International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Study of Mobile IPv6

Sonal V. Toshniwal

Department of Electronics &Telecommunication Engineering, Jagadambha College of Engg.& Technology, Yavatmal, India

Abstract: ***IP version 6 (IPv6) Is being designed within the IFTF as a replacement for the current version of the IP protocol used in the Internet (IPv4).We have designed protocol enhancement for IPv6, known as mobile IPv6, that allow transparent routing of IPv6 packets to mobile nodes, taking advantage of the opportunities made possible by the design of a new version of IP. In Mobile IPv6, each mobile node is always identified as by its home address, regardless of its current point of attachment to the Internet. While away from its home IP subnet, a mobile node is also associated with a care-of address, which indicates the mobile node's current location. Mobile IPv6 enables any IPv6 node to learn and cache the care-of address associated with a mobile node's home address, and then to send packet destined for the mobile node directly to it at this care-of address using an IPv6 routing header. But there are many security risks involved, when a malicious node might be able to establish a connection with the mobile node by sending the false binding messages. By doing so malicious node can divert the traffic, can launch the DOS Attacks and can also replay the authenticated messages.***

Keywords: Mobile node (MN), Correspondent node (CN), homeagent (HA), Care-of-address (CoA), Binding update (BU)

1. Introduction

Mobile IPv4 [4] is based on the idea of supporting mobility on top of existing IP infrastructure, without requiring any modifications to the routers, the applications, or the stationary end hosts.

However, in Mobile IPv6 [6] (as opposed to Mobile IPv4), the stationary end hosts may provide support for mobility, i.e., route optimization. In route optimization, a correspondent node (CN) (i.e., a peer for a mobile node) learns a binding between the mobile node's stationary home address and its current temporary care-of address. This binding is then used to modify the handling of outgoing (as well as the processing of incoming) packets, leading to security risks. The purpose of this document is to provide a relatively compact source for the background assumptions, design choices, and other information needed to understand the route optimization security design. The goal of this document is to explain the Mobile IPv6, Route Optimization, Security and Threats in details.

1.1 Mobility

One of design goals in the Mobile IP design was to make mobility possible without changing too much. This was especially important for IPv4, with its large installed base, but the same design goals were inherited by Mobile IPv6.Some alternative proposals take a different approach and propose larger modifications to the internet architecture. To understand Mobile IPv6 [2], it is important to understand the MIPv6 design view of the base IPv6 protocol and infrastructure. The most important basis assumptions [4]can be expressed as follows:

1) The routing prefixes available to a node are determined by its current location, and therefore the node must change its IP address as it moves.
2) The routing infrastructure is assumed to be secure and well-functioning, delivering packets to their intended destinations as identified by destination address.

2. Overview of IPv6

In this section, we outline some of the basic characteristics of the IP version 6(IPv6) that are particularly relevant to our mobility protocol. The most visible difference is that Iv6 addresses are all 128 bits long, instead of 32 bits long as in IPv4.Within this huge address space , a tiny part is reserved for all current IPv4 addresses , and another tiny part is reserved for the link local addresses, which are not routable but which are guaranteed to be unique on a link(i.e., on a local network).Nodes on the same link can communicate with each other even without any routers , by using their Link –Local addresses. Iv6 defines several kinds of extension headers, which may be used to include additional information in the headers of an IPv6 packet. The defined IPv6 extension headers include:

- Destination Option header
- Hop by Hop Option header
- Routing header and Authentication header.

The destination options header may be included in a packet to carry a sequence of one or more options to be processed only when the packet arrives at the final destination node. Similarly, the Hop-by-Hop options header may be included to carry a sequence of one or more options, but these options are processed by every intermediate router which receives and forward the packet as well as by the final destination node. In IPv4, every IP option is treated as a Hop-by-Hop option.

The routing header is particularly useful for our mobility protocol, and is similar to the Source Route option defined for IPv4. The IPv6 routing header can serve both as a strict source route and a loose source route, although Mobile IPv6 uses it only as a loose source route. Unlike the IPv4 Source Route options, however in IPv6, the Routing header is not examined or processed until it reaches the next node identified in the route. In addition the destination node receiving a packet with a routing header is under no obligation to reverse the route along which the packet was received, for routing packets back to the sender. The Authentication header provides a means by which a packet

can include optional authentication data, for example based on a one-way cryptographic hash (e.g.MD5[16, 18, 20]) of the packet's contents. The authentication data allows the receiver to verify the authenticity of the sender packet, also protect modification of the packet while in transit, since a modified packet will be viewed by the receiver. The authentication header may be used to provide a relay protection of packets. The computation of the authentication data and use of replay protection are controlled by a "security association" that the sender packet must be established with the receiver. Security association may be manually configured or automatically established.

3. Overview of MobileIPv6

Mobile IPv6 is intended to enable IPv6 nodes to move from one IP sub net to another .it is just as suitable for mobility between subnet across homogeneous media as it is across heterogeneous case other solution may also exist[7]. That is mobile IPv6 facilitates nodes movement from one Ethernet segment to another as well as it accommodates node movement from an Ethernet segment to a wireless LAN cell. The protocol allows a mobile node to communicate with other nodes (stationary or mobile) after changing its link layer point of attachment from one IP subnet to another, yet without changing the mobile node's IPv6 address. A mobile node is always addressable by its home address, and packets may be routed to it using this address regardless of the mobile node's current point of attachment to the Internet. The movement of a mobile node away from its home subnet is thus transparent to transport and higher layer protocol and applications. All packets used to inform another node about the location of a mobile node must be authenticated. Otherwise, a malicious host would be able to hijack traffic intended for a mobile node by the simple matter of causing the mobile node to seem to be elsewhere than its true location. Such hijacking attacks are called "remote redirection" attack, since the malicious node may be operating at a network location far removed from the mobile node, nevertheless effectively redirects traffic away from the true location of the mobile node[4].

4. Route Optimization Protocol

To enhance the performance, Route Optimization protocol is used. Route optimization is a technique which enables a mobile node and a correspondent node to communicate directly, bypassing the home agent completely [4]. The concept of route optimization is that, when the mobile node receives the first tunnelled message, the mobile node informs correspondent node about its new location, i.e. care-of address, by sending a binding update message .The correspondent node stores the binding between the home address and care-of address into its Binding cache [5].but this simple technique introduces the security threats like false binding updates, Bombing attack, DOS Attack, Reflection and Amplification Attack, etc.

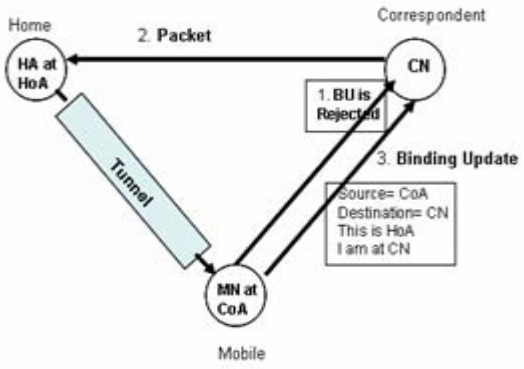

Figure 1(a): Mobile IPv6 route optimization

To elaborate our idea, we assume that the MN moves to the new location and registers its new care-of address with the HA. Any message from CN, which was communicating with MN, is tunnel to the mobile's care-of address by HA (As shown in Fig.1 (a)). On receiving the tunnelled message, the route optimization protocol is activated; in which MN directly communicates to the CN.

5. Security and threats

Route optimization Protocol makes mobile IPv6 more vulnerable. The attacker can either corrupt binding message, that are destined to the correspondent node or it can change the destination address so that packets to be delivered to the desired packets of the attacker. So secrecy and integrity of communication is no more valid and can lead to denial-of-service (DoS) attacks. In this section we describe different attacks which are possible in MIPv6.These attacks are described as follows:

5.1 Attacks against Address' Owners' (Address Stealing")

In address stealing an attacker illegitimately claims to be a given address [2] and tries to "steal" traffic destined to that address. It is the most dangerous attack, where traffic reaches to the malicious node instead of reaching to the actual destination .There are different variant of attack;

a. Basic Address Stealing: If binding updates were not authenticated at all[2], an attacker can send spoofed binding updates from anywhere in the Internet. IPv6 address can be or become mobile and there is no way of distinguishing a mobile and stationary host by just looking at its address [6] so potentially any node including stationary node, is vulnerable.

b. Attacks against Secrecy and integrity: By spoofing Binding Updates, an attacker could redirect all packets between to communicating nodes to itself [2].By sending a false BU to correspondent node, the attacker could get control over the data intended between MN and CN. It means that attacker can hijack the connections opened between mobile and correspondent node. The attacker could also launch man-in-the-middle attack by sending spoofed BU to both MN and CN. By doing so all traffic between two nodes will pass through the attacker. Hence the attacker would be able to see and modify the packets sent between MN and CN [6].

c. Basic denial-of-Service attacks: By launching this attack, the attacker prevents the legitimate node to access the resources of the node (victim of attack). This attack might stop or disrupt communication between the nodes [2]. This attack can be launched on any Internet node.

d. Replaying Binding Updates: An attacker may replay the binding message which is previously authenticated by the correspondent. Hence attacker can direct packets to the mobile node's previous location [2].

5.2 Basic Flooding

In this attack, the attacker redirects heavy data stream, which is intended for MN from CN, to the target address. This attack is serious in nature because by doing so target receiving cache is over flood, which also lead to DoS attack.

5.3 Reflection and Amplification

In this attack, attacker emphasis is to force node to send more number of packets to the target than the attacker sent to the node[4].Reflection is particularly dangerous as packet are being reflected multiple times. If packets are sent into a looking path this can halt the target node as well as the sender.

6. Conclusion

We have presented an efficient and deployable protocol for handling mobility with the new IPv6 protocol, and suitable for use with the coming multitudes of the mobile nodes. We believe our protocol is as light weight as possible, given the need to be transparent to higher level protocol; while proposing this protocol, we kept in mind that the Mobile IPv6 route optimization security design was never intended to fully secure. We described the major threats that are faced by the Mobile IPv6.

7. Acknowledgement

The authors would like to thank the other people that contributed the Mobile IPv6 Security Design Team effort either directly or indirectly.

References

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", Internet Draft draft-ietf- mobileip-ipv6-22.txt, work in progress, May 26, 2003
[2] PekkaNikander, JariArkko, Tuomas Aura, Gabriel Montenegro, "Mobile IP version 6 (MIPV6) Route Optimization Security Design", in Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th, 6-9 Oct. 2003, work in progress, pg. 2004-2008, Vol.3
[3] S. Zeadally and N. Deepakmavatoor, "Mobile IPv6 Support for Highly Mobile Hosts", in Proceedings of IASTED International Conference on Communications Systems and Networks (CSN'03), Benalmadena, Spain, September 2003.
[4] P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", Network Working Group Request for Comments: 4225, December 2005
[5] W. Al-Salihy, AzmanSamsudin, and R. Sureswaran, "New Approach to Secure Mobile IPv6 Signals", in IASTED, 22 April 2005.
[6] Tuomas Aura. "Mobile IPv6 Security", in 10th International Workshop, vol. 2845 of LNCS, pg. 215-228, Cambridge, UK, April 2002. Springer 2003.
[7] Ved P. Kafle, EijiKamioka, Shigeki Yamada, "Extended Correspondent Registration Scheme for Reducing Handover Delay in Mobile IPv6", in 7th International Conference on Mobile Data Management (MDM'06), May 2006.