Research Paper

Volume : 2 | Issue : 7 | July 2013 • ISSN No 2277 - 8179

Mobile IPv6 Route Optimization Enhancements

Computer Science

KEYWORDS : IPv4, IPv6, mobility, Route optimization, HoA, CoA, DHCPv6, IPSEC.

Sridevi Assistant Professor, Department of Computer Science, Karnatak University, Dharwad.

ABSTRACT

This paper briefly introduces the Mobile IPv6 (MIPv6) protocol, outlines its advantages over MIPv4, describes the Return Routability test for MIPv6 route optimization, presents some enhancements to the MIPv6 route optimization mechanism.

1. Introduction

IPv6 [3] is a new Internet protocol that was designed by the IETF as the future replacement for IPv4. The initial momentums to build IPv6 were the limited number of IPv4 addresses and the difficulty in managing the large and unwieldy IPv4 routing tables. However, IPv6 has been designed not only to provide plenty of addresses and ease in managing routing tables, but also to support other convenient aspects for the growth of the Internet, including Internet mobility. MIPv6 [1] is the mobility management protocol for IPv6. Although MIPv6 adopts the general design ideas from MIPv4, the mobility functions are much more closely integrated within IPv6, and therefore, it is considered much improved for Internet mobility.

There are a lot of important differences between IPv6 and IPv4. As shown in the IPv6 and IPv4 header formats (Figure 1 and 2 respectively), there are two obvious differences between the IPv6 and the IPv4 header: the address length of IPv6 is 128 bits, while that of IPv4 is 32 bits; and a number of fields in the IPv4 header which are not frequently used are deleted from the IPv6 header. Actually, some functions provided by these fields can be achieved using certain IPv6 extension headers [3] when needed, which do not need to be examined by every intermediate node between the source and the destination, and therefore accelerate packet processing in routers. MIPv6 mainly benefits from the large address space and three IPv6 extension headers: the Routing header, the Destination Option header, and the newly defined Mobility header [1]. Such a large address space makes it easy to realize the HoA and CoA auto-configuration by either the stateful method using DHCPv6 (Dynamic Host Configuration Protocol Ver-

sion 6 [4]) or the stateless method [5] by MNs themselves. FAs are no longer needed: in other words, the only type of CoA is the co-located CoA.

Figure 1: IPV6 Header Format

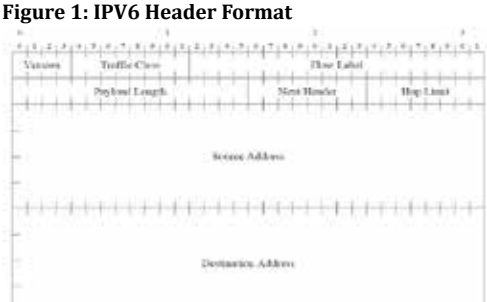
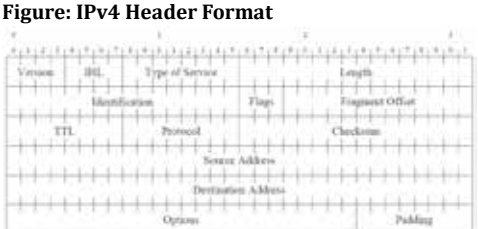


Figure: IPv4 Header Format



The Routing header and the Destination Option header used by MIPv6 are known as the type 2 Routing header and the Home Address Destination Option header respectively. They are usually used to deliver an MN's HoA when the MN is in a foreign network and directly communicating with its CNs bypassing its HA. The newly defined Mobility header is used to carry a number of mobility signallings, including the *Home Test Init* (HoTI), *Home Test* (HoT), *Care-of Test Init* (CoTI), *Care-of Test* (CoT), *Binding Update* (BU), *Binding Acknowledgement* (BA), *Binding Refresh Request* (BRR) and *Binding Error* (BE) messages. The first four messages are used to fulfill the *Return Routability* (RR) test in order to ensure the authorization of subsequent BU messages for supporting route optimization. The BU message is used by an MN to notify its HA or a CN of its current mobility binding. The BA message is used to acknowledge the receipt of a BU message. The BRR message is used by a CN to request the current mobility binding from an MN. The BE message is used by a CN to inform an MN of an error related to mobility.

2. Mobile IPv6 Return Routability Test for Route Optimization

Route optimization is an important feature provided by MIPv6 as a fundamental part of the protocol. In MIPv6, the process of deploying route optimization is more practical than in MIPv4 mainly due to the design of the RR (Return Routability) test. Using RR, no pre-configured SA and authentication infrastructure are required between the MN and the CN, and the possibility of suffering from attacks is limited to a very low level.

2.1 Major Threats against Mobile IPv6 Route Optimization

Two major threats against MIPv6 route optimization, while a more thorough threat description can be found in [6].

1. Address stealing attacks: If node A is sending packets to node B, an attacker would be able to redirect the packets to an arbitrary address C (e.g. the address of itself) by sending a fabricated BU to node A. In this case, the mobility service is stolen by the attacker. An attacker could also redirect all packets between two nodes to itself, by sending a spoofed BU to each of these two nodes. In this case, the attacker stands in the middle of the two nodes and is able to see and modify packets between them.
2. Denial of Service attack: An attacker could send spoofed BUs to redirect all packets between two nodes to a third party or a non-existent address. In this way, the communications between the two nodes would be interrupted. If the traffic between the two nodes was heavy, such an attack may also cause packet flooding to a third party.

Note that MIPv4 route optimization shares similar threats with MIPv6. In order to protect MIPv6 route optimization against these attacks, the RR test has been designed, so that the BU message can be authenticated.

2.2 Return Routability Procedure

In MIPv6 route optimization, a mobility option called the Binding Authorization Data option is defined to carry authentication data for protecting BU messages. A binding management key, Kbm, which can be established through the RR test procedure, is employed in this option. As mentioned earlier, four types of messages are involved in the RR test: the HoTI, CoTI, HoT and

CoT. The RR procedure can be briefly described as follows:
Each CN holds a secret node key, or Kcn. Each CN also periodically generates nonces. Each nonce is associated with a nonce index. An MN initiates an RR test by sending a HoTI and a CoTI to a CN. Note that the HoTI is reverse tunnelled using IPsec (IP Security) ESP (Encapsulating Security Payload) [7] to the HA first. Specially, a 64-bit random number called "home init cookie" is included in the HoTI, and another 64-bit random number called "care-of init cookie" is included in the CoTI by the MN. These cookies are to be returned by the CN in the HoT and CoT respectively later, in order to verify that the HoT and CoT match the HoTI and CoTI respectively.

On receipt of the HoTI, the CN returns an HoT, containing the home init cookie, home keygen token, and the index of the nonce used to calculate the home keygen token. The home keygen token is cryptographically generated from calculating a hash function over the concatenation of the Kcn, the source address of the HoTI message (the MN's HoA), and a nonce:
home keygen token = hash (Kcn | MN's home address | nonce | 0),

where | denotes concatenation. The HoT is usually sent to the MN's HA in plain text first, and then forwarded to the MN using the IPsec ESP tunnel.

On receipt of the CoTI, the CN returns a CoT, containing the care-of init cookie, care-of keygen token, and the index of the nonce used to calculate the care-of keygen token. The home keygen token is cryptographically generated from calculating a hash function over the concatenation of the Kcn, the source address of the CoTI message (the MN's current care-of address), and a nonce:
care-of keygen token = hash (Kcn | MN's care-of address | nonce | 1).

The CoT is sent directly to the MN in plain text.

After receiving both HoT and CoT, the MN is able to create a Kbm (binding management key) using a hash function over the home keygen token and the care-of keygen token obtained:

Kbm = hash (home keygen token | care-of keygen token)

Then the MN can send a BU message to the CN protected by the Kbm contained in the Binding Authorization Data option. Since the BU also contains both the MN's home address and care-of address, and the indices of the nonces used to generate the keygen tokens; given the Kcn, the CN is able to re-generate the keygen tokens, and then calculate the Kbm in order to authenticate the BU. This means before getting the first BU from the MN, the CN does not need to create any state for the MN, and this is why the RR test is thought of as a lightweight protocol.

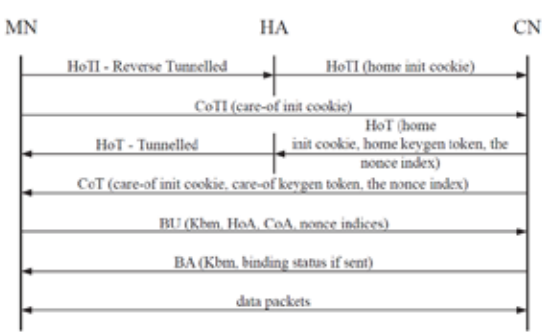


Figure 3: *Mobile IPv6 Route Optimization Procedure*

A successful RR test means that the node initiating the test is reachable at its claimed care-of address and its home address. In this way, route optimization can be run without the need for pre-configuring SAs between MNs and CNs. Since the Kbm is available to any nodes who can get both the HoT and CoT messages, the RR test cannot prevent attacks from nodes with such capabilities. However, these nodes can launch similar attacks even without the use of MIPv6.

3. Mobile IPv6 Route Optimization Enhancements
Although the RR test has been chosen as the default route optimization mechanism for MIPv6, it has several disadvantages, and hence corresponding enhancements can be done.

3.1 Latency Optimizations
An MN is able to send a BU to a CN to update its mobility binding, at least one RTT between the MN and the CN is required to perform the RR test, which is based on the assumption that the HoTI-HoT and CoTI-CoT message pairs are exchanged in parallel. Note that the exchange of the HoTI-HoT message pair usually has a longer RTT than that of the CoTI-CoT message pair, since the HA is involved in the path. The HoTI-HoT and CoTI-CoT exchanges are generally called HoA test and CoA test respectively. Moreover, normally2 an MN initiates the RR test after it successfully updates its mobility binding with its HA [8]. That is, an MN usually has to wait one RTT between itself and its HA and another RTT between itself and its CN (via the HA) before it can begin to update its CN's binding cache entry. Then an additional RTT between the MN and the CN is needed before the MN can get the first data packet from the CN. This total delay may well be intolerable to interactive and real-time applications, and may affect the performance of bulk data transfer using TCP or other transport protocols with congestion control mechanisms.

One way to minimize the latency is to perform the RR test in a proactive way. That is, to do the HoA test and the CoA test before a handover. Actually, the HoA test can be done anytime conveniently without violating the specification [1]. The lifetime of a home keygen token has a specified maximum value of 3.5 minutes. If an MN is unable to foresee a handover, it may just run the HoA test whenever a home keygen token is about to expire in order to guarantee that a valid home keygen token is available right after a handover. On the other hand, if a handover is foreseeable to an MN, the MN may initiate the HoA test right before a handover instead of doing it periodically. However, to perform the CoA test in advance of a handover is more difficult, because the MN needs to know its new valid CoA on its handover target link. Therefore, it is generally believed that this is only possible when the MN is capable of attaching to two links simultaneously (e.g. in the case that the MN has multiple interfaces) [8]. Since normally the CoA test cannot be done before an actual handover, the concept of concurrent CoA test has been brought forward recently. That is, a CN immediately starts to use the newly announced CoA by the MN while the CoA test is still in progress. [10] combines the idea of concurrent CoA test with the approach of proactive HoA test, thus the RTT caused by the RR test can be at least reduced to half. In [10], an MN sends an Early Binding Update (EBU) to its CN as soon as it acquires a new CoA. Since it is assumed that the HoA test has been done beforehand, the MN only uses the home keygen token to sign the EBU message. This helps the CN to authenticate the MN; however, the CN is still not sure whether the MN is reachable at the announced new CoA in the EBU message, and therefore it only creates a temporary binding for the new CoA and starts to use it tentatively. At the same time, the standard CoA test and binding update procedure are executed. After they are done, the CN creates a standard binding for the MN.

However, this EBU scheme brings a security hole due to the period of the tentative use of an unverified CoA. A malicious node may utilize this property to illegitimately redirect the traffic from the CN to the MN to a third party for flooding attacks. As a result, a mitigating approach called Credit-Based Authorization (CBA) has been proposed in [11]. The key idea of CBA is to limit the data volume and rate that the CN sends to the MN's unconfirmed CoA. A CBA-enabled CN maintains a credit account for each MN it is communicating with, and increases the credit based on the amount of traffic exchanged between itself and each individual MN with a verified CoA. When an MN registers a tentative CoA with the CN by sending an EBU message, the CN starts to reduce the MN's credit based on the traffic amount it sends to the tentative CoA. In this way, CBA reduces the motivation for a malicious node to perform a redirection-based flood-

ing attack, since the malicious node needs to make equal efforts to collect credits as it does to directly perform a flooding attack, which cannot be avoided by the current non-mobile Internet. However, CBA has problems collecting credits for MNs when they are moving rapidly, and the credit collecting method depends on the traffic pattern between the CN and each MN.

3.2 Signaling Optimizations

RR test consists of four messages. Moreover, the lifetime of a home keygen token and a care-of keygen token is 3.5 minutes respectively, and the lifetime of a mobility binding at a CN is 7 minutes. Therefore, the initializations and refreshments of mobility bindings may cause non-negligible traffic loads, especially when both ends are MNs experiencing frequent handovers. As a result, reducing the MIPv6 route optimization signaling.

Note that signalling optimizations are often combined with Security optimizations,since signalling optimizations boil down to reducing the number of signaling messages or the frequency of sending signaling messages while at the same time maintaining the same or an even higher security level than that of the standard MIPv6 route optimization mechanism. Moreover, signaling optimizations are also linked with latency optimizations, since the reduction of signaling exchanges results in the increase of route optimization efficiency.

For example, in [12], an OptimizedMIPv6 (OMIPv6) route optimization solution is proposed, in which a secret key with a longer lifetime is established between an MN and its CN on the basis of a successful initial RR test for authenticating the subsequent BU and BA messages, and consequently the amount of mobility signaling is substantially reduced by eliminating the need for the HoTI-HoT and CoTI-CoT exchanges afterwards. In this way, the security vulnerability is limited to the period of the initial RR test and the secret key establishment stages. However, successful attacks during this period will have effects lasting for a longer time because of the longer lifetime of the secret key. Moreover, there are still many other existing schemes. However, only a list of summary of observed solutions is provided, without further explanations in depth:

- [13] introduces a means to utilize Cryptographically Generated Addresses (CGAs) to optimize the MIPv6 route optimization signallings (CGA-OMIPv6) by removing most HoTI-HoT exchanges, since an MN can prove the ownership of its HoA to its CNs using CGA.
- In [14], a new mode called Binding Update Backhauling (BUB) for MIPv6 route optimization is proposed especially for highly mobile environments: that is, when both communicating nodes are mobile. The key idea of this scheme is to eliminate the need for the HoTI-HoT and CoTI-CoT messages by transferring BU messages along a more secure and reliable path going through the two HAs (trusting each other) of the two MNs.
- [15] proposes to dynamically change the lifetime of a mobility binding at a CN. That is, instead of the current fixed limit (7 minutes), an MN can continue to use an existing mobility binding 30% longer than the time it has already been reachable at the CoA (proved by providing the previously established Kbm's). In this way, the unnecessary signalling traffic load can be reduced when the MN stays at one location for a long time.
- A scheme called Certificate-based Binding Update (CBU) [16] allows an MN's HA to establish an end-to-end SA between the MN and its CN, on the basis that both the MN and the CN trust the HA and the HA trusts the MN, so that subsequent BU and BA messages can be directly exchanged without the need of address tests.
- Similar to HMIPv4 [2], Hierarchical Mobile IPv6 (HMIPv6) [17] provides a hierarchical architecture for MIPv6, which masks an MN's movements inside an administrative domain from its HA and CNs. The MN usually obtains two CoAs: a Regional Care-of Address (RCoA) and an on-link Care-of Address (LCoA). A new type of network node called a Mobility Anchor Point (MAP) that acts as the MN's local HA is introduced. The MN's movements inside its MAP domain only cause changes to its LCoA, while its RCoA remains constant to the outside world. Thus, RR tests to a CN outside the domain do not need to be triggered in this case for route optimization.

3.3 Security Optimizations

An RR test is vulnerable to attackers who are able to get both the HoT and CoT messages, since they contain all the required information to generate the Kbm for the subsequent BU and BA message authentications. In fact, RR tests can only ensure that a node that holds a valid Kbm is on the path towards the testing HoA and CoA. Normally a malicious node cannot be on both the paths of the HoT and CoT messages, however, if it is located in the same network as one of the communication end points (i.e. the MN or the CN), RR tests can consequently be compromised.

Sometimes, a stronger authentication mechanism may be needed. [18] describes how to use IPsec to protect the mobility signallings between the MN and its CNs. [19] defines the usage of a pre-configured Kbm to secure the BU and BA messages between the MN and its CNs. Moreover, an improvement of the RR protocol is proposed in [20] to better prevent redirect attacks.

4. Conclusion

MIPv6 route optimization enhancement is one of the most popular research topics being currently discussed in the IETF and IRTF (Internet Research Task Force). A scheme to optimize the RR test latency based on the assistance of the MIPv6 fast handover protocol [9]. According to [1], MIPv6 uses IPsec to protect the mobility signaling between the MN and its HA.

REFERENCE

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", RFC 3775,June 2004. | [2] E. Gustafsson, A. Jonsson, and C. Perkins, "Mobile IPv4 Regional Registration",draft-ietf-mobileip-reg-tunnel-09.txt, June 2004. | [3] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998. | [4] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003. | [5] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998. | [6] P. Nikander, T. Aura, J. Arkko, G. Montenegro, and E. Nordmark, "Mobile IP version 6 Route Optimization Security Design Background", draft-nikandermobileip-v6-ro-sec-00.txt, April 2003. | [7] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, | November 1998. | [8] J. Arkko and C. Vogt, "A Taxonomy and Analysis of Enhancements to Mobile IPv6 | Route Optimization", draft-irtf-mobopts-ro-enhancements-00.txt, January 2005. | [9] R. Koodli, "Fast Handovers for Mobile IPv6", RFC 4068, July 2005. | [10] C. Vogt, "Early Binding Updates for Mobile IPv6", draft-vogt-mobopts-earlybinding- | updates-00.txt, February 2005. | [11] C. Vogt, "Credit-Based Authorization for Mobile IPv6 Early Binding Updates", | draft-vogt-mobopts-credit-based-authorization-00.txt, February 2005. | [12] W. Haddad, F. Dupont, L. Madour, S. Krishnan, and S. Park, "Optimizing Mobile | IPv6 (OMIPv6)", draft-haddad-mipv6-omipv6-01.txt, February 2004. | [13] W. Haddad, L. Madour, J. Arkko, and F. Dupont, "Applying Cryptographically | Generated Addresses to Optimize MIPv6 (CGA-OMIPv6)", draft-haddad-mip6- | cga-omipv6-03, October 2004. | [14] W. Haddad, F. Dupont, L. Madour, A. Kavanagh, S. Krishnan, S. Park, and H. Kari, | "BUB: Binding Update Backhauling", draft-haddad-mipv6-bub-01.txt, February 2004. | [15] J. Arkko and C. Vogt, "Credit-Based Authorization for Binding Lifetime Extension", | draft-arkko-mipv6-binding-lifetime-extension-00, May 2004. | [16] F. Bao, R. Deng, Y. Qiu, and J. Zhou, "Certificate-based Binding Update Protocol (CBU)", draft-qiu-mip6-certificated-binding-update-02.txt, August 2004. | [17] H. Soliman, C. Catelluccia, K. Malki, and L. Bellier, "Hierarchical Mobile IPv6 | mobility management (HMIPv6)", draft-ietf-mipshop-hmipv6-04.txt, December 2004. | [18] F. Dupont and J. Combes, "Using IPsec between Mobile and Correspondent IPv6 | Nodes", draft-ietf-mip6-cn-ipsec-00.txt, January 2005. | [19] C. Perkins, "Precomputable Binding Management Key Kbm for Mobile IPv6", | draft-ietf-mip6-precfgkbm-01.txt, October 2004. | [20] F. BAO, R. Deng, Y. Qiu, and J. Zhou, "Improvement of Return Routability Protocol", | draft-qiu-mip6-rr-improvement-00.txt, August 2004.