Optimization Routing and Security Features for Transparent Mobile IP

Alessandra Giovanardi, Gianluca Mazzini
University of Ferrara, Via Saragat 1, 44100 Ferrara, Italy
and CSITE CNR/DEIS, Viale Risorgimento 2, 40136 Bologna, Italy
E-mail: {a.giovanardi,g.mazzini}@ieee.org

Abstract—**By considering the problem of transparently link mobile hosts (MH), i.e., without reconfigurations and host software modifications, this paper gives a possible solution and the relative details on implementation. Even if the communications between MH to fixed hosts (FH) have just been investigated, the main topic of this work concerns those of MH versus MH (MH-to-MH). The transparent implementation is based on the introduction of network agents with proxy, tunneling and signaling functions that have been changing and improving in order to optimize MH-to-MH links by means of suitable notification procedures. In order to avoid intruders and unauthorized users, or those who should acquire privileges or perform dangerous procedures, security features based on an authentication strategy and a secure hash algorithm have been implemented. The system has been designed, realized and tested in an actual environment, by verifying that the average performance of MH-to-MH optimized links are closer to those of FH-to-FH.**

I. Introduction

In recent years Internet has exponentially grown in terms of quality, services, developing tools and number of users. The necessity of accessing everywhere and the fall in the cost of electronic devices have increased the circulation of portable computers with the consequent growth of users requiring a mobile access. Success in mobility requires that no reconfigurations be performed and no privileges or access capabilities be lost by the user.

Recently, many works have been devoted to mobile computing for both wired and wireless networks [1] [2] [3] [4]. The main features of a mobile protocol are the following [5]: MH should not change the IP address; the software support should be developed at the network layer; a two address levels scheme (one which identifies the terminal and one binding to the mobility) should be utilized; mobile agents distributed on the networks to support mobiles management should be introduced; and security mechanisms should be included. Furthermore, basic functions of the network agents include: maintenance and management of an association scheme between the two address levels; MH traffic re-routing through redirection or tunneling procedures; exchange of authentication, registration and signaling messages; routing optimization. Furthermore, an efficient mobility support should be characterized by: user **transparency** both for the operative and performance point of view; compatibility with existent networks; simplicity, to keep the traffic overhead low; and scalability, to permit the growth of the system. Some implementations have been proposed by IETF regarding the IP version 4 and 6 and the management of network with firewalls [5].

As far as the MH **transparency** is concerned, in this paper and in [6], the concept described above is enlarged from the user to the terminal point of view, so that no change in the operating system or configuration parameters is required. Hence, all the intelligence of the system to support the mobility is on the mobile agents. As described in the following, all basic characteristics cited above are taken into account in the system implementation, which are based on a simple scheme, easy to export and without limits on the number of mobile hosts to manage. In order to guarantee a general routing optimization for each kind of communication considered, i.e. for MH-to-MH and MH-to-FH links, three kind of mobile agents have been introduced, in each possible network configurations and hosts locations: a Visitor Agent (VA) on each Foreign Networks (FNs), a Home Agent (HA) on each Home Networks (HNs) and an Extern Agent (EA) on each Extern Networks (ENs) [6].

In the following the attention is focused on a new signaling scheme between the mobile agents created to optimize the MH-to-MH links routing by extending the agents' functions already described in [6]. Great efforts have been made to implement security features [7], by considering both an authentication phase and a cryptographic algorithm. The former is controlled by the HA, the HN agent which, by means of a suitable procedure, knows all its potential MHs and can verify the correctness of the system access; the latter is used to hide important information, like IP and MAC addresses exchanged by the agents in the registration phase in order to avoid possible intruders from listening.

The association scheme between the two address levels is found on a server, named Extern Home Agent Server ($EHAS$) [6], which maintains and manages the information to identify the HA on the HN (giving the IP address of the MH) and the EA on the EN (giving the IP address of a host involved in communications with MH).

The paper is organized as follows: section II describes basic functions of the mobile agents, section III presents topics about MH-to-MH links optimization, section IV discusses on the security problem, section V gives some details about system implementation and section VI shows networks configurations and test field experiments. Finally, in sections VII some conclusions are made.

II. Basic Mobile Agents Functions

As in [6], let us summarize the main functional procedures of the system by focusing attention on the MH-to-FH communications and on the agents' role. By referring to the scenario of Fig. 1 three different kind of agents (VA, HA and EA) have to be described; their general functions include: network monitoring to achieve the

0-7803-4984-9/98/$10.00 ©1998 IEEE.

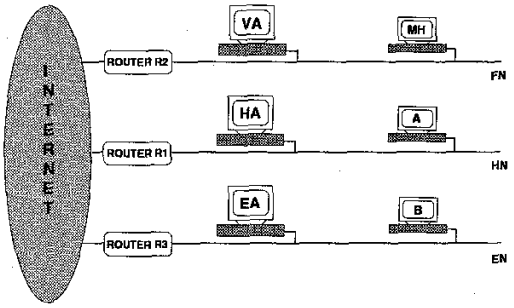

Fig. 1. General network configuration

proxy ARP functions in order to capture packets generated from or addressed to MH for correct delivery; localization, to identify the MH position [8]; mobility informations maintenance (such as IP and MAC addresses, timeouts, etc.); signaling, tunneling and routing management, working directly at the IP protocol layer. All three agents are integrated on the same server and have, built-in, a list (Allowed Address List) to achieve multiple logical subnetworks on the same physical structure, whose elements are: IP Address, Netmask and IP Router Address.

The VA should capture the ARP request not-intrinsic at the FN by monitoring actions and by referring to the Allowed Address List; it thus performs the relative ARP reply so that all the MH generated packets are directed to it. Then, the VA delivers directly the packets to the FH, i.e. B on the EN, by following the usual routing paths (forwarding). The described routing is called *forward path.*

The optimized *reverse path*, from a B FH on EN to the MH, should be obtained by means of the EA. By assuming that the EA knows the IP addresses of the target MH and of the source B FH, it publishes itself as the EN default router for B. This procedure is achieved by means of an ARP reply to B without requests, called *Gratuitous ARP*. All B packets are captured by the EA that sends them either to the router, if they are not addressed to the MH, or to the VA for finally delivery to MH, via a tunneling action.

The MH location is collected by the HA on the HN, which also allows the *reverse path* when the EA is not present on the EN by building a non-optimized path that involves sequentially EN, HN and FN. In this case the B packets are routed on the HN (where the MH should be), where the HA proxy feature makes it possible to capture and send them to VA on FN, through a tunneling procedure. Whenever the *reverse path* is not optimum the routing is called *pseudo-triangular*, due to the direct and triangular delivery of forward and *reverse paths*, respectively.

The IP addresses of all MHs and of their relative VAs should be known by the HA. The same information added to IP addresses of all EN FHs involved with MH communications should be known by the EA. These settings are driven by the VA in the initialization phase through an identification and a registration procedure. The identification phase is used by the VA to know the HA and EA IP addresses and it is achieved by querying the $EHAS$ which manages a list with IP network, Netmask and IP $\{HA, EA\}$ entries. The registration phase is based on a developed protocol at the IP level. Regarding the HA, VA notifies the MHs IP addresses that are inserted with the VA IP address into the HA cache, then HA replies with the registration acceptance. This registration is periodically repeated. Before starting with MH packets transmissions, the VA waits for the end of the HA initialization phase in order to achieve security and reliability, by forbidding all MH communications if, after several retries, it fails. Regarding with the EA, VA notifies MHs and EN FHs IP addresses that are inserted with the VA IP address into the EA cache. Due to the possibility of using the *pseudo-triangular path,* no reply from EA is requested. The VA maintains all useful informations regarding with MHs.

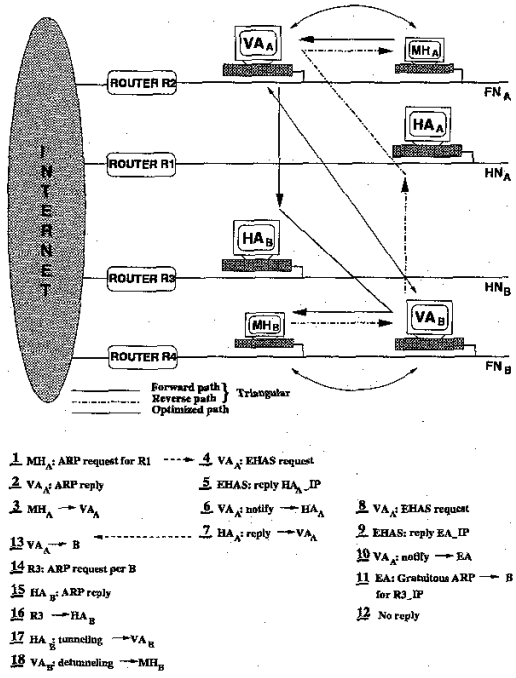

Fig. 2. Non-optimized MH-to-MH communications

III. MH-to-MH Optimizations

In the basic system implementation described above, triangular paths are not only present in the reverse path without EA, but also in all MH-to-MH communications. Let us consider Fig. 2 with two MHs, labeled MH_A and MH_B. When the MH_A sends packets to the MH_B, these are captured by the VA_A which forwards them to the MH_B on HN_B. Due to the absence of MH_B on HN_B, the HA_B captures these packets and tunnels them to the VA_B. During this process, VA_A attempts setting up the $EA = HA_B$ on HN_B without success. The path results triangular and the reverse one is specular.

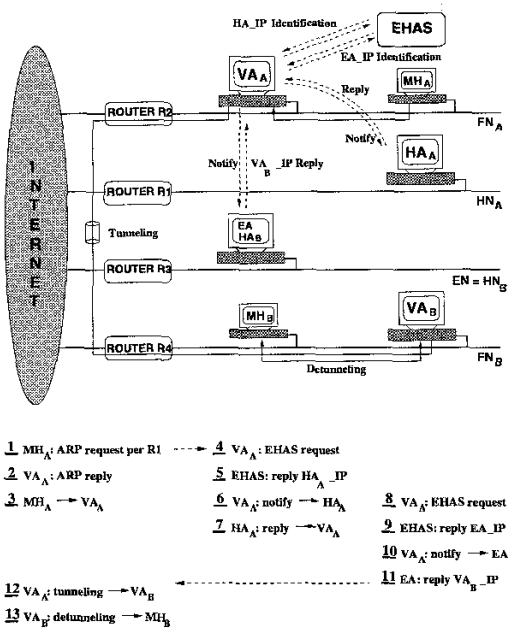

Fig. 3. Optimized MH-to-MH communications

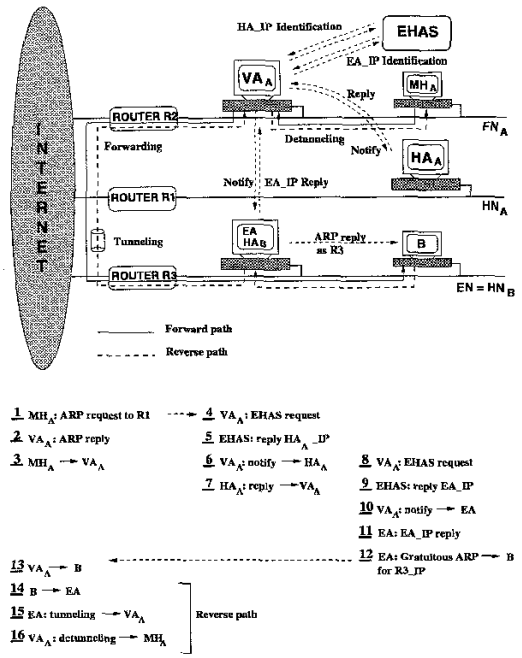

Fig. 4. Optimized MH-to-FH communications

This problem is a consequence of constantly applied direct forwarding where a tunneling action, from VA_A to VA_B, will be able to avoid the intermediate step in the path. To organize this tunneling, VA_A must have the knowledge of the MH_B location, given by a notify and reply procedure addressed to the HA_B, and obtained by modifying and completing the previously described EA notification. This modified registration process is always performed, given that it is not known if the target is a MH or a FH, and tunneling or forwarding actions are selected as a function of the host type. Let us observe that this methodology is the chief idea to achieve optimization in MH-to-MH communications.

In particular, when the VA_A makes a notification to the EA the reply contains an IP address which is relative to the VA_B if MH_B is moving from HN_B or to the EA if MH_B is on the HN_B. These two cases are detailed in Figs. 3 and 4. The VA_A decision action is based on the comparison between the received IP address and the EA one: if the reply matches, the target is a FH and the forwarding is adopted; otherwise, the target is a MH and the tunneling is performed.

Regarding the MH_A packet transmission, the VA_A waits for the end of the EA initialization phase in order to achieve the correct target localization by deciding for a fixed target if the procedure fails. Let us remember that in the approach discussed in section II there is not answer by EA, then packets are sent immediately.

Some particular cases due to FHs and MHs distributions on the networks, such as that of MH_A and MH_B on the same FN, have been considered and included in the implementation, even if they are not discussed in detail here. Finally, let us observe that, when an MH returns on HN, the relative HA verifies this condition and stops all relative MH mobility actions on itself and on the VA through a proper message of status updating. A similar updating is also performed by the HA when it receives, for the same MH, a registration from a new VA.

IV. Security

The proposed mobility system has some security holes due to the routing modification with respect to the classical one and to the use of non-certified agents. In the following security is addressed to avoid the traffic interception, diversion and not permitted production. However, no actions have been planned to neglect information damage and interference, which is a traditional problem of IP version 4 [9]. Moreover, let us assume the considered networks with authorized agents to be locally secure.

Two possible attacks have to be expected [7]: intrusion of MHs not authorized with invalid IP addresses; duplication of agents' functions with respect to signaling communications. In order to acquire security five different levels have been introduced and described in the following.

First level: in order to avoid the MH duplication, the VA-HA registration, in section II and III based on the MH IP address, is integrated with the MAC one. Let us observe that the MAC address is fixed on the network board and difficult to be modified. The HA must have knowledge of all possible couples of IP-MAC addresses through the management of an ARP security cache automatically built by the HN monitoring or via a hand-made insertion. If the VA registration does not match the HA cache informations, the reply informs the VA of the iden-

tification failure in order to avoid registration procedure retries.

Second level: by assuming that the MAC could be captured and modified, the following cryptographic algorithm has been introduced. By means of a one-way hash function [10] the MAC is encrypted by the VA and sent with the notification packet to the HA; the HA extracts the MH IP address and finds on the ARP security cache the associated MAC address; it then computes the relative hash function and compares it with the received one in order to decide on the identification.

Third level: to neglect the agents duplication the signaling messages must be authenticated by means of a digital signature procedure. A *secret key*, common to all agents, has been introduced and sent in all service packets, by using a one-way hash function. This is encrypted in conjunction with a piece of the message and the authenticity is verified by the target agent through the encryption of the local key with the received message. Let us observe that in VA-HA notifications the MAC is also used to generate the hash values. Inserting a piece of the message avoids the capture and the reuse of the encrypted *secret key*. Finally, the *secret key* distribution mechanism is not actually automatic.

Fourth level: the capture and retransmission of integral packets, with relative interference with usual agents actions, has been neglected through a replay protection base on a *timestamp*. In each signaling message is inserted, both encrypted and not, the transmission starting time; the target agent locally generates an encrypted string and accepts the packet if the matching is verified and if the difference between the transmission starting time and the actual time falls inside a given window. This window is selected on the basis of the averaged round trip time. This technique requires a time basis common to all agents, obtained by synchronizing them with the RFC 1305 NTP protocol.

Fifth level: some data fields in the signaling messages should be modified by compromising the agents functions, but this is avoided by the third level procedure when the complete signaling message is encrypted instead of a piece of it. This message digest approach has been adopted.

V. System Implementation

The agents communications are based on packets, sent at the IP level, by defining the service 37 [6], that has a constant length payload, structured in four 32-bits field: $TYPE$, IP_A, IP_B and $TIMEOUT$. $TYPE$ identifies the kind of communications, which always involve the VA, in the set of: *request to EHAS for HA, EHAS reply for HA, notification to HA, HA reply, request to EHAS for EA, EHAS reply for EA, notification to EA, EA reply, no reply from EHAS, HA update for VA*. IP_A is set to the MH IP address, while IP_B contains a variable IP address depending on the $TYPE$ field. $TIMEOUT$ gives a timeout value, where necessary, fixed in the initialization phase by the VA (VA driven approach) and sent to HA and EA. This field, where not used, is available for further developments. A $TYPE$ value is reserved for tunneling and in this case all other fields are not present.

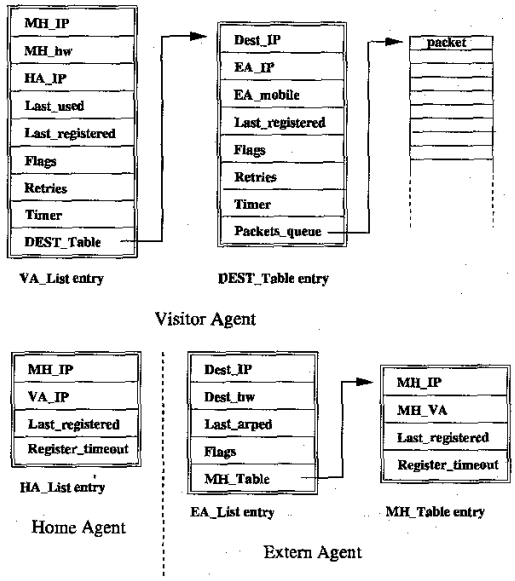

Fig. 5. Agents information organization

The agents information organization, shown in Fig. 5, is described in the following. By considering the VA: MH_IP is the MH IP address; MH_hw is the MH MAC address; HA_IP is the HA IP address relative to the MH; $Last\_used$ is the last time in which this entry has been used, refreshed by each MH incoming packet; $Last\_registered$ is the last time of the VA-HA registration process; $Flags$ identifies the registration status, $Retries$ counts the attempts number of registration for HA, due to the not reachability of the HA or of the $EHAS$, upper limited to the $TO\_resolve\_HA$ time; $Timer$ maintains the timeout status for the HA registration by forcing a new procedure when $TO\_resolve\_HA$ expires; $DEST\_Table$ is the table described below with informations of a possible host on an EN involved with MH communications. The $DEST\_Table$ entries are: $Dest\_IP$, the target IP address; EA_IP, the IP address of the EA on EN, if present; EA_mobile, an IP address, depending on the destination, set to EA_IP for FHs, to VA_B_IP for MHs and to 0.0.0.0 for a target unassisted by an agent; $Last\_registered$, the instant of the VA-EA registration process, which occur once only at the entry creation; $Flags$, identifies the registration status, $Retries$, counts the attempts number of registration for EA, due to the unreachability of the EA or of the $EHAS$, upper limited to the $TO\_resolve\_EA$ time, after which the target is considered fixed without EA; $Timer$,

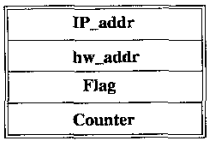

Fig. 6. ARP security cache entry

maintains the timeout status for the EA registration by forcing a new procedure when $TO\_resolve\_EA$ expires; $Packets\_queue$ the queued packets sent by the MH before the end of registration procedures.

By considering the HA, each entry contains the information of an MH visiting a FN after the VA registration phase: MH_IP is the MH IP address; VA_IP is the IP address of the relative VA; $Last\_registered$ is the last time of the VA driven registration process; $Register\_timeout$ is the HA entry life time sent by the VA.

By considering the EA, each entry contains the information of a FH involved with MH communications, after the VA registration phase: $Dest\_IP$ is the FH IP address on EN; $Dest\_hw$ is the relative MAC address; $Last\_arped$ is the last time in which EA has published itself at the FH as default router, procedure repeated every TO_ARP seconds; $Flags$ identifies the registration status; MH_Table is the table described below with informations of an MH involved with FH communications. The MH_Table entries are: MH_IP, the MH IP address; MH_VA, the IP address of the relative VA; $Last\_registered$, the last time of the VA driven registration process; $Register\_timeout$, the EA entry life time sent by the VA.

As far as the agents entries management is concerned, some times should be set. For the VA: the time between two successive entry scans; the lifetime of an MH entry; the time between two successive VA-HA registration procedures; the lifetime of a $DEST\_Table$ entry; the lifetime of an HA entry; the lifetime of an EA entry; the time between two successive VA attempts to identify or to register an MH on the HA, $TO\_resolve\_HA$; the time between two successive VA attempts to identify or register a FH on the EA, $TO\_resolve\_EA$. For the HA, only the time between two successive entry scans should be set and for the EA, both the time between two successive entry scans and the time between two successive *Gratuitous ARP* actions, TO_ARP, should be specified.

The ARP security cache on the HA, reported in Fig. 6, contains: IP_addr, the IP address of a generic host of the HN; hw_addr, the relative MAC address acquired by monitoring the ARP request on the HN or by an hand-made set up; $Flag$, the status flag to specify if the entry is permanent (hand-made) or temporary (acquired); $Counter$, the lifetime of this entry. The hashing function is based on an MD5 algorithm [11] which produces a hash value of 128 bit by processing, in our version, a 512 bit block.

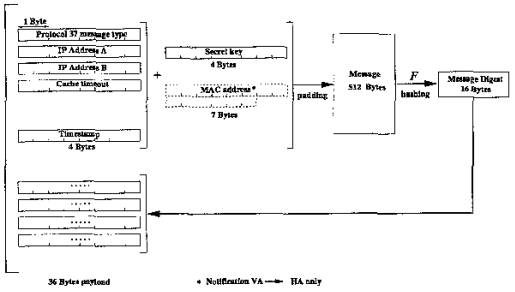

Fig. 7. IP signaling packet format

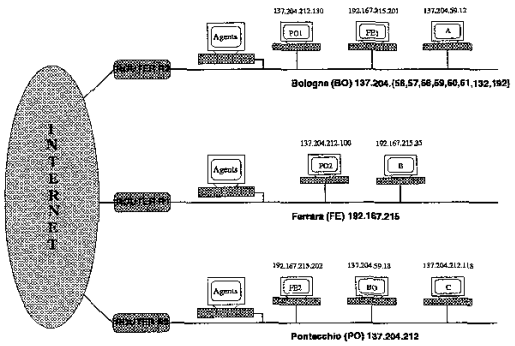

Fig. 8. Field test network setup

In Fig. 7, the complete IP signaling packet format is shown, where the first 16 bytes are the same of the implementation without security [6]. Finally, let us observe that the system has been implemented [12] by modifying a *Linux* Kernel version 2.0.0, as in [6].

VI. Network Configurations and Field Test Results

Three university networks have been considered and configured with transparent mobility agents support, in order to test and verify this new implementation. The test methodology is the same experimented on [6] and here the emphasis is given to the comparison between MH-to-MH versus FH-to-FH. The network setup involved is reported on Fig. 8, where the Bologna, Ferrara and Pontecchio Internet network links are 34Mbs, 64Kbs and 2Mbs, respectively. The MHs are labeled by means of the name of their HN (eventually followed by a successive number): BO for Bologna, FE for Ferrara and PO for Pontecchio; instead the FHs are identified by means of single capital letters. Many tests on functionality have been performed by stressing the system with *telnet*, *ftp*, *www* and *X11* screen redirection applications. In order to measure the performance, a ping field test has been carried out and the results are shown on Tab. I, by considering a set of 1000 ping at the peak traffic hour, with two different payload lengths (64 and 512 bytes). The table gives the couple MH-to-MH and FH-to-FH, evaluated at the same time in order to have the same traffic and network conditions.

Let us observe that: the MH-to-MH average times are

Communication on 1000 pkts	Payload length	min (ms)	avg (ms)	max (ms)
PO1-PO2	64	93	189	918
A-B	64	82	168	882
PO1-PO2	512	235	452	2189
A-B	512	212	397	3271
FE1-FE2	64	12	15	188
A-C	64	7	9	90
FE1-FE2	512	27	34	2451
A-C	512	17	19	121
FE1-BO	64	12	15	298
A-C	64	7	10	111
FE1-BO	512	27	33	1216
A-C	512	17	20	345

TABLE I

MINIMUM, AVERAGE AND MAXIMUM ROUND TRIP TIME FOR PINGING TEST

closer to the FH-to-FH ones and this proves the suitability of the described approach; tests involved with FE have high times due to FE network low speed; maximum times are due to the extreme networks conditions and the MH-to-MH cases have usually higher values than FH-to-FH ones due to agents signaling procedures; minimum times are always lesser in the FH-to-FH cases due to the processing time introduced by the agents. In all tests no packet loss has been measured.

Finally, some attempts to force the different security level proposed have been made, i.e. attempts to register non-authorized MHs, transmission of unexpected intruders signaling messages, attempts to use packets with *timestamp* invalid. All these attacks have been done without success.

VII. CONCLUSIONS

In this paper the problem of **transparent** mobile IP is investigated by developing the basic idea and the implementation proposed in [6]. Main efforts have been made to optimize the system for the MH-to-MH routes and to gain security features. The final implementation results stable, easy to export and all tests show the routing suitability and the efficacy in preventing attacks of possible intruders.

Further investigations regard with the optimization of characteristic times of the agents caches, by considering different traffic levels and network conditions.

REFERENCES

[1] L.F. Marshall, G. Cho, "An Efficient Location and Routing Scheme for Mobile Computing Environments", IEEE JSAC, No. 13, pp. 868-879, 1995.

[2] A. Myles, D. Skellern, "Comparing Four IP Based Mobile Host Protocols", Computer Networks and ISDN Systems, pp. 349-356, 1993.

[3] A. Myles, D.B. Johonson, C. Perkins, "A Mobile Host Protocol Supporting Route Optimization and Authentication", IEEE JSAC, pp. 839-849, 1995.

[4] C.E. Perkins, A. Myles, D.B. Johnson, "IMHP: a Mobile Host Protocol for the Internet", Computer Networks and ISDN Systems, pp. 479-491, 1994.

[5] C.E. Perkins, "Mobile IP. Design Principles and Practices", Addison-Wesley, 1997.

[6] A. Giovanardi, G.Mazzini, "Transparent Mobile IP: an Approach and Implementation", Procs. of IEEE Globecom'97, Phoenix, Arizona, pp. 1861-1865, 1997.

[7] W. Stallings, "Network and Internetwork Security", Prentice Hall, 1995.

[8] C. Chen, C. Liou, C. Wu, R. Wu, T. Hou, "Solving Location Problem of a Mobile Host by an Agent Group", Procs. of IEEE PIMRC '96, Taipei, Taiwan, pp. 708-712, 1996.

[9] S.M. Bellovin, "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communication Review, No. 19, 1989.

[10] G. Tsudik, "Message Authentication with One-Way Hash Functions", Procs. of IEEE INFOCOM 92, Firenze, Italy, 1992.

[11] R.L. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, 1992.

[12] D.E. Comer, D.L. Stevens, "Internetworking with TCP/IP Volume II, Design, Implementation and Internals", Prentice-Hall, 1994.