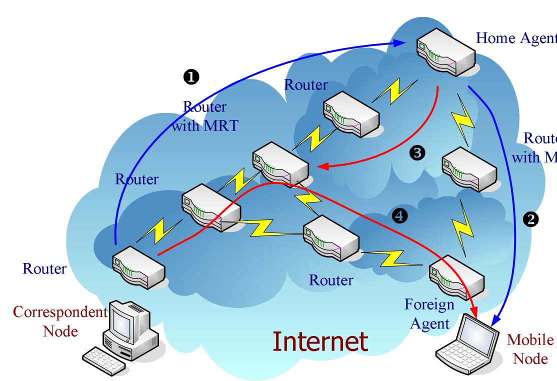

Figure 4. The proposed architecture of Mobile IP with MRT.

IV. Problem and Enhancement

This section shows some problems about the proposed schemes. The enhanced considerations are also covered.

A. Packet blocked by router

All the proposed five schemes use ICMP protocol to discover MRT-aware routers. Scheme 1 and 2 start the searching procedure with directed broadcast messages. Many routers may block directed broadcast messages to avoid DoS or DDoS attacks by default [7]. Thus, scheme 1 and 2 may not work as expected. Besides, enterprises may block ICMP echo messages for security concern. Hence, scheme 4 may not work well without ICMP echo messages. However, the traffic of traceroute-like method used by scheme 3 does not be blocked by routers; but it generates too much unused traffic that may decrease the transmission performance. Generally, ICMP destination unreachable messages are not filtered out by router. Scheme 5 should work well most likely.

B. Signaling Overhead

The first three proposed schemes are triggered by HA and may generate too many control messages. By contrast, the echo-based approach has the MN issues only one single ICMP echo request packet. If the value of "UpdateAll" header is "Yes," the MN will receive n+1 echo reply messages if there are n MRT-aware routers along the path. Otherwise, the MN receives only one echo reply message. The signaling overhead of the 4th proposed scheme is very low. Scheme 5 also needs few control messages. Moreover, the macro domain handoffs happen infrequently. It seems that these control messages are unlikely to impose serious overhead to the involved domains.

C. Handoff Operation

In original MRT approach, the binding cache is aged by LET and updated by MRT binding message. When the MN moves and changes its CoA, the MRT router has to update binding information to keep the accuracy of the MRT binding information. In order to trigger the MRT routers for modifying their binding information, we have to store the addresses of related MRT routers. Two nodes may be used to keep those addresses: HA and MN. Due to the address table size concern, using MN to maintain the address table is better then HA.

For scheme 1-3, we extend the original MRT mechanism by adding new messages sent by the HA to inform the MN of the addresses of related MRT routers after the HA finds them. The MN uses the table to store the addresses of MRT routers. For scheme 4, when the CN sends the echo reply message back to the MN, each intermediate MRT router appends its own address to the MRT header and forwards to the MN. The MN also uses a table to record addresses of MRT routers. For scheme 5, MRT-aware routers issue MRT binding request messages. After replying MRT binding response message, the MN also uses a table to keep addresses of MRT routers

Once the MN moves and changes its CoA, the MN sends the MRT binding update messages to the HA and all the related MRT routers simultaneously. Therefore, the MRT routers can quickly forward the following packets to the new CoA accurately.

In scheme 4, if the echo reply packet gets lost, the MN will never know the existence of MRT router. When the MN changes its point of attachment, it will not send new binding message to that MRT router. Therefore, there will be an address inconsistency problem. To resolve this problem, an "MRTupdate" field is added to the header in order to control whether an MRT-aware router needs to update its MRT table or not. If the value of "MRTupdate" is "No," the MRT router just inserts its address to the echo reply message and sends back to the MN. The MN will issue the reliable MRT binding update messages to those MRT routers.

D. Dynamic Routing

Most of the mobility management protocols, such as MIP and MIP-RO, assume that the propagation delay between the MN and the CN is faster then the triangular approach (CN→ HA → MN). However, this is not always true [8]. The end-to-end delay does not correlated with the distance relationship certainly. In this case, the MN can simply issue an echo request packet with the payload including "UpdateAll: Yes" and "MRTupdate: No" headers. The MN can update the selected MRT router which has the smallest end-to-end propagation delay based on the sequence of echo reply messages that the MN received.

Actually, the routing operation in the Internet is dynamic. Datagrams may be sent through different paths. The "UpdateAll: Yes" header can update all the MRT routers within the path from the CN to the HA. This can reduce the chance that packets of a CN detour, bypass all the MRT routers, and then reach the HA anyway. The HA will send those packets to the MN by tunneling as usual. However, the MN will receive out-of-order packets.

V. Performance Evaluation

We explore the transmission performance of MIP, MIP-RO and MRT-based schemes in this section. The topology of simulation contains 100*100 macro domains. Each macro domain may stand for a business enterprise or an autonomous system that may contain different networking facilities. The macro domain $D_{i,j}$ has a direct connection to $D_{i-1,j}$, $D_{i+1,j}$, $D_{i,j-1}$, and $D_{i,j+1}$, respectively, when $i > 1$ and $j > 1$. The new proposed approach is used to reduce the triangular routing and improve the performance of original MIP. Therefore, we just focus on the handoff among macro domains.

At first, we compare the transmission hop counts or distances among the different methods, including MIP, MIP-RO, and MRT-based approaches, to evaluate the improvement of MRT-based approach. In this scenario, we randomly select three macro domains where MN, CN, and HA locate. We set the probability that routers support MRT to be the value between 10% and 90%. The simulation executes 1,000 times and calculates the average hop-counts for each MIP, MIP-RO, and MRT approaches, combined with different selected probability. Figure 5 shows the simulation result.

We first observe a significant reduction of hop counts with MRT-based approach. When the probability that routers support MRT is small, the average hop count of MRT-based approach lies in between MIP and MIP-RO. We can see that the average hop count of MRT-based approach is close to MIP-RO approach when the probability that routers support MRT increases. It is clear that the performance of MRT approach is close to the MIP in the worst case, and is close to the MIP-RO in the best case.

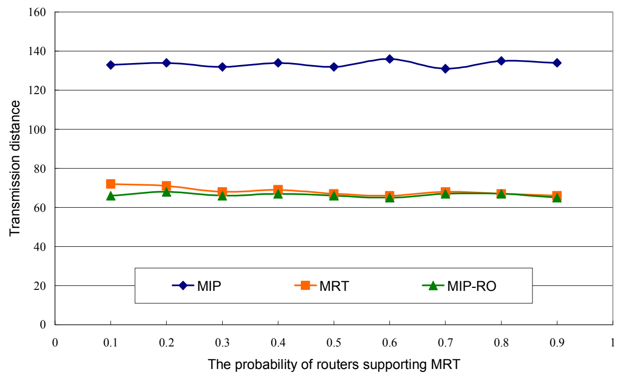

Figure 5. Comparison based on the transmission hop count.

As mentioned above, the end-to-end delay does not correlate with the distance relationship certainly. The most popular interior gateway routing protocol is RIP and the external gateway routing protocol is BGP. RIP is a distance vector routing technique that only uses hop count as routing metric. Distance vector is not a good routing approach because there are occasions in which the route with the smallest hop count is not the preferred route. BGP is a path vector routing technique which maintain its routing table based on the policy imposed on the router by the administrator. Therefore, both RIP and BGP may not send packets using optimal path. Figure 6 shows that transmission costs of MRT-based approaches decrease when the probability of routers supporting MRT increases. It is worth to note that we do not use shortest path routing algorithm in this case. Therefore, the MIP-RO may not send packets through the path at minimum cost. The average cost of the proposed scheme 4 or 5 is lower than the MIP-RO due to the fact that the MN will only update the MRT router with smallest cost.

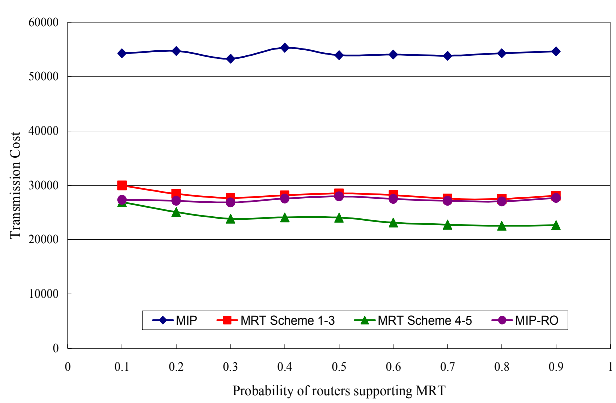

Figure 6. Comparison based on the transmission cost.

Figure 7 shows the additional signaling overhead generated by proposed schemes. For scheme 4 and 5, it seems that these control messages are unlikely to impose serious overhead to the involved domains. Moreover, the proposed schemes are executed only once for each CN.

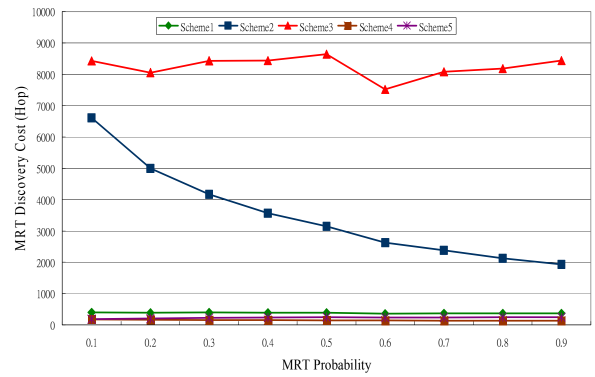

Figure 7. Additional MRT signaling overhead

VI. CONCLUSION

Mobile IP with MRT approach is a useful scheme to avoid the triangular routing problem and remove the need for binding cache for each CN. This paper illustrates an enhanced MRT approach suitable for mobile wireless environment. Five new enhanced schemes are proposed to cooperate with the MRT to remove all the limitations of original MRT approach. Under the proposed architecture, the advantage is that the CN is not required to support any mobility management protocol. The proposed method still can work well even only few routers supporting MRT. In this approach, only MNs and MRT-aware routers are required to support mobility management. Therefore, the deployment of the system becomes easier.

REFERENCES

[1] C. Perkins, “IP mobility support for IPv4,” *RFC 3344*, Aug. 2002.

[2] Y. -H. Hwang, J. -Y. Chen, C. -C. Yang, and W. -S. Chen, "A Comparison between SIP and Network Layer Mobility Management Protocols in Wireless IP Networks," *Proceedings of Fifth IEE International Conference on 3G Mobile Communication Technologies (3G 2004)*, pp. 317-321, London, UK, Oct. 2004.

[3] D. Johnson and C. Perkins, “Route optimization in mobile IP,” *draft-ietf-mobileip-optim-11.txt*, Setp. 2001.

[4] I.-W. Wu, W.-S. Chen, H.-E. Liao and F.-R. Young, “A seamless handoff approach of mobile IP protocol for mobile wireless data networks,” *IEEE Trans. on Consumer Electronics*, vol. 48, No. 2, pp. 335-344, May 2002.

[5] J. Postel, “Internet control message protocol,” *RFC 792*, Sep. 1981.

[6] J. Rosenberg, H. Schulzrinne, G. Camarillo, et. al, “SIP: Session Initiation Protocol,” *RFC 3261*, Jun. 2002.

[7] Cisco Systems, “Improving security on Cisco routers,” *http://www.cisco.com/warp/public/707/21.pdf.*

[8] Q. Wang; M. Abu-Rgheff, and A. Akram, “Design and evaluation of an integrated mobile IP and SIP framework for advanced handoff management,” *2004 Proceeding of International Conference on Communications (ICC 2004)*, vol. 7, pp. 3921-3925, Jun. 2004.