Network Working Group
Internet-Draft
Expires: June 1, 2009

K. Weniger

G. Velev (Ed.)
Panasonic

November 28, 2008

MIPv6 Correspondent Node-Targeted Location Privacy and Optimized Routing
draft-weniger-mobopts-mip6-cnlocpriv-03

Status of this Memo

Abstract

This document discusses the problem of correspondent node-targeted location privacy in Mobile IPv6 and proposes a mechanism to achieve simultaneous optimized routing and full correspondent node-targeted IP address location privacy. The mechanism utilizes the MIPv6 bootstrapping mechanisms and does neither require any new network entities nor changes to home agent or correspondent node implementations.

Table of Contents

1. Terminology

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].

The terminology of [RFC3775] and [RFC5026] is used. Additionally, the following terms are introduced:

IP Reachability Home Agent (IRHA): A home agent as specified in [RFC3775] that provides IP reachability and global session continuity for the mobile node.

Home Address for IP Reachability (HoA_IR): A home address used for IP reachability and session continuity and that is registered at the IRHA. This home address is independent of the location of the mobile node and is disclosed to potential correspondent nodes (e.g., by publishing the address in DNS).

Optimized path: A path between mobile node and correspondent node that is shorter than the IP reachability path, but may be longer than the optimal path. The IP Reachability path is the path between mobile node and correspondent node if the mobile node uses bi-directional tunneling mode with the IRHA. The optimal path is the end-to-end path between mobile node and correspondent node, e.g., the path in MIPv6 Route Optimization mode.

Optimized routing: Routing data packets over the optimized path

Optimized Routing Home Agent (ORHA): A home agent as specified in [RFC3775] that is used for providing optimized routing. It must support the bootstrapping mechanisms specified in [RFC5026] and should be located close to the correspondent node.

Home Address for Optimized Routing (HoA_OR): A home address used for optimized routing and session continuity and that is registered at

the ORHA. This home address is usually not public (i.e., not published in DNS).

Eavesdropper-targeted location privacy: Hiding the mobile node's location from nodes eavesdropping on the path between mobile node and correspondent node (and home agent)

Correspondent node-targeted location privacy: Hiding the mobile node's location from the correspondent node

Full IP address location privacy: Ensuring that no information about a mobile node's current location can be derived from the mobile node's IP address by other nodes, not even the current access network or subnet of the mobile node.

2. Introduction and Problem Definition

Location privacy is the ability to hide a user's location from other users. This is considered to be an important feature, since disclosure of the location can have serious impacts on the user's life. In general, location privacy can be achieved by hiding the relation between identity and location of a user. In Mobile IPv6 [RFC3775], the care-of address and the home address typically represent topological location and identity of a mobile node, respectively. Note that a dynamically assigned home address does not represent a permanent identity itself, but a mapping to one of the mobile node's permanent identifiers is typically published for IP reachability reasons (e.g., in DNS), so that other nodes are able to find out the mobile node's current home address to initiate a session with the mobile node. Consequently, in Mobile IPv6 at least either the care-of address or the home address must be hidden from anyone that is not authorized to obtain the location of the mobile node. Two rather orthogonal sub-problems of location privacy for Mobile IPv6 can be distinguished: hiding the location from eavesdroppers on the path and hiding the location from the correspondent node, which we henceforth call eavesdropper-targeted and correspondent node-targeted location privacy, respectively (see [RFC4882] for details

about the Mobile IPv6 location privacy problem). This document is concerned with correspondent node-targeted location privacy only, especially with the problem of providing optimized routing at the same time. Eavesdropper-targeted location privacy is out of scope, but can be achieved by combining the mechanisms in this document with pseudo home address mechanisms [I-D.irtf-mobopts-location-privacy-solutions]. Any location privacy issues not directly related to Mobile IPv6 are out of the scope of this document.

An example scenario illustrating the problem is the following: A mobile node uses Mobile IPv6 with a public home address and wants to hide its location. The home address can be a dynamically assigned home address that is linked to a mobile node's public permanent identifier (e.g., FQDN in DNS). The mobile node requires full correspondent node-targeted IP address location privacy, i.e., hiding only the mobility within an access network and revealing the access network prefix to the correspondent node is not acceptable. An application on the correspondent node initiates a delay-sensitive session such as VoIP by sending packets to the mobile node's public home address. Initiating an IP session typically requires the correspondent node to already know the mobile node's identity and thus the mobile node's public home address. The mobile node receives the packets in bi-directional tunneling mode from its home agent and may start sending packets back to the corresponding node. Let's assume the mobile node is located in the United States and the

correspondent node is located in Canada, whereas the mobile node's home agent is located in Europe. Since the mobile node is far away from home, the packet delay and hence the user experience is far from what could be achieved. One approach to reduce the end-to-end packet delay is to use MIPv6 route optimization. However, if the mobile node uses route optimization mode, it reveals its CoA and hence its location to the correspondent node. Note that the correspondent node can also be an attacker that just initiates a session to find out the mobile node's location. Consequently, the mobile node has the choice: it can have good user experience without location privacy or location privacy with bad user experience. Currently, there is no way to achieve both simultaneously with Mobile IPv6.

This document proposes a mechanism that can provide full correspondent node-targeted IP address location privacy and optimized

routing simultaneously. Home agent and correspondent node are unchanged and no new entities or messages are introduced. The basic idea is that the mobile node uses a mobility service provided close to the correspondent node's domain. More specifically, the mobile node bootstraps with a home agent (henceforth called the ORHA), which is located topologically close to the correspondent node (in the above example, e.g., in Canada) and which is used for optimized communication with this correspondent node. A location close to the correspondent node ensures that no location information is contained in the home address HoA_OR anchored at the ORHA while ensuring that the route via the ORHA is shorter (or at least not significantly longer) than the route via the IRHA in bi-directional tunneling mode. For mobile node-initiated sessions with a particular correspondent node, the mobile node uses the ORHA located topologically close to the correspondent node in bi-directional tunneling mode and HoA_OR is used as IP address for the session by higher layers. For correspondent node-initiated sessions, the public home address HoA_IR is used as IP address by higher layers and the mobile node registers the HoA_OR as care-of address at the correspondent node.

3. Related work

Qui et. al. [I-D.irtf-mobopts-location-privacy-solutions] propose a solution to the correspondent node-targeted location privacy problem. The basic idea is to hide the home address from the correspondent node in route optimization mode by using a pseudo home address instead of the real home address. Although the care-of address is revealed to the correspondent node, location privacy is protected by

hiding the identity (i.e., real home address) of the mobile node from the correspondent node. This approach has also been proposed in [I-D.dupont-mip6-privacyext]. However, if the correspondent node initiates the communication, location privacy is usually compromised, since the real home address is already known by the correspondent node. And even if the real home address can be hidden from the correspondent node, location privacy is compromised if the correspondent node is able to figure out the mobile node's identity by any other means on higher layers (e.g., during the conversation).

[RFC5026] and [I-D.ietf-mip6-bootstrapping-integrated-dhc] specify the mechanisms for Mobile IPv6 bootstrapping in the split and the integrated scenario, respectively. They allow a mobile node to bootstrap with any home agent, for which the necessary trust relationships are in place. When bootstrapping with a local home agent, optimized routing can be achieved in bi-directional tunneling mode. However, since the home address obtained from a local home agent belongs to the network the mobile node is currently visiting, it contains location information. Consequently, location privacy is compromised, if the correspondent node knows that the home agent is local to the mobile node (see security considerations of [RFC5026]). Although in many cases the correspondent node will not know, there are cases where the correspondent node can find out whether the mobile node's home agent is local or remote. For instance, a correspondent node may know that a mobile node's home agent is local because the mobile node's Mobility Service Provider (MSP) is known to always assign local home agents for routing efficiency reasons.

4. Applicability Statement

The mechanisms defined in this document require that the mobile node is able to utilize a mobility service, which is offered close to the correspondent node's domain. To allow optimized communication with many or even any correspondent node, it is required that home agent services are offered to the mobile node from various topological locations. This typically requires that an MSP offers mobility service from many different locations or that multiple MSPs have some kind of roaming relationships with the mobile node's mobility service authorizer (MSA), so that a group of MSPs offers mobility service from many different locations. Such roaming relationships can be based on an AAA infrastructure.

This assumption is not particular to this document: the MIPv6 bootstrapping solutions for the split scenario [RFC5026] and the integrated scenario [I-D.ietf-mip6-bootstrapping-integrated-dhc] also require that a roaming relationship between MSP and MSA exist (see also [RFC4640]). In the integrated scenario the access service authorizer (ASA) is also the mobility service authorizer (MSA). An important point of the integrated scenario is that the access service provider (ASP) that the mobile node is currently visiting is typically also an MSP, which provides local home agent service. This means that roaming relationships between many MSPs and the mobile node's MSA are required and, assuming global roaming, that home agent services must be offered to the mobile node from various topological locations. This represents the requirements mentioned in the beginning of this section. So the assumptions are basically not different from the assumptions for MIPv6 bootstrapping and can be met by re-using the home agents, roaming relationships, and the credentials that are already deployed for MIPv6 bootstrapping.

Note that it is not required that the ORHA is located within the correspondent node's domain. A domain nearby to the correspondent node's domain is sufficient to achieve location privacy and improved routing efficiency. However, if the mobile node is not able to discover a home agent located close to the correspondent node or if no roaming relationship to the MSP of such home agent exists, simultaneous optimized routing and correspondent node-targeted location privacy cannot be provided by the mechanisms defined in this document.

It is further assumed that the mobile node is authorized by the MSA to use ORHAs which are located close to the correspondent node and which potentially belong to an MSP different from the MSA. Since location privacy can be seen as a value-added service, a user may be willing to pay for this service. This may be an incentive for an MSA to offer this service and delegate the mobility management to an MSP

located close to the correspondent node.

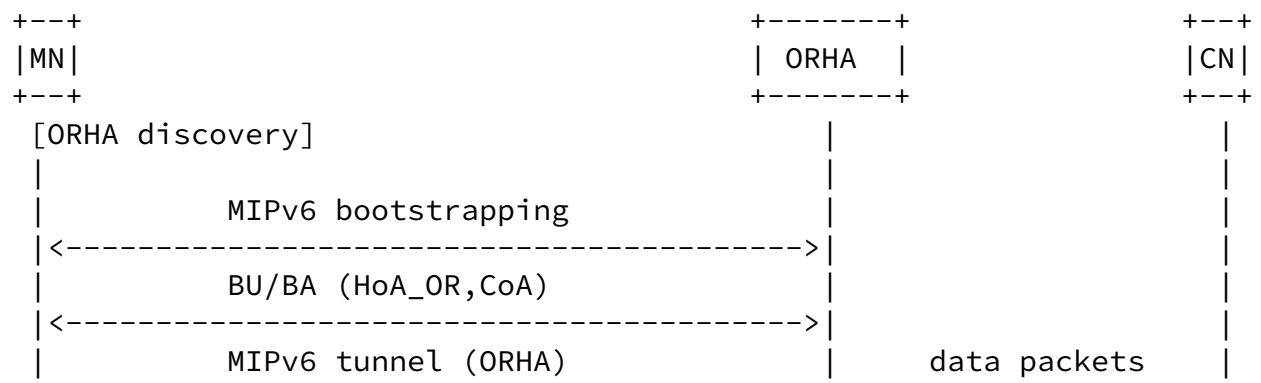
Finally, this optimization requires that the mobile node is able to handle multiple simultaneous registrations with different home agents and multiple home addresses. Also, the MSA/MSP must support the assignment of multiple home agents and home addresses to the same mobile node.

5. Changes to Mobile Node Operation

The mobile node operation is split in two cases: route optimization for new sessions (i.e., communication sessions that have not yet started) and route optimization for ongoing sessions. A session is defined in this context by an application layer context bound to the IP addresses of the two endpoints, with one of them being the mobile node's home address. The first case applies, e.g., if the mobile nodes wants to initiate a session with a correspondent node and decides to optimized the route before sending the first data packets. The second case applies, e.g., if the correspondent node initiates a session with the mobile node or if the mobile node decides to optimize the route of an ongoing session.

5.1. Route Optimization for New Sessions

The mobile node first tries to discover an ORHA (refer to Section 6 for details about the ORHA discovery). If the discovery is successful, the mobile node bootstraps with the ORHA and uses it in bi-directional tunneling mode for communication with the correspondent node. Existing registrations with other home agents are kept for communication with other correspondent nodes. The HoA_OR is not made public, i.e., no DNS update should be triggered for this home address. Since no correspondent node registration is initiated, the care-of address is hidden and correspondent node-targeted location privacy is ensured. An exemplary signaling flow is shown in Figure 1.



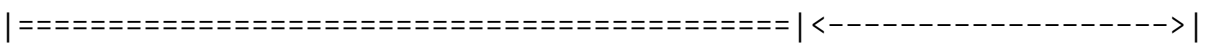


Figure 1: Signaling flow for optimization of the route for a session that has not yet started

Location privacy is provided, since the correspondent node only learns the HoA_OR, which contains no information about the mobile node's location.

5.2. Route Optimization for Ongoing Sessions

After the mobile node has decided to optimize the route of a session (e.g., after receiving the first data packets tunneled by the IRHA and originated from the correspondent node), it discovers an ORHA and bootstraps with this ORHA. Since the communication session is based on HoA_IR, packets are routed through the IRHA. To achieve optimized routing, the mobile node uses route optimization mode over the reverse tunnel to the ORHA, i.e., care-of test messages, binding update messages, and later data packets destined for the correspondent node are sent over the reverse tunnel to the ORHA. While establishing the optimized path over the ORHA, the mobile node can send and receive data packets over the IRHA.

To achieve location privacy, the mobile node uses HoA_IR as home address and HoA_OR as care-of address in the context of the route optimization mode. This results in the following headers for packets sent by the mobile node for the session with the correspondent node (IPsec for signaling protection to ORHA assumed):

Data packets and binding updates:

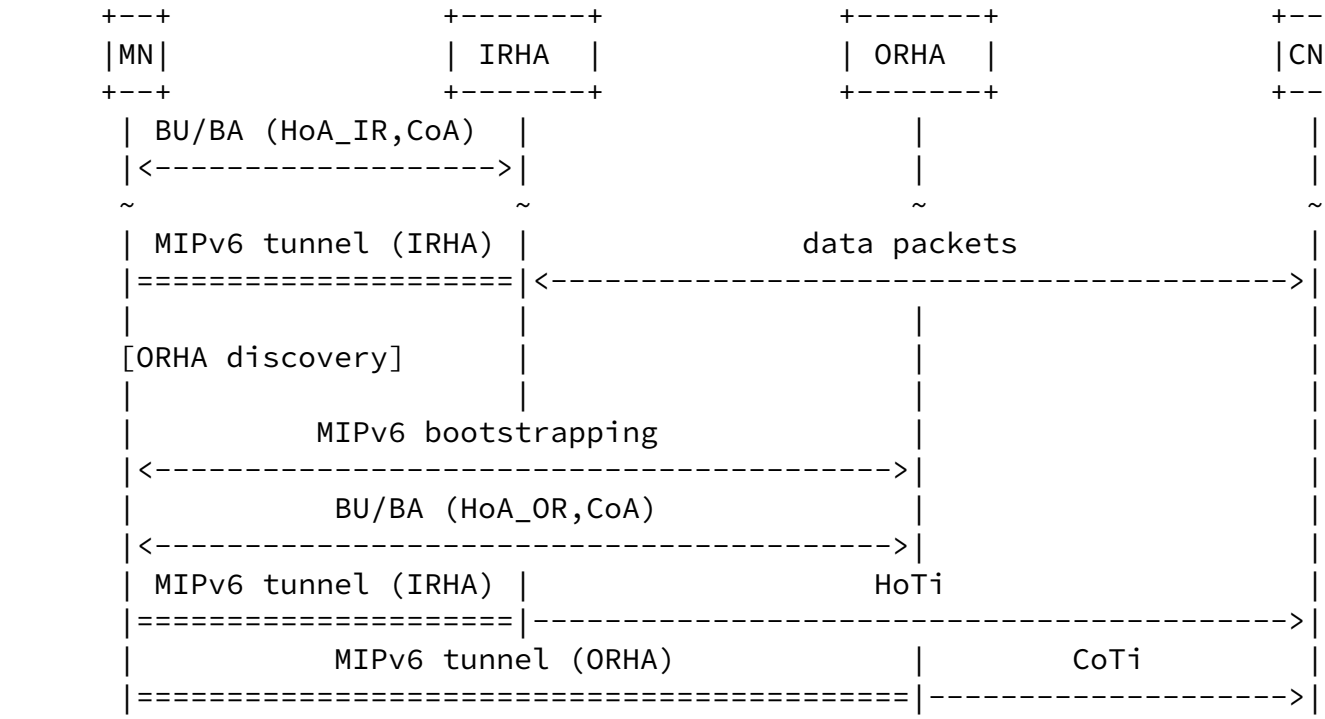
```
IPv6 header (source      = care-of address,
             destination = ORHA)
ESP header in tunnel mode
IPv6 header (source      = HoA_OR,
             destination = correspondent node)
Destination Options header
   Home Address option (HoA_IR)
Any protocol
```

Care-of Test Init:

```
      IPv6 header (source      = care-of address,
                   destination = ORHA)
      ESP header in tunnel mode
      IPv6 header (source      = HoA_OR,
                   destination = correspondent node)
      Any protocol
```

Since from the correspondent node's point of view, HoA_OR is the care-of address and the HoA_IR is the home address of the mobile node, data packets sent by the correspondent node to the mobile node

contain the HoA_IR in the type 2 routing header and the HoA_OR in the destination address field of the IP header. Consequently, the data packets are intercepted by the ORHA and tunneled to the mobile node. An exemplary signaling flow is shown in Figure 2.



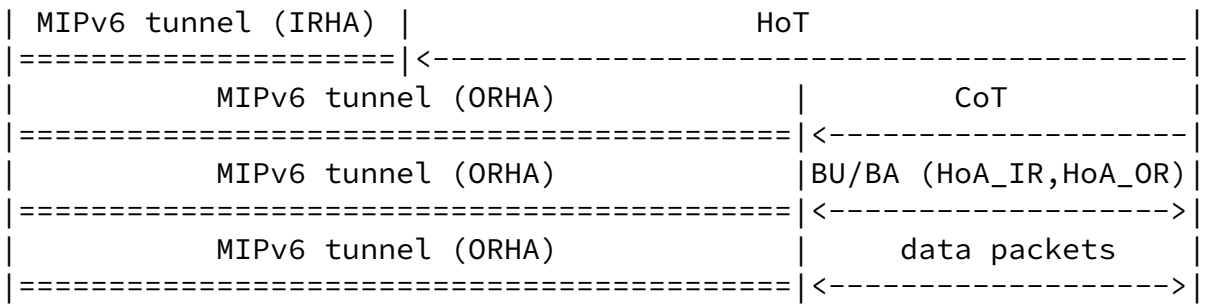


Figure 2: Signaling flow for optimization of the route for an ongoing session

Location privacy is provided, since the correspondent node only learns HoA_OR and HoA_IR, which both do not contain any information about the mobile node's current location.

Note that upon changing the care-of address, the mobile node does not send binding updates to the correspondent node over the reverse tunnel to the ORHA, because the care-of address in this context is the HoA_OR.

5.3. Route Optimization Mode Selection

The mobile node has to decide for every correspondent node, whether it wants to use bi-directional tunneling mode, route optimization mode or the mechanisms described in this document. How this decision is made and when the route optimization is triggered is implementation specific. Generally, for non-delay-sensitive services such as simple web browsing, bi-directional tunneling to the home agent is sufficient and achieves full correspondent node-targeted IP address location privacy. If no location privacy is required, Mobile IPv6 route optimization mode can be used.

Since the number of simultaneously used home agents have impacts on the overall signaling overhead and resource consumption on the mobile node, the mobile node should try to minimize the number of simultaneously used ORHAs and only use the mechanisms specified in this document for sessions that require simultaneous optimized routing and correspondent node-targeted location privacy. Note

however that we are currently not aware of any realistic scenario where a mobile node would have active sessions with a large amount of different correspondent nodes simultaneously and all those sessions require simultaneous optimized routing and correspondent node-targeted location privacy. Optimizations to improve scalability in such extreme scenarios may be developed later.

5.4. Source Address Selection

Since the mobile node will typically use different home addresses for communication with different correspondent nodes when using the route optimization mechanisms defined in this document, the mobile node must be able to select the right home address as source address for packets to be sent to a specific destination address. This can be achieved with the source address selection mechanisms defined in [RFC3484]. If the ORHA is located in the correspondent node's domain, the prefix of the home address anchored at the ORHA is similar to the prefix of the correspondent node and rule 8 of the default source address selection [RFC3484] applies. For other cases, dynamically adding entries for HoA_OR and correspondent node address with matching labels in the policy table [RFC3484] when route optimization according to this document is triggered would prefer a home address as source address for communication with a specific correspondent node. However, since this is implementation specific, the details of the source address selection are out of the scope of this document.

6. Location-dependent Home Agent Discovery

The mechanisms defined in this document require the discovery or assignment of an ORHA, i.e., of a home agent located close to the correspondent node. One options is to pre-configure the necessary information on the mobile node, e.g., a list containing home agent addresses and distances to various prefixes. Two options for dynamic discovery are proposed in the following.

The first option is to re-use the DNS-based home agent discovery specified in [RFC5026]. The mobile node would construct the FQDN,

e.g., based on the correspondent node's address, prefix or host name. The DNS entry can be maintained by the MSP of the ORHA (e.g., "ORHA.CNdomain.com") or by the MN's MSA (e.g., "CNdomain.ORHA.MSAdomain.com"). Anycast-based home agent discovery using IKEv2 extensions [I-D.dupont-ikev2-haassign] or DHAAD [RFC3775] is also possible. The mobile node would, e.g., construct the anycast destination address based on the correspondent node's prefix.

A second option is to query a dedicated server that is able to map an FQDN, prefix or address of a correspondent node to an FQDN or address of a home agent that is located in or topologically close to the correspondent node's domain. This server can, e.g., be provided by a third party in the public Internet or by the mobile node's Mobility Service Authorizer (MSA). The mobile node would query this server to discover the ORHA address.

This option can, e.g., be realized by re-using DHCP-based HA assignment with the options and mechanisms defined in [I-D.ietf-mip6-bootstrapping-integrated-dhc] and [I-D.ietf-mip6-hiopt]. During network authentication, the MSA would send to the Network Access Server (NAS) the home agent information for all the MSPs, which the mobile node is authorized to use. Once the mobile node wants to request a home agent close to the correspondent node, it sends a DHCP Information Request message and appends a Home Network Information Option [I-D.ietf-mip6-hiopt] with a home network parameter suboption containing the correspondent node's domain as target domain. The id-type can be set to 1 (target MSP) or to a newly defined value for this purpose. The NAS would then select a home agent from the set of authorized home agents that is in (id-type 1) or close (new id-type) to the target domain specified in the Home Network Information Option. How this selection is done may be done in an implementation and operator specific way. A simple selection algorithm would be to return a home agent with the domain name equal to the target domain, if such home agent is part of the list of authorized home agents, and otherwise return an home agent from the home MSP or an empty Home Network Information option. Finally, the NAS would assign the selected home agent to the mobile

node by putting the corresponding information in the Home Network Information Option of the DHCP reply message.

Since the ORHA learns the location of the mobile node, the mobile

node must be sure that the ORHA doesn't reveal the mobile node's location to nodes not authorized to get this information, i.e., the ORHA must be trusted by the mobile node. How the trust verification is done depends on the ORHA discovery mechanism in use. One option is that the MSA knows which home agents are trusted with respect to location privacy and only assigns such home agents to the mobile node (i.e., only sends addresses of trusted home agents to the NAS or only maintains DNS entries for trusted home agents). The MSA could also deny the authorization request if the MN tries to bootstrap with an untrusted home agent. Another option is that the mobile node verifies the trust by itself, e.g., by pre-configuring a list of trusted home agent addresses on the mobile node or by using certificates.

7. Security Considerations

With the solution described in this document, a correspondent node may learn at most the mobile node's addresses HoA_OR and HoA_IR. HoA_IR is a permanent address used for IP reachability and hence doesn't contain any information about the mobile node's current location. Since HoA_OR is anchored close to the correspondent node, there is no relation between HoA_OR and the mobile node's current location as well and the correspondent node cannot infer mobile node's real location from HoA_OR. The correspondent node may wrongly believe that mobile node is close to himself, though. If the correspondent node knows both HoA_OR and HoA_IR (the latter e.g., from DNS or during the return routability procedure), it may wrongly think that the mobile node has roamed from HoA_IR to HoA_OR. However, since the mobile node can bootstrap with a new ORHA and use a new HoA_OR without moving and since the mobile node does not change HoA_OR cased on movements, the correspondent node cannot infer the mobile node's real movement patterns just from HoA_OR and HoA_IR.

An attacker could initiate many faked communication sessions by spoofing the source address in order to trigger the mobile node to discover and bootstrap with many home agents. This could consume significant resources on the mobile node and in the network and may cause a DoS. As a countermeasure, the mobile node should not start bootstrapping automatically without further checks when the correspondent node initiates a session (especially if active ORHA sessions already exist) or it should limit the number of ORHAs it may be registered with simultaneously. Faked sessions should be identified as such as quickly as possible and the mobile node should de-register immediately from ORHAs that only served faked sessions.

The ORHA knows the location of the mobile node and could distribute it to third parties without authorization from the mobile node. Hence, the mobile node must be sure that the ORHA is trusted before the mobile node reveals its location to the ORHA. How this can be done is detailed in Section 6. Note that the fact that the ORHA and the correspondent node may be in the same administrative domain doesn't imply that the ORHA reveals the mobile node's location to the correspondent node. This is also true in today's cellular networks, where it is ensured that users of a service provided by a particular mobile operator don't know the location of other users using a service provided by the same operator.

The return routability procedure over the reverse tunnel to the ORHA is not considered less secure than the standard return routability procedure as long as the ORHA is trusted and the ORHA link is not vulnerable to eavesdropping.

This document is concerned with correspondent node-targeted location privacy only. Eavesdropper-targeted location privacy and any location privacy issue not directly related to Mobile IPv6 are out of the scope of this document.

8. Acknowledgements

Thanks to Kuntal Chowdhury, Vijay Devarapalli, Rajeev Koodli, and Ahmad Muhanna for their valuable comments and suggestions to improve this document.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4882] Koodli, R., "IP Address Location Privacy and Mobile IPv6: Problem Statement", RFC 4882, May 2007.

[RFC5026] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

9.2. Informative References

[I-D.dupont-ikev2-haassign]
Weniger, K. and F. Dupont, "IKEv2-based Home Agent Assignment in Mobile IPv6/NEMO Bootstrapping", draft-dupont-ikev2-haassign-02 (work in progress), January 2007.

[I-D.dupont-mip6-privacyext]
Dupont, F., "A Simple Privacy Extension for Mobile IPv6",

draft-dupont-mip6-privacyext-04 (work in progress), July 2006.

[I-D.ietf-mip6-bootstrapping-integrated-dhc]
Chowdhury, K. and A. Yegin, "MIP6-bootstrapping for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-06 (work in progress), April 2008.

[I-D.ietf-mip6-hiopt]
Jang, H., Yegin, A., Chowdhury, K., and J. Choi, "DHCP Options for Home Information Discovery in MIPv6", draft-ietf-mip6-hiopt-17 (work in progress), May 2008.

[I-D.irtf-mobopts-location-privacy-solutions]
Ying, Q., Zhao, F., and R. Koodli, "Mobile IPv6 Location Privacy Solutions", draft-irtf-mobopts-location-privacy-solutions-10 (work in progress), November 2008.

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[RFC4640] Patel, A. and G. Giaretta, "Problem Statement for bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006.

Authors' Addresses

Kilian A. Weniger

Email: kilian.weniger@googlemail.com

Genadi Velev
Panasonic R&D Center Germany
Monzastr. 4c
Langen 63225
Germany

Email: genadi.velev@eu.panasonic.com

Intellectual Property