A Routing Technique for Visiting Mobile Nodes in NEMO

M. Dinakaran
Assistant Professor
School of IT & Engineering,
VIT University, South India

Dr. P. Balasubramanie
Professor
School of Computer Tech & Applications
Kongu Engineering College, Erode

ABSTRACT

The success of mobile communication, shows that the interest in users to access the Internet or their official networks on the move. This mobility support may be needed for a single user or group of nodes called as movable sub networks. Network Mobility (NEMO) protocol developed by IETF enables the mobile nodes and networks to maintain connectivity to their network or Internet by change their point of attachment to from one access network to another. NEMO is an extension of Mobile IPv6, this works based on tunneling the data from home agent to mobile router. Though the tunneling process ensures the security of data it leads to suboptimal routing, packet overhead, latency, drops and these demerits are amplified when the networks are nested. Apart from these demerits, NEMO protocol fails to give a shortest routing path when the external node visits the sub network for communication. This article proposes an optimized routing path between visiting mobile node and local fixed or mobile node. The proposed routing technique is implemented through NS2 simulation environment and the result proves that the proposed system is efficient.

Keywords

Visiting Mobile Nodes, Mobile IPv6, NEMO, Route Optimization.

1. INTRODUCTION

The demand for Internet access in heterogeneous environments is keeps on increasing, especially in mobile platforms such as trains, buses. The request for connecting with Internet on the move is for entertainment, some times to connect with official network of the mobile users too. In order to support the movable networks, the IETF has been working to develop the basic support protocol called as Network Mobility (NEMO) protocol. NEMO extends the basic end-host mobility support protocol, MIPv6 [1] [2] for providing mobile network support. There are various issues in terminal mobility like routing, hand-off, QoS and security [3] [9] [13].

The Home agent (HA) and Mobile Router (MR) are the only two nodes in the network which knows about the mobility, which can provide support for other mobile nodes in the network [10]. Though the MR keeps on changing the attaching points based on its mobility, it maintains connectivity with HA by updating the Care of Address (CoA). As MR access HA through public or other private networks, IPv6 tunnel between these two devices helps to maintain secured communication. A vehicle with set of nodes inside can be compared with mobile networks, MR inside vehicle will take care of connectivity [4] [5].

NEMO supports mobility for the entire network through MR [15]. External device which wants to communicate with mobile network node (MNN) is called as Correspondent Node (CN). This CN may be far away from the home and sub network, some scenarios it may be near to sub network compare to home network. But irrespective of the distance between CN and sub network, NEMO remains the same [6]. Some times a mobile node from one network may visit the mobile network of other for communication purpose. The new mobile node from other home network can be called as Visiting Mobile Node (VMN) [17]. Though the VMN stays in the mobile network and very near to destination itself, the routing procedure remains same [16]. But this routing procedure will not be efficient, as the sender and receiver are in the same coverage area. In this article we propose a route optimization technique between Visiting Mobile Node and Mobile Network Node. This technique requires only minor changes, which can provide good performance results in routing and other performance metrics.

2. VMN IN NEMO

A mobile network (also known as a "network that moves," or *NEMO*) is defined as a network whose attachment point to the Internet varies with time. Network Mobility support is needed, when the sub network of a home network starts moving, MR maintains connectivity by changing its point of attachment and a regular binding updates to HA[7]. The NEMO basic support protocol must be upgraded, so that it's capable of maintaining all the sessions of mobile network, even on the high level of mobility. This communication and session maintenance, with minimum delays and data loss is called as mobility support. Researchers are concentrating more on providing solutions for regular connectivity and uninterrupted service between MR and HA [16]. So this could be a mobility support for sub network. But basically the nodes like MNN in the sub network are also mobility based devices.

In our scenario, we are considering two home networks with NEMO enabled sub networks respectively. This sub networks are mobility based so it can also be called as mobile networks. MN maintains connectivity with its HN through Mobile Router (MR) and Access Router (AR). Any communication between CN and MN will be only through MRHA tunnel. Mobile nodes in the sub network will not involve in mobility support for the sub network as it will be taken care by MR. When a mobile node from one network visits other network, then it is called as visiting mobile node. The VMN will be treated as guest for the new mobile network. When MN from sub network2 visits sub network1it will be called as VMN, which is updated in Figure - 1.

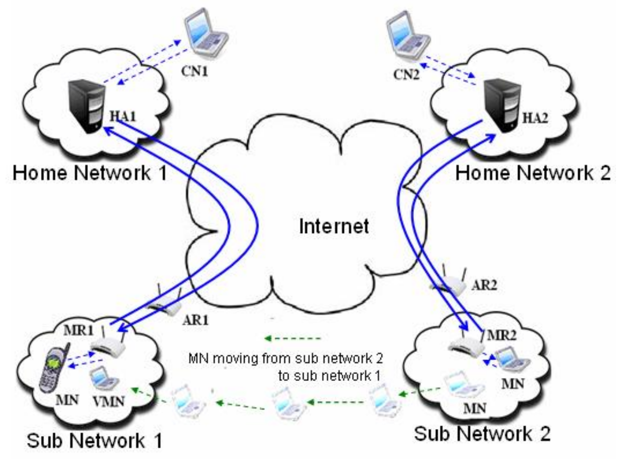

Figure1 – VMN

Once VMN joins in sub network1 it sends a regular binding update about its availability to the HA through the visiting networks MR and HA. Hence the connectivity to VMN is through sub network1 all the communications between VMN and any node will be through MR1, HA1 and HA2. Whenever VMN sends data packets to any node, it just sends the original data to MR after encapsulation, as it is in foreign network. But the data packets sent to MR by VMN will be addressed to HA2 considering that HA2 will forward data to the correct destination after decapsulation. So the data to destination is routed to MR with single encapsulation and from MR to HA1 the data will travel with double encapsulation. Once the HA1 receives the packet from MR, it finds that the packets are to HA2 and forwards the same to HA2. When HA2 receives the data packets with a single encapsulation, it will decapsulate the packet and gets the correct destination. Once the destination is identified by HA2, it will be forwarded to correct path, based on destinations network. This data flow rule is applicable even the destination is in the same sub network1.

3. PROBLEM DEFINITION

Assuming that a mobile node from sub network2 joins in sub network1, the mobile node becomes a Visiting Mobile Node to sub network1. It sends a binding update to its home agent through MR1 and HA1 as any communication for VMN will be through MR1, HA1 and HA2. After joining in the network, if VMN needs a data transfer to any node it will follow the same path flow. This rule is going to be same, even if the destination resides in subnetwork1 as VMN may not aware that the destination is in the same network. The destination may be a mobile node or local fixed node of sub network1. When VMN sends a data to MN it will create a data packets addressed to MN and encapsulates them and sends to HA2. As per the flow, the encapsulated packets to HA2 will be forwarded to MR. MR will not be aware of that the destination is its own member node, as the packet is encapsulated. So MR will forward the packets to HA1 with an additional encapsulation. HA1 decapsulates the second tunnel and forwards the data packets to HA2. When HA2 decapsulates the packet further, it is identified that the destination is MN which is in home network1. Figure 2 shows the packet flow path between VMN and MN.

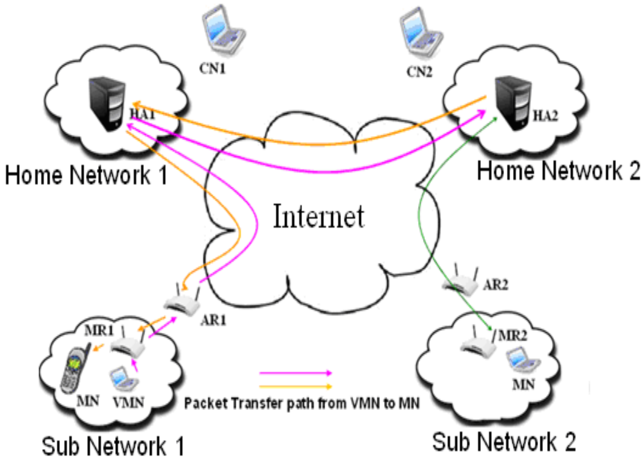

Figure 2 – Data transfer between VMN and MN

When the destination is in home network1, the HA2 just forwards the data packets to HA1 without encapsulation. HA1 gets the packets and forwards to MR with a single encapsulation, and MR will forward the original data to MN after decapsulates it. The same flow will occur, when MN replies to VMN and for further data transfer. Figure 3, shows the packet flow path between VMN and MN through a sequence diagram.

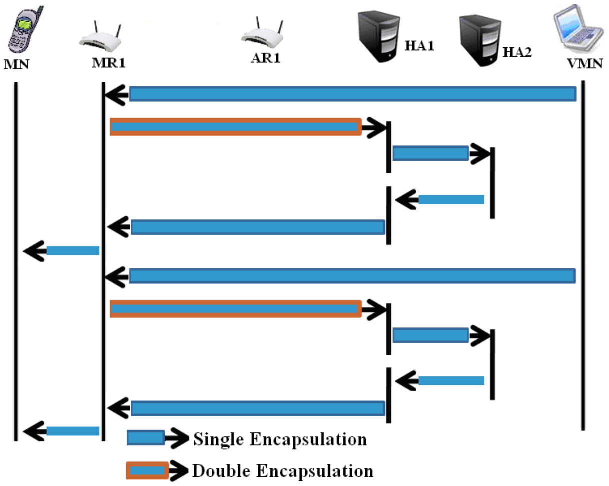

Figure 3- Data flow between VMN and MN

Demerits: Though the source and destination are in the same network, the data is in the situation to travel a long path. Considering the above existing system, the following are the issues

i. Increased chances of packet fragmentation and packet overhead
ii. Increased Packet processing time.
iii. Additional encapsulation amplifies the same.
iv. It's not an optimized route.
v. Packet loss or packet drop chance is very high.
vi. Bandwidth is wasted.

4. PROPOSED SOLUTION

Considering the same scenario, a mobile node joins in the new network and act as a VMN. The existing scheme is transferring the data through an additional long path, which may not need. This longer route, adds usual demerits too. This regular routing process includes tunneling the data twice through external link. When data travels through external network, security issues must be considered. We are proposing a solution which can avoid the data path to HA2, if the destination is in the same network. This solution is a minor change in VMN, so it will not affect topologically or node level changes. When a node moves and joins in new network, it will take a regular hand off process [14]. This hand off process will includes authentication and binding request of the new node i.e. VMN in to the visited network. A router if it finds a new node in its network, it sends a router advertisement to the new node or VMN may search any available routers (like access router search) in its range [12]. But in both the cases router advertisement will be sent to VMN. When VMN gets the router advertisement, it can able to get the address prefix of the MR1 [11]. This prefix is common to the entire mobile network nodes address. This proposed idea is to record this address prefix as a table entry in VMN. The sample table is given in Table 1.

Mobile Router Address	Address Prefix

Table 1 – Address prefix table

As soon as the VMN joins in the network, it will make an entry of the table for address prefix and sends a regular binding update to HA2 through MR1 for further external communication. Once HA2 gets the binding update, it responds as a binding acknowledgement to VMN through HA1 and MR1. Further more, before sending the data an additional process is included in VMN. VMN just verifies the destination address prefix, with the table entry and compares that if the destination is in the same network. If the destination is in the mobile network, the VMN will not encapsulate the data and update the destination address as directly (like when it sends data from its own network). So when MR gets data packet with a destination address of a node in its network, it will automatically transfer the data packets to the destination node, which is in its network. In existing system MR was not given a chance to identify the destination address, as the data is encapsulated from the VMN itself. This encapsulation process is avoided if the destination is in the same network, so that MR involves directly in routing process. A reply from the local node to VMN is in the same path, as MR aware of the care of address assigned to the VMN by the HA1. This intern avoids additional path of MR, HA1, HA2 and HA2, HA1, MR. When, this solution is implemented packet loss, packet over head and additional demerits can be avoided. As the data is not at all forwarded to the external network, we need not to worry about security also. The process of proposed system is given as a sequence diagram in Figure 4.

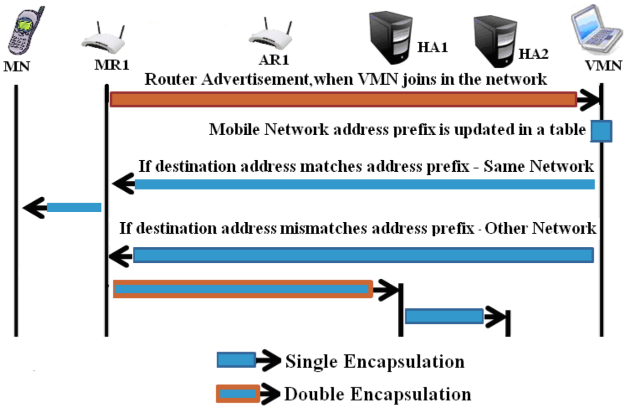
MN
MR1
AR1
HA1
HA2
VMN
Router Advertisement,when VMN joins in the network
Mobile Network address prefix is updated in a table
If destination address matches address prefix - Same Network
If destination address mismatches address prefix - Other Network
Single Encapsulation
Double Encapsulation

Figure 4 – Proposed routing process

If the data packets are not for same network i.e. destination is in other network, regular path is followed. HA2 will take care of forwarding the packets to the destination. If the data is in the same network, we are proposing to send to MR1 with out encapsulation, which is not a security problem. If the data packets are to a destination in other network, as per the regular process packets are encapsulated from VMN itself [8]. MR1 will not have a chance to view even the destination address of other packets.

5. RESULT AND ANALYSIS

The proposed system is tested with the existing system, considering a common count of packet transfer from VMN to mobile node in sub network1 in NS2 simulation environment. We tested both systems, by transferring approximately 10000 data packets from VMN to MN. The result is analyzed between existing and proposed systems by comparing the time taken to deliver the data, packet loss percentage and additional packets used for encapsulation. The result shows that the packet loss percentage is highly reduced in proposed system and it’s proved that the time taken to transfer the data is also decreased. Apart from this, in proposed system we are avoiding additional packets for encapsulation. The following Table 2 compares results.

Mechanism	**Total Packets transferred**	**Time taken to deliver the packets (seconds)**	**Packet loss percentage**	**Additional packets for Encapsulation**
VMN data path - Existing System	10000	113	2.7	6432
Proposed System	10000	29	0.9	0 (No Encapsulation)

Table 2 – Existing and Proposed system comparison

Figure 5 shows the performance comparison of existing and proposed system, which is through the bar graph.

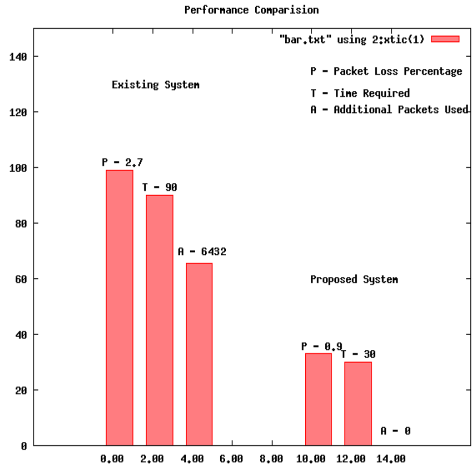

Figure 5 – Existing and Proposed comparison

Figure 6 and 7 shows the results of existing and proposed systems, in terms of time taken for data transfer and packet loss percentage.

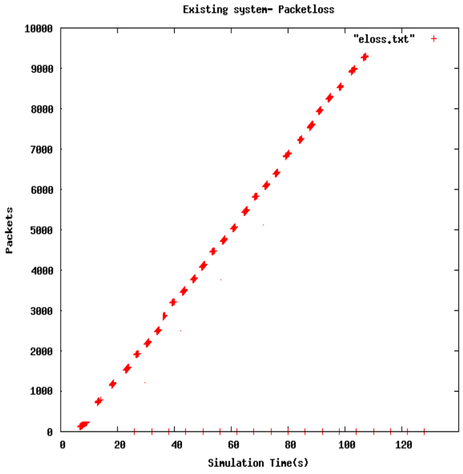

Figure 6 – Existing system, simulation time and packet loss.

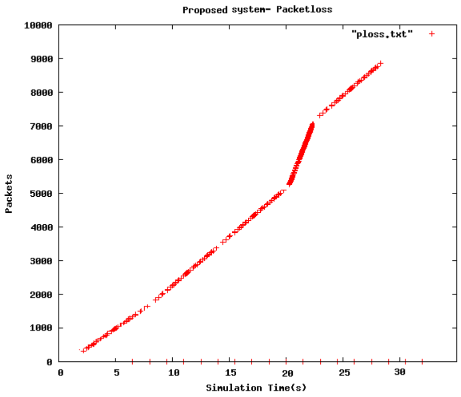

Figure 7 –Proposed system, simulation time and packet loss.

Figure 8 and 9 shows the results of existing and proposed systems, in terms of packet delay, when delivering the data packets.

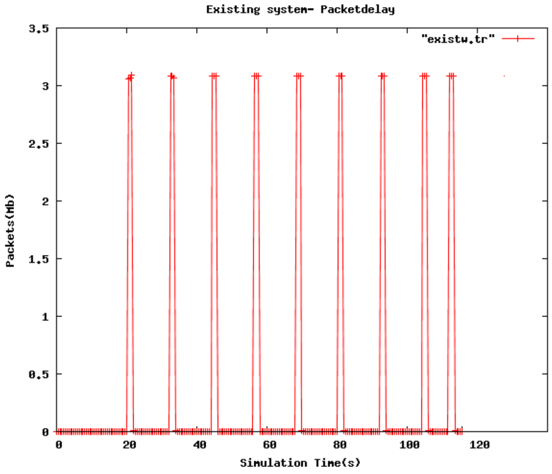

Figure 8 – Existing system, packet delay.

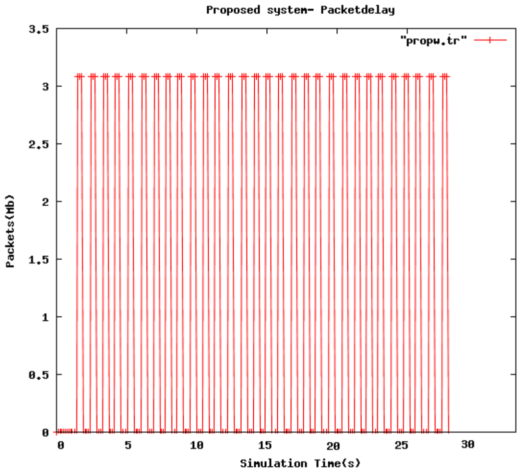

Figure 9 – Proposed system, packet delay.

6. CONCLUSION

We have analyzed the specific routing issue, when a node visits a new network. By doing a minor change in VMN, we can able to optimize the route for VMN and MN communication and routing process remains same if the node is external. Compared to the standard routing process we can able to provide best solution, which is proved in simulation environment too. Further more we are planning to test this solution in real time environment. In future it’s proposed to extend this solution to a mobile node, which roams in multiple networks.

7. REFERENCES

[1] C. Perkins “IP Mobility Support for IPv4”, RFC 3344. August 2002.

[2] D. Johnson, C. Perkins, J. Arkko, “Mobility Support in IPv6”, RFC 3775, June 2004.

[3] J. Mangues, A. Cabellos, R. Serral, J. Domingo, A. 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.

[4] “OverDRiVE (Spectrum Efficient Uni- and Multicast Over Dynamic Radio Networks in Vehicular Environments),” IST project IST-2001.

[5] Mikl´os, Aur´el R´onai, Ralf T¨onjes, Michael Wolf, and Alexandru Petrescu, “Mobility Issues in OverDRiVE Mobile Networks,” in Proceedings of the IST Mobile & Wireless Communications Summit, June 2003.

[6] Vijay Devarapalli, RyujiWakikawa, Alexandru Petrescu, and Pascal Thubert, “Nemo Basic Support Protocol,” RFC3963, Jan. 2005.

[7] Imed Romdhani, A. Yassin al-dubai “Mobile IP Conditional Binding Update”, IEEE workshop, May 2007.

[8] Pekka Nikander, Jari Arkko, Tuomas Aura, Gabriel Montenegro “Mobile IP version 6 (MIPv6) Route Optimization Security Design”, RFC 4225, Dec 2005.

[9] P. Thubert, M. Watari, F. Zhao “Network Mobility Route Optimization Problem Statement”, RFC 4888, July 2007.

[10] Carlos J. Bernard’s, Ignacio Soto, Maria Calderon, “IPv6 Network Mobility”, http://www.cisco.com

[11] Kyeong-Jin Lee, Jae-Hoon Jeong, Jung-Soo Park, and Hyoung-Jun Kim, “Route Optimization for Mobile Nodes in Mobile Network based on Prefix Delegation”, IEEE Journal, Feb. 2004.

[12] T. Narten, E. Nordmark, and W. Simpson, “Neighbor Discovery for IP Version 6 (IPv6),” RFC2461.

[13] P. Calduwel Newton, L. Arockiam, “An Intelligent Technique to Improve Quality of Service (QoS) in Multihomed Mobile Networks”, International Journal of Advanced Science and Technology, Vol. 7, pp. 11-19, June 2009.

[14] Luke Niesink “A comparison of Mobile IP Handoff Mechanism”, 6th twente student conference on IT, Enschede, Feb 2007.

[15] Neeraj Sharma, Naveen Sharma, and Dimple Malik, "Problems of Inefficient Routes in Network Mobility in Wireless Multihop Gateway Networks and their Resolution", International Journal of Electronics Engineering, 3 (1), 2011, pp. 29– 31

[16] Tim Leinmueller, Christian Maihöfer, Michael Wolf and Alexandru Petrescu, "Local Route Optimization for Visiting Mobile Nodes in Mobile IPv6 Networks", IST Mobile Summit 2004.

[17] T. Ernst, INRIA, H-Y. Lach, "Network Mobility Support Terminology", RFC 4885, July 2005