ISSN No. 0976-5697

Volume 1, No. 3, Sept-Oct 2010

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

# An Analysis on QoS of Network Mobility

Dinakaran M*
Assistant Professor, School of IT & Engg,
VIT University, Vellore,
Tamil Nadu, South India
dinakaran_vit@yahoo.com

Dr. P. Balasubramanie
Professor, Department of Computer Science,
Kongu Engineering College, Perundurai,
Erode, South India.
pbalu_20032001@yahoo.co.in

***Abstract:*** Technology demands uninterrupted ubiquitous Internet access in mobile nodes. NEMOWG (NEtwork MObility Workging Group), a new working group in IETF (Internet Engineering Task Force) is formed to provide mechanisms to manage the mobility of a network as a whole, enabling that network to change its point of attachment to an IP-based fixed infrastructure without disturbing the ongoing communications or sessions through the Network Mobility (NEMO) protocol. Significant performance criteria's like handoff, route optimization and security threats degrades the performance of the NEMO basic support protocol, because each has its own demerits. This article focuses on an analysis of QoS of network mobility with respect to the above criteria's.

***Keywords:*** Mobile IP**,** NEMO**,** Network Mobility, QoS of NEMO

## I. INTRODUCTION

Since mobility and ease of connection are crucial considerations for mobile device users, organizations that want to promote mobile communications are putting a great *deal of effort into making mobile connection uncomplicated* for the user. Mobile nodes are devices that are capable of connecting to the Internet from a variety of different points of entry. The benefit of this type of Internet-connected device is that persons who are on the go may establish a connection to the Internet from a wide range of locations. This kind of node is often a cellular telephone or handheld or laptop computer, although a mobile node can also be a router. Special support is required to maintain Internet connections for a mobile node as it moves from one network or subnet to another, because traditional Internet routing assumes a device will always have the same IP address. Therefore, using standard routing procedures, a mobile user would have to change the device's IP address each time they connected through another network or subnet. Internet Engineering Task Force (IETF) Mobile IP working group has developed several standards or proposed standards to address these needs, including Mobile IP and later enhancements, Mobile IP version 6 (MIPv6) and Hierarchical Mobile IP version 6 (MHIPv6) [11]. NEMO Basic Support protocol is an extension of the Mobile IP.

## II. NEMO BASIC SUPPORT PROTOCOL

The IETF has been working for the problems in terminal mobility; the NEMO group in IETF comes up with IP layer solutions for both IPv4 and IPv6 that enable the movement of terminals without stopping their ongoing sessions [1]. These solutions are even being completed with proposals that improve the efficiency of the base solution, particularly in micro mobility environments. The issue of terminal mobility has been analyzed recently in [2].

NEMO stands for Network Mobility. It manages the mobility of the entire network which changes its point of attachment to another network, and then connects the home network through the internet. The mobile network includes one or more mobile routers which connect it to global Internet. Mobile network is assumed to be a leaf network, i.e. it will not carry transit traffic. However, it could be multihomed, either with a single MR that has multiple attachments to the Internet or by using multiple MRs that attach the mobile network to the Internet. In NEMO only the MR will be aware of the movement of the network. Thus nodes, which are unaware of the movement of the network, are accommodated under MR, which is aware to the mobility of the network [3]. Each Mobile Router must have a Home Agent; this is the basic requirement for supporting network mobility. A bidirectional tunneling between MR and HA helps in preserving the continuity of the session while the MR moves. The MR will acquire a Care-of-address from its attachment point i.e. the Foreign Agent. Each MR will appear to its attachment point as a single node; this approach allows nesting of mobile networks. Figure 1 gives a view of NEMO.

*Terminology*

The following definitions are important for understanding the basics of Mobile IP and NEMO.

Home Network (HN): Network that a Mobile Network belongs to when it is not roaming. i.e. the network that is associated with the network link of the Home Agent.

Mobile Network (MN): A sub network of the home network, which can be mobile as a whole.

Home Agent (HA): Host on the Home Network that enables the Mobile Router to maintain connectivity with the Home Network.

Mobile Router (MR): A router capable of changing its point of attachment to the Internet without disrupting higher layer connections of attached devices.

Visited Network / Foreign Network: A network which provides connectivity to the MN through MR and Access Router.

Access Router (AR): Router that provides connectivity to a Mobile Router from Visited Network.

Care-of Address (CoA): IP address of Mobile Router at its current Internet attachment point(AR).

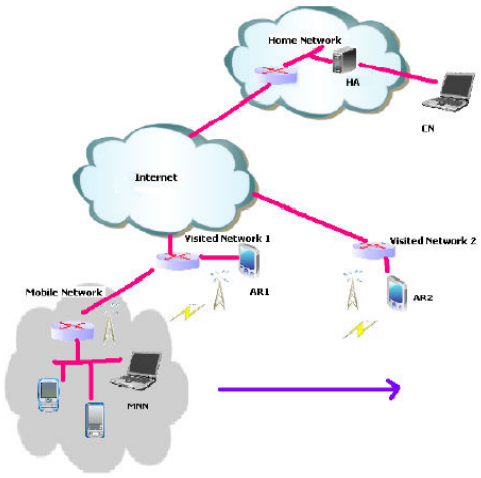


Figure 1 - NEMO

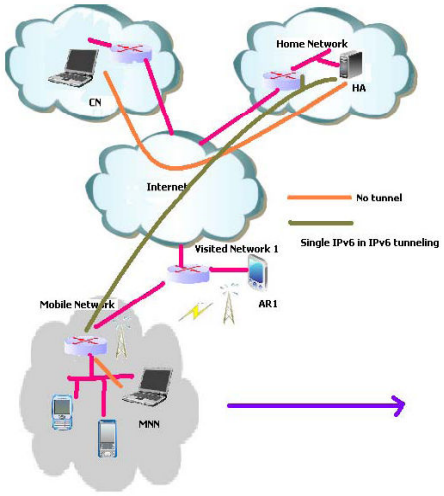


Figure 2 – NEMO Operation

Correspondent Node (CN): An external IP device that is communicating with Mobile Network Node.
Mobile Network Node (MNN): Any IP device on a mobile network. Mobile Network Nodes may be fixed to the mobile network or visiting the mobile network as mobile nodes. MNNs do not need to be aware of the network's mobility.

## III. OPERATION OF NEMO

If the MR moves away from the home link and attaches to a new AR, it acquires CoA from the visited link. As soon as the MR acquires a CoA, it immediately sends a Binding Update (BU) to it's HA. When the HA receives this BU, it creates a cache entry binding the MR's Home Address to its CoA at the current point of attachment, so that the HA can forward packets meant for nodes in the MN to the MR. The HA acknowledges the BU by sending a Binding Update Acknowledgement (BUA) to the MR. Once the binding process finishes, a bi-directional tunnel is established between the HA and the MR. The tunnel end points are the MR's Care of Address and the HA's address.
When an external node CN sends a message to MNN it's acquired by HA, then HA will encapsulate the packet and forward the same to MR through the bi-directional tunnel. The MR decapsulates the packet and forwards it through the interface where the MNN is connected. Before decapsulating the tunneled packet, the MR has to check whether the source address on the outer IPv6 header is the Home Agent's address. This check is not necessary if the packet is protected by IPsec in tunnel mode. The MR also has to make sure that the destination address on the inner IPv6 header belongs to a prefix used in the MN before forwarding the packet to the MNN. If it does not, the MR should drop the packet. If a packet with source address belonging to the Mobile Network Prefix (MNP) is received from the MNN, the MR reverse tunnels the packet to the HA. This reverse tunneling is done by using IP-in-IP encapsulation. The HA decapsulates this packet and forwards it to the CN. Figure 2 shows the NEMO operation.

The MN could include nodes that do not support mobility and nodes that do. A node in the Mobile Network can also be a fixed or a Mobile. The protocol described here ensures complete transparency of network mobility to the nodes in the Mobile Network. Mobile Nodes that attach to the Mobile Network treat it as a normal IPv6 access network and run the Mobile IPv6 protocol. The MR and the HA can run a routing protocol through the bi-directional tunnel; In this case, the MR need not include prefix information in the Binding Update. Instead, the HA uses the routing protocol updates set up forwarding for the Mobile Network. When the routing protocol is running, the bi-directional tunnel must be treated as a tunnel interface. The tunnel interface is included in the list of interfaces on which routing protocol is active. The MR should be configured not to send any routing protocol messages on its egress interface when it is away from the home link and connected to a visited link. Finally, the HA may be configured with static routes to the Mobile Network Prefix via the MR's Home Address. In this case, the routes are set independently of the binding flows and the returning home of a MR. The benefit is that such movement does not induce additional signaling in the form of routing updates in the home network. The drawback is that the routes are present even if the related MR's are not reachable (at home or bound) at a given point of time. The CN transmits an IP data gram destined for MNN-A. This datagram carries as its destination addresses the IPv6 address of MNN-A, which belongs to the MNP of the NEMO. This IP data gram is routed to the home network of the NEMO, where it is encapsulated inside a new IP datagram by a special node located on the home network of the NEMO, called the HA. The new datagram is sent to the CoA of the MR, with the IP address of the HA as source address. This encapsulation preserves mobility transparency (that is, neither MNNA nor the CN are aware of the mobility of the NEMO) while maintaining the established Internet connections of the MNN. The MR receives the encapsulated IP datagram, removes the outer IPv6 header, and delivers the original datagram to MNN-A. In the opposite direction, the operation is analogous. The MR encapsulates the IP datagram's sent by MNN□A toward it's HA, which then forwards the original datagram toward its destination (that is, the CN). This encapsulation is required to avoid problems with ingress filtering, because many routers implement security policies that do not allow the forwarding of packets that have a source address that appears topologically incorrect.

Additionally, mobile networks can be nested as shown in figure 3. A mobile network is said to be nested when it attaches to another mobile network and obtains connectivity through it. The inefficient routing model that occurs in Nested NEMO Networks is commonly referred to as "Pinball Routing" [6].

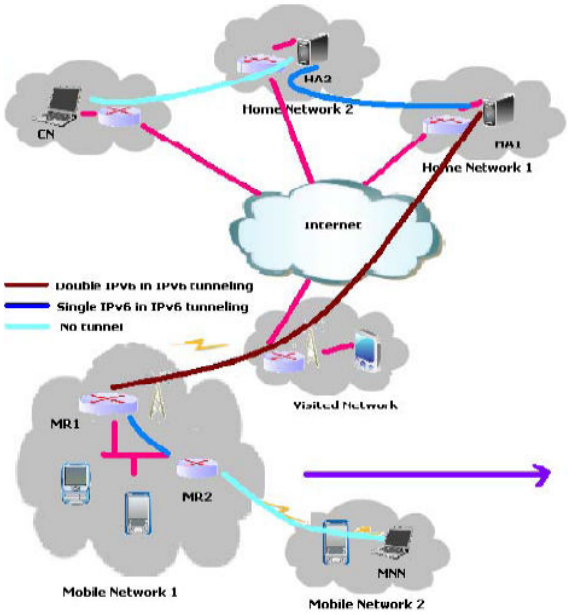


Figure – 3 – Nested NEMO

## IV. QOS ANALYSIS

The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results. We are considering the following parameters for NEMO.

*Routing* We discussed the routing operation of NEMO in the earlier section. Incase of NEMO, the bi-directional tunnel acts as the bridge between the CN and MNN, however it has its own merits and demerits.

*Merits:*

*Transparency:* In NEMO a bi-directional tunnel has to be established between the HA and the MR before the communication, which provides transparency between the CN and MNN, that is either the CN or the MNN is aware of the intermediate nodes through which the packets passes.

*Security*: All the communication between the correspondent node and the mobile network node has to pass only through MR-HA tunnel ensuring authentication such that only the secured nodes can send information to the nodes in the mobile network. NEMO uses the technique of ingress filtering, which prohibits an attacker within the network from launching a flooding attack using forged source addresses that do not confirm to ingress filtering rules. NEMO uses strict traffic filtering routing, that prohibits traffic which originates from outside of the network. Another advantage of implementing this type of filtering is that it enables to easily trace the true source where the packet originated by using the mobile network prefix, this provides authentication for the mobile networks [5].

Demerits

Given the NEMO Basic Support protocol, all data packets to and from Mobile Network Nodes must go through the HA, even though a shorter path may exist between the MNN and its CN. In addition, with the nesting of MRs, these data packets must go through multiple HA's and several levels of encapsulation, which may be avoided. This results in various inefficiencies and problems with packet delivery, which can ultimately disrupt all communications to and from the Mobile Network Nodes. The following are the significant limitations of NEMO Basic Support,

1) Sub-Optimality with NEMO Basic Support: With NEMO Basic Support, all packets sent between a Mobile Network Node (LMN or LFN) and its CN is forwarded through the MRHA tunnel, resulting in a pinball route between the two nodes.

2) Bottleneck in the Home Network: Apart from the increase in packet delay and infrastructure load, forwarding packets through the HA may also lead to either the HA or the Home Link becoming a bottleneck for the aggregated traffic from/to all the MNN. Congestion at home would lead to additional packet delay, or even packet loss. In addition, HA operations such as security check, packet interception, and tunneling might not be as optimized in the HA software as plain packet forwarding. This could further limit the HA capacity for data traffic.

3) Amplified Sub-Optimality in Nested Mobile Networks: By allowing other mobile nodes to join a mobile network, and in particular MR, it is possible to form arbitrary levels of nesting of mobile networks. With such nesting, the use of NEMO Basic Support further amplifies the sub optimality of routing.

4) Security Policy Prohibiting Traffic from Visiting Nodes: NEMO Basic Support requires all traffic from visitors to be tunneled to the MR's HA. This might represent a breach in the security of the Home Network Administrators might thus fear that malicious packets will be routed into the Home Network via the bidirectional tunnel

*Handoff:* Whenever a Mobile Router moves from one access network to another access network, it has to obtain a new CoA from AR and register this CoA with it's HA. There are two methods of solving this, router advertisement and router solicitation. In both methods the MR eventually receives a new CoA from the new access router. MR has to register the new address with the HA. To register, a request message is sent by the MR to the HA, the methods the MR eventually receives a new CoA from the new access router. MR has to register the new address with the HA. To register, a request message is sent by the MR to the HA, the HA then replies with a registration reply message. After this binding, a bi-directional tunnel is established. The process of dealing with the movement of the MR to a new access network is called a handoff. To support the mobility of nodes NEMO has implemented various handoff mechanisms [10]. Some of the criteria's related to hand off are discussed here.

.The total latency is the sum of the address gathering latency and the registration latency. The address latency is the time taken to detect the movement of the MR and time taken to obtain a new CoA from the access network [9]. The registration latency represents the time it takes to send the binding update message to the HA and to receive the binding acknowledgement from the HA.

*Scalability:* A handoff mechanism with good scalability can handle a large amount of hosts at the same time, without severely affecting the overall performance. The total amount of traffic generated by the mechanism must be less, so that the scalability can be better.

*Latency:* The delay that occurs during handoff is called as handoff latency. This latency is made up of several factors. of traffic generated by.

*Packet loss:* An important objective for many hand off mechanisms are to reduce the amount of packet loss that

occurs during a handoff. Packet loss can occur during or after the actual movement of the mobile host.

*Packet reordering:* Packet reordering can occur when the MN is connected to a new AR and receives packets that are forwarded from the old AR. In most situations this criterion is closely related to the aforementioned criterion, the occurrence of packet loss.

*Throughput:* In communication networks throughput is referred to as the average rate of successful message delivery over a designated channel. It is measured as data packets per time slot usually in bits per second. Bandwidth is referred to as the amount of data carried from one device to another device in a given period of time. It is usually measured as bits per second (bps) or bytes per second (Bps). However it represents the capacity of data that can be carried in a particular link. NEMO poses few restrictions over bandwidth since in wireless networks it is difficult to send large packets over time. This bandwidth is limited by the bi-directional tunnel which doesn't admit larger data to be transmitted [9]. Incase of NEMO throughput depends on source processing delay, transmission delay, packet processing delay and the limited bandwidth of the network.

*Error Rate:* In digital transmission bit error rate is defined as the number of received bits that have been altered due to noise or distortion to the total number of bits transferred during the given time interval. It is defined as the number of incorrectly transferred data packet to the total number of packets transferred. Error rate defines the degree of errors encountered during a communication. When error rate is high the communication becomes less reliable. Concerning NEMO errors usually occur during handoffs where there are chances for packet loss [5]. Some handoff mechanisms like fast handoff and simultaneous binding mechanisms allow the same packet to be buffered in several routers leading to multiple delivery of the same packet. This results in error leading to inefficiency of NEMO.

*Jitter:* The term jitter refers to the measurement of variability over time of the packet latency across a network. It is defined as the deviation from the network mean latency known as Packet Delay Variation (PDV). The main cause of jitter is due to large packet overhead leading to delay in packet processing and delivery. Incase of nested NEMO a mobile router contacts another mobile router to access internet leading to establishment of several tunnels and numerous encapsulations for a single packet delivery. This type of packet encapsulation in MR-HA tunnels add to packet overload since each encapsulation adds 40 bytes of header to the original datagram leading to inefficient usage of bandwidth [8]. Incase of simple voice application like VoIP which takes a voice sample for every 20 milliseconds, each encapsulation adds 320 bits per packet which is thrice the actual payload. This increases the processing delay for each packet leading to occurrence of jitters.

*Security Threats:* In NEMO the security mechanisms are needed to ensure secured packet transmission between the Correspondent Node and Mobile Network Node. The Binding Update provides authenticity and integrity to the packets therefore incorrect Binding Update can lead to malicious attacks such as traffic hijacking or denial of service. IPsec Transport ESP is used to protect the binding update messages between HA and MN/MR. IPsec provides strong cryptographic components under its architecture. Mobile IP and NEMO are network layer protocols which are built on top of the security strength of IPsec. IPsec is quite secure, but it is not properly glued with the rest of the system so that the whole system (such as the MR in NEMO) can be easily attacked by the attackers. The components putting packets into the IPsec module may not be doing its job perfectly secure. Basic threats to NEMO BS are classified into three different categories [4],

1) Threats on the tunnel between MR and HA
2) Threats on the path among multiple MRs
3) Threats to the MR and HA themselves.

Some ways to provide security using IPsec are

1) The IPsec AH/ESP security mechanisms are activated on MR-HA tunnels.
2) No compromise of the prefix and binding cache tables in HA.
3) No compromise of critical information like MNP and HoA on MR.
4) Multiple HAs have their own trust relationships provided by ISP.
5) No current security mechanisms are applied among multiple MRs.

*Threats on interaction between MR and HA:* Packets transmitted using tunnel can be forged using fake source and destination address. The MR or HA should be responsible to verify the validity of those packets. Two attacks are possible in the MR-HA IPsec Transport SA as referred in [4]. They are

1) BU spoofing attack: no ingress filtering at MR
2) BU spoofing attack: with ingress filtering at MR

*Modifications of the signaling messages:* Some part of the signaling messages between MR and HA are delivered in clear text. Attackers may modify the destination address in the signaling messages between MR and HA. This mis-destined message shall be dropped at the destination. Another type of attack is by modifying the flag option bit (R) which leads to incorrect processing of signaling messages; this is better described in [7].

*Threats on interactions among multiple MR's:* In multi homing, where two or more MR exists, several bi-directional paths are established to forward packets to a HA or multiple Has as proposed in [7]. If one of the tunnel path of MR1 is broken, then the MR1 finds an alternative path through MR2 and becomes nested. A malicious MR may advertise a RA with a fake CoA to MR1. Then the MR1 will get wrong CoA information.

*DoS attack to MR or HA:* Attackers can initiate packet flooding attack to MR or HA using the MR-HA tunnel. IP-in-IP packets with topologically correct address to avoid ingress filtering are flooded from outside to their access routers. HA or MR have to filter this type of packets thus leading to denial of service to other essential packets.

## V. CONCLUSION

This document presents an analysis over the Quality of Services provided by the NEMO Basic Support protocol. Though NEMO enhances the concept of mobility of the network, it has its own sub-optimality's. Based on the analysis report it is recommended that the field of route optimization, handoff mechanism and security issues implemented in NEMO must be enhanced for fast, easy and secure delivery of packets.

## VI. ACKNOWLEDGEMENT

We thank Dr. R.S.D. Wahida Banu and Dr.S.P.Shantharajah for giving their valuable suggestions to prepare this article.

## VII. REFERENCES


[1] Antonio De La Oliva , Bernardos C J, Dirk von Hugo, Holger Kahle, "NEMO: Network Mobility. Bringing ubiquity to the Internet access" , IEEE Infocom, April 2006

[2] J. Mangues, A. Cabellos, R. Serral, J. Domingo, Gómez, T. de Miguel, M. Bagnulo. A. García. "IP Mobility: Macromobility, Micromobility, Quality of Service and Security," UPGRADE, Vol. 5 (1), pp. 49-55, February 2004.

[3] Ben McCarthy, Matthew Jakeman, Dr Chris Edwards, Pascal Thubert , "Protocols to Efficiently Support Nested NEMO (NEMO+)", MobiArch 2008, August 2008, pp. 43-48

[4] Souhwan Jung, Fan Zhao, S. Felix Wu, "Threat Analysis on NEMO Basic Operations", IETF, July 2004, http://tools.ietf.org/html/draft-jung-nemo-threat-analysis-02

[5] Lorchat, Jean and Kuntz, Romain (Keio), "Evaluation of NEMO Communications Using Hybrid Measurement", 6th International Conference on ITS Telecommunications (ITST), Chengdu, China, June 21st-23rd 2006

[6] Pekka Paakkonen, Milka Rantonen and Juhani Latvakoski, "Integration of Network Mobility approach in a heterogenous environment", Med-Hoc-Net 2004, pp 57-67

[7] Gloria Tuquerres, Marcos Rogerio Salvador and Ron Sprenkels, "Mobile IP: Security and Applications"

[8] Fayza Nada, "Performance Analysis of Mobile IPv4 and Mobile IPv6", The International Arab Journal of Information Technology, Vol.4 (2), April 2007.

[9] Ignacio Soto, Carlos J.Bernardos, Maria Calderon and Albert Banchs, "NEMO enabled Localized Mobility Support for Internet Access", IEEE Communications Magazine, Vol. 47 (5), pp 152-159, May 2009.

[10] Niesink, L.D.J, "A comparison of mobile IP handoff mechanisms", 6th Twente Student Conference on IT, Feb 2007, Track A.

[11] Paul Moceri, "Enabling Network Mobility: A Survey of NEMO", http://www.cse.wustl.edu/~jain/cse574-06/ftp/network_mobility/