Network Working Group
Internet-Draft
Expires: April 24, 2006

K. Weniger
T. Aramaki
Panasonic

October 21, 2005

Route Optimization and Location Privacy using Tunneling Agents (ROTA) draft-weniger-rota-01

Status of this Memo

Copyright Notice

Abstract

Mobile IPv6 in route optimization mode reveals mobile node's care-of address to the correspondent node and hence cannot provide location privacy. In contrast, Mobile IPv6 in bi-directional tunneling mode can provide location privacy, but the resulting route may be far from optimal, especially when correspondent node is mobile as well. This may be an issue for conversational mobile-to-mobile communication scenarios, e.g., using VoIP. The draft discusses the problem of providing both location privacy and route optimization with Mobile

IPv6 and describes a solution in terms of an optional extension to Mobile IPv6. The basic idea is that mobile nodes switch the reverse tunnel endpoint in bi-directional tunneling mode from their home agent to a so-called tunneling agent in an on-demand manner. To ensure location privacy, the tunneling agent selection is done by the home agents. The solution does not require the mobile node to change its home address and does not rely on visited network support.

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 [1].

In addition to the terminology used in [3], the following acronyms are used:

Acronym	Meaning
MN	Mobile node
CN	Correspondent node
HA	Home agent
HoA	Home address
CoA	Care-of address
BU	Binding update
BA	Binding acknowledgement
TA (of node X)	A tunneling agent (TA) is a logical entity that is a tunnel endpoint for node X on behalf

		of node X's HA, with node X's HoA matching a subnet prefix of node X's HA, but not matching a subnet prefix of the TA. A TA can be co-located with an HA (with both entities serving different nodes) or MAP.

2. Introduction and Problem Description

2.1 Background

Location privacy is the ability to hide the location from others. This is considered to be an important feature for mobile users, since the disclosure of the location can have serious impacts on the user's life. Because the routing in the Internet is hierarchical, IP addresses used for global routing usually contain location information. Moreover, protocol extensions, e.g., to DNS as well as software tools exist that can be used to derive the approximate geographic location from a globally routable IP address [10][7].

In Mobile IPv6 [3], HoA and CoA usually represent identity and location of the MN, respectively. Currently, two modes are defined in [3]: bi-directional tunneling and route optimization. While the former mode requires all data packets to be routed over the home agent of the MN, the latter utilizes the direct path between MN and CN. As a consequence, route optimization mode usually reduces the packet delay, which is beneficial for interactive applications. However, it does not provide location privacy, since the CN learns MN's CoA and, thus, the topological location of the MN. In contrast,

bi-directional tunneling mode does not reveal MN's CoA to CN, since BU messages containing MN's CoA and data packets with MN's CoA in the IP header are terminated at MN's HA. Thus, MN's location can be hidden from CN (see section 2.1 of [8]). However, bi-directional tunneling may lead to long routes, especially if CN is mobile as well. Since mobile-to-mobile communications with conversational nature (e.g., with VoIP) is considered to be a common scenario in the future, the utilization of standard Mobile IPv6 in bi-directional tunneling mode for location privacy-enabled communication may be inefficient and may delay packets to an extent that is harmful to the communication. Hence, a mechanism that provides both location privacy and route optimization, resulting in higher efficiency and lower packet delays than bi-directional tunneling mode, is desirable.

2.2 Problem Statement

The first part of the problem is to provide location privacy to mobile nodes. In the context of Mobile IPv6, two problems are considered to be the most important: preventing the disclosure of MN's CoA to CN and preventing the disclosure of MN's HoA to eavesdropper [7]. While many currently discussed proposals address the second problem, this document addresses the first one, i.e., the disclosure of the CoA to CN. The solution shall support full and bi-directional location privacy, meaning that the MN's location may not be revealed to a mobile CN and vice versa and that disclosing the location with lower resolution (e.g., MN's visited domain prefix is

disclosed instead of prefix of MN's AR) is not an acceptable level of privacy. Profiling and tracking issues such as hiding MN's HoA from eavesdroppers or other aspects of privacy not directly related to Mobile IPv6 addresses, such as the profiling based on lower- or upper-layer identities or based on protocol values [9] are out of the scope of this document. However, it should be possible to combine solutions for those problems with the solution proposed in this document.

A second part of the problem is to provide route optimization also for privacy-enabled communication sessions. In Mobile IPv6, the bi-directional tunneling mode can provide location privacy. However, in many scenarios bi-directional tunneling mode results in long routes (see Figure 1) and thus may be problematic for delay-sensitive applications such as VoIP. This is becoming even worse if CN is

mobile, too. Note that the terms route optimization as used in this document means improved efficiency of routing by shortening the route. The optimized route does not need to be optimal (i.e., equal length than the direct route between MN and CN), but it must be good enough, e.g., to support conversational communications. Further, route optimization of active communication sessions shall be possible. This is especially beneficial when a node travels large topological distances during an active session, which is considered to happen frequently in case of inter-domain and inter-technology handovers.

Another issue to be considered is deployment. If a solution relies on support from visited network infrastructure (e.g., modified ARs), every visited network must support this solution. Otherwise either the route optimization or the privacy support (or even the communication session itself) breaks when the MN moves to a network without support. However, global universal deployment is very difficult to achieve. Hence, the solution should not rely on visited network support, but should benefit from it if available.

In summary, the problem this document addresses is hiding MN's CoA from CN and providing route optimization at the same time without relying on support from visited networks. The solution shall not create any significant new security problems in comparison to Mobile IPv6/IPv6. Since the problem is especially severe if CN is mobile and since mobile-to-mobile communication is expected to be very common in the future (e.g., with VoIP), this is considered as the main target scenario. However, stationary nodes shall be supported as well.

2.3 Related Work

Various protocols have been proposed, which could be used to provide

both route optimization and location privacy to some extent [11] [12] [13] [14]. Since most of the protocols have been developed for other purposes, deficiencies exist and they do not meet the requirements listed in Section 2.2. For instance, they require universal deployment of modified (access) routers or only provide uni-directional location privacy (i.e., only for MN or CN, not both) or limited location privacy (i.e., only a topological area containing MN's location is known).

It may seem that the Mobile IPv6 bootstrapping solution (see [22] for split scenario) can provide both route optimization and location privacy, since route optimization in bi-directional tunneling mode can be achieved by reverse tunneling to dynamically allocated local HAs or HAs of nearby networks. However, the problem is that in this case the new HoA belongs to the visited network (or a nearby network) and hence contains location information. The bootstrapping solution provides means to update DNS with the new HoA, so that other nodes are able to start communication sessions with MN using the new HoA. But updating DNS with the new HoA or disclosing the new HoA by other means (e.g., during a VoIP call setup) may reveal information about MN's location. This is especially an issue if other nodes are able to find out that the new HoA belongs to the MN's visited network (or a nearby network), e.g., because MN's HA selection policy is known. In contrast, if the new HoA is not disclosed, other nodes are not aware of it and hence cannot initiate communication session with MN using the optimized route. Consequently, route optimization and full location privacy support cannot be provided at the same time. Another disadvantage with respect to route optimization by bootstrapping with local or nearby HAs is that route optimization of active communication sessions is not possible in a manner transparent for higher layers due to the need for changing the HoA.

3. Overview of ROTA

3.1 Assumptions about Trust Model

To allow a large scale applicability and deployment, no pre-established trust relationship shall be required between MN and CN or between MN/CN and HAs located outside the home link, respectively. Also, no "global PKI" is assumed, i.e., MN and CN shall not require public/private key pairs or host certificates.

3.2 The ROTA Approach and its Benefits

ROTA is an extension to Mobile IPv6 that optimizes the path in bi-directional tunneling mode between two mobile nodes in order to achieve both route optimization and full, bi-directional location privacy in terms of hiding the CoA from CN. The basic idea is to separate the packet interception and bi-directional tunneling mode functionality of an HA and allow the tunneling functionality for a specific node to reside on external entities, such as other HAs or MAPs. This external entity is then serving as a TA for a node, whose HoA does not match the subnet prefix of this HA. Consequently, the route can be optimized without changing the HoA of the MN. To ensure bi-directional location privacy, most of the procedure is controlled by MN's HA and CN's HA, e.g., they determine and configure appropriate TA(s) to be used as tunnel endpoints.

ROTA can operate with and without visited network support, which significantly eases deployment of ROTA. In the latter case, only MN's HA or CN's HA may act as TA for MN or CN, respectively. However, the route becomes less optimal when both MN and CN move far away from their home. Further route optimization is possible when leveraging TAs in visited networks (e.g., co-located with local HAs or MAPs), if available.

In contrast to the bootstrapping solution (see [22] for split scenario), ROTA does not change the home link in order to achieve route optimization. Hence, the HoA does not contain location information and can be rather static, i.e., it can be used as long-term identifiers regardless of the location of the MN and without sacrificing efficient routing. Dynamic DNS updates are not necessary as well. Furthermore, route optimization of active communication sessions is supported, which is especially beneficial if MNs travel topologically large distances during a session, e.g., because of vertical handovers.

A nice side-effect of the ROTA approach is that it provides benefits over route optimization mode beyond location privacy support by being able to utilize stronger authentication and authorization mechanisms

than the Return Routability procedure. Hence, longer binding lifetimes can be used, BU message can be sent less often, and temporary unavailability of HAs result in no or less loss of data packets. Since no end-to-end signaling is necessary on every movement, the handover latency as well as the signaling overhead over the air may be lower than in route optimization mode.

In the following, the operation of ROTA is described for scenarios without and with visited network support, respectively.

3.3 ROTA in scenarios without visited network support

The following basic scenario is assumed: First, a communication session between MN and a mobile CN has started and both nodes are in bi-directional tunneling mode. It is assumed that MN and CN have different home links. Figure 1 shows the data path between MN and CN with MN and CN both being in a foreign network. The MN reverse tunnels all data packets (addressed to CN's HoA) to its HA, which decapsulates and forwards them. The routing infrastructure routes the packets to CN's home network, where CN's HA intercepts and tunnels them to CN's CoA. Data packets in the other direction are handled accordingly. It is obvious that the route between MN and CN is far from optimal in this case and in many other cases. In general, the further MN and/or CN are away from home, the less optimal is the route.

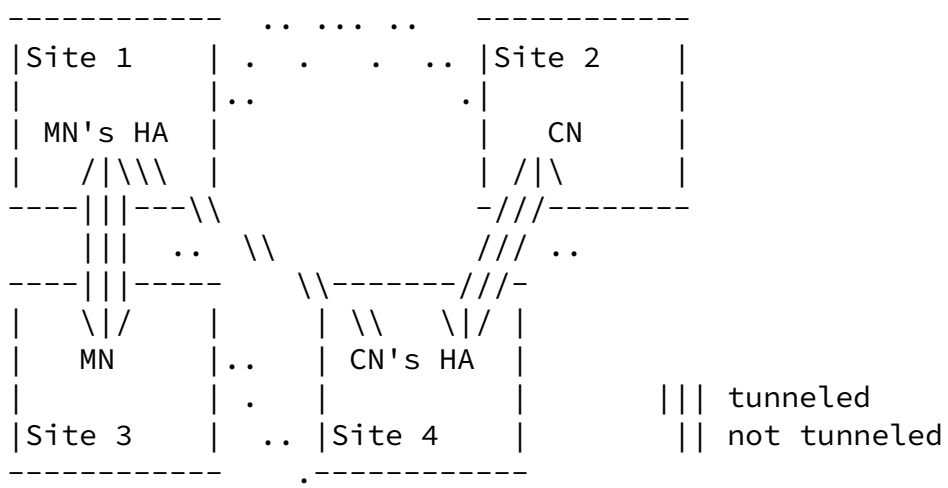


Figure 1: Data path between MN and CN in bi-directional tunneling mode

The basic idea of ROTA is to switch the reverse tunnel endpoint from the HA to TAs to shorten the route between MN and CN. In this

section we assume no visited network support. Hence, we assume that only MN's or CN's HA may serve as TA. Figure 2 shows the data path between MN and CN when CN's HA is TA, i.e., MN reverse tunnels all data packets addressed to CN's HoA to CN's HA and CN's HA tunnels all data packets addressed to MN's HoA to MN's CoA. As can be seen, the route is shorter than in Figure 1. Depending on the location of to MN, CN and their HAs, the data path is shorter when MN's HA or CN's HA acts as TA, respectively. For an optimal selection, ROTA can determine the best TA location based on distance information.

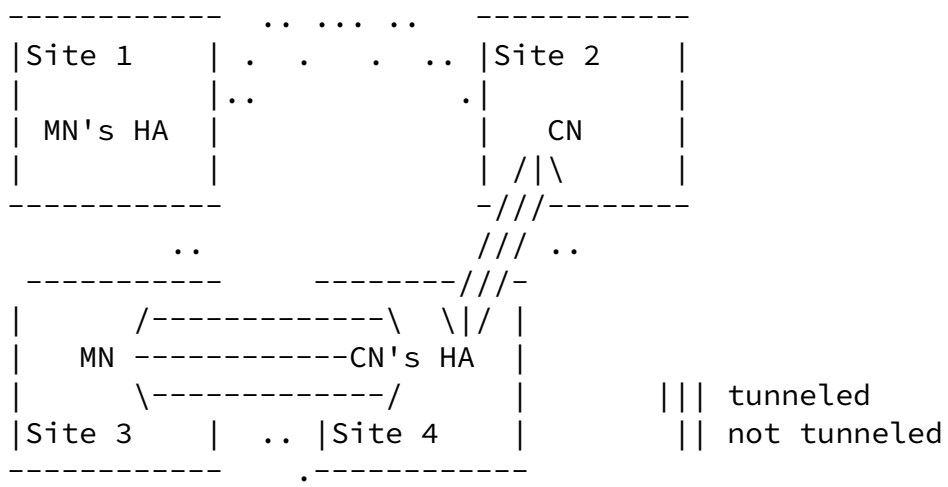


Figure 2: Data path between MN and CN with only CN's HA being TA

In the following, the operation of ROTA in scenarios without visited network support is described. The initial procedure can be divided in the following steps:

- Initiation of ROTA, which comprises requesting ROTA, checking whether CN and CN's HA support ROTA and, if not already known, discovering CN's HA address.

- Collecting distance information for TA selection (optional).

- Selecting TA(s) that provide(s) the shortest route.

- o Sending binding information to TAs.

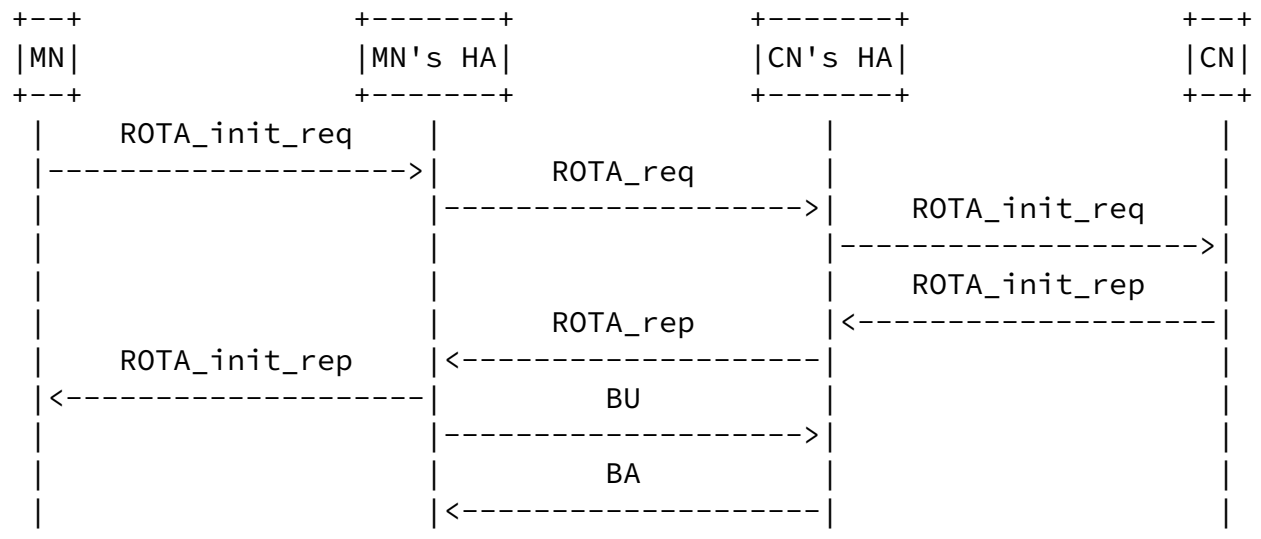
- o Requesting tunnel establishment from new tunnel entry-point(s) and notifying corresponding tunnel exit-point(s).

Note that this is only the initial procedure. Once this is completed, basically only binding updates must be sent after handovers. It is assumed that some kind of security association

exists between MN's HA and CN's HA to provide message authentication and integrity protection of signaling messages. This can be achieved by IPsec SAs, which are dynamically established with IKE [16] [17]. The signaling messages exchanged between MN/CN and HAs are sent over the IPsec SAs, which exist for Mobile IPv6 signaling messages [3]. A discussion of threats and possible countermeasures can be found in Section 8.

3.3.1 Signaling Flow

The initial procedure of ROTA in a scenario without visited network support is explained by means of the signaling flow shown in Figure 3, resulting in the data path depicted in Figure 2, i.e., CN's HA acts as TA for MN. See Section 5 and Section 6 for a detailed description of the MN and HA operation, respectively, and Section 4 for new message types.



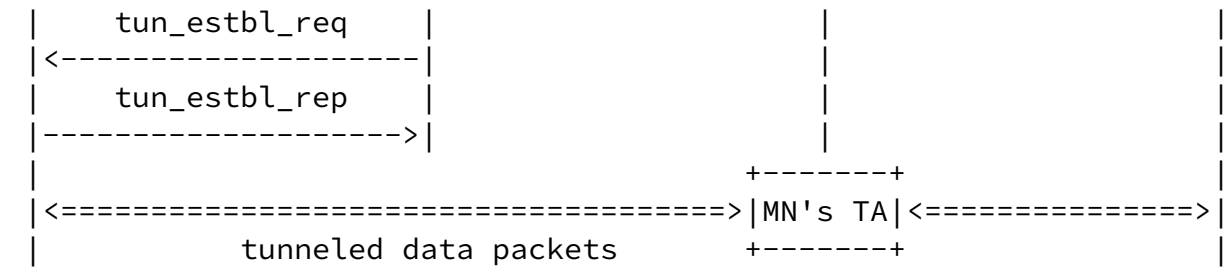


Figure 3: Signaling flow for initial procedure without visited network support

ROTA execution can either be triggered by MN or MN's HA. In the first case, the MN sends an ROTA Initiation Request message containing CN's and MN's HoA to its HA. In the latter case, the HA starts ROTA, e.g., after first data packets from/to CN's HoA were

tunneled. Subsequently, MN's HA sends an ROTA Request message to CN's HA. If CN's HA address is unknown, it first must be discovered. This can for instance be done by utilizing a modified DHAAD procedure and/or by the use of DNS, or by sending the ROTA Request message to CN's HoA and enabling CN's HA to intercept the message.

If CN's HA supports and accepts ROTA, it sends an ROTA Initiation Request to CN, which may accept or reject ROTA by sending a corresponding ROTA Initiation Reply message. Then, CN's HA sends a ROTA Reply message back to MN's HA. Subsequently, both HAs perform an TA selection procedure, which among other things is based on distance information. The distance metric can be hops or delay. Although delay would be a more meaningful metric for determining the best path to be used for conversational communications, it is less stable and the distance in hops can easier be measured. Hence, it is proposed to use hops as default metric. The distance can partly be passively acquired from the routing table, from previously received signaling messages or tunneled data packets. In the latter two cases, the initial hop limit used by the sender must be known by the receiver. Furthermore, some distance values might be pre-assigned, e.g., between roaming partners. Otherwise, distances may be measured by active probing (a specification of probe messages and a mechanism to secure active probing is left for future work).

A simple TA selection strategy would be to select the HA that is

closer to its MN as TA, since this usually provides the shorter path. In this case, the HAs can passively measure the distance to their MN/CN, e.g., with the ROTA Initiation Request/Reply messages and exchange them using the ROTA Request/Reply message with the own address and the distance information contained in the Candidate TA option. However, this strategy does not always select the better TA. A more accurate, but also more expensive strategy is to measure all distances needed to determine the current route length between MN and CN as well as the route length when MN's HA and/or CN's HA were TA(s) and, subsequently, select the best TA in terms of route optimization. Therefore, both HAs have to exchange BU messages to be able to measure the distance to MN's and CN's CoA. Note that a valid result of the selection is that no route optimization is necessary (see Appendix A for TA selection recommendations).

After an TA has been selected, binding information is introduced in the TA and Tunnel Establishment Request messages are sent to the new tunnel entry-point(s) (here: MN) to set up a tunnel. Additionally, Tunnel Establishment Notification messages may need to be sent to inform new tunnel exit-points about new tunnel entry-points to allow them to perform a check on the source address of incoming tunneled data packets as described in [3].

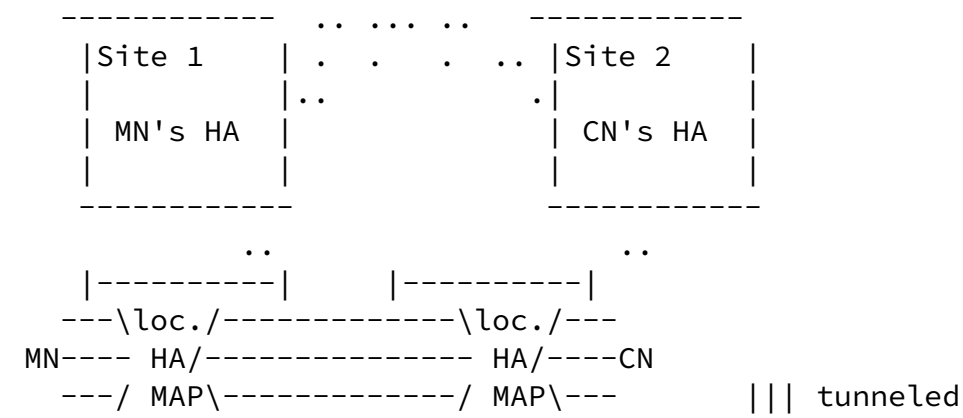
Note that this signaling flow applies to the initial ROTA procedure only. When MN moves to another subnet, basically only binding update messages must be sent to MN's HA and to MN's TA (as long as the TAs do not change). The latter can be sent by MN's HA or, to improve handover signaling efficiency and delay, by the MN itself. In this case the MN must be able to dynamically establish an SA to CN's HA. This may require an interface between CN's HA and an AAA infrastructure to transfer cryptographic material needed to establish the SA to CN's HA. Such an interface is currently in development (see [21]) and may be re-used by ROTA.

Furthermore, the optimal TA may change after movements. Hence, distance measurements and the TA selection may be repeated after movements. To reduce signaling, it is recommended to use passive measurements as much as possible. Further, it is not recommended to re-execute TA selection after every handover of MN or CN, but instead, e.g., after every nth handover. If the new distance information results in a new TA providing a shorter route, Tunnel

Establishment/Notification messages MAY be sent to adapt the route. To minimize data packet loss, new tunnels should be set up before the old tunnels are deleted ("make-before-break").

3.4 ROTA in scenarios with visited network support

Especially if both MN and CN are far away from the home network, neither MN's HA nor CN's HA can provide good route optimization by acting as TA. The route can be further optimized by considering TAs close to the direct path between MN and CN, e.g., local HAs or MAPs with TA functionality, which are located in or close to the visited networks of MN and CN. Another issue is that the scenario shown in Figure 2 may not achieve complete location privacy, since MN can find out that the path over CN's HA is shorter than over MN's HA, because otherwise CN's HA would not have been selected as TA (assuming that distance information is the dominant parameter in the TA selection). Since MN can determine the distances to MN's HA and CN's HA, it can conclude whether CN is closer to MN's or CN's HA. Although the geographical area derivable from this information is considered to be very large, it may be a reason to use other TA locations for improved location privacy. Note that if local TAs are selected, the disclosure of the MN's local TA prefix to CN and vice versa must be prevented, if both MN and CN require location privacy. This can be achieved by an HA-controlled TA selection and by routing of data packets over two intermediate TAs, e.g., a local HA or MAP in MN's and CN's visited networks as shown in Figure 4.



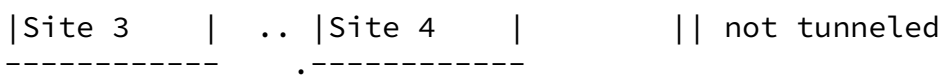


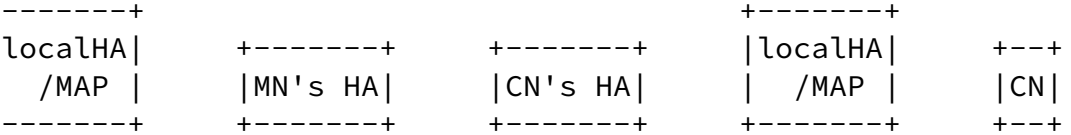
Figure 4: Data path between MN and CN with a TA in the visited network of MN and CN, respectively

New issues must be considered in such scenarios. First, a local candidate TA must be discovered. This can, e.g., be done by DNS using some location-dependent HA names, e.g., as mentioned in [22], or by some local announcements, e.g., via DHCP or Router Advertisements. The discovery can be done by the HAs or by MN/CN, which then propose candidate TAs to their HAs. Furthermore, the HAs must agree on the TAs to be used. MN and CN cannot be involved in the TA selection, because this would reveal the prefix of CN's/MN's visited network.

Another issue is that binding updates may need to be sent to multiple TAs and that those must contain TA addresses as CoAs. E.g., in Figure 4, TA1 must manage the bindings <MN's HoA, MN's CoA> and <CN's HoA, TA2 address> for traffic directed to MN and CN, respectively. Finally, it may be necessary for security reasons that a binding may only be introduced in an TA by the HA that belongs to the corresponding HoA. In this case, some co-ordination between MN's HA and CN's HA is necessary to ensure that MN and CN first are notified to switch their reverse tunnels after both HAs have introduced their bindings in all TAs and the end-to-end tunnel is established.

3.4.1 Signaling Flow

Figure 5 shows the signaling flow for the initial procedure resulting in the scenario shown in Figure 4, i.e., with local TAs in the visited networks of MN and CN. See Section 5 and Section 6 for a detailed description of the MN and HA operation, respectively, and Section 4 for new message types.



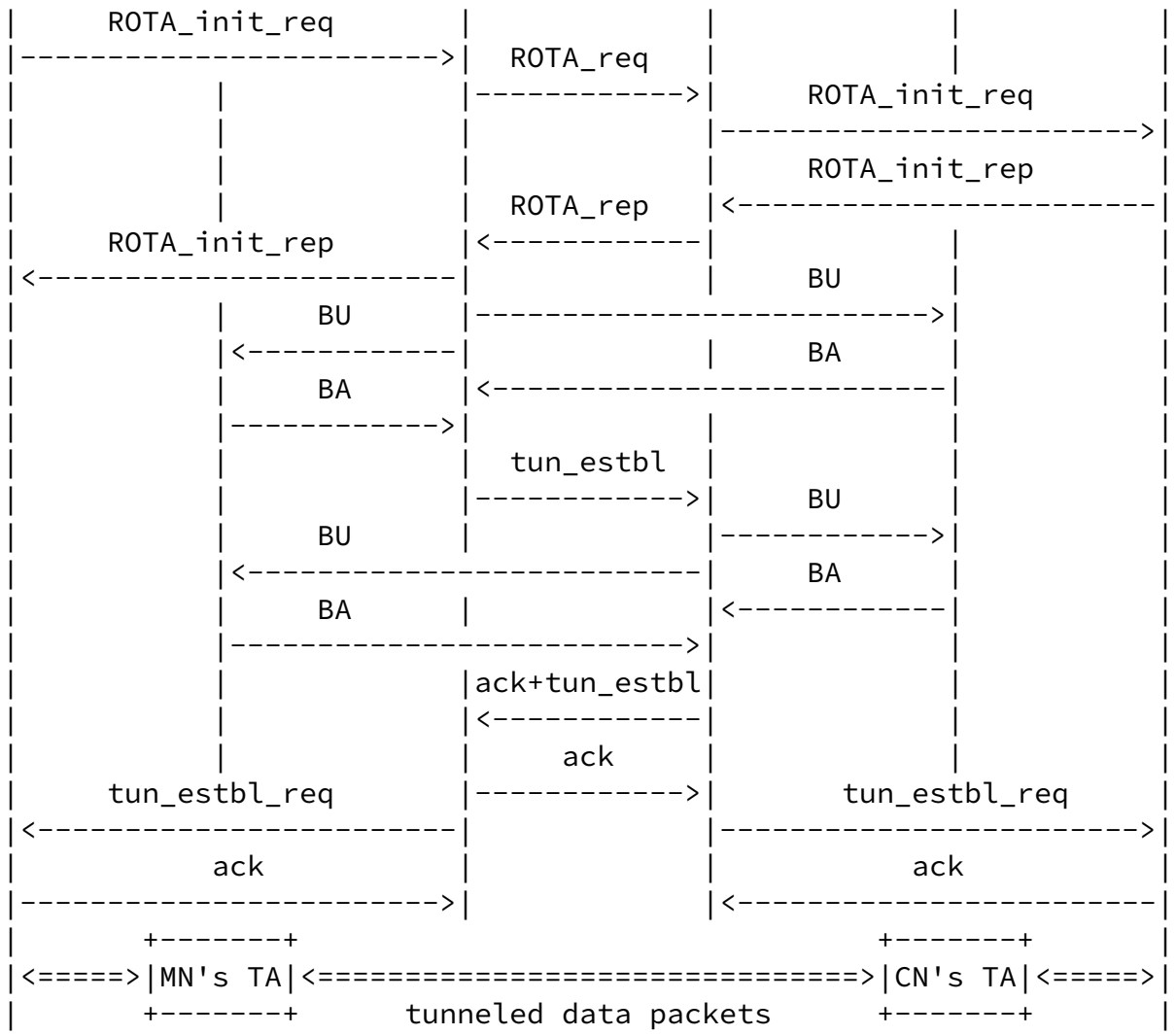


Figure 5: Signaling flow for the initial procedure with local TAs in visited network

First, MN or HA initiate ROTA as described in Section 3.3.1. The MN may propose candidate TA address(es) such as a local HA/MAP address and the distances to those using a new Mobility Option, the Candidate TA option, in ROTA Initiation Request or BU messages. The HA checks the validity of those addresses and may delete or add candidate TAs before sending them in a ROTA Request message with Candidate TA option to CN's HA. Similarly, CN and CN's HA may add or delete TA addresses. Note that both HAs should at least add their own address to the candidate TA list for the case that no visited network supports and hence no local TAs exists. If the distances in hops are passively measured using ROTA messages, CN's HA already has the

distances <MN to MN's HA>, <MN's HA to CN's HA> and <CN to CN's HA> at this point in time. It also knows whether a local TA exist in MN's and CN's visited network, respectively, and if both MN and CN require location privacy (the latter is indicated by the P-flag in ROTA Request messages). E.g., by using the recommendations described in Appendix A, CN's HA can select TAs to be used and propose them to MN's HA by setting the respective O-bits in the Candidate TA option of the ROTA Reply message. Here, it is assumed that MN's HA agrees with the proposal of CN's HA. Otherwise, another round of request and reply messages may be needed. Note that MN's and CN's HA may request distance measurements from candidate TAs using ROTA Distance Information Request messages in order to find the best TAs providing the shortest path.

After TAs have been selected, binding information about MN and CN must be sent to them using BU messages with alternate CoA option. Depending on the mechanisms used for authenticating and authorizing of binding updates, this can be done by one HA only or by both HA independently. Although many signaling messages could be saved if done by only one HA, it is proposed that both HAs introduce bindings independently for security reasons. It is assumed that an HA may only introduce binding information into an TA, when its prefix matches the HoA in the binding (see Section 8). The binding update messages contain MN's or CN's HoA as HoA and MN's or CN's CoA or the address of the corresponding TA as CoA. Finally, the HAs send Tunnel Establishment Notification messages to each other to indicate the successful establishment of bindings and notify MN and CN to switch their reverse tunnels.

Note that this signaling flow applies to the initial ROTA procedure only. When MN moves to another subnet, basically only binding update messages must be sent to MN's HA and to MN's TA. The latter can be sent by MN's HA or, to improve handover signaling efficiency and delay, by the MN itself. In this case the MN must be able to dynamically establish an SA to the local HA/MAP. This may require an interface between TA and the AAA infrastructure to transfer cryptographic material needed from the home network to establish the SA. Such an interface is currently in development (see [21]) and may be re-used by ROTA. Note that MN cannot send a binding update to CN's TA if CN requires location privacy, because the address of CN's TA can contain location information about CN and, hence, must be hidden from MN.

Again, the optimal TAs may change after movements. MN and CN may propose new local candidate TA addresses to their HAs after moving to a new local HA/MAP area, e.g., with BU messages using the Candidate TA option. The HAs then may decide to execute the TA selection

algorithm again (using ROTA Request/Reply messages) and switch the

tunnels to new TAs, if necessary.

4. New Message Types

The ROTA protocol messages are defined as new Mobility Header Types and Mobility Options.

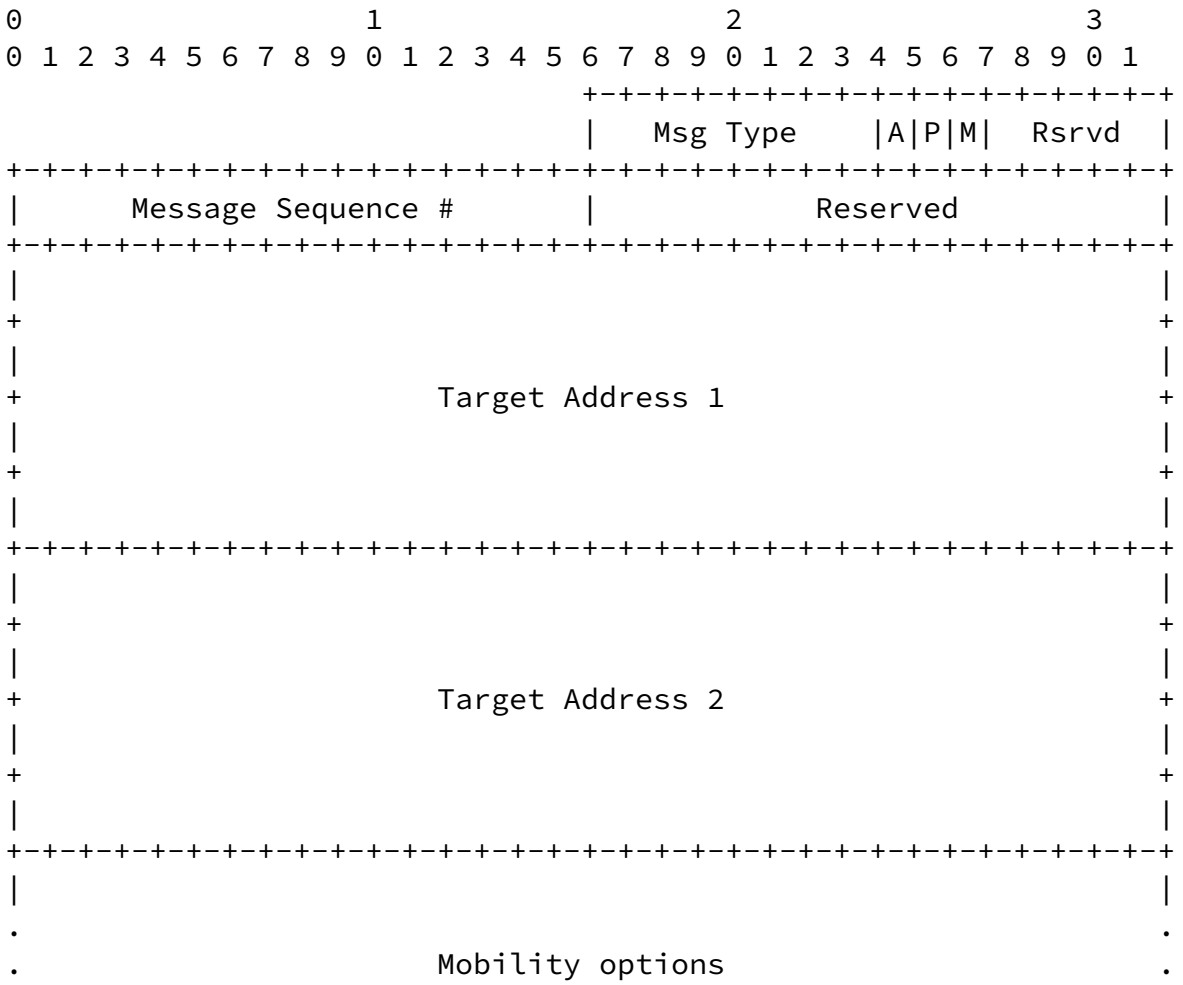
4.1 Message Headers

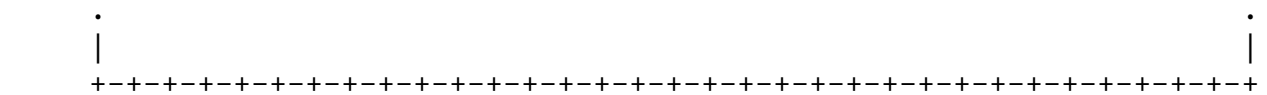
4.1.1 Binding Update and Acknowledgement Message

Binding Update and Acknowledgement messages are defined in [3]. The only modification is a new "TA registration" flag to be used when a binding shall be introduced in an TA.

4.1.2 ROTA Request/Notification Message

The ROTA Request/Notification Message is the general request and notification message of ROTA. It contains a Message Type field to distinguish different ROTA Request/Notification messages. The value of the hop limit field in the IPv6 header MUST be set to 255 to support passive distance measurements. The MH type is TBD.


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Msg Type
A
P
M
Rsrvd
Message Sequence #
Reserved
Target Address 1
Target Address 2
Mobility options



Msg Type

This field specifies the type of ROTA Request/Notification message. The following types are currently registered:

0: ROTA Initiation Request

This message requests ROTA initiation.

1: ROTA Request

The purpose of this message is to check whether CN's HA supports ROTA and, optionally, to discover the address of CN's HA. This message MAY be sent to CN's HoA, if CN's HA address is unknown. In conjunction with the Candidate TA option it can be used to negotiate TA address(es).

2: ROTA Abort Notification

The purpose of this message is to abort an ROTA session and switch back to standard bi-directional tunneling mode.

3: ROTA Tunnel Establishment Notification

The purpose of this message is to notify about an established tunnel and to inform about a new tunnel entry-point address.

4: ROTA Tunnel Establishment Request

This message requests from a tunnel entry-point the establishment of a new tunnel.

5: ROTA Distance Information Request

The purpose of this message is to request distance

information from an TA. The corresponding reply message is the ROTA Distance Information message. The candidate TA mobility option may be used to request the distance to multiple candidate TAs.

Message Sequence #

A 16-bit unsigned integer used by the receiving node to sequence ROTA messages and by the sending node to match a returned acknowledgement with this message.

Acknowledge (A)

This flag is set when an acknowledgement is requested upon receipt of a notification message. It MUST be set if the message transport service is considered unreliable. The flag can be ignored in request messages, since they are acknowledged by a reply message anyway.

Privacy (P)

This flag is used to inform the receiver of the message about the privacy requirements of the sender. If set, location privacy is required by the sender. MN and CN can inform their HAs about privacy requirements in ROTA Initiation Request messages, HAs can inform each other about privacy requirements of their MN/CN in ROTA Request messages.

Metric (M)

The flag has only meaning for ROTA Distance Information Request messages. It indicates the metric to be used for requested distance measurements. If set to 0 the metric is hops, otherwise it is delay. Note that all nodes involved in a ROTA session MUST use the same metric.

Reserved

These fields are unused. They MUST be initialized to zero and MUST be ignored by the receiver.

Target Address 1

The meaning of this field depends on the value of the Message Type field:

If 0, 1 or 2 target address 1 is MN's HoA.

If 3 and the message is sent to/received by an HA, the target address 1 is the address of MN's HoA.

If 3 and the message is sent to/received by MN or CN, the target address 1 is the address of the new tunnel entry-point.

If 4, the target address 1 is the address of the new tunnel exit-point.

If 5, the target address 1 is an address, to which the receiving TA shall determine the distance (e.g., MN's CoA or correspondent TA).

Target Address 2

The meaning of this field depends on the value of the Message Type field:

If 0, 1 or 2 target address 2 is CN's HoA.

If 3 and the message is sent to/received by an HA, the target address 2 is the address of CN's HoA.

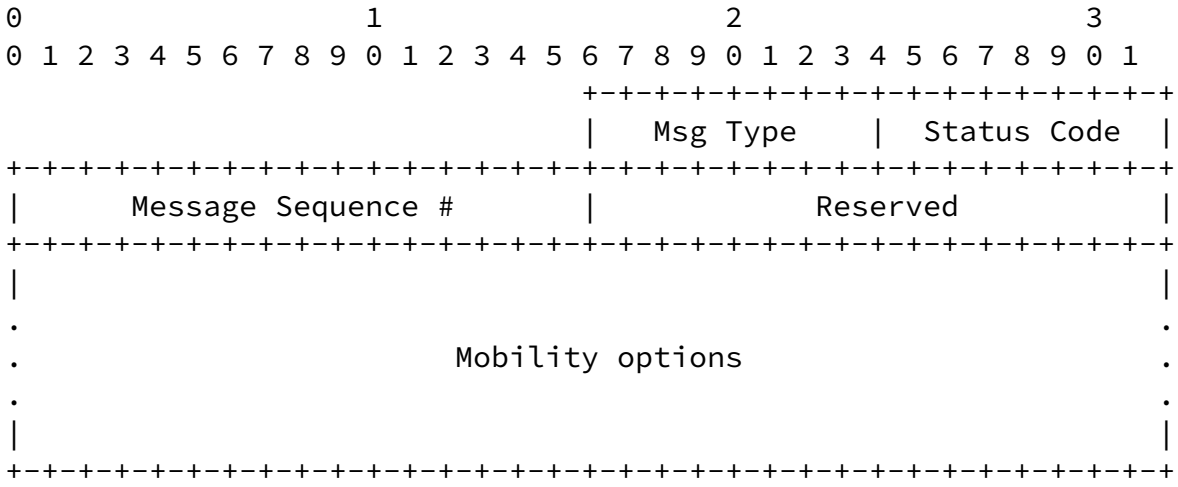
If 3 or 4 and the message is sent to/received by MN, the target address 2 is CN's HoA.

If 3 or 4 and the message is sent to/received by CN, the target address 2 is MN's HoA.

If 5, the target address 2 is an address, to which the receiving TA shall determine the distance (e.g., CN's CoA or correspondent TA).

4.1.3 ROTA Reply/Acknowledgement Message

The ROTA Reply/Acknowledgement Message is the general reply and acknowledgement message of ROTA. It contains a Message Type field to distinguish different ROTA Reply/Acknowledgement messages. The value of the hop limit field in the IPv6 header MUST be set to 255 to enable passive distance measurements. The MH type is TBD.



Msg Type

This field specifies the type of ROTA message. The following types are currently registered:

0: ROTA Initiation Reply

The purpose of this message is to indicate the outcome of the ROTA Initiation Request.

1: ROTA Reply

The purpose of this message is to indicate whether CN's HA and CN support and accept ROTA and to inform the sender about the address of CN's HA. In conjunction with the Candidate TA option it can be used to negotiate TA address(es).

2: ROTA Abort Acknowledgement

The purpose of this message is to acknowledge the abort of an ROTA session.

3: ROTA Tunnel Establishment Reply

The purpose of this message is to indicate the outcome of the Tunnel Establishment Request.

4: ROTA Tunnel Establishment Notification Acknowledgement

The purpose of this message is to acknowledge ROTA Tunnel Establishment Notification Message.

5: ROTA Distance Information Acknowledgement

The purpose of this message is to acknowledge the ROTA Distance Information Message.

Status Code

This field indicates the result of an request:

0: Request accepted

128: Request not accepted, reason unspecified

129: Request not accepted, ROTA not supported

130: Request not accepted, insufficient resources

131: Request not accepted, candidate TAs not accepted

Message Sequence #

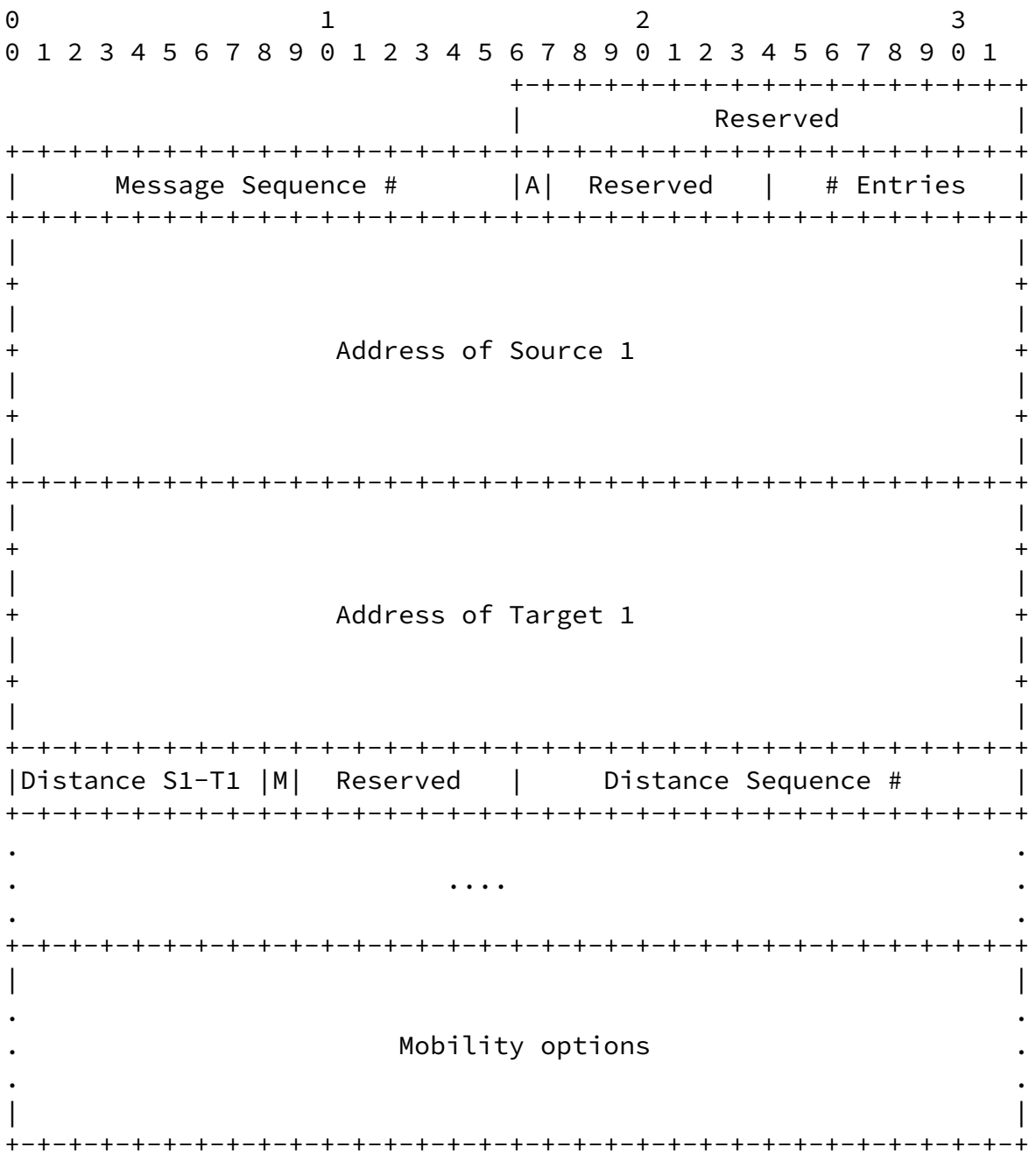
A 16-bit unsigned integer used by the receiving node to sequence ROTA messages and by the sending node to match a returned Acknowledgement with this message.

Reserved

These fields are unused. They MUST be initialized to zero and MUST be ignored by the receiver.

4.1.4 ROTA Distance Information Message

The ROTA Distance Information Message is used to notify other entities about distances between two nodes. The MH type is TBD.



Message Sequence #

A 16-bit unsigned integer used by the receiving node to sequence ROTA messages and by the sending node to match a returned Acknowledgement with this message.

Acknowledge (A)

This flag is set when an Acknowledgement is requested upon receipt of this message. It MUST be set if the message transport service is considered unreliable.

Reserved

These fields are unused. They MUST be initialized to zero and MUST be ignored by the receiver.

Entries

An 8-bit unsigned integer indicating the number of distance information entries in this message.

Address of Source X

Address of source X.

Address of Target X

Address of target X.

Distance SY-TY

An 8-bit unsigned integer indicating the measured distance between source X and target X. If the metric is delay, the value of this field is the delay divided by 10ms. Any delay higher than 2550ms is represented by 255.

Metric (M)

The flag indicates the metric of the distances. If set to 0 the metric is hops, otherwise it is delay.

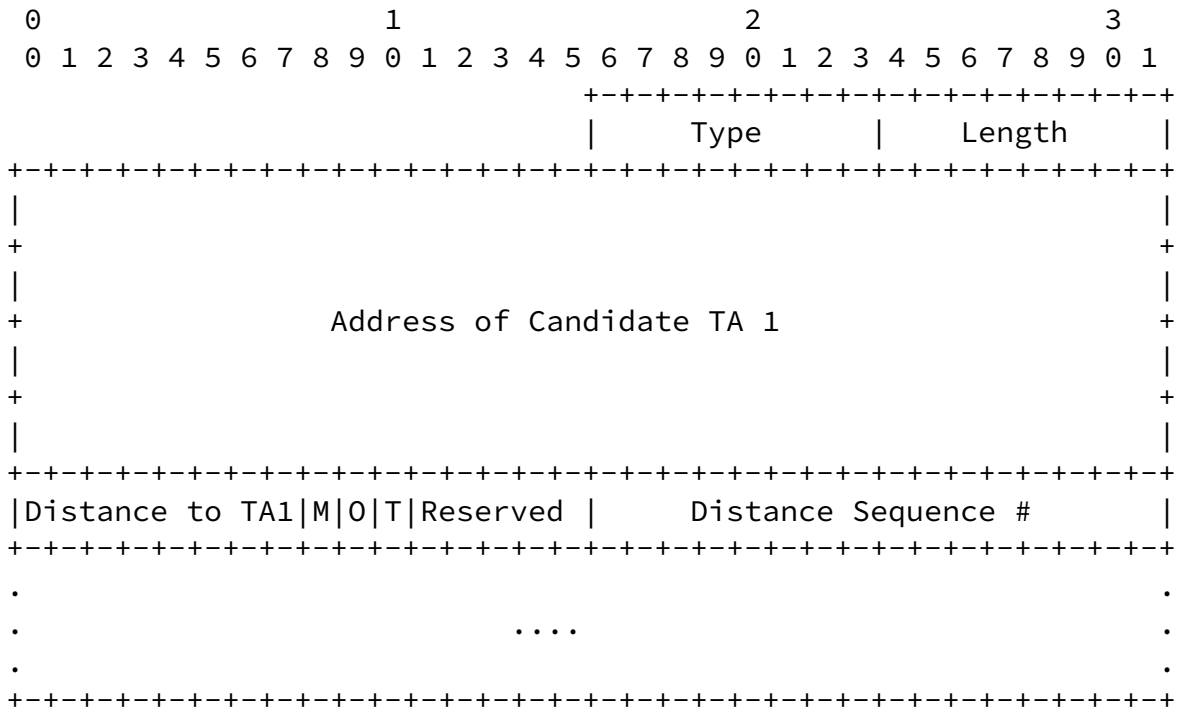
Distance Sequence #

A 16-bit unsigned integer indicating the freshness of the distance information. It must always be provided by the node that measured the distance.

4.2 Mobility Options

4.2.1 Candidate TA Option

This option can be used to propose candidate TA addresses. Type is TBD.



Reserved

These fields are unused. They MUST be initialized to zero and MUST be ignored by the receiver.

Address of Candidate TA X

Address of candidate TA X.

Distance TA1

An 8-bit unsigned integer indicating the distance between the MN belonging to the sender and the candidate TA. The distance can be omitted by setting it to 0, meaning "unknown distance". If metric is delay, the value of this field is the delay divided by 10ms. Any delay higher than 2550ms is represented by 255.

Metric (M)

The flag indicates the metric of the distances. If set to 0 the metric is hops, otherwise it is delay.

Proposed TA (O)

The entries which have the P-flag set represent the set of TAs proposed by the sender. Other entries are alternative TAs.

TA proposal modified (T)

If this flag is set, the O-flag of this TA has been changed, compared to the Candidate TA Option of the last Request/Reply message. If the entry is new and the O-flag is set, the T-flag MUST be set as well.

Distance Sequence #

A 16-bit unsigned integer indicating the freshness of the distance information. It must always be provided by the node that measured the distance.

5. Modified Mobile Node Operation

5.1 Conceptual Data Structures

A new flag is added to Binding Update List entries to indicate an active ROTA session. Additionally, an ROTA MN Cache entry is maintained for every ROTA session. A ROTA session identification is implicitly given by the tuple <MN's HoA, CN's HoA>. ROTA Binding Update List entries conceptually point to ROTA MN Cache entries.

Each ROTA MN Cache entry contains the following data

- CN's HoA

- TA address(es) for incoming data packets
- TA address for outgoing data packets
- Message Sequence Number

A Candidate TA Cache may be maintained, which contains addresses of known candidate TAs and the distance to those.

5.2 Using Security Associations

All ROTA messages MUST be sent authenticated and integrity protected, e.g., over the MN-HA IPsec SAs required for Mobile IPv6 signaling messages.

5.3 Sending ROTA Initiation Request

The MN MAY request ROTA initiation for a communication session with a specific CN at any time by sending an ROTA Initiation Request to its HA. This message must contain CN's HoA. It MUST set the P-bit if it requires privacy and it MAY propose candidate TA address(es) and the corresponding distances. The message sequence number field in the message as well as in the ROTA MN Cache is increased for every Request message sent. The MN updates the corresponding entry in its ROTA MN Cache.

5.4 Receiving ROTA Initiation Reply

After receiving a positive reply with a sequence number matching the corresponding request message, the ROTA MN Cache is updated accordingly.

5.5 Receiving ROTA Initiation Request

When receiving a ROTA Initiation Request, the MN is acting as CN. It MUST reply with a ROTA Initiation Reply.

5.6 Sending ROTA Initiation Reply

The ROTA Initiation Reply message contains a status code indicating that ROTA is either accepted or rejected. The sequence number must be set to the value of the corresponding request message. If accepted, a ROTA MN Cache entry must be created. The P-bit is set according to the privacy requirements. TA addresses may be proposed in a Candidate TA option.

5.7 Sending Reverse Tunneled Packets

If an ROTA session for the destination address exists and the ROTA MN Cache indicates that the tunnel is established, data packets are reverse tunneled to the corresponding outgoing tunnel endpoint address.

5.8 Receiving Reverse Tunneled Packets

Incoming data packets are accepted if the IP source address of the IP tunnel header matches one of the TA addresses for incoming data packets in the ROTA MN Cache entry corresponding to the IP source address in the inner IP header.

5.9 Sending Binding Updates

Binding Updates to MN's HA are sent as described in [3], i.e., over the MN-HA IPsec SA. Binding Updates sent to MN's TA MAY be sent by MN. In this case it must be able to dynamically establish an SA to the TA. This may require an interface to an AAA infrastructure to transfer cryptographic material needed to establish the SA. Such an interface is currently in development (see [21]) and may be re-used by ROTA.

5.10 Receiving Tunnel Establishment Request messages

The MN checks whether the ROTA MN Cache contains a valid entry for CN's HoA contained in the Tunnel Establishment Request. If this is not the case, the request MUST be rejected. Otherwise, the sequence number in the message is checked. If it is higher than the one in the ROTA MN Cache, the MN sets up the tunnel. The corresponding fields, such as the tunnel endpoint fields, and the sequence number field in the corresponding ROTA MN Cache entry are updated accordingly. The MN MUST return a Tunnel Establishment Reply

indicating the outcome of the check.

5.11 Sending Tunnel Establishment Reply messages

The message must contain a status code indicating the outcome of the check. The sequence number is set to the value of the corresponding Request message.

5.12 Receiving Tunnel Establishment Notification messages

On receipt of a Tunnel Establishment Notification, the same checks as described in the last section apply. If successful, the MN updates the corresponding fields, such as the sequence number field, and the tunnel endpoint fields in the corresponding ROTA MN Cache entry. The MN MUST return a Tunnel Establishment Notification Acknowledgement with the sequence number set to the value of the corresponding Notification message.

6. Modified Home Agent Operation

6.1 Conceptual Data Structures

Each HA maintains an ROTA HA cache and a Binding Update List. The latter is the same as specified for the MN in section 11.1 of [3], but without the data required for the return routability procedure. Binding Cache entries with home registration and Binding Update List entries conceptually point to each other and to ROTA HA Cache entries.

Each ROTA HA Cache entry of MN's HA contains the following data

- CN's HoA
- MN's privacy requirements
- CN's privacy requirements
- CN's HA address
- Current TA address(es) of MN
- Message Sequence number
- A Candidate TA Cache, which contains addresses of known candidate TAs and their distance to MN/CN.

A Certificate Cache may be maintained, which contains recently received public keys and certificates.

A Distance Information Cache is used to store distances between MN/CN and TAs. It contains entries with the following data

- Source address
- Destination address
- Distance measured in hops and/or delay
- Distance Sequence Number
- Lifetime

An HA acting as a TA additionally maintains an ROTA TA Cache. Binding Cache entries are extended by a TA registration flag to distinguish TA registrations from home registrations. TA registration entries conceptually point to ROTA TA Cache entries.

Each ROTA TA Cache entry contains the following data

- MN's HA address
- Message Sequence Number

6.2 Using Security Associations

All ROTA messages sent between MN's HA and MN and CN's HA and CN MUST be sent authenticated and integrity protected over the MN-HA IPsec SAs required for Mobile IPv6 signaling messages. All ROTA messages sent between MN's HA and CN's HA or MN's/CN's HA and TA MUST be sent authenticated and integrity protected over beforehand (e.g., with IKE/IKEv2 [16] [17]) established IPsec SAs.

6.3 ROTA Initiation

The HA starts ROTA initiation for a specific MN-CN session on receipt of an ROTA Initiation Request from an MN or on an internal trigger, e.g., after the first received data packets from a specific CN. For the latter it MUST be ensured that the preferences of MN comply with HA's decision to initiate ROTA, e.g., from some prior arrangement. If triggered by an ROTA Initiation Request sent by MN, the HA MUST return an ROTA Initiation Reply indicating the outcome of the initiation. The Message Sequence Number in the ROTA Initiation Reply MUST match those in the corresponding Initiation Request. During ROTA initiation, the HA creates the corresponding entries in its ROTA HA Cache. If the message contains a Candidate TA Mobility Option, the HA must check whether a trust relationship exists to those TAs. New valid TAs may be added to the Candidate TA Cache.

6.4 Sending ROTA Request

ROTA Request messages are only exchanged between MN's HA and CN's HA. MN's HA sends an ROTA Request to CN's HA. If CN's HA address is

unknown, the Request may be sent to CN's HoA and intercepted by CN's HA. The ROTA Request message MUST contain CN's HoA and a current message sequence number. The P-flag in the message MUST be set to the value set by the MN in the corresponding ROTA Initiation Request message. If the HA has triggered ROTA, it must know MN's privacy requirements from some prior arrangement. The HA MUST propose at least its own address as candidate TA address in the Candidate TA Mobility Option and MAY include more candidate TAs, e.g., proposed by MN in the Candidate TA option. It MAY set the O-flag to propose one or multiple of the candidates as TA. If no reply is received after sending multiple Request messages, it can be concluded that CN's HA does not support ROTA and ROTA must be aborted.

6.5 Receiving ROTA Request

If an HA supports ROTA and receives a ROTA Request addressed to one of the addresses associated to its network interfaces or to one of its Binding Cache entries with home registration, it SHOULD send a ROTA Initiation Request to CN in order to check if CN supports and accepts to execute ROTA. This message may not contain the candidate TAs proposed by MN in a Candidate TA option, since they may reveal location information. If such an Initiation message is not sent, the HA must know the preferences of CN, e.g., from some prior arrangement. If a valid and positive Initiation Reply is received, the ROTA Request message is processed. Before a ROTA Reply message is sent, the HA creates or updates the corresponding entry in its ROTA HA Cache.

6.6 Sending ROTA Reply message

If CN does not have an active communication session with the address contained in the ROTA Initiation Request message or does not accept to execute ROTA route optimization, the HA sends a negative reply and MN's HA informs MN accordingly. Otherwise the HA sends a positive ROTA Reply message to the sender address of the corresponding Request message. The message sequence number is set to the value of the corresponding Request messages. The P-flag in the message MUST be set to the value set by the CN in the corresponding ROTA Initiation Reply message sent by CN or known from some prior arrangement. The HA MUST propose at least its own address as candidate TA address in the Candidate TA Mobility Option and MAY include more candidate TAs, e.g., proposed by CN in a Candidate TA option. It also adds the

agreed candidate TAs that were proposed by MN's HA in the ROTA Request message. It MUST set the O-flags in the Candidate TA option to propose a set of TAs to be used.

6.7 Receiving ROTA Reply

The receiver only processes the Reply message if it has sent a corresponding Request with the same sequence number to the sender address before. If this is not the case, the HA MAY return an ROTA Reply indicating the rejection of ROTA. The HA checks the proposed TAs in the Candidate TA option. If the HA does not accept the set of TAs proposed by CN's HA, it MUST sent a new Request message with a modified list of candidate TAs and new set of TAs marked with the O-flag. In this case, the T-flag MUST be set in the corresponding entries in the Candidate TA Option. The TA selection may be supported by additional distance measurements, which may require MN's and CN's HA to exchange BU messages for being able to measure the distance to MN's and CN's CoA. Furthermore, Distance Information messages may be exchanged to report measured distances. If both HAs

have agreed on a set of TAs, the HAs may proceed with sending BU messages to those.

6.8 Sending Binding Updates

A Binding Update may only be sent to a TA by an HA with a subnet prefix matching the HoA in the binding. The newly defined TA registration flag must be set and the alternate CoA option MUST contain MN's/CN's CoA or an TA address. Additionally, the Binding Update List MUST be updated as specified in [3].

6.9 Receiving Binding Updates

If an HA receives a BU from one of its MNs, it processes it as described in [3]. Additionally, it sends a corresponding BU to the current TA(s).

An HA acting as TA may receive a Binding Update from an HA with TA registration flag set. It does not necessarily reject a binding containing an HoA which is not an on-link IPv6 address with respect to the HA's current prefix list, as described in [3]. Instead, it checks whether the sender is authorizes to act as an HA for the HoA

contained in BU message (this could, e.g., be realized with certificates by comparing the HoA in the binding with the prefixes contained in an IP address extension of the certificate of the sender HA. See Section 8 for details). If the sender is not authorized, the BU MUST be rejected.

If accepted, the TA adds the binding to its Binding Cache. The lifetime of the entry is set according to the rules for bi-directional tunneling mode as described in [3]. The TA MUST set the TA registration flag of the corresponding entry. The home registration bit MUST NOT be set. Additionally, it adds an entry in its ROTA TA Cache with the address of the sender HA. Finally, a pointer to this entry is added in the corresponding Binding Cache entry. Regardless of the A-bit in the binding, the TA MUST return a Binding Acknowledgement to the sending HA as described in [3].

6.10 Receiving Binding Acknowledgements

The checks described in [3] apply. If the HA has sent BUs to TAs different from CN's HA and all corresponding BAs has been received, a Tunnel Establishment Notification message is sent to CN's HA.

6.11 Sending Tunnel Establishment Notification message

After the BAs from all TAs have been received, a Tunnel Establishment Notification message is sent to the CN's HA.

6.12 Receiving Tunnel Establishment Notification message

After the Tunnel Establishment Notification message has been received by CN's HA and BAs from all TAs have been received, a Tunnel Establishment Notification Acknowledgement message is sent to the CN's HA. Furthermore, a Tunnel Establishment Request message is sent to CN.

If no Tunnel Establishment Notification message is received by CN's HA, this might be an indication that the ROTA Reply message got lost. In this case, CN's HA may resend the ROTA Reply message.

6.13 Receiving Tunnel Establishment Notification Acknowledgement message

On receipt of a Tunnel Establishment Notification Acknowledgement message from CN's HA, a Tunnel Establishment Request message is sent to MN.

6.14 Intercepting Data Packets

An TA MUST NOT intercept data packets for nodes with TA registration, i.e., it MUST NOT perform Proxy Neighbor Discovery for those nodes. An HA may only perform packet interception for home registrations as described in [3]

6.15 Sending and Receiving Reverse Tunneled Packets

Reverse tunneled packets are handled the same way as in [3]. E.g., the TA MUST verify that the Source Address in the tunnel IP header of received data packets is equal to the CoA specified in the corresponding entry in the Binding Cache, if IPsec ESP is not used for those packets.

6.16 Receiving a ROTA Abort Notification message

MNs can abort a ROTA session and switch to standard Mobile IPv6 bi-directional tunneling mode by sending a ROTA Abort Notification message to its HA. The Abort message MUST set the A-flag. The HA then sends a corresponding message to all active TAs and to CN's HA, which then will send an abort notification to CN. The corresponding ROTA HA and MN Cache entries may first be deleted after the corresponding acknowledgements have been received.

6.17 Management of ROTA HA Cache Entries

ROTA HA Cache entries are deleted when the corresponding Binding Cache entries are deleted or the ROTA session is aborted.

7. IANA Considerations

ROTA introduces new Mobility Header Types and Mobility Options (see Section 4).

8. Security Considerations

Different issues have to be considered to ensure that ROTA does not introduce new security leaks. For instance, a trust relationship between MN's and CN's HA and between MN's/CN's HA and TAs must exist. Since multiple ways of establishing and managing trust relationships exist and the choice depends on deployment scenarios, we only give a short discussion of attacks and possible countermeasures in this section. A detailed specification of the security solution is left for future work. Most attacks are taken from [18], which describes them in more detail in the context of an analysis of the Mobile IPv6 route optimization mode.

8.1 Address Stealing

A serious attack is the injection of false binding information in a correspondent node, since this allows an attacker to steal a victim's traffic by redirecting it to itself or a node under its control, e.g., to analyze or tamper the traffic. Note that the victim may be a mobile node as well as a stationary node, since addresses used by stationary nodes are not distinguishable from addressed used by mobile nodes. This attack is especially serious in case of ROTA, since binding information is sent to potential Internet router (here: HA acting as TA). To prevent such attacks, data origin authentication and integrity protection for BU messages are required and the sender of a BU message must be authorized to inject a specific binding.

Data origin authentication can be achieved with sender address ownership proof, e.g., with public/private keys and X.509v3 certificates [2]: The certificate binds the public key to the sender address. Alternatively, Cryptographically Generated Addresses (CGA) [6] could be used to bind the public key to the sender address. BU messages from MN's HA to CN's HA must be sent integrity protected, e.g., by using a beforehand with IKE/IKEv2 [16] [17] established IPsec ESP [15] SA.

In Mobile IPv6 authentication of BU messages sent from MN to its HA and authorization of MN to use a particular HoA in the BU message is achieved by linking the HoA to a specific IPsec security association [3]. However, the CoA in the BU message is not checked for correctness. As discussed in [3], it is assume that "an HA can always identify an ill-behaving MN", which "allows the operator to discontinue MN's service" (see section 15.3 in [3]). An option giving a higher level of security would be to conduct additional CoA reachability tests, e.g., as described in [19].

BU messages sent from HA to TA can be authenticated with IPsec as

well. The HoA in BU messages can be authorized with certificates: every certificate contains the set of subnet prefixes that the corresponding HA is allowed to serve (for home registrations, not for TA registrations), e.g., in an IP address extension [4]. This is similar to the approach taken by SEND [5], where certificates contain prefixes a router may advertise. Besides verifying the signature, a TA receiving a BU from an HA compares the prefix of the HoA in the BU message to the set of home subnet prefixes contained in the certificate of the sender HA. Only if the prefixes match, the BU is accepted by the TA. Note that in contrast to SEND [5], MN and CN do not require additional pre-configuration, such as a shared trusted anchors, since they are not involved in the verification of digital signatures. The CoA cannot be checked by certificates. Instead, an ill-behaving MN must be identified as such as described above and the corresponding HA must be notified, which then can discontinue the service. Alternatively, CoA reachability tests can be introduced.

If BUs are sent from MN/CN to TAs directly, an SA must exist. This can be dynamically established using an interface to an AAA infrastructure (to transfer cryptographic material needed to establish the SA). Such an interface is currently in development (see [21]) and may be re-used by ROTA.

8.2 Replay Attacks

Even with the measures discussed above, an attacker could redirect traffic by eavesdropping a valid BU message and re-sending it later to an TA. Such replay attacks can be prevented when the freshness of received signaling messages can be determined by the receiver, e.g., using (integrity protected) nonces or sequence numbers. IPsec can provide replay protection. For other cases, ROTA messages include 16-bit message sequence numbers.

8.3 Denial of Service (DoS) Attacks

8.3.1 Reflection

The introduction of false binding information in another node's Binding Cache, either with false CoA or false HoA, enables DoS attacks. For instance, an attacker could mount a DoS attack by redirecting traffic to a victim that cannot handle the amount of traffic, e.g., because it has a low-bandwidth Internet connection or because many traffic flows are redirected to one victim. Since the node that redirects all the traffic acts as reflector, such attacks are also called reflection attacks. Another related DoS attack redirects all traffic to a non-existent address. Those attacks can

be prevented by the measures described in Section 8.1.

8.3.2 Amplification

Amplification can make reflection attacks even more dangerous. If an attacker sends protocol packets with a spoofed source address to a node and this node answers with a higher amount of protocol packets or larger protocol packets, a victim node having the spoofed source address can be flooded with unwanted protocol packets. Thus, a well-designed protocol should ensure that requests, especially those without data origin authentication, are always replied with a single packet of about the same or less size and are sent to the sender address of the request. Although ROTA follows this guideline, the Candidate TA option may result in reply messages bigger than the corresponding requests. Hence, data origin authentication is very important here: Requests may only be replied if their origin is authenticated and if received from trusted nodes. This can, e.g., be achieved if ROTA Request/Reply messages are only sent over IPsec SAs.

8.3.3 Memory Exhaustion

Other DoS attacks which should be prevented are memory exhaustion attacks, i.e., an attack achieving the consumption of all memory resources of a victim by sending special sequences of protocol packets. To prevent such kind of attacks, no state should be established in HAs before the initiator of ROTA has proven to be authorized to do so. If IKE is used to establish an IPsec SA in the first place, this requirement can be achieved. Between MN and its HA as well as between CN and its HA IPsec SAs are required for Mobile IPv6 signaling anyway [3].

8.3.4 CPU Exhaustion

Verification (e.g., digital signature verification) can require significant CPU resources, which can be exploited for another type of attack, the CPU exhaustions attack. Though this attack only affects HAs, since MNs are not required to perform computationally expensive operations in ROTA, the attack would be especially dangerous if one attacker would send multiple signed ROTA Requests with spoofed source address.

Data origin authentication without using computationally expensive public key cryptography can alleviate this problem. Such a weak "pre-authentication" is for instance be done by IKEv2 or in [20] using cookies. Hence, the use of IKEv2 to establish IPsec SAs between HAs and TAs can alleviate this problem.

If IKEv2 is not used, another weak countermeasure could be to first start verification after receiving a positive ROTA Initiation Reply from CN. CN additionally checks, whether it has an active

communication session with the MN's HoA contained in the ROTA Request, e.g., by checking its IPv6 Destination Cache. This way, the attacker needs to have knowledge about active communication sessions of CN or first has to start a communication session with CN.

Additionally, a limit on the amount of resources used for verifications should be set. This approach is also used as a countermeasure for a similar attack ("Inducing unnecessary binding updates") against the Mobile IPv6 route optimization mode (see section 3.3.1 in [18]).

8.4 Other Attacks on Sending Binding Information

Other attacks are described [18] such as blocking of BU messages or forcing non-optimized bindings are considered less severe and are applicable to both ROTA and route optimization mode. Hence they are not discussed in this memo.

8.5 Attacks against Location Privacy

To ensure location privacy, an attacker MUST NOT be able to successfully pretend to be a TA. Otherwise it could find out MN's CoA and thus its location. For this reason, the intended receiver of a BU message must prove to MN's HA that it is a valid TA, i.e., it must be authorized to act as a TA. Also, the TA must be trustworthy and it may not be under control of an attacker. This can, e.g., be achieved by using authorization certificates, which can be verified when a shared trusted anchor exists. This approach is again similar to SEND [5], where certificates are used to authorize routers to act as routers.

Note that partial protection against profiling attacks by hiding the

HoA from eavesdroppers might be possible with ROTA as well by encrypting signaling and data traffic on all IPsec tunnel segments, as described in [8] for the MN-HA segment. However, this approach is considered computationally expensive for the HAs since the data packet payload is unnecessarily encrypted as well. Other approaches, which only replace the HoA with a privacy label [8] seem more appropriate and may be combined with ROTA.

8.6 Overlay Re-routing Attacks

Since the optimized route depends on distance information obtained from Probe and Distance Information messages, those messages must be sent authenticated and integrity protected. Otherwise an attacker may be able to change the overlay route in way that is of benefit for him, e.g., to eavesdrop traffic. All ROTA messages including Distance Information messages are required to be sent authenticated

and integrity protected. However, the format of active probe messages and their protection is not yet specified. This is left for future work.

9. References

9.1 Normative References

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

[2] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

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

[4] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, June 2004.

9.2 Informative References

[5] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[6] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[7] Koodli, R., "IP Address Location Privacy and IP Mobility", draft-koodli-mip6-location-privacy-00 (work in progress), February 2005.

[8] Koodli, R., "Solutions for IP Address Location Privacy in the presence of IP Mobility", draft-koodli-mip6-location-privacy-solutions-00 (work in progress), February 2005.

[9] Haddad, W., "Privacy for Mobile and Multi-homed Nodes: MoMiPriv Problem Statement", draft-haddad-momipriv-problem-statement-01 (work in progress), February 2005.

[10] Haddad, W., "Privacy for Mobile and Multi-homed Nodes (MoMiPriv): Formalizing the Threat Model", draft-haddad-momipriv-threat-model-00 (work in progress), February 2005.

[11] Wakikawa, R., "Optimized Route Cache Protocol (ORC)", draft-wakikawa-nemo-orc-01 (work in progress), November 2004.

[12] Soliman, H., Castelluccia, C., Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 mobility management (HMIPv6)",

draft-ietf-mipshop-hmipv6-04 (work in progress), December 2004.

[13] Thubert, P., "Global HA to HA protocol", draft-thubert-nemo-global-haha-00 (work in progress), October 2004.

[14] Krishnamurthi, G., Chaskar, H., and R. Siren, "Providing End-to-End Location Privacy in IP-based Mobile Communication", IEEE WCNC 2004, March 2004.

[15] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload

(ESP)", RFC 2406, November 1998.

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

[17] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-17 (work in progress), October 2004.

[18] Nikander, P., "Mobile IP version 6 Route Optimization Security Design Background", draft-ietf-mip6-ro-sec-03 (work in progress), May 2005.

[19] Dupont, F. and J. Combes, "Care-of Address Test for MIPv6 using a State Cookie", draft-dupont-mipv6-rrcookie-01 (work in progress), June 2005.

[20] Bao, F., "Certificate-based Binding Update Protocol (CBU)", draft-qiu-mip6-certificated-binding-update-03 (work in progress), March 2005.

[21] Giaretta, G., "Goals for AAA-HA interface", draft-ietf-mip6-aaa-ha-goals-00 (work in progress), May 2005.

[22] Giaretta, G., "Mobile IPv6 bootstrapping in split scenario", draft-ietf-mip6-bootstrapping-split-00 (work in progress), June 2005.

Authors' Addresses

Kilian A. Weniger
Panasonic R&D Center Germany

Monzastr. 4c
Langen 63225
Germany

Phone: +49 6103 766 137
Email: kilian.weniger@eu.panasonic.com

Takashi Aramaki
Matsushita Electric (Panasonic)
5-3 Hikarinooka
Yokosuka 239-0847
Japan

Phone: +81 46 840 5353
Email: aramaki.takashi@jp.panasonic.com

Appendix A. Recommendations for TA Selection

The TA selection algorithm must meet the privacy requirements of MN and CN, should provide good route optimization and should minimize the signaling traffic. The input parameters of the algorithm are at least the privacy requirements of MN and CN (as indicated with the P-flag in ROTA Initiation Request/Reply messages), a list of candidate TAs (provided by MN, CN, MN's HA and CN's HA), and optionally distance information. The candidate TA list should contain the addresses of MN's HA and CN's HA and may contain local HAs or other external HAs that may act as TA. However, the list may only contain TAs that are trusted by MN's and CN's HA. Untrusted TA addresses must be deleted from the list by MN's and CN's HA.

In order to minimize the signaling traffic, ROTA should be aborted if the route is already short enough without using any TAs or if the benefit of route optimization is small. Otherwise, it should be checked whether the route is short enough when ROTA without visited network support is used, i.e., either MN's or CN's HA serves as TA. If true and if the privacy requirements allow it, either of both HAs should be preferred as TA, since establishing tunnels over local HAs/ MAPs requires more signaling traffic and is only possible if the visited networks support ROTA. A single local TA may only be used, if the respective MN/CN does not require location privacy, whereas two local TAs can provide location privacy for both MN and CN.

Note that if MN's and CN's HA cannot agree on TAs in a first round of Request/Reply messages, multiple rounds of Request/Reply messages may be necessary. If the proposed set of TAs is modified, corresponding entries in the Candidate TA Option MUST be marked with the T-flag. Further, it must be ensured that the TA selection eventually terminates, e.g., by counting the additional rounds and aborting after a certain number of rounds.

Appendix B. Support of Stationary Correspondent Nodes

ROTA targets mobile-to-mobile communication scenarios, but can also be used for communication with stationary nodes. If CN is mobile, MN's HA and CN's HA perform the ROTA initiation and TA selection on behalf of MN and CN to ensure location privacy and thus can be called Privacy Agents (PA) of MN and CN, respectively. ROTA-aware stationary CNs require a similar pre-arranged trust relationship to an PA. Additionally, the PA should be able to act as TA and the PA must have a trust relationship with other HAs. Of course, a stationary CN does not require a CoA. Hence, the PA does not serve as an HA and does not manage a binding or intercept any packets for the stationary node. Note that either the TA to be used by CN is always on the path (e.g., because it is co-located with a gateway router) or the stationary CN must be adapted to be able to reverse tunnel data packets to the TA.

The PA service could, e.g., be provided by CN's ISP or by a dedicated Privacy Service Provider. It could also be provided by a Mobility Service Provider with the PA co-located with an HA. However, topologically the PA should not be too far away from the stationary node for good route optimization and location privacy support.

Appendix C. Discussion of Further Optimizations

One drawback of ROTA is the additional overhead due to encapsulation of data packets. To alleviate this problem, header compression schemes can be applied to all tunnel segments. Other possible optimizations include support for an improved TA selection that considers more parameters, e.g., more detailed privacy requirements (e.g., location privacy is required, but disclosing location in country size-like resolution is o.k.), application requirements for the route length/delay or load factors. Additional features to be considered in future version is the support for mobile networks and an interface to an AAA infrastructure, which may be required for service authorization and charging. Such an interface is currently in development (see [21]) and may be re-used by ROTA.

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.