International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 2, ISSN 2455-2143, Pages 22-25
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

MOBILITY AMONGST HETEROGENEOUS NETWORKS

Garima Rani
Department of Computer Engineering
S.I.T.E., Swami Vivekanand Subharti University, Meerut,
Uttar Pradesh, India

***Abstract*— Due to roaming, a mobile device may change its network attachment each time it moves to a new link. This might cause a disruption for the Internet data packets that have to reach the mobile node. Mobile IP is a protocol, developed by the Mobile IP Internet Engineering Task Force (IETF) working group, that is able to inform the network about this change in network attachment such that the Internet data packets will be delivered in a seamless way to the new point of attachment. It allows transparent routing of IP data grams over the Internet. Mobile IP is most often found in wired and wireless environments where users need to carry their mobile devices across multiple LAN subnets with different IP addresses.**

In this paper we pointed out the issues related to mobile IP and present the practical implementation of mobile IP over the network. We also stated the concept of triangle routing and finally, we describe the concept of reverse tunneling as a solution to the problems that are imposed by the security measures employed over the network.

I. INTRODUCTION

The Mobile IP protocol allows the (mobile nodes) MNs to retain their IP address regardless of their point of attachment to the network, and maintain uninterrupted connectivity while traveling across networks. Thus we can say that the main objective of Mobile IP is to maintain continuous IP connectivity while crossing network boundaries.

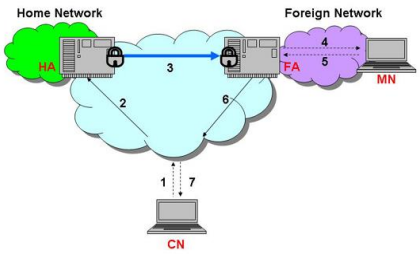

Fig.1. Mobile IP Operation

II. THE MOBILITY INDUCED PROBLEM

Fig.2. shows a scenario where mobility causes the problem. This is a scenario of heterogeneous networks where certain nodes are mobile and others are fixed to a backbone network. When a correspondent host (CH), say B wants to communicate with another node (IP 171.68.69.24) belonging to a mobile router connected via a backbone gateway A (IP 171.68.0.0), it does it via its own intermediate gateway. This gateway further sends the packets to the internet, where it's routed to the appropriate destination gateway.

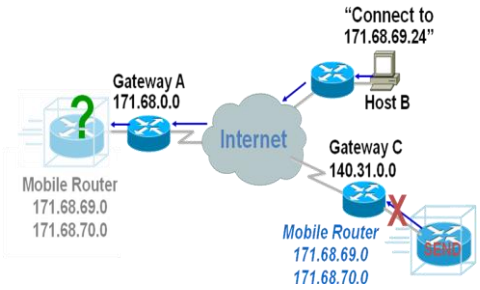

Fig.2. Mobile IP Requirement

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 2, ISSN 2455-2143, Pages 22-25
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

There are two scenarios after this; firstly, the desired destination is connected to its home network and secondly, the destination is unavailable. The former case is simple and the connection is simply established. The mobile router connected to its home network will receive the packets and will respond in similar manner.

But in the latter case, i.e. when the mobile router is not connected to the home network, the packets destined to such a router will not be able to find the destination. Moreover when such a mobile routers tries to communicate via some other foreign agent (Gateway C) it is restricted because of IP conflict. The conflict occurs because of the differences in the IP addresses of home and foreign networks. This is where the problem is induced because of mobility. The solution to this is provided by Mobile IP.

Mobile IP is the method which allows use of a unique IP even in the presence of mobility. The following section describes the implementation of Mobile IP in the heterogeneous network.

III. Practical Implementation of Mobile IP

In short the scenario can be understood in two points:

- Mobile Router sends Registration Request [RRQ] to Home Agent (HA)
- Home Agent forwards packets to Mobile Router via Care of Address [CoA]

A mobile node can have two addresses - a permanent home address and a care of address (CoA), which is associated with the network the mobile node is visiting. A home agent maintains a mobility binding of home address and care-of address. Before we go into the details of the mechanism, let's first list all the players of the game.

- Mobile Node (MN): Mobile IP enabled clients identified by home address or NAI (notebooks, cell phones, PDAs) updates CoA via registrations
- Home Agent (HA): Mobile IP enabled gateway acts as location database for MNs
- Foreign Agent (FA): Mobile IP enabled gateway [Optional] off-loads CPU processing of encapsulation/Decapsulation, enforces local network administration policy, allows for billing of MNs, conserves IP address space, reduce access link usage.

The comprehensive Mobile IP solution process:

Step1. **Agent Discovery**: Initially MR sends out advertisement request (Solicitation) to "all router" multicast address 224.0.0.2. FA responds to his with a unicast advertisement to MR, this response includes CoA. Fig.3. depicts the mobile router advertisement.

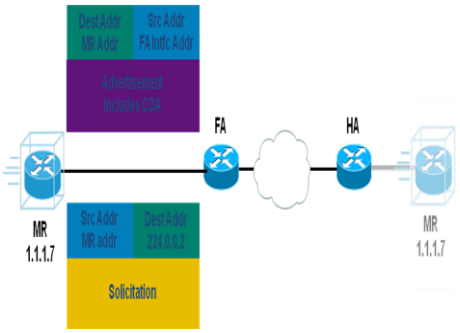

Fig.3. Mobile Router Advertisement

Some of the options for FA advertisement are as follows:

- **R Registration required.** Registration with this foreign agent (or another foreign agent on this link) is required even when using a co-located care-of address.
- **B Busy.** The foreign agent will not accept registrations from additional mobile nodes.
- **H Home agent.** This agent offers service as a home agent on the link on which this Agent Advertisement message is sent.
- **F Foreign agent.** This agent offers service as a foreign agent on the link on which this Agent Advertisement message is sent.

Step2. **Registration Request**: MR retrieves CoA from Advertisement and sends in RRQ to it's HA via FA. FA checks requested services and either rejects and replies or forwards the RRQ to HA. Fig.4. shows the registration process.

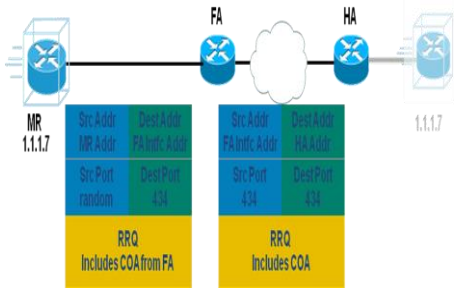

Fig.4. Sending RRQ

Some of the options for registration:

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 2, ISSN 2455-2143, Pages 22-25
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

- **S Simultaneous bindings.** If the 'S' bit is set, the mobile node is requesting that the home agent retain its prior mobility bindings.
- **B Broadcast datagram's**. If the 'B' bit is set, the mobile node requests that the home agent tunnel to it any broadcast datagram's that it receives on the home network.
- **D Decapsulation by mobile node**. If the 'D' bit is set, the mobile nodes will itself decapsulate datagram's which are sent to the care-of address. That is, the mobile node is using a co-located care-of address.
- **M Minimal encapsulation**. If the 'M' bit is set, the mobile node requests that its home agent use minimal encapsulation for datagram's tunneled to the mobile node.

Step3. **RRQ Reply (RRP):** HA authenticates the MR using its address in RRQ. On finding a proper MR it sends RRP and proxy ARPs for MR. Finally it brings up tunnel and adds host route. At the FA end it sees that MR is authenticated by HR and thus forwards RRP to MR and brings up tunnel. Following diagram shows a tunnel.

Outer Header		Inner Header		Original Packet
HA	FA	HA	MR	
100.100.100.1	30.30.30.1	100.100.100.1	65.1.1.1	<src> <dest> Data

The IP tunnel is used in secure routing by encapsulating the datagram with a new IP header using the care-of address of the mobile node. Fig.5. shows the tunneling process.

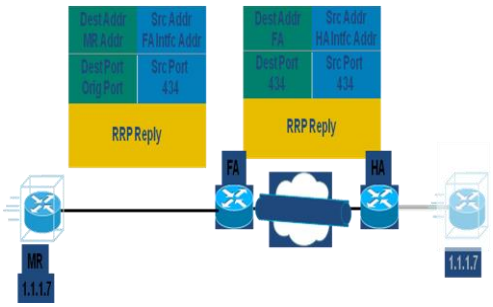

Fig.5. RRQ Reply

IV. TRIANGLE ROUTING

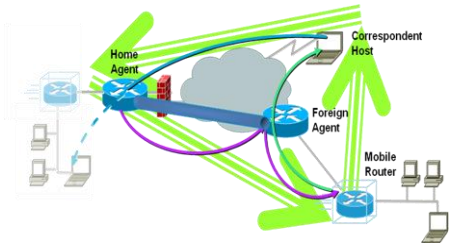

Fig.6. Triangle routing

- Traffic from the correspondent host is sent as usual to the home subnet (HA) by the internet. The home agent intercepts the traffic while the Mobile Router is registered as 'away' from its home location.
- This traffic is tunneled to the CoA of the MR which is forwarded to MR by FA.
- From now on all response traffic from the Mobile Networks can go directly to the correspondent host. The requirement of communication via HA is omitted.

This forms a triangle of routing paths as shown in Fig.6. And the phenomenon is termed as "Triangle Routing".

V. REVERSE TUNNELING

Foreign agent could employ reverse tunneling by tunneling the mobile node's packets to the home agent, which in turn forwards them to the communicating node. This is needed in networks whose gateway routers have ingress filtering enabled and hence the source IP address of the mobile host would need to belong to the subnet of the foreign network or else the packets will be discarded by the router.

Triangle routing no doubtly saves routing delays by reducing the total distance travelled by a packet in network. It also prevents the congestion by preventing unnecessary traffic on unnecessary routes. But the security measures impose a problem over this scenario. Normally, routers route packets by looking at the destination address only. A security measure against attacks (such as spoofing), ingress filtering on a router checks the source and destination addresses on a packet to make sure that they are topologically correct. This poses a problem for Mobile IP because the source address of a packet from a mobile node does not belong to the network

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 2, ISSN 2455-2143, Pages 22-25
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

from which it emanated. This makes the triangle routing impossible.

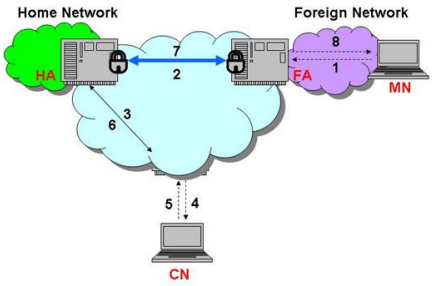

Fig.7. Reverse Tunneling

Reverse tunneling provides a solution to this. Reverse tunneling satisfies ingress filtering done by the security measures imposed by the network. Packets from the mobile network are sent back to the HA through the tunnel. HA decapsulates the packets and forwards them to their destination through normal routing. Thus, the received packets' path is topologically correct.

The reverse tunnel is formed for the communication between MR and correspondent host. This prevents their direct communication as in triangle routing, rather all communication takes place only via the HA. This prevents all the ambiguities imposed by addresses during mobility.

VI. CONCLUSION

In this paper we pointed out the issues related to mobile IP and present the practical implementation of mobile IP over the network. We also stated the concept of triangle routing and finally, we describe the concept of reverse tunneling as a solution to the problems that are imposed by the security measures employed over the network.

The future work in this field is to provide security measures to the packets in addition to providing address hiding or encapsulation by a proper packet tunneling.

VII. REFERENCES

1. Perkins, C., E., "(ed.) "IP Mobility Support", RFC2002, proposed standard. IETF Mobile IP Working Group, Oct., 1996.
2. Pierre Reinbold and Olivier Bonaventure,"A Survey of IP micromobility protocols," Technical report at Infonet group, University of Namur, Belgium, March 2002.
3. S. Debashis, M. Amitava, M. I Saha, and C. Mohuya, "Mobility Support in IP: A Survey of Related Protocols," IEEE Network, November 2004.
4. Hesham Soliman, Claude Catelluccia, Karim El Malki, and Ludovic Bellier, "Hierarchical Mobile IPv6 mobility management (HMobile IPv6)," Internet Draft, Internet Engineering Task Force, draft-ietf mipshop-hmipv6-04.txt, December 2004.
5. Yazid Mohamed, Norsheila Fisal, and Alias Mohd, "Performance of TCP on Mobile IP network during handoffs," Research and Development, 2002. (SCOReD 2002) July 2002 Pages: 390 - 393.
6. Weng Su-xiang, Liu Shu-fen, and Yao Zhi-lin, "An implementation of mobile IP's tunnel technology in Linux kernel," Computer Supported Cooperative Work in Design, 2004.
7. Abdul Sakib Mondal, "Mobile IP: Present State and Future," Springer, 2003.
8. G.Montenegro, "RFC 2344: Reverse Tunneling For Mobile IP".
9. "Internet Engineering Task Force (IETF)", www.ietf.org
10. D. Forsberg, J.T. Malinen, T. Weckstrom, M. Tiusanen, "Distributing Mobility Agents Hierarchically under Frequent Location Updates," Sixth IEEE International Workshop on Mobile Multimedia Communications (MOMUC'99), San Diego 1999.
11. F. Bari and V. C. M. Leung, "*Automated Network Selection in a Heterogeneous Wireless Network Environment*", *IEEE Network*, vol. 21, no. 1, Jan/Feb. 2007, pp. 34-40.
12. I. Smaoui, F. Zarai, R. Bouallegue and L. Kamoun, "*Multi-Criteria Dynamic Access Selection in Heterogeneous Wireless Networks", IEEE ISWCS'09, Sienna-Italy.*
13. B. Xing and N. Venkatasubramanian, "*Multi-Constraint Dynamic Access Selection in Always Best Connected Networks*", IEEE MobiQuitous'05, pp. 56-64, San Diego, CA, July 2005.
14. E. Stevens-Navarro and V.W.S. Wong, "*Comparison between Vertical Handoff Decision Algorithms for Heterogeneous Wireless Networks*", VTC 2006-Spring. IEEE 63rd Vehicular Technology Conference, vol.2, pp. 947-951.
15. D. Johnson, "Mobility Support in IPv6", IETF RFC 3775, 2004.
16. R. Koodli, Ed., "Mobile IPv6 Fast Handovers", IETF RFC 5568, 2009.
17. H. Soliman, C. Castelluccia, K.E. Malki, L Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", IETF RFC 5380, 2008.