Performance Evaluation of Mobile IP Agents' Auto-Reconfiguration Mechanisms in MANET

Cláudia J. Barenco Abbas[1], Georges Amvame-Nze[2] and L. Javier García Villalba[3]

[1] Departamento de Computación y Tecnología de la Información
Universidad Simón Bolívar - USB
Oficina MYS 213-B, Apartado Postal 89.000
Caracas, 1080 Venezuela
barenco@ldc.usb.ve

[2] Faculty of Technology, Electrical Engineering School
University of Brasilia – UnB
Brasília, 70900 Brazil
georges@labcom.unb.br

[3] Grupo de Análisis, Seguridad y Sistemas (GASS)
Departamento de Sistemas Informáticos y Programación (DSIP)
Facultad de Informática, Despacho 431
Universidad Complutense de Madrid - UCM
C/ Profesor José García Santesmases s/n, Ciudad Universitaria
28040 Madrid, Spain
javiergv@sip.ucm.es

Abstract. This paper presents a Dynamic Reconfiguration of Mobile IP Agents (DRMIPA) and failure free architecture integrated in Mobile Ad hoc Networks (MANETs). The proposal is due to the fact that: actual infra-structured networks do not implement the Mobile IP (MIP) protocol, all MIP agents are static and the cost of having redundancy for MIP agents' failure is often high. As MANETs are created temporarily at any location, we propose a solution that would allow the integration of MIP with MANET. Doing so, groups of MIP nodes in MANETs would enjoy the IP mobility at any foreign or local network that doesn't implement MIP. New algorithms and messages are proposed for the new Dynamic Reconfiguration and fault tolerant Mobile IP Agents in MANET. A simulation performance analysis using the Network Simulator (NS2) is presented.

Keywords: DRMIPA, MIP, AODV, MANET, Fault Tolerance.

1 Introduction

The Ad hoc network nodes have great flexibility and responsiveness after being implemented [1]. Nonetheless, there might be a need for those nodes in the new network to be able to use an internet connection and still be reached by their Home Network from a fixed or another distant Ad hoc network area. For such matter, the Mobile IP group foresaw the need for a mobile node attached to its Home Network to

be able to move to other networks (called Foreign Networks) keeping its Home Address (its logical address obtain at the Home Network) throughout the path to the next destination and, having the possibility to keep track of local services it had at the home network [2]. For this reason, two IP addresses have to be assigned to the Mobile node so it would be reached in the Home Network by a fixed and permanent IP address and at the Foreign Address by the so called Care-Of Address (COA), which would represent its new point of attachment away from home, Figure 1 (a).

The current work proposes a solution to integrate both architecture, MIP and MANET. The new scenario would not depend of an infrastructure network with or without MIP Gateways. The new approach would make groups of MIP nodes, in MANETs; enjoy Internet access and IP mobility at any foreign or local network.

This approach is different from related works because MIPv4's Foreign Agent (FA) and Home Agent (HA) are now mobile and part of a mobile ad hoc network [4], [5], [6] and [13], Figure 1 (b). In [8], [9] and [10], an Efficient Fault-Tolerant Protocol for Mobility Agents in Mobile IP is proposed, but the issue takes place in an infrastructure network.

We believe that there is a need in having an independent MIPv4 architecture, from the one studied in [4], [5] and [6], to attend this kind of situation. So why not making all agents mobile and having total freedom from networks that have no MIP. As these agents are now mobile there would also be a need to turn them failure free.

For that reason, we propose new Mobile IP agents by naming them Active and Passive Agents where the active agent would be the one in service and the passive agent the one in idle, the system will be known as DRMIPA (*Dynamic Reconfiguration of Mobile IP Agent*) [14]. The contributions of the present work are as follow:

- The challenge of having a Home and Foreign Agent inside the Ad hoc network. Therefore, we would have to maintain the Mobile IP Agent's functionalities from the fixed Network into MANET.
- A DRMIPA node can operate as a MIPv4 node. The algorithm ensures session continuity for all nodes in MANET, even as the mobile agents' shutdown or move to another IP network.
- The new DRMIPA network can be created temporarily at any foreign or local network to allow nodes in having Internet and IP mobility. Access of their Home Network would be available anytime, anywhere.
- The election of a passive agent HA (FA) to provide a fault tolerance mechanism if the active agent HA (FA) leaves or ceases its participation in the network. This would support MN users with continuous network connections while at the Home or Foreign Network.
- The solution proposes a bidirectional tunnel between DRMIPA nodes and their HA (FA) agents. So, all traffic between nodes passes through the home and/or foreign agent. The AODV protocol is used for all routing purposes.

In all the above cases, we agree on the need of a foreign network implementing a gateway having two interfaces for this scenario to work: one to access the Internet and the other one to access any MANET network.

2 Dynamic MIP Agent in MANET

2.1 Mobile IP in Ad hoc Network

The current MIP proposal is to support IP mobility in different environments. The HA, being a router located at the Home Network, provides information regarding the service location to the Mobile Node (MN) when away from home and serves as one of the end tunnels to be built during a data transaction, [3]. Located at its Home Network, the MN uses its home address to receive and exchange data with other nodes in the area such as the correspondent host (CH). When moving to another network (a Foreign Network) it receives a Care-Of Address (COA) in that location and will be able to maintain its communication data when roaming, Figure 1 (a). To facilitate the transaction of data between the HA and the MN, a FA is used as the other end tunnel during the registration's request, reply and data exchange. The routing protocol used in this work is the Ad hoc On demand Distance Vector (AODV) for being more reliable and scales better than DSDR. This is a reactive protocol that uses Route Request (RREQ) and Route Reply (RREP) for route discoveries between Ad hoc nodes, which are maintained active upon discovery, [7].

In the Ad hoc Network there is no infrastructure that can allow a greater control of MNs. When they move from one IP area to another, their current services should be available as needed at the foreign Ad hoc Network, similar to what occurs with Mobile IP in an infrastructure network. To that extent, the MANET and MIP should be combined to allow the registry of any mobile nodes entering and leaving its IP area of propagation and forcing all MANETs to implement a Mobile Home and Foreign Agents (named in this work as MHA and MFA), for further node connectivity.

Figure 1 (b) shows the suggested system having a virtual path between the origin and destination nodes (the represented destination MN in *DRMIPA2* is originally from *DRMIPA1*). The data leaves its origin passing thru the active MHA and MFA; both will always serve as end tunnels up to the desired destination node. When away from home network, all MNs data transaction has to be between active agents so that MIP mechanisms behave as before when they were part of the WLAN topology. The routing process is supported by AODV along both MANETs' path.

2.2 Issues facing Agent Mobility

As we expect any MHA (MFA) to be shutdown, leave its IP area or move to another Ad hoc Network at anytime, the proposed DRMIPA algorithms have to be installed in all MNs to maintain dynamic reconfiguration and fault tolerance. In such conditions, the associated services to mobility of a visiting MN, previously registered at the foreign MFA, need to be preserved outside its MANET Home Network. Therefore, each new Mobile Agent (MA $\Leftrightarrow$ {MFA or MHA}) should be duplicated, one serving as an active agent and the other as a passive agent. This technique helps to maintain a fault tolerance mechanism for these mobile agents. By this mean, it is assured that in case a MA is being deactivated or leaves its functionality of MFA (MHA), it will be replaced by a previously preconfigured passive MFA (MHA), which would then

exercise its activities as a new active MFA (MHA) and in turn elects the next passive MFA (MHA).

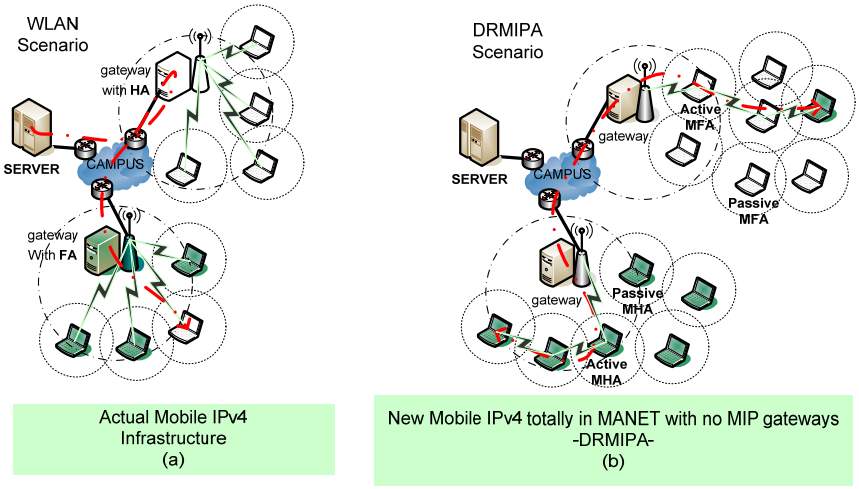

Fig. 1. MIPv4 in WLAN (a) and the proposed MIPv4 in MANET with WLAN access: DRMIPA (b).

3 Proposed Algorithm

The following steps exemplify a passive agent election and binding signaling from an active MFA to a MN in the same network. The active agent uses actual MIP agent advertisement with the existence of a new 2-bit *A*-flag, Figure 2. If a MN has only the MIP algorithm implemented and not DRMIPA, the *A*-flag would not be an issue but this MN would not participate at the election process, as described bellow:

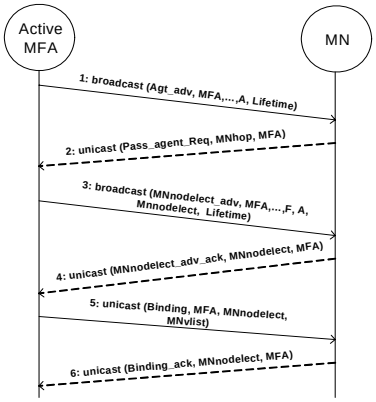

Fig.2. Passive agent election and binding signaling.

1: The agent broadcasts the message into MANET and all routes are created on demand using the AODV protocol.
2: The MN sends a passive agent request message to notify the MFA his willingness to be a future passive MFA.
3: After a thorough research for the best future passive agent, the MFA broadcasts a $MN_{nodelect}$ message including the elected passive MFAs' logical address to all nodes in the MANET. This will cease passive agent request messages of MN from flooding the network.
4: Only the elected MN will acknowledge the previous broadcast to the MFA.
5: The MFA starts sending a copy of his MN visiting list to the new passive agent (this procedure would be similar to the active MHA that communicates with another elected passive MHA except when sending the list of MNs away from home).
6: For system robustness, all critical transactional messages taking place between active and passive agent need an acknowledgement message. This would guarantee the correct replica of an active MA in a passive MA so that node workload redirection is softer in case of failure.

All MN implementing DRMIPA would have their state as shown in Figure 3. The EXIT state would occur if an algorithm failure is detected. At the LISTEN state, all messages from the network are analyzed.

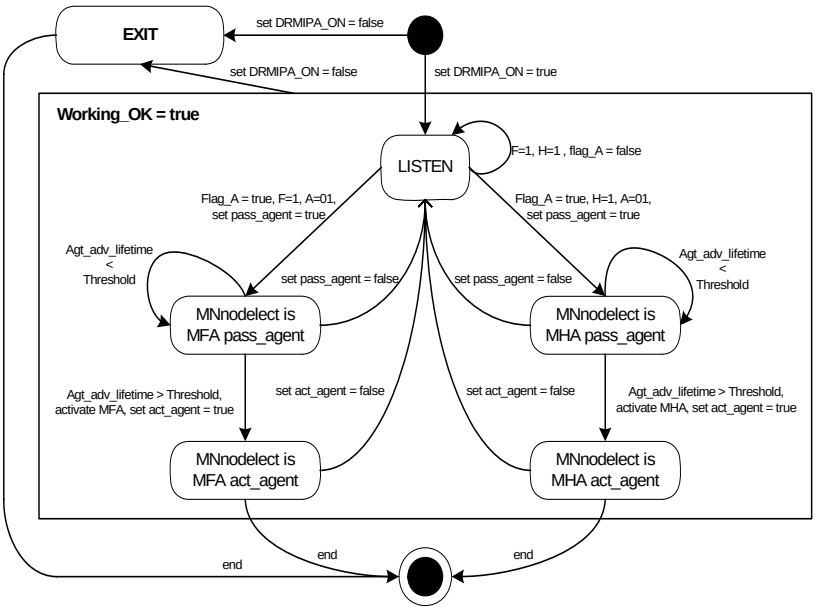

Fig. 3. $MN_{nodelect}$ basic state diagram.

If no *A*-flag appears in the advertisement, it means that the MN is in a normal MIP network. This would guarantee a transparent MIP functionality and no DRMIPA

process will take place. If a MIP agent advertisement contains the *A*-flag, one of two things can take place for the message to be process as coming from a MFA (having the *F*-flag set) or MHA (having the *H*-flag set). The elected MN, known as MNnodelect would be in a MFA (MHA) passive agent state. While agent advertisements lifetime are less than a certain threshold time, the MNnodelect will monitor any eventual active MFA (MHA) failure. Meanwhile, the MFA (MHA) synchronizes their MN list to the new MNnodelect.

If the agent advertisements' lifetime exceeds the threshold time, the node goes to a MFA (MHA) active agent state and the previously obtained lists would be included in the new MFA (MHA) list. At this point the other active agent should cease operations. And by doing so, the new active agent would be aware of previously registered MN at the old active agent. Now the active agent algorithm is working and an auto configuration mechanism begins for passive agent election. If any MNnodelect leaves the network or ceases operation as active (passive) agent, it must return to its original LISTEN state. The present work emphasizes the fact that a node can be an active or passive agent as long as it maintains its normal MIP functionalities as a simple MN. And this is due to the fact that: if a MN has an undergoing data transmission with another MN and is elected as passive agent, it must not cease its operations as a normal MIP node.

If after a certain period of time the active MFA does not send any agent advertisement, the passive agent assumes his functionalities as new active agent. The active agent's activation algorithm is as fallowed:

```
Gratuitous_exit := true
pass_agent := true
receive(Gratuitous_exit, MHA/MFA, MNnodelect ) message
from MHA/MFA;
    if Gratuitous_exit ∧ pass_agent then begin
unicast (Gratuitous_exit_ack, MNnodelect, MHA/MFA)
message to MHA/MFA;
    activate MFA/MHA algorithm;
set Flag-A=11 ∧ broadcast (Agt_adv,MHA/MFA,…, A,
Lifetime) message to Network{MFA ∧ MHA} nodes;
    set pass_agent := false;
    set act_agent := true;
    end
      else if (Adv_lifetime > Threshold) ∧ pass_agent
  then activate MFA/MHA algorithm;
set    Flag-A=11    ∧    broadcast(Agt_adv,MHA/MFA,…,A,
Lifetime) message to Network{MFA ∧ MHA} nodes;
          set pass_agent := false;
          set act_agent := true;
  end
```

4 Implementation

The DRMIPA is implemented on the HUT Dynamics' MIP software in conformance to RFC 2002, [3] and [12], for real world scenario. For the purpose of tracing the new DRMIPA messages, *ethereal version-0.10.12's* source code has been modified. The initial configuration of the system requires a manual setup of the MHA (MFA) for all further processes explained previously, in session 3, to be implemented. The present work does not allow more than one active and passive agents running in the network at the same time. We assume that all MANETs' MN implements the DRMIPA algorithm. Meanwhile, a performance analysis has being done under NS2 as we shall see in session 5. Between all messages, one is used for all MNs in the network, implementing DRMIPA, to cease their requests as candidates for passive agent (this is a way to stop flooding inside the network), as seen in Figure 4. This message is a $MN_{nodelect}$ Advertisement. A 32 bits field is used for MNs to know which one has being elected by the active agent and start behaving as a passive agent. The new elected passive agent is now a redundant active agent in idle. We have defined the type this advertisement with the decimal value 82, and an *A=01* flag. This *01* flag means that the message is coming from the active agent.

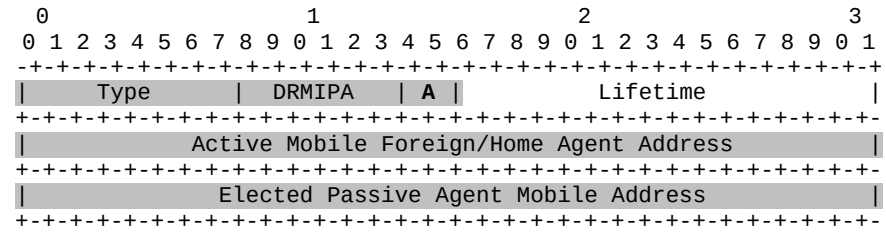

Fig. 4. MNnodelect Advertisement (*Type = 82, A=01*)

5 Simulation Analysis

The DRMIPA protocol has being implemented under NS2 version 2-27 [11]. The original CMU-Trace file was partially modified such that MIP and DRMIPA traces could appear at the NS2 trace file interpreter. The simulation scenario has 10 static mobile nodes using a Two-Ray channel characteristic in a 670x670 flat grid size. This would help in a better way for understanding the delay and bandwidth utilization between the MHA (MFA) and elected passive agent when compared to receiving and transmitting MIP and DRMIPA messages at the same time. From (1), the percentage of bandwidth utilization between active and passive agents can be obtained making *data_sent = data_recv = 54bytes*. Due to overhead messages used in the wireless scenarios, a bandwidth of 5,5 Mbps is used instead of 11Mbps. The average latency of DRMIPA messages was *0,011s* according to DRMIPAs' trace file. The above numbers in (1) give us a bandwidth utilization of *1,4%*. This value shows us how small the occupation of such messages is during the simulation.

$$\%Utilization = \frac{(data\_sent + data\_recv)*8}{(bandwith*time)}100 \tag{1}$$

The delay in Table 1 was measured using a one way mean delay scenario. The purpose of doing so is for a better comparison of MIP and DRMIPA messages. Equation (2) for delay calculation is:

$$\begin{aligned} Delay = {} & Act\_Agt(created\_and\_sent\_msg) \\ & + Pass\_Agt(processed\_msg) \\ & + Pass\_Agt(created\_and\_sent\_msg) \end{aligned} \tag{2}$$

The *Act_Agt (created_and_sent_msg)* reflects the time at which a message leaves the active agent network interface after being created. The *Pass_Agt (processed_msg)* is the time used by the passive agent to process a message coming from the active agent. The *Pass_Agent (created_and_sent_msg)* is the time a passive agent uses for creating and sending a message to respond at the previous received message from the active agent. DRMIPA messages in Table 1 are in bold characters. As MIP and DRMIPA agent advertisements have the same size and include an *A*-Flag for DRMIPA message differentiation, no changes in delay should be noticeable during simulation as can be seen in Table 1.

Table 1. MIP and DRMIPA Messages Performance Comparison

	Flags	Mean Delay (ms)	From - To
MIP_Agt_adv	H=1/F=1	1,89	
DRMIPA_Agt_adv	A=11	**1,89**	Active MFA (MHA) - MN
Reg_Request	-	2,11	
Pass_agent_Req	A=00	**2,11**	MN - Active MFA (MHA)
Reg_Reply	-	2,16	
MNnodelect_adv	A=01	**4,31**	Active MFA (MHA) - Passive MFA (MHA)
MNnodelect_adv_ack	A=10	**2,64**	Passive MFA (MHA) - Active MFA (MHA)

One way end to end delay results show that the election mechanisms are fast enough compared to the current MIP registration messages. All data where taken during a 30s simulation time. Figure 5 shows that the *MN$_{nodelect}$_ADV* have the highest overhead in transmissions due to the fact that all nodes should be aware of the elected IP node's address. Once elected, the passive agent sends small *MN$_{nodelect}$_ACK* messages to the active agent. That explains its small overhead compared to the rest. With this unicast approach, the passive agent will only send his acknowledgement to the MHA (MFA). The *DRMIPA_pass_REQ* stays between both messages in overhead transmissions because each node has to send a unicast message to the active agent. This method seems to be better for the current implementation as

not all nodes in MANET would be DRMIPA nodes. The present scenario can also have MIP, DRMIPA and MANET nodes at the same time. So, making the *DRMIPA_pass_REQ* a unicast message would prevent other non DRMIPA nodes to receive the message and flood the network.

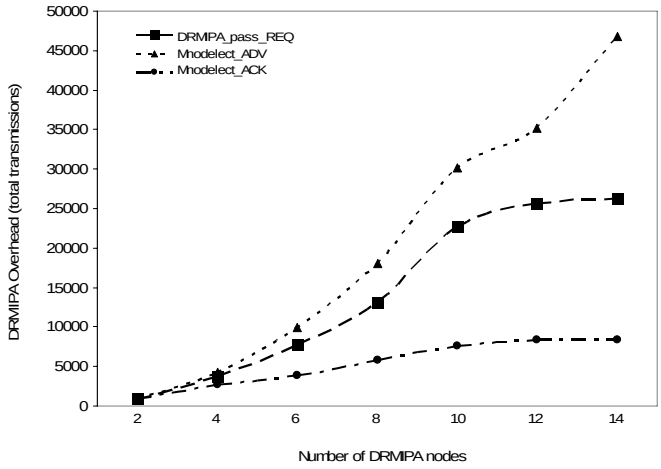

Fig. 5. DRMIPA messages overhead

In Figure 6, the simulation time taken for the passive agent election is shown. The node's positions were set randomly during simulation. The elected nodes are chosen from a passive agent list maintained in the MFA (MHA). When the simulation had 2 DRMIPA nodes it took about *0.82s* for the elected node to receive the message. This value is higher than the ones appearing in other scenarios, because the MHA was too far away from the MN during simulation. In other cases, the actual passive agent is sometimes less than 30 meter away from active agent which would explain small delay times when sending the election message.

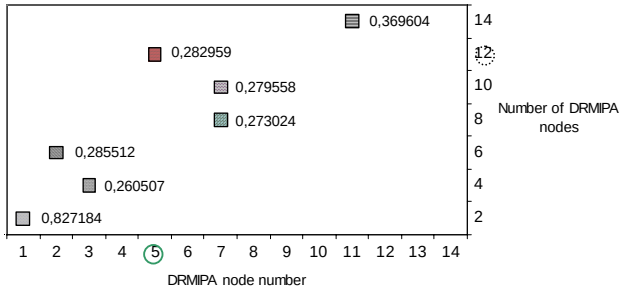

Fig. 6. Time taken for DRMIPA's Passive Agent election (in seconds).

6 Conclusions

In this article, we propose new algorithms and messages for a Dynamic Reconfiguration of Mobile IP Agents in MANET (DRMIPA) using the on demand AODV routing protocol. DRMIPA's solution can help in the integration and mobility of Mobile IP Agents and Hosts between several MANET-Internet-MANET networks. We believe that the principal gain is to maintain the interworking of multiple MIP and MANETs using MFA (MHA) in a failure free architecture. It means a total freedom in using any wireless infra-structured network where MIP doesn't exist. Now it would be possible for groups of MIP nodes in MANETs to enjoy their Internet access and IP mobility at any foreign or local network that doesn't implement MIP.

Acknowledgements

The authors thank the CNPQ (*Conselho Nacional de Desenvolvimento Científico e Tecnológico*), MEC (Ministerio de Educación y Ciencia, Spain, under Project TSI2005-00986) and MITyC (Ministerio de Industria, Turismo y Comercio, Spain, under Project FIT 360000-2005-65) for their financial support.

References

1. C. E. Perkins and E. M. Royer: Ad-hoc On Demand Distance Vector Routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, (1999) 90-100
2. C. Perkins: Mobile IP Support, Technical Report IETF RFC 3220 (2002)
3. IEEE P802.11: The Working Group for Wireless LANs. At: http://grouper.ieee.org/groups/802/11/
4. U. Jonsson, F. Alroksson, T. Larson, P. Johansson, G. Q. Mauire Jr.: MIPMANET-Mobile IP for Mobile Ad Hoc Networks. In: Proceedings of MOBIHOC, (2000) 75-85
5. Y. Sun, E. M. Belding-Royer, C. E. Perkins: Internet Connectivity for Ad Hoc Mobile Networks, International Journal of Wireless Information Networks special issue on "Mobile Ad hoc Networks (MANETs): Standards, Research, Applications
6. C. Ahlund, A. Zaslavsky: Integration of Ad hoc Network and IP Network Capabilities for Mobile Hosts. In: Proceeding of IEEE, (2003)
7. RFC-3561, Ad hoc On demand Distance Vector (AODV) Routing, (2003)
8. R. Ghosh and G. Varghese: Fault-Tolerant Mobile IP, Technical Report WUCS-98-11, Washington Univ., (1998)
9. J. H Ahn and C.S. Hwang: Efficient Fault-Tolerant Protocol for Mobility Agents in Mobile IP," Proc. 15th Int'l Parallel and Distributed Processing Symp, (2001) 1273-1280
10. Jenn-Wei Lin, Joseph Arul: An Efficient Fault-Tolerant Approach for Mobile IP in Wireless Systems, IEEE Transaction on Mobile Computing, Vol.2. no.3, 207-220
11. NS-2. At: http://www.isi.edu/nsnam/ns
12. HUT Dynamics Mobile IP. At: http://dynamics.sourceforge.net/
13. RFC-3963, NEMO Basic Support Protocol, at: http://www.mobilenetworks.org/nemo/
14. G. Amvame, C. Abbas and L. Villalba: Novel Dynamic Reconfiguration of Mobile IPv4 Agents Fully Integrated in MANET. In: Proceedings of the 4th International Information and Telecommunication Technologies Symposium - I2TS, IEEE R9, (2005) 46-51