

Mobility for IP (MIPSHOP)  
Internet-Draft  
Intended status: Standards Track  
Expires: April 23, 2010

W. Haddad  
M. Naslund  
Ericsson  
October 20, 2009

On Using 'Symbiotic Relationship' to Repel Network Flooding Attack  
draft-haddad-mipshop-netflood-defense-03

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on April 23, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Internet-Draft

Network Flooding Defense

October 2009

## Abstract

This memo describes a simple defense mechanism against a specific type of network flooding attacks. The suggested mechanism requires a mobile node to establish a 'symbiotic relationship' with the infrastructure, in order to empower it to repel such attack while giving enough insurance to the source(s) of the traffic about the need to cease sending traffic to the targeted network.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Conventions used in this document . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Motivation . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Protocol Overview . . . . .	<a href="#">6</a>
<a href="#">5.</a>	New Messages and Options . . . . .	<a href="#">8</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">9</a>
<a href="#">7.</a>	References . . . . .	<a href="#">10</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">10</a>
<a href="#">7.2.</a>	Informative References . . . . .	<a href="#">10</a>
	Authors' Addresses . . . . .	<a href="#">11</a>

## 1. Introduction

Network flooding attacks aim to saturate the targeted network, e.g., the access infrastructure, with junk packets in order to create an environment where all hosts located on a particular link(s) become victims to a denial-of service attack (DoS).

As the name suggests, network flooding attacks targets a whole portion of the network infrastructure instead of targeting one particular node (e.g., SYN flooding attack) and thus, can have a more devastating effect.

This memo describes a simple defense mechanism against a specific type of network flooding attacks. The suggested mechanism requires a mobile (and potentially multihomed) host to establish a 'symbiotic relationship (SR)' as described in [\[I-D.haddad-csi-symbiotic-sendproxy\]](#), with the network infrastructure in order to empower it to repel such attack. In order to be successful, the defense mechanism described as a "counter attack" mounted by the targeted infrastructure must provide enough insurance to the source(s) of harmful traffic about the need to cease sending packets towards the targeted network.

## 2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

### 3. Motivation

It is safe to assume that any practical defense against network flooding attacks does not need to be motivated! However, we feel important to highlight how such attack can be mounted in a mobile and/or multihomed environment(s) and describe the current defense mechanism and its consequences on the mobile node (MN).

A specific type of network flooding attack can be launched from using Mobile IPv6 protocol (described in [[I-D.ietf-mext-rfc3775bis](#)]). Such attack is mounted by having the malicious MN attaching to the targeted network then updating each of its correspondent nodes (CNs) about its new care-of address (CoA) by sending binding updates (BU) messages. Once the update(s) is done, each CN is supposed to start re-routing data packets to the MN's new CoA. The next step for the attacker is to detach itself from the foreign link while keeping sending ACK messages to each CN via its home agent (HA). Such step requires the MN to switch to another network or to use another interface in case it is multihomed. However, the impact will be the same on the targeted network in both scenarios, since each CN will keep sending data packets to the MN's CoA as long as it keeps receiving ACK messages and the binding lifetime has not expired (for

more details, refer to [[RFC4225](#)]).

In MIPv6 protocol, the defense against the type of network flooding attack described in the above, is provided by repeating the return routability (RR) procedure every 7 minutes. This means also that even if the MN is not moving, then it has to perform the HoTI/HoT and CoTI/CoT signaling exchange with each correspondent node (CN). It follows that a significant amount of signaling messages can be imposed on the MN in some cases.

Enhanced Mobile IPv6 (EMIPv6), described in [[RFC4866](#)], introduces a strong optimization to MIPv6 protocol by exploiting the crypto-generated address technique [[RFC3972](#)] for the purpose of establishing a long lifetime bidirectional security association (SA) between the MN and the CN. However, while EMIPv6 succeeds in reducing the load of signaling messages, it does not provide strong defense against the type of network flooding attack described earlier.

Our main motivation in this document is to provide an efficient and simpler mechanism, which enables the targeted (visited) network to repel network flooding attacks mounted by an attacker using mobility and multihoming protocols.

#### [4.](#) Protocol Overview

In order to empower the network infrastructure to repel the type of network flooding attack described earlier, the suggested protocol puts a strong -yet neutral in its effect- requirement on any node attaching to the network access infrastructure. The new requirement consists on establishing an SR with any public key(s) advertised by the access router (AR) in the router advertisement (RtAdv) messages. This is motivated by the fact that an AR may or may not be the node(s), which can launch a counter attack to repel the flooding attack. Consequently, the AR has to advertise the public keys of other dedicated node(s), which has this feature. It follows, that a main assumption in our protocol is to have the secure neighbor discovery [[RFC3971](#)] protocol deployed in the targeted infrastructure. For simplicity reasons, we assume in the following that the AR is the

node able to carry counter attacks if/when needed. This means that no additional public key(s) is advertised in the RAdv messages.

When configuring its IPv6 address, e.g., CoA, the MN MUST establish the SR and sends back the RAN(128) to the AR. The MN SHOULD encrypt the RAN(128) with the AR's public key and the latter SHOULD NOT allow access to any node which does not establish an SR upon attachment to its corresponding link(s). Upon receiving a neighbor discovery message [[RFC4861](#)] carrying the SR component, the AR should validate it before storing it in its cache memory. Only after storing the SR in its cache memory and approving it in a signed NDP message, that a MN can trigger the exchange of mobility signaling messages with the CN(s), in order to request re-routing data traffic to its new CoA.

Let's assume that after resuming data packets exchange using its new CGA, the MN (being malicious!) decides to mount the same type of network flooding attack against the visited network. This means that once it has synchronized the transmission of ACK messages sent via other paths with data packets rates received from the CNs, it can detach itself from the foreign link and keep sending ACK messages to the CNs at the appropriate frequencies.

After leaving the link, the AR will notice at some point (e.g., using NDP messages) that the MN has vanished while data packets are still routed to the MN's CoA. At this stage, the AR MAY decide to act immediately or within a pre-configured time interval. In both scenarios, the AR will launch its counter attack by fetching first all IP source address(es) carried in data packets sent to the MN's CoA, then sending a new mobility message (called "Flush Request (FR)") to each corresponding CN. The FR message MUST carry the MN's CoA together with the SR corresponding "proof of relationship (PoR)" and MUST be signed with the AR's CGA private key.

Upon receiving a FR message, the CN validates it by checking first if the CoA is stored in its binding cache entries (BCE) table. Then, it checks in the following order:

- the SR PoR
- the AR's CGA address
- the signature

If the FR message is valid, the CN MUST immediately flush out the MN's CoA from its BCE and tear down all ongoing sessions using the MN's IPv6 home address which is bind to the CoA carried in the FR message. Then, the CN SHOULD send a "Flush Acknowledgment (FA)" message to the AR which MUST carry the token and the PoR. Finally, the CN MUST also sign the FA message with its CGA private key. In case any of the above validation steps fail, the CN SHOULD silently discard the message and keeps exchanging data packets with the MN.

As mentioned earlier, the AR MUST send a FR message to each CN in order to completely stop the attack. This means that the intensity of the flooding attack should gradually decrease gradually before it comes to a halt.



TBD

## 6. Security Considerations

This document describes a defense mechanism against a specific type of network flooding attack which can be mounted by one or many malicious node(s) having to attach to the targeted network before triggering the attack. Consequently, the main goal behind this document is to increase the overall network infrastructure security. It should be noted however, that the suggested defense mechanism loses its efficiency when the CN is also involved in the attack.

A key feature in our mechanism is the SR between any host and the AR. However, such feature can easily be turned into a denial-of-service (DoS) attack against the host itself in case it accepts to establish an SR with any node whose claimed certificate cannot be verified. It follows that a key requirement is to have SeND deployed in order to protect the link between the AR and the MN. Note that in case the AR gets compromised then it can send at anytime an FR message to the CN to tear down the MN's ongoing session(s). However, such scenario is no different than having the AR dropping data packets sent to the MN.

Finally, it should be noted that the AR is not taking any step in order to protect the CN against attacks which aim to exhaust its processing power by flooding it with fake FR messages. In fact, there are three reasons for not imposing a preventive step, e.g., a CoTI/CoT message exchange. First, the CN is able to check the SR before it validates the signature. This means that the CN will drop the message in case the SR is not valid. The second reason is that the RAN(128) parameter is sent in an encrypted form to the AR only. Consequently, prior to sending an FR message, the SR is known only by the MN and its AR. The third one is the fact that after sending a FR message, the MN's CoA won't be used anymore so disclosing it in a FR message should not introduce any new threat against the CN.

Internet-Draft

Network Flooding Defense

October 2009

## [7.](#) References

### [7.1.](#) Normative References

- [I-D.ietf-mext-rfc3775bis]  
Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [draft-ietf-mext-rfc3775bis-04](#) (work in progress), July 2009.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.
- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.
- [RFC4225] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", [RFC 4225](#), December 2005.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.
- [RFC4866] Arkko, J., Vogt, C., and W. Haddad, "Enhanced Route Optimization for Mobile IPv6", [RFC 4866](#), May 2007.

### [7.2.](#) Informative References

- [I-D.haddad-csi-symbiotic-sendproxy]  
Haddad, W. and M. Naslund, "On Secure Neighbor Discovery Proxying Using 'Symbiotic' Relationship", [draft-haddad-csi-symbiotic-sendproxy-01](#) (work in progress), July 2009.

Internet-Draft

Network Flooding Defense

October 2009

Authors' Addresses

Wassim Michel Haddad  
Ericsson  
6210 Spine Road  
Boulder, CO 80301  
US

Phone: +1 303 473 6963  
Email: [Wassim.Haddad@ericsson.com](mailto:Wassim.Haddad@ericsson.com)

Mats Naslund  
Ericsson  
Torshamnsgatan 23  
SE-164 80 Stockholm  
Sweden

Phone: +46 8 58533739  
Email: [Mats.Naslund@ericsson.com](mailto:Mats.Naslund@ericsson.com)

Haddad & Naslund

Expires April 23, 2010

[Page 11]