Routing Protocol Evaluation for IP Mobility

Rossano Marchesani, Sebastiano Schillaci
Thales Italia S.p.A
Via E. Mattei 20
66013 Chieti Scalo (Chieti)
ITALY

email: {rossano.marchesani | sebastiano.schillaci}@it.thalesgroup.com

ABSTRACT

Since IP is becoming the leading protocol to interconnect heterogeneous networks , much effort is done to investigate if Internet technology can be usefully employed for military applications. This paper deals with some aspects related to mobility management in tactical environments with deployable networks. Less effort has been done to study the applicability of Mobile IP in tactical networks although this topic would give nodes a great flexibility and allow them to use all existent low-cost TCP/IP based applications.

In order to verify performance of Mobile IP in tactical environments a network, composed by three LANs, has been made up and the mobility agents have been implemented on the nodes and tested. Then many tests have been performed in order to verify the behaviour of Mobile IP on links with different bit-rates and with nodes moving at different speeds. It has been evidenced that the control traffic, needed to update the routing tables, and mobility management depend on link speed. Also nodes' speed influences time needed to perform a data transfer. However the results demonstrates that, with some adjustments, Mobile IP can be usefully employed within certain limits in tactical networks. The experimental results have also been compared to those obtained by means of a specific model developed with the network simulator software OPNET and agreements with simulation results have been verified.

1 INTRODUCTION

Commercial networks differ in many aspects from tactical ones, thus Mobile IP has to be adapted to military requirements. Tactical networks are characterized by variable and dynamically changing topologies where users have limited resources at one's disposal. Moreover there are often different links with very different BERs and bit-rates, rendering mobility management a hard job to address.

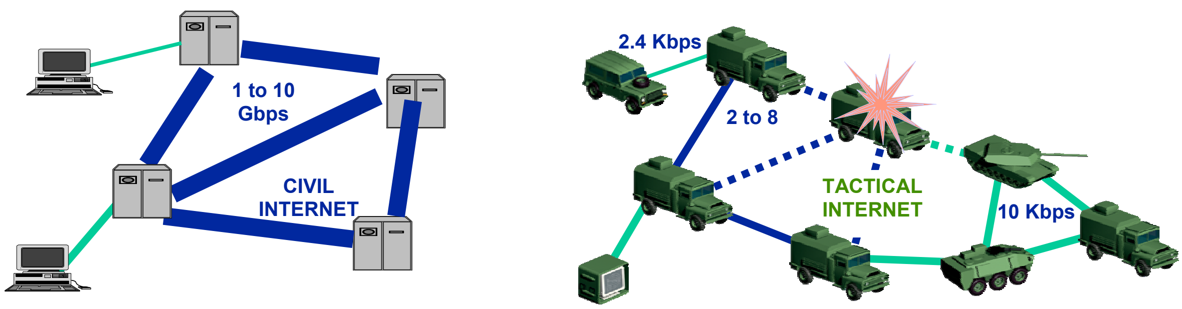

Figure 1: Comparison between civil and military networks.

Marchesani, R.; Schillaci, S. (2006) Routing Protocol Evaluation for IP Mobility. In *Military Communications* (pp. 13-1 – 13-8). Meeting Proceedings RTO-MP-IST-054, Paper 13. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

Civil networks, as depicted in Figure 1, are characterized by a fixed and hierarchical architecture while tactical networks are flat and have a very variable topology. Moreover, tactical users are much less than civil ones but they have to be served not on a best-effort basis but priorities have to be taken in account. Another important aspect is related to the transmission medium. In tactical environments bandwidth is a precious resource that has not to be wasted and is often characterized by links with low bit-rates ([12]).

Tactical networks are often a set of heterogeneous networks and in order to interconnect them a common network protocol is needed. Since the TCP/IP protocol ([1], [5-6]) is independent on the physical and data link layer, it represents a natural choice to investigate. Using TCP/IP as network protocol allows a user to download web pages, transfer files and use multimedia applications. These applications could be employed to patrol an area and exchange information among nodes or with remote connections while moving.

There are some differences regarding the way mobility is handled in civil and tactical networks. In civil field the *de-facto* standard that allows TCP/IP users to support mobility in the Internet is the Mobile IP protocol. This protocol permits a mobile node to keep active connections while moving between two different networks. Nodes are able to move from one network to another keeping their own IP address, without losing active connections while moving and being always reachable wherever they are actually located.

2 MOBILE IP

In civil networks, as shown in Figure 2, mobility is managed by two particular software modules: the *home-agent*, located in the user's home network, and the *foreign-agent*, located on the new network where the mobile node will be located when it moves away from the home network.

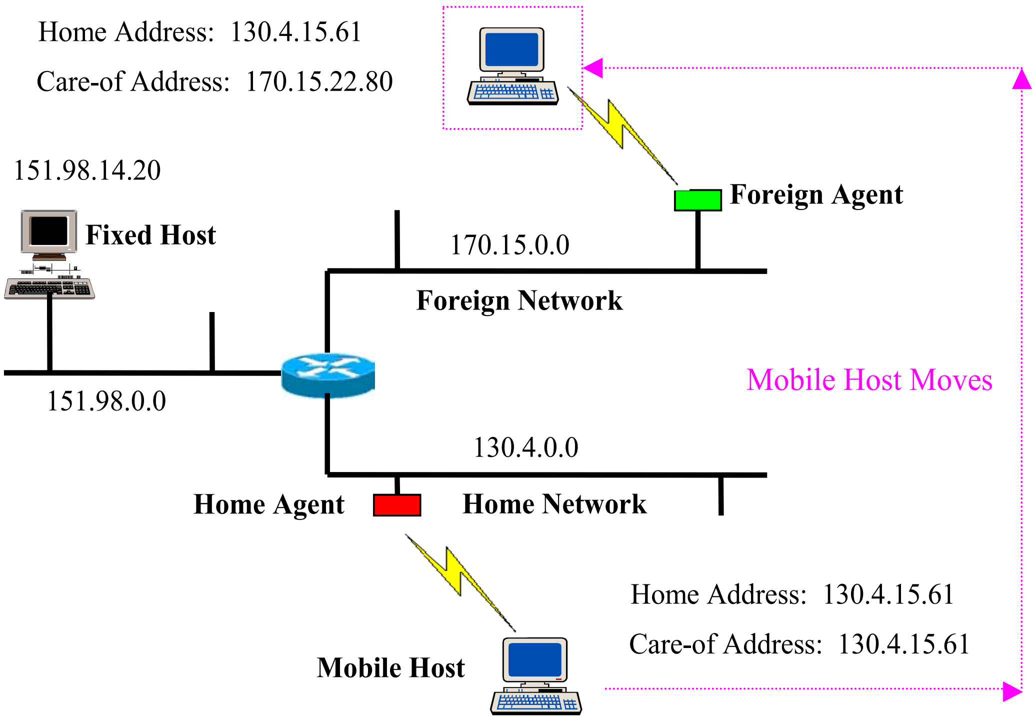

Figure 2: Mobile IP.

The Mobile IP standard ([2-4]) foresees that each mobile host has two addresses:

- *Home-Address*: this address is assigned to a mobile node to identify TCP connections regardless of where the node is attached to the Internet. It makes it appear that the mobile node is continually able to receive packets on its *home network*. The network prefix matches with that of mobile node's home netwok.
- *Care-of-Address:* this address changes at every new point of attachment and is directly related to the network the node is currently attached to. The protocol can use two different types of care-of addresses: a *foreign agent care-of address*, that is the IP address of the foreign agent where the mobile node is registered, and a *co-located care of address*, that is the local address that the mobile node has associated with.

If the node doesn't move, the co-located care-of address is the same as the home address. When the node moves from one net to another only the care-of address changes .To allow correct routing a *home agent* and a *foreign agent* are needed. The home agent is a special router, attached to the node's home network. If the mobile node is attached to the home network it delivers datagrams directly to the node. If the node is instead attached to a foreign network the home agent stores the current location of the mobile host and tunnels datagrams towards the foreign agent. A foreign agent is a router on the mobile node's visited network that provides routing services to the mobile host. The originator sends packets towards the home agent. The home agent checks if the mobile host is attached to the home network using ICMP packets ([7]). If so it delivers directly the data packets. Otherwise, using the IP tunneling mechanism described in RFC 2003 ([8-11]), packets are relied towards the foreign agent. This mechanism is called *redirection*. The care-of-address is known to the home agent because when the node moves it registers the current care-of address with its home agent. The mobile host can then send its data packets directly to the originator without tunneling them towards the home agent.

In summary, there are three mechanisms that makes IP mobility possible:

- Discovering the care-of-address
- Registering the care-of-address
- Tunneling to the care-of-address

The Mobile IP agents for tactical networks that have been developed and tested allow a node to act both as client and server. The latter is very important in military applications because in these scenarios it's often the server itself, located for example on a vehicle, that moves and that has to be configured with a static IP address. On the other hand, a node could also act as a simple client. Thus there is often no need to maintain always the same IP address since a new one can be given to it, by means of a DHCP server, whenever it moves towards a new network. The difference, respect to ordinary dynamical IP address distribution, is that active connections have to be kept alive with the old IP address. There has been implemented a particular function that assigns a new IP address only if all active connections have been closed. This is an optimization of the Mobile IP protocol that works well in tactical environments because it reduces the traffic and delay in the network.

3. TEST RESULTS

In order to evaluate Mobile IP in a tactical network, the test-bed shown in Figure 3 Three LANs have been connected by means of three gateways. The mobile software modules optimizing Mobile IP for tactical networks have been installed on a *Home Agent* and a *Foreign Agent*. As shown in Figure 3 the test-bed reflects a real situation where several vehicles move from a cluster, managed by a Command Posts, to another without losing its IP address.

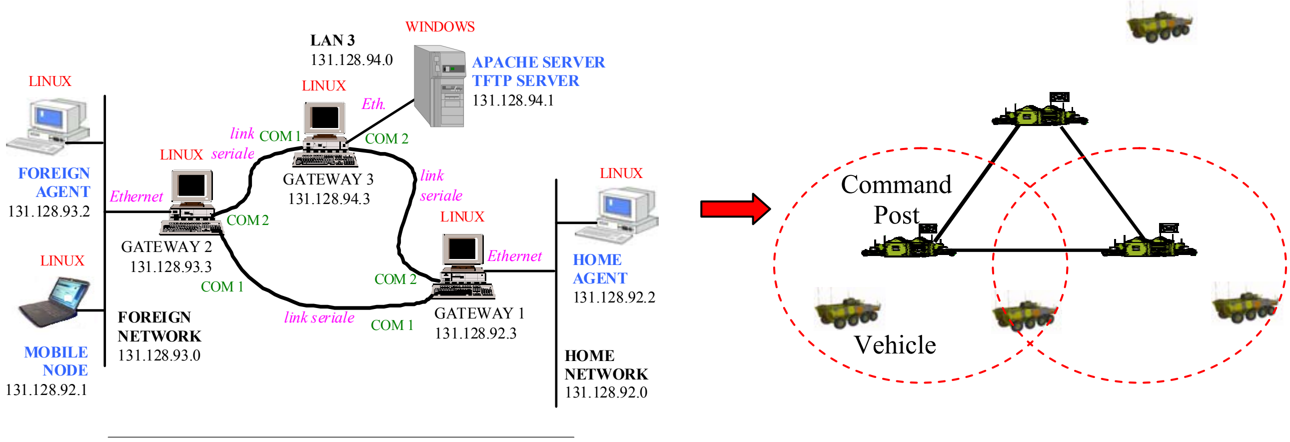

Figure 3: Test-Bed.

Different tests have been executed in order to evaluate the control traffic, the data traffic and the delays. Figure 4 shows the test results where the foreign agent sends agent advertisements every 10 seconds and the registration updates every 250 seconds. The chosen data rate on the serial links has been 19200 bps.

The figure shows an increase in download time when the Mobile IP technique is used. This is due to registration and tunneling time but, in spite of this , all files have been successfully transferred.

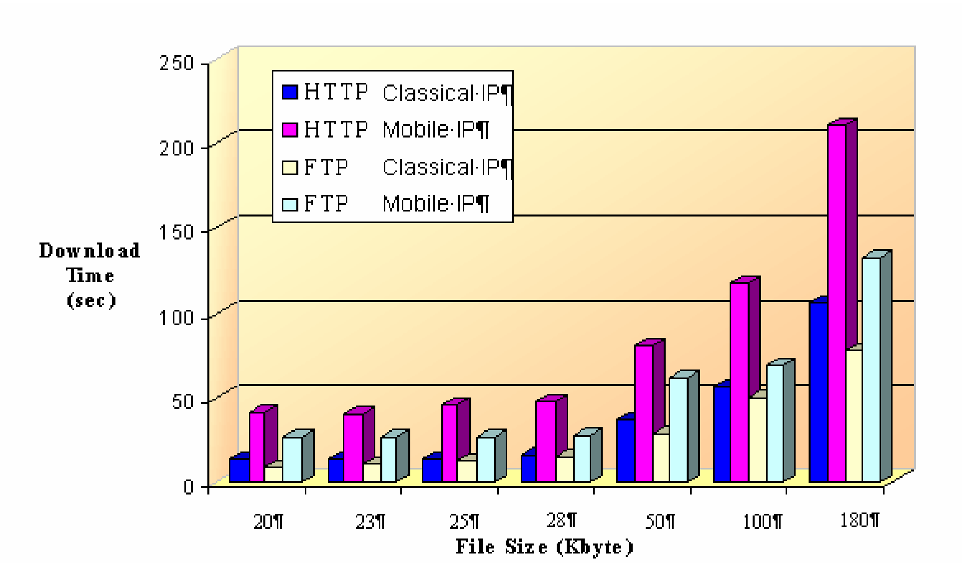

Figure 4: HTTP and FTP download times for files of different size.

During the second test, the foreign agent sends agent advertisements every 5, 10 and 20 seconds; the registration can be updated every 30, 50, 100, 250 seconds. The bit-rates on serial links are 19200 bps and 9600 bps. The test results performed on HTTP web-browsing, as shown in Figure 5, prove that Mobile IP can be adapted to the network where the technique is applied. Figure 5 refers to agent advertisement packet sent every 10 seconds and updates every 250 sec.

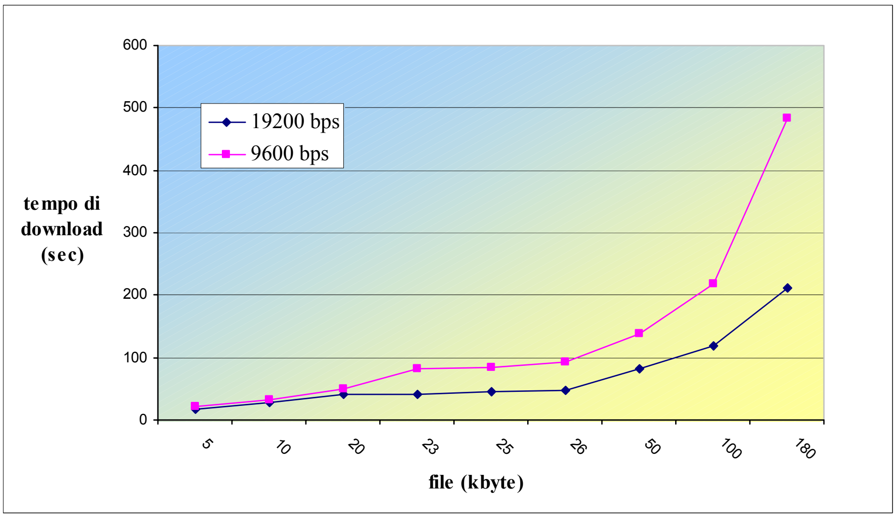

Figure 5: HTTP download time

4 SIMULATION RESULTS

The results obtained by means of the test-bed have been compared to those obtained by means of simulations with the network simulation tool OPNET. The reference scenario is depicted in Figure 6. A mobile node moves from its home network to a foreign network. It is supposed to have WLANs supporting 1 Mb/s data transmissions with a radio range of 250 m.

The first simulation consisted in downloading, by means of FTP, two times a 6 MB file. Three graphics have been obtained as shown in Figure 7. The fist one is related to the mobile node being and transmitting in its home network (MN – HA). The second graphic is related to the mobile node when it's in a foreign network. In both situations the registration timeout is set to 60 seconds.

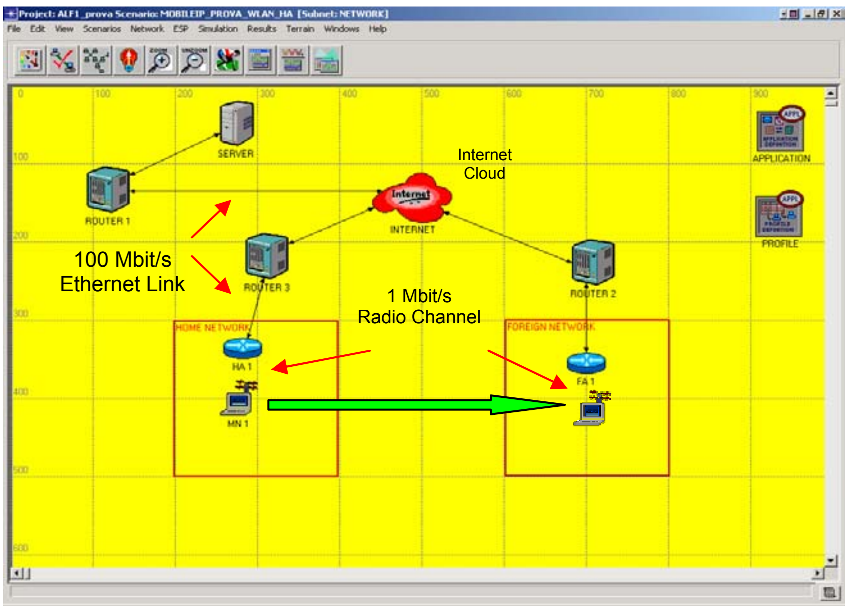

Figure 6: OPNET reference scenario.

Both times the files were downloaded but it can be noticed that, when the mobile node is in a foreign network, the download time is higher. This is due to registration latency meaning that the registration is renewed after 60 seconds while the mobile node is still downloading the file. Consequently some packets get lost and the TCP retransmission timer is increased leading to higher download times. If the registration timeout is increased to 200 seconds, as shown in the third graphic (MN – FA Extended Registration), the download times are the same as those registered when the node is in the home network.

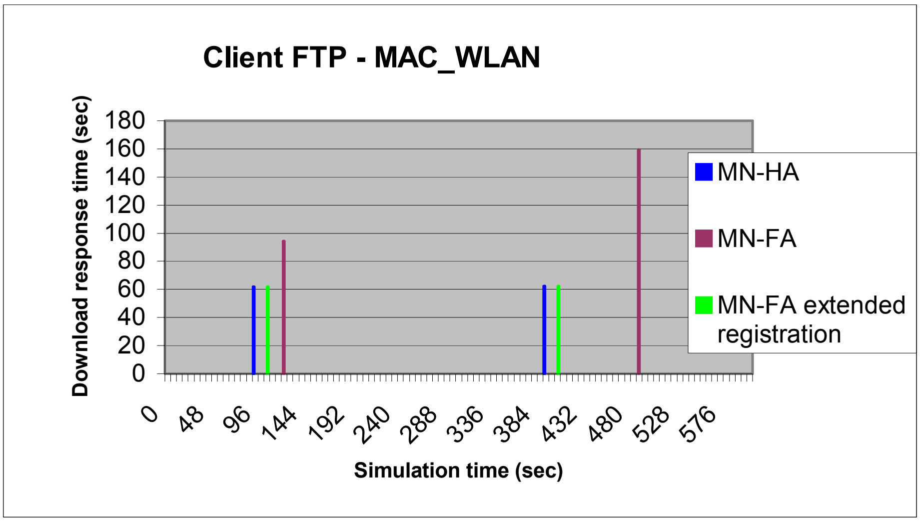

Figure 7: FTP download times of a 6 MB file with a mobile node being in its home network and then moving to a foreign network.

Another simulation has been performed increasing the number of mobile nodes to 4 elements, as shown in Figure 8. In this situation the download times, as shown in Figure 9, increase sensibly because bandwidth is shared between multiple users. It has been also evidenced that the medium access method influences network performances.

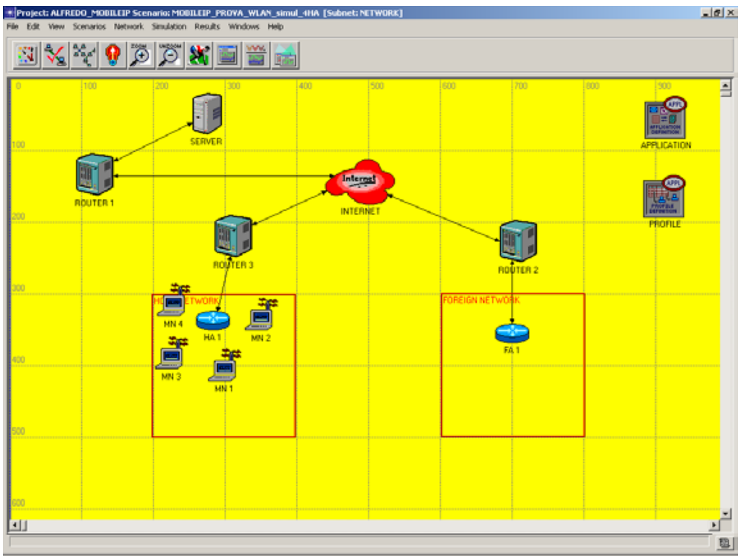

Figure 8: OPNET scenario with 4 mobile nodes.

To get better performances either the file dimension or the MAC protocol must be changed. Simulations show that in both cases the download time can be sensibly decreased.

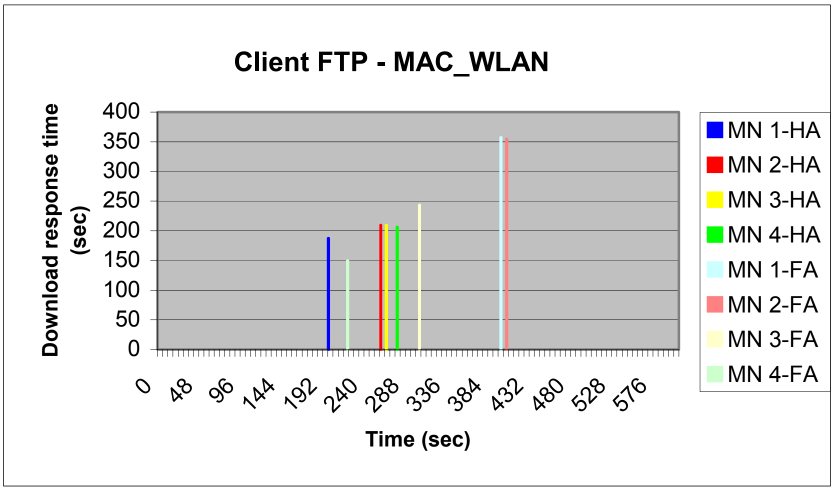

Figure 9: FTP download times of a 6 MB file with 4 mobiles node being in their home network and then moving to a foreign network.

The last simulation has been focalized on collecting statistics on SMTP and HTTP traffic of a node moving from the home to the foreign network. As shown in Figure 10, some packets are lost when the mobile node passes from the area covered by the home agent to that covered by the foreign agent. This causes an increase in transmission time. Packet loss is due mainly to registration latency and handover problems. Anyway, files are always correctly transmitted.

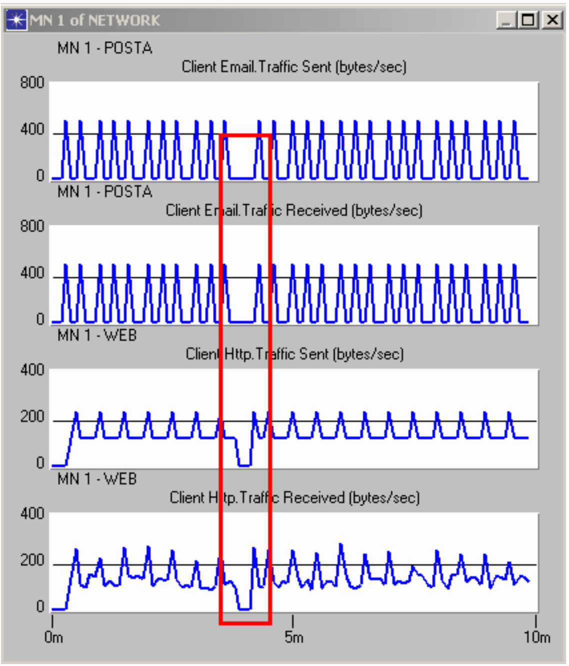

Figure 10: SMTP and HTTP traffic sent and received by a mobile node that moves from its home network to a foreign network.

5 CONCLUSIONS

The Mobile IP technique has been analyzed in order to investigate its applicability in tactical environments and the mobility management modules have been modified in order to address tactical requirements. The performances of the developed software modules have been tested both by means of a laboratory test-bed and by OPNET simulations.

Use of TCP/IP in military applications results very useful due to the independence of the internet protocol on the physical and data link layers. Another aspect that has to be considered is that mobile agents are independent on the TCP/IP applications running on a node and can be installed as simple add-on modules on existing systems. Mobile IP agents don't block or interfere with ordinary applications running on a node because they run as background services and modify only routing tables. These programs may encounter only a little increase in delays due to control traffic and update management actions. This allows to introduce mobility in any existing network. Moreover varying some parameters, as the agent advertisement and discovery timeouts, the mobile agents can be successfully adapted to almost every tactical scenario.

An interesting application of mobile agents is in Mobile Ad-Hoc Networks (MANETs). This offers the advantages to connect a mobile node, belonging to a MANET, with the rest of the Internet and to overcome the problem of having the foreign agent always available and within the transmission range of the mobile node. Ad-Hoc routing protocols offer, indeed, a multi-hop service that allows a node to reach another one even if it is not directly reachable. Moreover a mobile node may, occasionally, connect to a node located on fixed network, such as a Command Post, without modification of the IP address. This combination results very powerful and particularly applicable in tactical networks.

6 REFERENCES

[1] J. B. Postel, *Internet Protocol*, IETF RFC 791, September.1981.

[2] C. Perkins, *IP Mobility Support*, IETF RFC 2002, October.1996.

[3] C. Perkins, *IP Mobility Support for IPv4*, IETF RFC 3344, August 2002.

[4] C. Perkins, *Mobile IP: Design Principles and Practice*, Addison-Wesley Longman, Reading, Massachusetts, USA, 1998.

[5] J. B. Postel, Transmission Control Protocol, IETF RFC 793, September 1981.

[6] J. B. Postel, User Datagram Protocol, IETF RFC 768, August 1980.

[7] S. E. Deering, *ICMP Router Discovery Messages*, IETF RFC 1256

[8] W. Simpson, *IP in IP Tunneling*, IETF RFC 1853, October 1995.

[9] C. Perkins, *IP Encapsulation Within IP*, IETF RFC 2003, May 1996.

[10] C. Perkins, *Minimal Encapsulation Within IP*, IETF RFC 2004, May 1996.

[11] S. Hanks, *Generic Routing Encapsulation (GRE)*, IETF RFC 1701, October 1994.

[12] C. Graff, M. Bereschinsky, M. Patel, *Application of Mobile IP to Tactical Mobile Internetworking*, IEEE, Fort Monmounth, NJ, USA, 19