A Seamless and Transparent MN-Proxy based Mobility Support For (n,n,1) Multihomed NEMO Model

Zohra Slimane [1], **Mohamed Feham** [1] and **Abdelhafid Abdelmalek** [1,2]

(1) STIC Laboratory, University of Tlemcen, Algeria
(2) LAMIH Laboratory, University of Valenciennes and Hainaut Cambrésis, France

Summary

Multihomed Network Mobility is a research field being widely explored because of its importance in military and vehicular applications. Multihoming is a promising solution for providing ubiquitous Internet and some other benefits such as Load-Sharing and Policy-based Routing. Unfortunately, extensions of NEMO Basic Support proposed for the purpose of managing multihomed NEMO are still sub-optimal and too immature for standardization. Indeed, the proposed solutions are partial and don't benefit from all advantages offered by multihoming. Further design, implementation and evaluation are still needed to obtain powerful, secure and flexible solutions. In this paper, we propose a new solution for both mobility and traffic management in the context of (n,n,1) multihomed NEMO networks. The proposed approach relies on beforehand Mobile Routers registration and unidirectional tunnels establishment. A Router-Proxy is also introduced inside the Mobile Network as a central entity to mange mobility and traffic. NS2-Mobiwan simulation results show excellent performance improvement in terms of handoff delay and packet loss rate, proving a really transparency and seamless Internet connectivity.

Key words:

Network mobility, NEMO, Multihoming, Mobile Router, Handover.

1. Introduction

Network mobility management constitutes today a true challenge for the Internet fourth-generation. With the proliferation of wireless devices and mobile network services, one posts an increasing desire on behalf of the users to be profited from ubiquitous Internet access, i-e without discontinuity anywhere at any time during their displacements, so that we have whole networks made up of mobile devices moving together and wishing this quality of service. Public transportation systems (train, tram, subway, buses …) are typical environments.

Network mobility cannot be enough served by MIPv6 [1] (including improved versions, Hierarchical Mobile IPv6 (HMIPv6) [2], Fast Handover for MIPv6 (FMIPv6) [3] and Proxy based Mobile IPv6 (PMIPv6) [4]), because MIPv6 manages only host mobility and has some limitations of supporting Network Mobility. The main problem is that it could only possible to forward packets addressed to a mobile router, but not those nodes behind the mobile router in the mobile network. The deployment scenario of MIPv6 by hosts individually requires also, on one hand that each device support MIPv6, and on the other hand, that each device carries out when handover is involved the functionalities of the protocol MIPv6 leading thus to an increased signaling traffic overhead.

These issues were actively investigated in NEMO (Network Mobility) WG in IETF which has extended MIPv6 protocol to support a collective mobility of an entire single-homed mobile network by introducing mobile router and prefix binding update option. The NEMO Basic Support protocol specified by the NEMO WG [5] is designed so that network mobility is transparent to the nodes inside the mobile network. The mobile network is viewed and managed as a single unit, which changes its point of attachment to the Internet through the mobile router. However, the most interesting NEMO scenario that will practically provide ubiquitous internet is the multihoming. A mobile network is considered as multihomed when either it is simultaneously connected to the Internet via multiple mobile routers, or via only one mobile router which has more than one egress interface. Different interfaces may indeed be active simultaneously; a mobile network must be able to deal with both horizontal and vertical handover. A taxonomy for classifying the potential multihomed configurations and the associated issues is described in [6] and [7] in the context of NEMO-IPv6. Multihoming yields some benefits like Fault-Tolerance/Redundancy, Load Sharing and Policy-based Routing. NEMO Basic Support protocol unfortunately does not specify any particular mechanism to manage multihoming and must be improved to deal with multihomed networks, as it suffers from some problems such as ingress filtering mechanisms, session interruptions during handover, registration procedure latency, multiple Care-of-Addresses registration and Home Agents

---

Manuscript received April 5, 2010
Manuscript revised April 20, 2010

synchronization. Recently, much work dealing with multihoming has been made to solve these issues, and several seamless mobility approaches have been proposed but they still remain sub-optimal because of their relatively longer handoff delays and higher packet-loss rates.

The multihoming analysis draft [7] classifies multihomed mobile networks using (x, y, z) notation. Variables x, y, and z respectively mean the number of Mobile Routers intended to connect the mobile network to Internet, the number of Home Agents, and the number of Mobile Network Prefix. In this paper, we propose a new solution for mobility and traffic management in the context of multihomed NEMO networks. Our special interesting is concentrated on the (n,n,1) multihomed NEMO configuration. We introduce a new entity called Mobile Network Proxy (MNPx) at the Mobile Network level to manage Handoffs and traffic distribution between the multiple Network Routers ensuring transparently to nodes inside the Mobile Network.

The remainder of this article is organized as follows. In Section 2, we provide essential background about network mobility and multihoming. In section 3 we re-examine multihoming capabilities and issues for the (n,n,1) NEMO configuration. Section 4 presents our Mobile Network Proxy based multihoming solution and describes its behavior in a common scenario. We show performance evaluation in section 5. Finally, section 6 concludes the paper.

2. Related Work

NEMO Basic Support protocol is an extension of MIPv6 to support mobility for a whole Mobile Network (MN) that changes its point of attachment to internet, in such a way that session continuity is maintained transparently for every Mobile Network Node (MNN) within the MN. The MN is attached to the Home Network/Visited Network via Mobile Router (MR) to which an IPv6 Mobile Network Prefix (MNP) is delegated to advertise to MMNs inside the MN.

The MR has at least two interfaces: ingress (IIF) and egress (EIF). The IIF is configured with an IP from MNP whereas the EIF will be configured with the Home Address (HoA) when the MR is attached to the Home Network. This HoA is the permanent address of the MR used as an identifier. When the MN moves away from the Home Network and the MR attaches to a new Access Router (AR) belonging to the Visited Network, the MR acquires a temporal address called Care-of-Address (CoA) used as a locator with which it configures its EIF (Fig. 1).

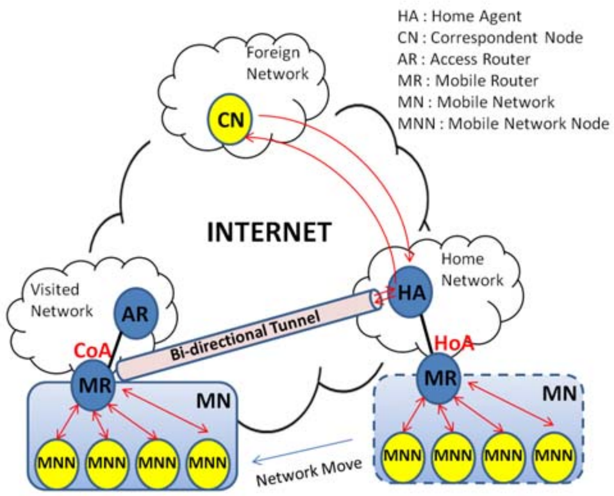

Fig. 1. NEMO Support Mobility

The NEMO protocol relies on a pair of Binding Update (BU) and Binding Acknowledgement (BA) messages exchanged between MR and its Home Agent (HA) to establish a bidirectional tunnel between them. All IPv6 traffic to and from MR is sent through this tunnel using IP-in-IP encapsulation.

When a MR attaches to a new AR and acquires a CoA, it sends a router BU (Mobile Router Flag (R) set) including MNP information to its HA. When the HA receives this Binding Update, it creates a cache entry binding the Mobile Router's HoA to its CoA. Then, if a successful BA is received the MR initiate the establishment of a bidirectional tunnel MR-HA. All packets exchanged between a MNN and a Correspondent Node (CN) in the Foreign Network pass through this tunnel.

The NEMO mechanism described above concerns only the simple case (1,1,1) i.e single MR, single HA and single MNP. Although its advantages compared to MIPv6, NEMO Basic Support still present weaknesses when dealing with multihomed networks. Some of the proposed methods to solve these problems are available in literature, but still there is considerable requirement of effort to build a powerful, secure and flexible solution.

Paik et al. [9] addressed many issues in multihomed NEMO and analyzed the influence of mobility on load sharing and session preservation when deploying multiple MRs. In [10], Cho and al. considered multiple MRs and HAs multihomed mobile networks to provide HA-based dynamic load sharing. A neighbor MR authentication and registration mechanism was also introduced. Choi et al. have proposed then a transparent failover mechanism (TFM) to provide seamless Internet services by introducing a “peer” relationship among the multiple MRs of the same NEMO [11]. Wang et al. [12] proposed the MULTINET approach: a policy-based multi-access support for NEMO multihoming using a single Mobile Router with multiple egress interfaces. This approach exploits the multiple care-of addresses extension (MCoA) [8]. A Host Identity Protocol (HIP) extension called HIP-NEMO was introduced by Novaczki et al. [13] to provide secure and efficient multihoming NEMO solution. Park et al. introduced in [14] a novel concept of a virtual mobile network in the context of multihomed NEMO based on single MR with multiple egress interfaces. The MR can advertise information of access networks to its subnet so that each MNN can select appropriate access network to forward the MNN's traffic. Recently, a solution to support multihoming in NEMO based on Proxy Mobile IPv6 (PMIPv6) [4] was proposed by Li et al. [15].

Although the improvement brought by these contributions to NEMO BS protocol, the multihoming issues are still open. Further design, implementation and evaluation are still needed for standardization. In the remainder of this paper, we investigate the (n,n,1) multihoming NEMO configuration and propose a new transparent and seamless approach to manage mobility and traffic at the Mobile Network level.

3. Multihoming Capabilities and Issues for the Configuration case (n,n,1)

When dealing with Multiple Mobiles Routers based multihomed NEMO, the choice of (n,n,1) multihoming configuration instead of (n,n,n) configuration is essential because of its capabilities to achieve multihoming benefits in a transparent fashion with respect to transport and application layers. In the (n,n,n) model, each MR has its MNP. There are two solutions for multihoming mechanisms. The first solutions use multiple encapsulation levels by considering a Nested Mobile Network model [16] and leave configured IP addresses unchanged (i.e there will be no change in already assigned IP addresses for MNNs). This leads to more complexity and relatively higher delays. Other solutions recommend configuring MNNs with new IP addresses from the MNP delegated to the substitute MR that will provide the new path to internet. Unfortunately, changing these addresses will cause more damages to applications. This is so because current applications and transport layers, such as TCP and UDP, identify the endpoints of a communication through the IP addresses of the nodes involved, implying that the IP addresses selected at the communication establishment time must remain invariant through the lifetime of the communication. So, any change in the source addresses will lead to a high latency and causes the re-establishment of the transport sessions. The (n,n,1) configuration however allows us to avoid these performance degradations.

Though, the mobility must be achieved in an optimized and a seamless fashion. In the (n,n,1) configuration , each MR independently maintains its own bidirectional tunnel. When a failure in the currently used path occurs, it must be detected, in order to change the tunnel that has failed. Hence mechanisms to detect failures and check tunnel keepalive are needed. On the other hand, once a failure in the currently used path is detected, alternative paths have to be explored in order to identify an available one.

Another issue that has to be solved is related to the optimization of the latency of these operations. Indeed, the overall delay to detect the failure of the current tunnel, discover and select others paths and configure one of them would be relatively high. Fast mechanisms are so needed.

Moreover, a mechanism to manage the distribution of outbound traffic for Load-Sharing and Policy-Routing is required.

4. Proposed Multihoming Mobility Support

To overcome the lack of multihoming support in NEMO BS, we introduce a new approach for network mobility by proposing a Router-Proxy as a central gateway inside the Mobile Network to perform mobility and traffic management and by using unidirectional HA-MR tunnel instead of bidirectional ones.

Furthermore, because of failure detection delay and multihoming operation, packets destined to the MN network may be delayed or lost during handoff period. To this end, we introduce other mechanisms to improve our solution.

4.1 Unidirectional HA-MR Tunnel

One of the main drawbacks of NEMO Basic Support that affect the efficiency of the protocol is the bidirectional tunnel. Indeed, the NEMO BS does not allow direct routing between MR and CN. Outbound traffic has to be sent to the HA first, and then forwarded to the CN, even when a much more efficient route exists between the CN and the MR. Sending outbound traffic via the MR-HA tunnel is not really necessary.

This triangular routing mechanism takes in general much more time than the direct routing because of the operations of encapsulation and decapsulation, leading hence to increased transmission delay. To overcome this weakness, we propose to use only a unidirectional tunnel from HA to MR for inbound traffic as illustrated in (Fig. 2). On the other hand, outbound traffic will be forward directly to the correspondent node using routing optimization. Obviously, this policy routing must be implemented at the Mobile Router level.

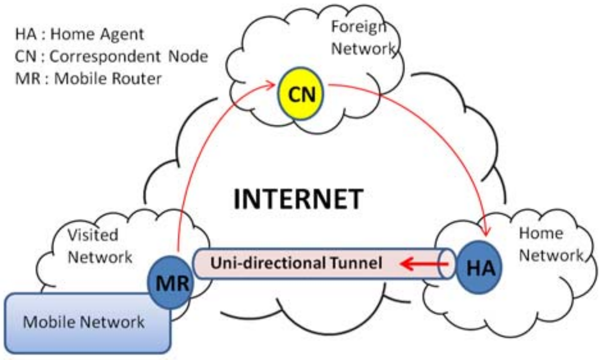

Fig. 2. MNN-CN Communication via Ha->MR Unidirectional Tunnel

4.2 Mobile Network Proxy (MNPx)

In our proposal, the Mobile Network Proxy (MNPx) will be the unique default gateway for all MNNs. All outbound traffic from MNNs as well as inbound traffic to MNNs must pass through MNPx. (Fig. 3)

A MN has one primary MR and one or more secondary MRs. The MNP delegated to the primary MR is also communicated to MNPx which has to advertise it to MNNs. Inside the MN, MRs can only communicate with MNPx and have not to communicate to each other nor to MNNs. Once a failure in the currently used path to Internet is detected one of the registered MRs that have already tunnels with the primary MR's Home Agent must replace the failed MR.

The MNPx has the exclusive responsibility to choose and to designate the substitute MR on the basis of information it holds about all MRs. As a result, we define in our approach two principal components to be implemented in the MNPx: (i) the Environment Detector Component and (ii) the Policy Decision Component which are detailed below.

4.2.1 Environment Detector Component

This component has the responsibility of detecting all the changes which could occur on the level of mobiles routers and from which some triggering events are created. At this stage, we are confronted with various problems: which information the Environment Detector should detect, how to get this information and how to use it. However, addressing all these issues is out of the scope of this paper. We focus here only on necessary information for Mobility/Traffic management purpose, especially those related to tunnel failure detection and access links capabilities.

At the MN level, the detection of tunnel failures between the primary MR's HA and MRs should rely on Router Advertisements from Access Routers to MRs, or other L2 trigger mechanisms to detect faults. The MR then transmits a notification about the failure to MNPx. However, this mechanism suffers enough from latency particularly when MR itself or its ingress interface fails.

To expect fast detection, we propose the use of a proactive keepalive test mechanism handled periodically by the Environment Detector. This latter performs at very short periods the keepalive test with all its MRs to see whether the established tunnels with the primary MR's HA are still alive. Likely, the Environment Detector should generate periodic requests to ask MRs for access links capabilities.
Information collected by the Environment Detector Component is automatically forwarded to the Policy Decision Component who must trigger consequently the appropriate events and update its *MR_Data Cache* (see Table 1).

4.2.2 Policy Decision Component

a) Mobility management

The main idea behind our proposal is, when possible, to register and establish tunnels in advance between each secondary MR and the primary MR's HA and use them when the primary MR fails or loses link connectivity. We point out here that all MRs belonging to the MN are registered at the MNPx (e.g. by physical addresses) and their ingress interfaces are IP configured by MNPx from the delegated MNP, so that they are easily authenticated.

MR_Data Cache at MNPx: MNPx maintains an information Cache (called MR_Data Cache) for all MRs belonging to the Mobile Network. Each entry in the MR_Data Cache Table contains the following fields:

MR field: the MR identifier (e.g. its ingress interface physical address)

MRType field: primary MR (1) or secondary MR (0)

HoA field: MR Home Address

CoA field: acquired CoA

Tunnel Status field: established (1) or not yet (0)

Active field: indicates whether the tunnel is active (1) at this time or not (0)

Other fields: Bandwidth, Packet Loss Rate and Round Trip Time (RTT) represent some necessary information about the actual access links that should be used for eventual traffic management.

Table 1 : MR_Cache Table at MNPx

MR	MRType	HoA	CoA	Tunnel Status	Active	Bandwidth	Packet Loss Rate	Round Trip Time (RTT)	Service Cost	Others Fields
MR1	1	HoA1	MR1 CoA	1	1					
MR2	0	HoA2	MR2 CoA	0	0					
MR3	0	HoA3	MR3 CoA	1	0					

b) Traffic management

Since several paths to internet through the different MRs will be available at the same time, path selection and load sharing can provided by the MNPx if necessary information of access networks is gathered by the Environment Detector. Then, on the basis of this information and user application preferences MNPx can select appropriate path to forward the MNN's outbound traffic independently from the downlink tunnels. In this paper, we focus only on mobility management. The traffic management issue will be addressed in further work.

4.3 Multihoming Mobility Mechanisms

Let us consider the example of (Fig. 3) where MR1 is the primary MR. Assume that the secondary MR3 has obtained a CoA and established a tunnel with its Home Agent HA3. MR3 then notifies MNPx with an authenticated message including the MR3 home Address HoA3, the acquired CoA and a Nonce (a random integer) used as a return routability check, instead of using the long return routability procedure of IPv6.

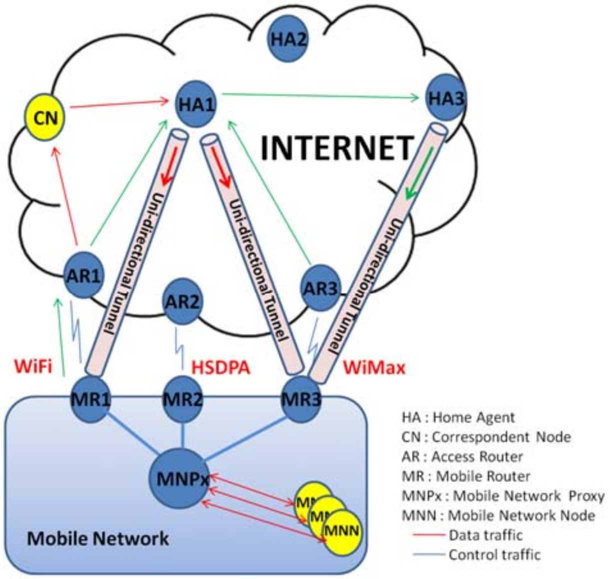

Fig. 3. Principe of the MNPx based Support Mobility

MNPx first updates MR_Data cache entry for MR3 then it communicates information sent by MR3 to MR1 and orders it to request its Home Agent HA1for registering MR3 as a substitute for MR1. Then MR1 sends to HA1 a substitute registration request message including the information it receives from MNPx. On receiving this message, HA1 sends an invitation message to MR3 to register. This message includes the MNP of MR1, the MR3's Nonce and another Nonce generated this time by HA1. The message arrives at MR3 via its Home Agent HA3. MR3 checks the validity of the message, if so it replies to HA1 with a substitute Binding Update (SBU) message including the acquired CoA, MNP and HA1's Nonce. After checking the validity of this message, HA1 then register MR3 as a substitute for MR1 in its binding cache and sends a Binding ACK to MR3.

To provide fast handover, a unidirectional tunnel between HA and MR3 is established in advance and will be used when needed. Then, HA1 sends a notification message to MR1 to inform it that MR3 has been registered as a substitute. This information is immediately forward to MNPx which consequently updates its MR_Data Cache. This procedure is illustrated at (Fig. 4).

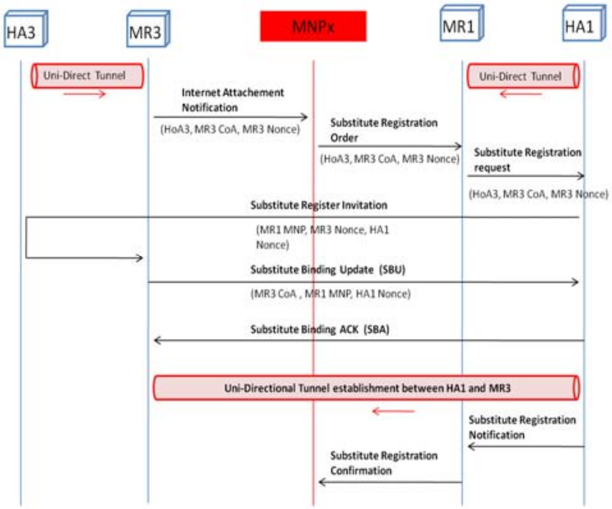

Fig. 4. Substitute MR Registration

4.3.1 Change in BU Message Format

A new MR Type Flag (T) is included in the Binding Update (Fig. 5) to indicate to the Home Agent whether the Binding Update is coming from a primary Mobile Router or a secondary Mobile Router. The BU message must include also another field for the HA1's Nonce value.

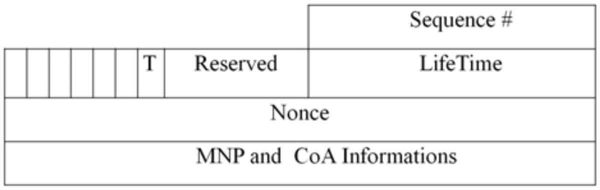

Fig. 5. Substitute BU Message Format

4.3.2 Change in Binding Cache Table at HA1

With MIPv6 basic support [1], a Mobile Node can register only one CoA with its HA. Hence, the registration of multiple CoAs with a single HoA is not possible. To accommodate multiple binding registrations at the HA1, we modify the binding cache structure of the HA1 to take into account information about possible substitute Mobile Routers. We add three fields (Table 2):

- MR-type Field: indicates whether the registered MR is a primary MR (value set to 1) or a secondary one (value set to 0).
- Tunnel Field: indicates whether this tunnel is active (opened) or not (closed).
- ExpireTime: indicates the time at which this tunnel is considered unavailable. The value of this field is obtained by the following equation (1):

  ExpireTime = CurrentTime + LifeTime (1)

Table 2: Binding Cache Table at HA1

Prefix	CoA	MRType	Tunnel	ExpireTime
MNP	MR1 CoA	1	Opened	-
MNP	MR3 CoA	0	Closed	-
---	---	---	---	---

4.3.3 Transparent and Seamless Session Continuity

When the MNPx detects the MR1 failure by means of the Environment Detector Component, it immediately looks in its MR_Data Cache for the available substitute MRs (Tunnel status = 1), chooses one according to a predefined policy and orders it to request HA1 to open the associated tunnel. Let's again consider the example of (Fig. 3). Assume that MNPx chooses MR3 to replace the failed MR. MR3 requests HA1 to open its tunnel for traffic destined to the MN indicating a MR1 failure. On receiving this message, HA1 opens the HA1-MR3 tunnel through which traffic destined for the MN is immediately forward. HA1 will use both HA1-MR1 and HA1-MR3 tunnels simultaneously until it confirms that MR1 has failed. HA1 will use a special check procedure to see whether MR1 is alive or not (this test include the path until MNPx). If MR1 has effectively failed, HA1 removes the MR1 entry from its binding cache Table, otherwise it maintains the HA1-MR1 tunnel opened and closes the HA1-MR3 tunnel. Except if a routing policy is implemented at HA1, this latter should always forward incoming packets toward the MN, in priority through the tunnel established with the primary MR.

We propose that HA1 maintains a copy of the last forwarded packets toward the MN (the size of this cache depends on the overall delay for tunnel change operation (failure detection, choice of the substitute MR and tunnel change request). When, HA1 receives a tunnel change request, it will retransmit them through the new tunnel. Thus, no packet loss can be achieved.

Since we do not use any tunnel for outbound traffic, on MR1 failure the outbound traffic is immediately and directly routed by the selected substitute MR without being buffered. However, a cache of the last forwarded packets by The MNPx will also prevent packet loss delay.

Thus, MNNs are not involved in this process and the transparency is guaranteed.

5. Performance Evaluation

Simulation experiments were performed using the network simulator NS-2 [17] with Mobiwan [18] extensions to evaluate the performance of our proposed mechanisms in terms of handover latency and packet loss. Our results are compared to the NEMO BS solution.

We implemented the MNPx based mobility support within NS-2 by creating new three types of Agent inheriting from Agent class: ProxyPolicyAgent, MRMobilityAgent and HAMobilityAgent. In our simulation, a MNPx is a Node attached with a ProxyPolicyAgent, a MR is a Node attached with a MRMobilityAgent and a HA is a Node attached with a HAMobilityAgent.

5.1 Simulation Topology and Parameters

(Fig. 6) describes our simulation network topology. According to Mobiwan extensions we have created a Wide Area IPv6 network that represents the core of internet and two Base Stations BS1 and BS2 to be used as Access Routers. The Mobile Network consists of four 802.11

mobile nodes: two Mobile Routers, MR1 as primary and MR2 as secondary, the proxy MNPx and a MNN (A). The protocol AODV was used, although any routing protocol can be used. The wireless transmission range was set to 100 m. The topology is designed in such a way that BS1 can reach only MR1, BS2 can reach only MR2, and MNPx covers all mobile nodes inside the MN, but no one of the mobile nodes can reach the others.

The simulation time was set to 60 seconds. We create a CBR traffic source and attach it to a UDP agent at the Correspondent Node (B) level. This traffic is directed from B toward A at the data rate of 200Kbps. Packet size was set to 1500 bytes. Internet latency is supposed random following a uniform distribution in the interval [50ms, 250 ms]. We start the simulation with the tunnel established with MR1. At t= 20 s, we intentionally make MR1 failure and reactivate it at t=40 s.

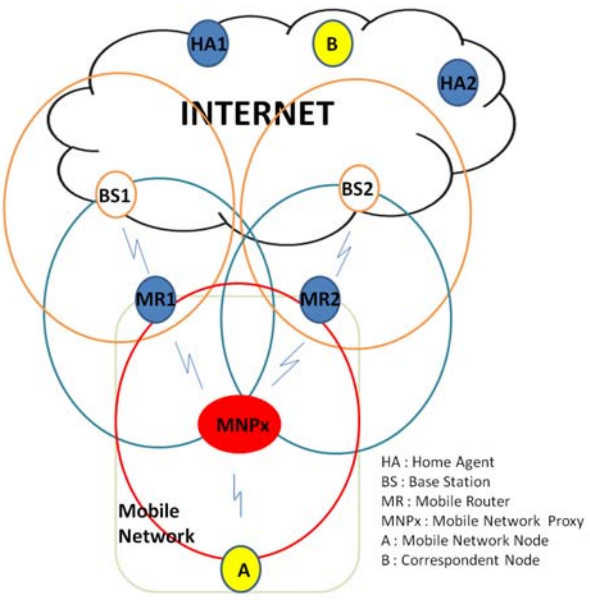

Fig. 6. Proposed Simulation Topology

5.2 Simulation Results

We first compare the performance of our proposed MNPx based support to NEMO BS. (Fig.7) show measured throughput at node A. Because of the lack of multihoming support, at t=20s once MR1 fails the throughput for NEMO BS falls to zero and stay equal to zero until the MR1 is again registered. Notice that even if MR1 is activated at t=40s few seconds are needed before the tunnel is again available.

However, in MNPx based support, the substitute mobile router MR2 provides an alternative tunnel almost immediately after detecting the failure achieving hence a seamless Internet service. The multihoming Handoff is performed in less than one second. This delay can also be improved by a good parameter setting of keepalive test period.

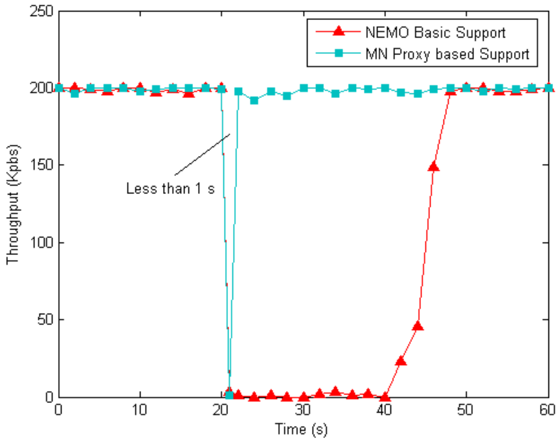

Fig. 7. Throughput over time (Failure Detection Delay=500 ms)

In the second simulation experiment we examine the impact of Failure Detection Delay (FDD) and Last Forwarded Packet (LFP) cache size on Packet Loss. It was observed that Packet Loss increases with FDD and decreases with LFP (Fig. 8). Packet Loss can be totally eliminated if these parameters are rightly configured.

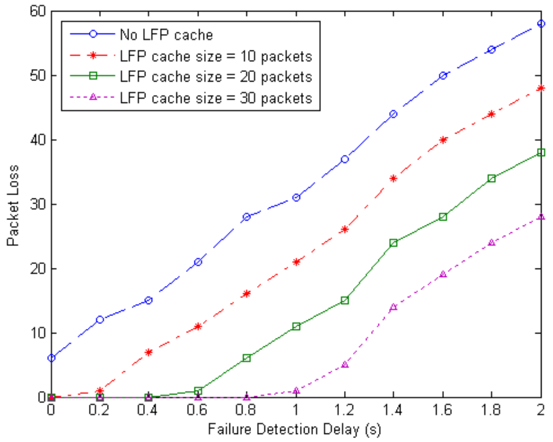

Fig. 8. Packet Loss vs Failure Detection Delay (vs LFP cache size)

6. Conclusion

In this paper, we have proposed a novel network mobility support in the context of (n,n,1) model based multihomed NEMO networks. Our approach uses MRs registration at the Home Agent delegating the Mobile Network Prefix and beforehand establishment of unidirectional tunnels. We introduced also a Mobile Network Proxy to manage mobility and outbound traffic at the mobile network level.

Simulation results show that our proposition provides excellent performance in terms of Handoff delay and Packet Loss. Our improving mechanisms for the proposed architecture are very efficient and make it possible to achieve a really transparent and seamless connectivity as well as routing optimization.

References

[1] D.Johnson, C.Perkins, and J.Arkko, "Mobility Support in IPv6," IETF, RFC 3775, June 2004.

[2] H. Soliman, C. Castelluccia, K.-E. Malki, and L. Bellier, “Hierarchical mobile IPv6 mobility management,” IETF, RFC 4140, Aug. 2005.

[3] R. Koodli, Ed."Fast Handovers for Mobile IPv6", IETF, RFC 4068, July 2005.

[4] S. Guidiville, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil (2008). “Proxy Mobile IPv6,” IETF, RFC 5213, August 2008.

[5] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," IETF, RFC 3963, January 2005.

[6] N. Montavont, T. Noel and T. Ernst, "Multihoming in nested mobile networking," SAINT 2004 Workshops on 26-30 Jan. 2004 Page(s):184 – 189.

[7] C. Ng, E. Paik, T. Ernst, M. Bagnulo, “Analysis of Multihoming in Network Mobility Support,” IETF, RFC 4980, October 2007.

[8] R. Wakikawa, V. Devarapalli, G. Tsirsis and T. Ernst and K. Nagami, "Multiple Care-of Addresses Registration," IETF, RFC 5648, October 2009.

[9] E. K. Paik, H. S. Cho, T. Ernst and Y. H. Choi, "Load sharing and session preservation with multiple mobile routers for large scale network mobility," The proceedings of AINA 2004: Page(s):393 - 398 Vol.1.

[10] S. H. Cho, J. K. Na and C. K. Kim, "A dynamic load sharing mechanism in multihomed mobile networks," ICC 2005 16-20 May 2005 Page(s):1459 - 1463 Vol. 3.

[11] N. Choi, J. Ryu, E. Paik, T. Kwon, and Y. Choi, Senior, “A Transparent Failover Mechanism for a Mobile Network with Multiple Mobile Routers”, IEEE COMMUNICATIONS LETTERS, VOL. 11, NO. 7, JULY 2007.

[12] Q. Wang, R. Atkinson, and J.Dunlop, “Towards Always Best Connected Multi-Access: the MULTINET Approach”, IWCMC '08. August 2008.

[13] S. Novaczki, L. Bokor, G. Jeney, and S. Imre, “A HIP based network mobility protocol,” JOURNAL OF NETWORKS, VOL. 3, NO. 1, JANUARY 2008

[14] C. Park, N. Choi, E. Paik, T. Kwon and Y. Choi, “Multiple Interface/Prefix Selection for Virtual Mobile Networks”, ICACT, February 2008

[15] Y. Li, D. Kum, and Y. Cho, “Multihoming Support Scheme for Network Mobility Based on Proxy Mobile IPv6”, ISECS International Colloquium ICCCM’08, August 2008.

[16] N. Montavont, T. Ernst, and T. Noel, “Multihoming in Nested Mobile Networks”, In International Symposium on Applications and the Internet (SAINT)-IPv6: Technology and Deployment Workshop”, Tokyo, January 2004.

[17] The Network Simulator manual, The NS2 homepage http://www.isi.edu/nsnam/ns

[18] T. Ernst. MobiWan: NS-2 extensions to study mobility in Wide-Area IPv6 networks http://www.inrialpes.fr/planete/mobiwan/

Zohra Slimane received her Engineering Diploma in Telecommunication in 2006, and her Magister Diploma in SRT Telecommunication Systems and Networks in 2008 from Tlemcen University (Algeria). Since 2008, she has been a system engineer at Sonatrach Aval Research Group and a PhD student researcher at STIC Laboratory (Tlemcen Algeria). Her research interests include networking, information systems, mobile networks, ubiquitous internet and fourth-generation networks.

Mohammed Feham received his Dr. Eng. degree in optical and microwave communication from the University of Limoges (France) in 1987, and his PhD in Science from the University of Tlemcen (Algeria) in 1996. Since 1987, he has been an Assistant Professor and Professor of microwave and communication engineering. He has served on the Scientific Council and other committees of the Electronics and Telecommunication Departments of the University of Tlemcen. His research interests include telecommunication systems and mobile networks and services.

Abdelhafid Abdelmalek received the Laurea degree in Telecommunication Engineering from Institute of Telecommunications Oran (Algeria) in 1991, and Diploma of deepened studies in optoelectronic at Nancy (France) in 1993. From 1994 to 2000, he worked as engineer in charge of design and management of ISDN networks at Algerie Telecoms Company. In 2002, he received a Magister Diploma in Signals and systems at Tlemcen University, Algeria. From 2004, he is a PhD researcher. His research interests include data communications, Mobile networks, security, protocols and next generation networks.