Mobile IP Working Group
Internet-Draft
Expires: August, 2004

Jahanzeb Faizan
Hesham El-Rewini
Southern Methodist University
Mohammad Khalil
Nortel Networks
February, 2004

Problem Statement: Home Agent Reliability
draft-jfaizan-mipv6-ha-reliability-01.txt

Status of this Memo

Copyright Notice

Abstract

In Mobile IPv6, the Mobile Node is dependent on a single Home Agent for the seamless roaming over the Internet. Mobile IPv6 also allows deployment of multiple Home Agents on the home link for providing continuous service to Mobile Node in case of Home Agent failure. But switching of service from the failed Home Agent to another functional Home Agent on the home link is problematic and the base Mobile IPv6 specifications does not currently have well-described solutions. This document aims to describe and illustrate these problems, and propose some guidelines for possible solutions.

Internet-Draft Home Agent Reliability, Problem Statement February, 2004

Table of Contents

1. Introduction

Mobile IPv6[1] is designed to allow a Mobile Node(MN) to change its point of IP subnet attachment in the Internet at the network or IP layer. MN is always identified by it Home Address regardless of its current location. Its mobility is not limited by conventional IP network boundaries. In Mobile IPv6 system the Home Agent(HA) remains at conventional IPv6 subnet called the home link and when the MN is at the home link then the packets sent to it are routed through conventional IPv6[5] routing mechanisms. When the MN is not at home link it registers its remote point of attachment address called Care-of Address with the HA. This allows HA to forward packets, addressed to the MN at its home link, to its current location.

In Mobile IPv6 system, as currently specified, a single HA services multiple MNs. Mobile IPv6 also allows deployment of multiple HAs on the same link so that if the serving HA fails then any other HA on the link can provide service to the MN.

The goal of this draft is to:

- Articulate the problems resulting from the failure of a serving HA and switching of service to another HA.

- Specify a set of framework guidelines to evaluate proposed solutions.

1.1 Overview of the Problem

In Mobile IPv6, MN registers and establishes a connection with only one HA. The MN is reliant on this HA for its connectivity. Thus the HA represents the possibility of a single point of failure for Mobile IPv6. A HA may be responsible for multiple MNs on the home link. The failure of a single HA may then result in the loss of connectivity for numerous MNs located throughout the Internet. Thus the HA and MN

taken together have a shared fate. A MN cannot afford the loss of its HA. To overcome this problem Mobile IPv6 allows deployment of multiple HAs on the home link so that upon the failure of serving HA, another HA can take over the functions of failed HA and thus provide continuous service to the MN(s) registered with failed HA. This transfer of service from the failed HA to a new working HA is problematic and the current specification of Mobile IPv6 does not provide solution to these problems.

1.2 Terminology

Following terms are not re-defined. They are included for the convenience of the readers.

Mobile IPv6
: Mobile IP for IPv6 [1]

Mobile Node (MN)
: A node that can change its point of attachment from one link to another, while still being reachable via its home address.

IP
: Internet Protocol Version 6 (IPv6).[5]

Home Address
: A unicast routable address assigned to a MN, used as the permanent address of the MN. This address is within the MN's home link. Standard IP routing mechanisms will deliver packets destined for a MN's home address to its home link.MNs can have multiple home addresses, for instance when there are multiple home prefixes on the home link.

Home Link
: The link on which a MN's home subnet prefix is defined.

Home Agent (HA)
: A router on a MN's home link with which the MN has registered

its current Care-of address. While the MN is away from home, the HA intercepts packets on the home link destined to the MN's home address, encapsulates them, and tunnels them to the MN's registered Ccare-of address.

Care-of Address
: A unicast routable address associated with a MN while visiting a foreign link; the subnet prefix of this IP address is a foreign subnet prefix. Among the multiple Care-of addresses that a MN may have at any given time (e.g., with different subnet prefixes), the one registered with the MN's HA for a given home address is called its "primary" care-of address.

IPsec Security Association
: An IPSec security association is a cooperative relationship formed by the sharing of cryptographic keying material and associated context. Security associations are simplex. That is, two security associations are needed to protect bidirectional traffic between two nodes, one for each direction.

Home Registration
: A registration between the MN and its HA, authorized by the use of IPsec.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [6].

2. Mobile IPv6 Deployment Scenario

This section describes a basic deployment scenario where multiple HAs, referred as HAs 1..n, have to coexist on the same home link to provide continuous service to MN in case of failure of the serving HA. MN runs Mobile IPv6 MN functionality with the mobility signaling messages protected by IPsec. Also all the HAs 1..n run Mobile IPv6 HA functionality along with IPsec server software. Initially MN is registered and has IPv6 tunnel with HA_1.

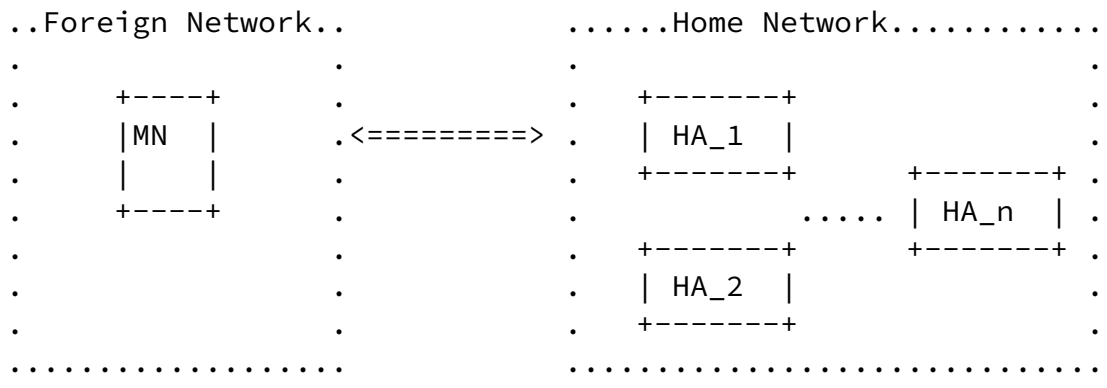

Figure 1

3. Problem statement

This section uses the scenario discussed in section 2 to describe the problems associated with the failure of serving HA and as the result of this switching of service to another HA on the home link. Consider the failure of HA_1. and switching of service to a new HA_x (where x = 2..n) on the same home link. This whole process of failure detection and switching is problematic. The problems are discussed in the following sub-sections.

3.1 Failure

The following sub-sections introduce two possible scenarios of failure.

3.1.1 Home Agent Failure

There could be single or multiple HAs failure on the home link. Since MN could register only with a single HA on the home link which is HA_1 in our scenario, so failure of multiple HAs is not going to effect the normal operation of Mobile IPv6. We are only concerned with the serving HA failure on the home link.

3.1.2 Home Link Failure

There could be failure of home link which will make it inaccessible to the MN. If this occurs then even the serving HA_1 is operational, to the MN it would appear that its serving HA_1 has failed.

3.2 Failure Detection

Transfer of service from the failed HA_1 to new HA_x will occur after the detection of failure by MN. MN could detect the failure of HA_1 under certain conditions. These are listed below.

- o When MN sends Binding Update(BU) message to the failed HA_1 and does not receive matching Binding Acknowledgment(BA) message, it will retransmit BUs until timeout occurs. Upon this MN will come to know about the failure of HA_1.

- o Similarly when MN sends Mobile Prefix Solicitation(MPS) message to the failed HA_1 and does not receive Mobile Prefix Advertisement, it will retransmit MPSs until timeout occurs and that's how it will come to know that HA_1 has failed.

According to Mobile IPv6 MN after sending first BU or MPS message to failed HA_1 will wait for a initial timeout period which is set to INITIAL_BINDACK_TIMEOUT (1 second) in case of BU and INITIAL_SOLICIT_TIMER (3 seconds) in case of MPS. This timeout period will be doubled for each subsequent BU or MPS message until value of MAX_BINACK_TIMEOUT (32 seconds) is reached. MN MAY send infinite BUs or MPSs to failed HA_1 before the final timeout occurs.

So the detection of failed HA_1 will be delayed by a considerable amount of time. Also there will be many messages transmitted over the air interface during this period. Moreover BU and MPS are not periodic rather on demand. MN will send BU only to register new Care-of Address or to extend the lifetime of existing registration with its serving HA. Similarly MN will send MPS only when its serving HA's address is about to become invalid. As a result MN will suffer packet loss and disconnectivity problems. This could have noticeable performance implications on real-time applications.

3.3 Recovery

Once the failure is detected, according to the current specifications of Mobile IPv6 MN will try to register its Care-of Address with any other HA on the home link. For this MN must know which other HAs are available on the home link. MN MAY start Dynamic Home Agent discovery(DHAD)[1] protocol and as a result will get a list of

available HAs on the home link. MN could then select HA_x (in our scenario) on the list as its potential serving HA. MN will send BU message to HA_x setting Home Registration(H) bit.

But this recovery mechanism is problematic. If there is only one HA available on the home link then according to current specifications of Mobile IPv6 even if the retransmission parameter MAX_BINACK_TIMEOUT (32 seconds) is reached MN will continue to send BU messages to the HA_1 until it receives valid BA message and this will never happen because HA_1 has failed. This makes the MN enter into an endless loop.

Even if there are multiple HAs exist (as in our scenario), besides failure detection, there is an extra burden on MN to perform Home Registration with the new HA and in some cases multiple Home Registrations if there are unsuccessful attempts. Also if there is no information about the available HAs on the home link then MN has to perform DHAD. All these factors together result in extra messages overhead on the air interface, service interruption and burden on MN.

3.4 IPsec Security Association with new Home Agent

According to the current specifications of Mobile IPv6 MN and HA_x MUST use IPsec Security Associations to protect the integrity and authenticity of the BUs and BAs. There are two methods of establishing such Associations.

3.4.1 Dynamic Keying

If MN and the new HA_x does not have existing Security Association to protect the BU, IKE[2] (referred as Dynamic Keying) will be initiated according to the guidelines defined in [3]. The latency caused by IKE transactions might cause performance degradation.

3.4.2 Manual Keying

The problem of Dynamic Keying can be avoided by Manual Keying. It involves out-of-band entry of Security Associations in MN and HA. MN can be statically configured for a set of HAs among HAs 1..n and

corresponding Security Associations before launching MN in the Mobile IPv6 network. This will allow MN to register with any other HA and use appropriate Security Associations upon the failure of it's serving HA. But this policy is not flexible enough to accommodate the dynamic nature of home link.

3.5 Correct Ordering

Upon the HA_1 failure the sequence number information in the Binding Cache of HA_1 will also be lost. The new HA_x to which MN will switch will not have the knowledge about the sequence number of last sent BU by the MN. This introduces new security vulnerabilities to the Mobile IPv6.

3.6 Load Balancing

Mobile IPv6 does not include any specification about how the HAs on home link will do load balancing among them. This is important for utilizing the services of all HAs on the home link efficiently.

4. Solution Guidelines

This section describes guidelines for a solution to the above mentioned problems. The sub-sections discuss the guidelines in a decreasing order of importance.

4.1 Security Implications

The solution MUST NOT introduce any new security vulnerabilities to the Mobile IPv6.

4.2 IPsec Security with new Home Agent

The solution SHOULD provide a mechanism to quickly establish IPsec Security Association between the MN and the new HA such that the service interruption is minimal.

4.3 Seamless failure

It is recommended that the failure of HA should be transparent from the MN. This will contribute in minimizing the period of service interruption.

4.4 Mobile Node functionality

The solution SHOULD cause minimal modification to the MN operation as it is defined by Mobile IPv6.

4.5 Messages over air interface

The solution SHOULD use minimal new messages.

4.6 Home Agent addition and failure

The solution SHOULD provide recovery mechanism for the failed HA. Also any new HA added on the home link SHOULD be ready to serve in minimum amount of time possible.

4.7 Load Balancing

The solution SHOULD provide load balancing mechanism for the HAs on the home link. It could be of centralized or distributed nature.

References

[1] Perkins, C., Johnson, D. and J. Arkko, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-24 (work in progress), August 2003.

[2] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[3] Arkko, J., Devarapalli, V. and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", draft-ietf-mobileip-mipv6-ha-ipsec-06 (work in progress), June 2003.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[5] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[6] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Authors' Addresses

Jahanzeb Faizan
Southern Methodist University
Computer Science and Engineering Department.
6425 N Ownby Dr., SIC #300D
Dallas, TX, 75205, USA

Phone +1 214-768-3712, Fax +1 214-768-3085
EMail: jfaizan@smu.edu

Hesham El-Rewini
Southern Methodist University
Computer Science and Engineering Department.
6425 N Ownby Dr., SIC #306C
Dallas, TX, 75205, USA

Phone +1 214-768-3278, Fax +1 214-768-3085
EMail: rewini@engr.smu.edu

Mohammad Khalil
Nortel Networks
Richardson, TX, USA

Phone: +1 972-685-0564
EMail: mkhalil@nortelnetworks

Acknowledgements

The authors would like to thank Vijay Devarapalli and Ryuji Wakikawa for their continuous feedback and helping us improve this draft.

Funding for the RFC Editor function is currently provided by the

Internet Society.

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and

standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary

Full Copyright Statement

Appendix: Changes from Previous Version

The following changes have been made to this document from version 00:

- Addition of types of failure, correct ordering and load balancing sections in the problem statement.

- Also failure detection and recovery sections are explained in more detail in the problem statement.
- IPsec Security Associations with the new Home Agent section is organized into Dynamic and Manual Keying sub-sections.
- Load balancing requirement is added in the solution guidelines section.