NEMO Working Group
Internet-Draft
Expires: April 7, 2005

C. Ng
Panasonic Singapore Labs
J. Hirano
Panasonic

October 7, 2004

Extending Return Routability Procedure for Network Prefix (RRNP)
draft-ng-nemo-rrnp-00

Status of this Memo

Copyright Notice

Abstract

This memo highlights the inadequacy of existing return routability procedure when one takes network prefix into consideration under the context of route optimization with Network Mobility (NEMO). An extended return routability procedure, called Return Routability with Network Prefix (RRNP), is thus proposed to address this problem. With RRNP, a correspondent node can verify the collocation of care-of

address, home address, and network prefix(es) specified in a binding update message.

Table of Contents

1. Introduction

Currently, mobile node uses a procedure known as the Return Routability (RR) procedure [1] to allow a correspondent node to be assured of the collocation of the mobile node's home address and care-of address. When one consider network mobility [2], it is foreseeable that for route optimization to work [3], it might be

necessary for a mobile router to inform the correspondent node which network prefixes the mobile network is using, so that the correspondent node can forward packets destined to mobile network nodes in the mobile network directly to the mobile router's care-of address.

In such situation, the original return routability procedure is inadequate since it does not provide a means for the correspondent node to ascertain that the network prefixes specified by the mobile router are in fact handled by the mobile router. In order to solve this problem, this memo describes an improved procedure known as the Return Routability with Network Prefix (RRNP) procedure where the mobile router will first list the network prefixes it owns in the Home Test Init (HoTI) message. The correspondent node tests the collocation of these network prefixes by generating some cryptographic tokens and sending each of these tokens to an address randomly selected from each network prefix. The mobile router must capture these packets, extract the cryptographic tokens, and use these tokens to generate a hash value in the binding update message it later sends to the correspondent node. In this way, the correspondent node can verify that the mobile router indeed owns the network prefixes it claims to own.

It is assumed that readers are familiar with the original return routability procedure specified in [1], and the terminology related to network mobility (NEMO) defined in [4].

We begin by first describing the problem of the existing return routability procedure when Mobile Network Prefix option is inserted into Binding Update messages in Section 2. Section 3 then presents an overview of the extended return routability procedure to solve this problem. The new mobility message and option formats are then introduced in Section 4 before we explain the improved procedure with greater detail in Section 5. Finally, Section 6 discusses some security considerations in the design of the RRNP.

2. Inadequacy of Existing RR Procedure

2.1 Possible Route Optimization Mechanism in NEMO

There is currently no accepted route optimization solution for Network Mobility. However, it is foreseeable that a possible approach to route optimization involves sending binding updates with Network Prefix Options as defined in [2] to correspondent nodes. As an illustration of how this will work, consider the deployment scenario depicted in Figure 1 below.

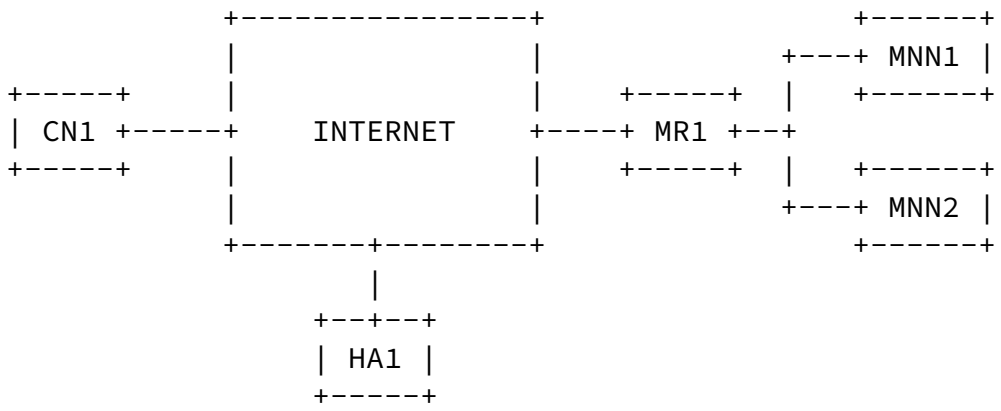

Figure 1: Deployment Scenario

Here, the mobile network with mobile network prefix MNP consists of a mobile router MR1 with two mobile network nodes, MNN1 and MNN2, behind MR1. The home address of MR1 is MR1.HoA, and current care-of address of MR1 is MR1.CoA. HA1 is the home agent of MR1 and CN1 is the correspondent node communicating with, say MNN1. If route optimization is not used, a packet sent from CN1 to MNN1 will follow the path:

CN1 ---> HA1 ===> MR1 ---> MNN1

Now, suppose MR1 sends CN1 a Binding Update message with the Mobile Network Prefix option, such that within CN1, it will insert a route

into its own routing table that all packets sent to the prefix MNP will be tunneled to the address MR1.CoA, then route optimization will have been achieved. The path of the packet will now be:

```
CN1 ===> MR1 ---> MNN1
```


2.2 Security Threats with Unverified Network Prefixes

Although the inclusion of Mobile Network Prefix option allows route optimization to be setup between a mobile network and a correspondent node, existing return routability procedure as defined in [1] does not provide a means for correspondent node to verify that the Mobile Network Prefix option specified in the binding update is valid and legitimate. This exposes the correspondent node to additional security threats.

One immediate threat is that the Mobile Network Prefix option may be changed, or inserted, by an attacker. This cause the correspondent node to send data packets meant for other network to the mobile router. This can be used to launch a flooding attack on the mobile router, overwhelming the mobile router with data packets not meant for its network. However, this attack is inherently diverted by the existing return routability procedure, since the integrity of the Binding Update message is protected by the binding management key, Kbm. So any change in the Mobile Network Prefix option will cause the Binding Authorization Data option to carry a wrong Authenticator value. This could be easily checked by the correspondent node.

Another threat is when a "mobile router" is itself malicious. It can specify prefixes that it does not actually own in the Mobile Network Prefix option. This way, the correspondent node is tricked into forwarding packets (which it intends to send to some other network)

to the malicious "mobile router". Thus, this allows the "mobile router" to spoofed into packets sent by the correspondent node to some destination, which is otherwise not possible. This threat is illustrated in Figure 2 below.

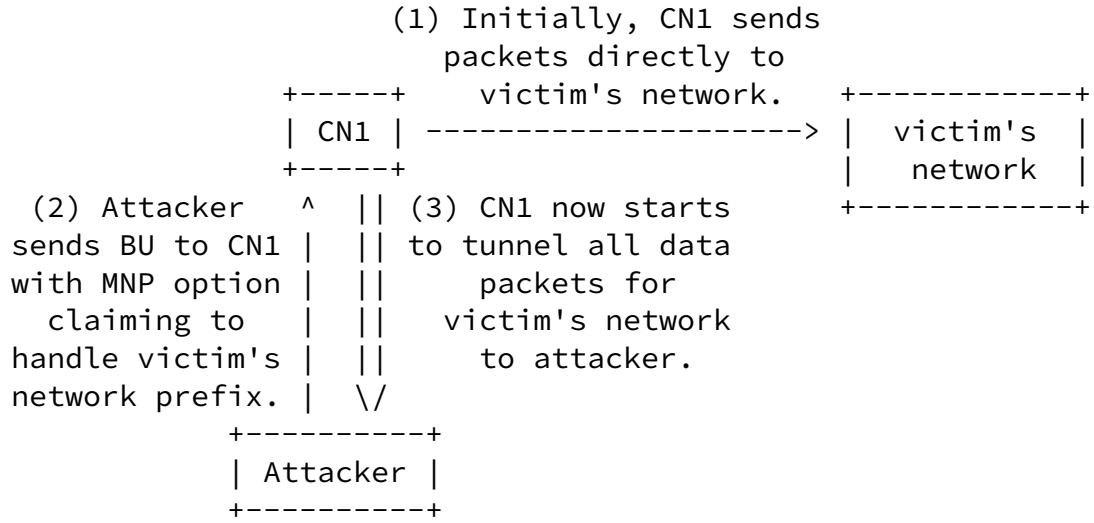

Figure 2: Attacker claiming to handle victim's network prefix

Existing return routability procedure cannot prevent such attacks. This is because return routability procedure can only verify that the home address and care-of address are collocated. Thus an attacker may very well own both the home address and care-of address specified in the Binding Update, causing the return routability procedure to pass successfully. The correspondent node has no way of checking if the network prefix claimed to be owned by a sender of the Binding Update message is indeed owned by the sender.

Thus, an improved return routability procedure has to be designed to allow the correspondent node to check the validity of the Mobile Network Prefix option, before route optimization between CN and MR can be established without exposing the nodes involved to additional security threats.

3. Overview of RRNP

The improved return routability procedure, known as the RRNP, is meant to extend the existing return routability procedure to bindings

of network prefixes. In the RRNP, the mobile router will first list the network prefixes it owns in the Home Test Init (HoTI) message. When the correspondent node sees these prefixes, it sends, in addition to the normal HoT message, a new message referred to as Network Prefix Test (NPT) message for each network prefix included in the HoTI message. The NPT message contains a token that is cryptographically generated based on the network prefix, and is addressed to an address that is randomly generated from the network prefix. The mobile router must intercept all the NPT messages, and store these tokens. In the Binding Update message the mobile router send to the correspondent node, the Authenticator value of the Binding Authorization Data option is generated using the tokens contained in the Home Test (HoT), Care-of Test (CoT) and NPT messages sent from the correspondent node. In this way, the correspondent node can verify that the care-of address and home address of the mobile router are collocated, and that the mobile router indeed owns the network prefixes it claimed to own.

Figure 3 below illustrates the message sequence diagram of the RRNP.

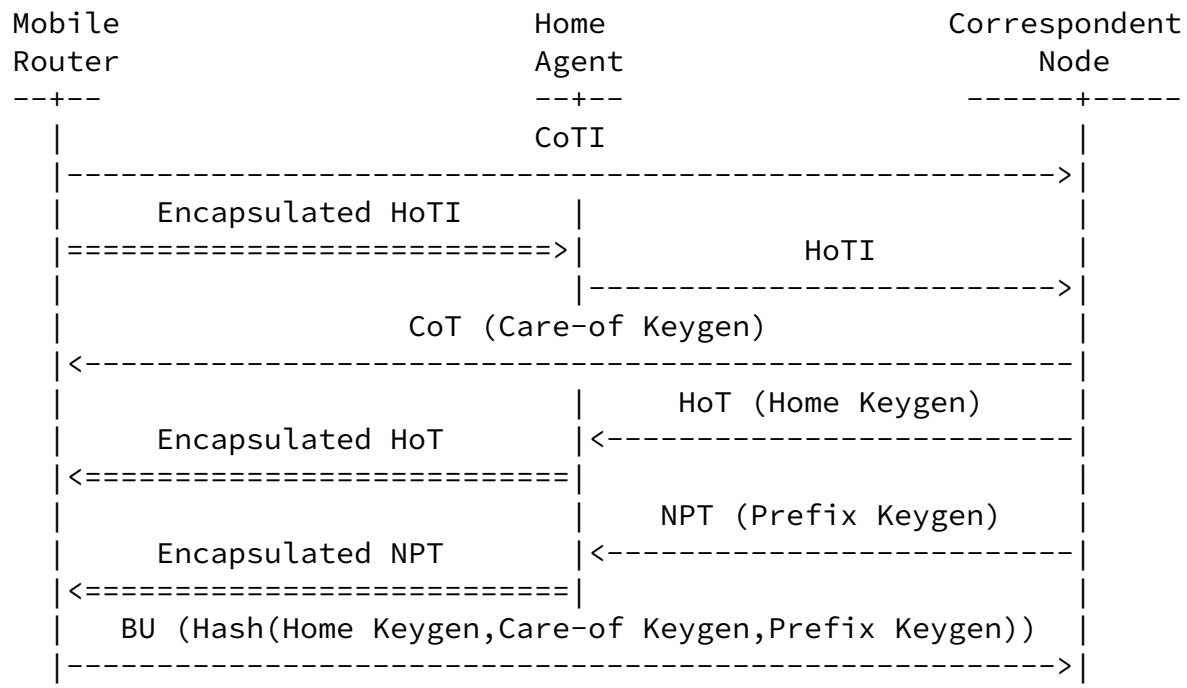

Figure 3: Message sequence diagram of a RRNP procedure

4. Modifications to Existing Protocols

4.1 New Network Prefix Test Message

The Network Prefix Test (NPT) message is sent by a correspondent node to a random address selected from a prefix. This message is meant to be intercepted by a mobile router owning the prefix. Figure 4 below shows the format of Network Prefix Test message.

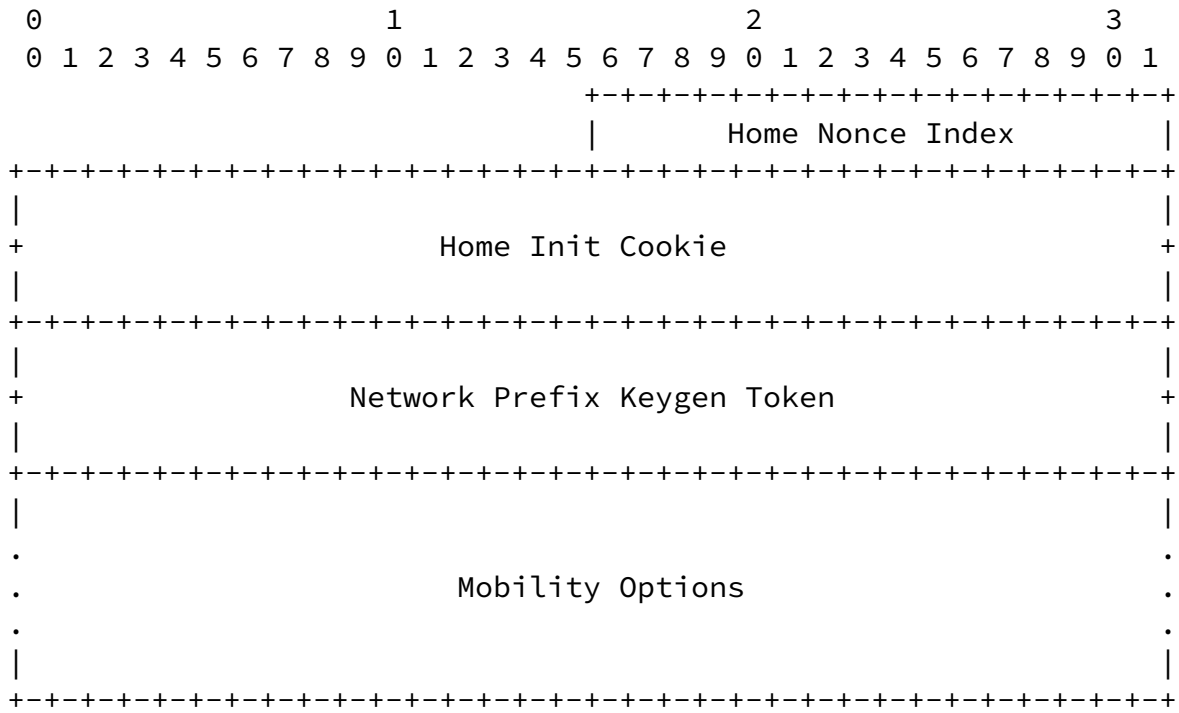

Figure 4: Network Prefix Test Message

MH Type

To be assigned. Identifies the mobility message as a Network Prefix Test message.

Home Nonce Index

The index of the nonce used to generate the Network Prefix Keygen Token. Note that this should be the same as the once used to generate the Home Keygen Token.

Home Init Cookie

This value is copied from the Home Test Init message.

Network Prefix Keygen Token

This is the keygen token generated based on the network prefix specified in a Mobile Network Prefix option.

Mobility Options

The Network Prefix Test message should contain one (and only one) Mobile Network Prefix option as defined in [2]. This value is copied from the Home Test Init message.

4.2 New Number of Prefixes Option

The Number of Network Prefixes option is included in a Home Test (HoT) message sent by a correspondent node to indicate to the mobile router how many network prefixes is accepted. This option is included to allow the mobile router to know how many Network Prefix

Test message it needs to intercept. In addition, it also serves to indicate to the mobile router that the correspondent node understands the Mobile Network Prefix options included in the Home Test Init message. Figure 5 below shows the format of option.

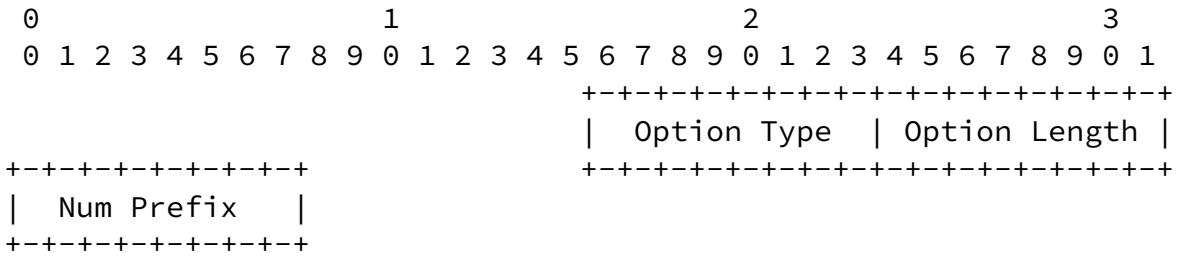

Figure 5: Number of Prefixes Option

Option Type

To be assigned. Identifies the mobility option as a Number of Prefixes option.

Option Length

The length in octets of this option, excluding the first 2 octets. Always equal to 1.

Num Prefix

The number of prefixes the correspondent node is willing to accept.

4.3 Modifications to Home Test Init Message

There is no change to the format of the Home Test Init (HoTI) message as per defined by Mobile IPv6 [1], except that the Home Test Init message is now extended to be able to include the Mobile Network Prefix option as defined by NEMO Basic Support [2].

4.4 Modifications to Home Test Message

There is no change to the format of the Home Test (HoT) message as per defined by Mobile IPv6 [1], except that the Home Test message is now extended to be able to include the Number of Prefixes option as defined in Section 4.2.

5. Detailed Description of RRNP

5.1 Initiating the RRNP: Sending HoTI and CoTI

Once the mobile router determines that it wishes to perform route optimization with a correspondent node, it initiates the return routability procedure by sending the Home Test Init and Care-of Test messages to the correspondent node.

Sending of the Care-of Test Init message is exactly the same as the original return routability procedure. The packet contents is shown below:

```
IPv6 Header {
    Source = care-of address of mobile router
    Destination = correspondent node
}
Mobility Header {
    MH Type = Care-of Test Init
    Care-of Init Cookie = random value
}
```

Sending of the Home Test Init message is also largely similar to that in the original return routability procedure, except that the mobile router inserts one (or more, depending on the number of prefixes the mobile router owns and wishes to perform route optimization with the correspondent node) Mobile Network Prefix option in the Home Test Init message. It may not be to the benefit of the mobile router to inform the correspondent node of all the NEMO prefixes it owns since this may result in a longer message and a longer time period of intercepting NPT messages (see Section 5.4).

The packet contents of the HoTI message is shown below:

```
IPv6 Header {
    Source = home address of mobile router
    Destination = correspondent node
}
Mobility Header {
    MH Type = Home Test Init
    Home Init Cookie = random value
    Mobile Network Prefix Option {
        Prefix Length = length of prefix
        Mobile Network Prefix = prefix of the mobile network
    }
}
```


Since the Home Test Init message is sent using the home address as the source, this packet is encapsulated into a tunnel back to the home agent of the mobile router.

5.2 Responding to the CoTI with CoT

When the correspondent node receives the Care-of Test Init message, and decides to accept route optimization with the mobile router, it responds with a Care-of Test message. Preparation of the Care-of Test message is exactly the same as that specified in Mobile IPv6 [1]. First, the correspondent node selects a nonce to generate a keygen token. The nonce selected should be identifiable by a 16-bits nonce index. The Care-of Keygen Token, CoK, is then generated by

```
CoK := First(64,
       HMAC_SHA1(Kcn, (care-of address | nonce | 0x01)))   (Eq 1)
```

where

First(L,m) is to truncate the message m leaving the leftmost L bits,

HMAC_SHA1(K,m) is the hash result of taking the HMAC-SHA1 hash function [5][6] on the message m using the cryptographic key K,

Kcn is a secret key of the correspondent node, and

'|' denotes concatenation of bit stream.

The Care-of Keygen Token and the nonce index are then included in a Care-of Test message to be returned to the mobile router, including the Care-of Init Cookie copied from the Care-of Test Init message. The packet contents is shown below:

```
IPv6 Header {
    Source = correspondent node
    Destination = care-of-address of mobile router
}
Mobility Header {
    MH Type = Care-of Test
    Care-of Nonce Index
    Care-of Init Cookie = copied from CoTI
    Care-of Keygen Token = generated as per (Eq 1)
}
```


5.3 Responding to the HoTI with HoT and NPT

When the correspondent node receives the Home Test Init message, and decides to accept route optimization with the mobile router, it

responds with a Home Test message. In addition, for every network prefix specified in a Mobile Network Prefix option in the Home Test message it is prepared to accept, the correspondent node will reply with a Network Prefix Test message. Note that it is up to the discretion of the correspondent node whether to respond to the HoTI/CoTI message, and the number of network prefixes to accept (see Section 6).

In preparation of the Home Test message, the correspondent node first selects a nonce to generate the keygen token. The nonce selected should be identifiable by a 16-bits nonce index. The Home Keygen Token, HoK, is then generated by

```
HoK := First(64,
         HMAC_SHA1(Kcn, (home address | nonce | 0x00)))    (Eq 2)
```

The Home Keygen Token and the nonce index are then included in a Home Test message to be returned to the mobile router, including the Home Init Cookie copied from the Home Test Init message. In addition, a Number of Network Prefix option is also included to indicate to the mobile router how many network prefixes specified in the Home Test Init message the correspondent node is prepared to accept. For every network prefix the correspondent node is willing to accept, the correspondent node will sent a separate Network Prefix Test message. The packet contents is shown below:

```
IPv6 Header {
    Source = correspondent node
    Destination = home address of mobile router
}
Mobility Header {
    MH Type = Home Test
    Home Nonce Index
    Home Init Cookie = copied from HoTI
    Home Keygen Token = generated as per (Eq 2)
    Number of Network Prefix Option {
        Number of Prefix = maximum number of prefixes accepted
    }
}
```

For the Network Prefix Test message, a Network Prefix Keygen Token is also generated. The nonce selected is the same as the one used to generate the Home Keygen Token. The Network Prefix Keygen Token,

NPK, is given by

```
NPK := First(64,
       HMAC_SHA1(Kcn, (network prefix | nonce | 0x02)))    (Eq 3)
```

The Network Prefix Keygen Token and the nonce index are then included in a Network Prefix Test message to be returned to the mobile router, including the Home Init Cookie copied from the Home Test Init message. In addition, a Mobile Network Prefix option is also included to indicate to the mobile router which mobile network prefix this Network Prefix Test message is for. The packet contents is shown below:

```
IPv6 Header {
    Source = correspondent node
    Destination = random address selected from network prefix
}
Mobility Header {
    MH Type = Network Prefix Test
    Home Nonce Index
    Home Init Cookie = copied from HoTI
    Network Prefix Keygen Token = generated as per (Eq 3)
    Mobile Network Prefix Option {
        Copied from the HoTI message
    }
}
```

The Network Prefix Test message is sent to an address randomly selected from the mobile network prefix that this Network Prefix Test message is for. Because the correspondent node sent more than one packet for each Home Test Init message with Mobile Network Prefix option received, the correspondent should add a random delay before sending each Network Prefix Test message sent to avoid amplification effect. The delay, however, must be within a known limit. For the purpose of this document, we specify the random delay selected must be within the range of (0, MAX_NPT_DELAY). A suitable value of

MAX_NPT_DELAY can be 0.5 seconds.

In addition, the correspondent node should also take note of the mobile router sending the HoTI message. Should multiple HoTI messages are received from the same mobile router within a short time span, the correspondent node should reject subsequent HoTI messages as it is possible that the mobile router is trying to stage a denial-of-service attack against the network prefix specified.

5.4 Intercepting the NPT messages

After sending the Home Test Init and Care-of Test Init messages, the mobile router must start intercepting the Home Test, Care-of Test, and Network Prefix Test messages. The Home Test and Care-of Test messages should not pose any problem, as they are addressed to the home address and care-of address of the mobile router respectively. To intercept the Network Prefix Test messages, the mobile router must inspect every packet addressed to the mobile network to see if they are indeed a Network Prefix Test message.

It is recommended that the mobile router starts a timer after sending the Home Test Init message. During this time period, the mobile router will inspect every packet that satisfies all of the following criteria to check if it is a Network Prefix Test message:

- the packet arrives in a tunnel from the home agent
- the packet bears the correspondent node's address as the source address
- the packet bears a destination address that is formed from a

network prefix that is sent to the correspondent node in a Mobile Network Prefix option in the Home Test Init message

The timer value should be chosen such that it is sufficiently long for all Network Prefix Test message to be received by the mobile router. A reasonable value is given by

$$timer = T\_rtt + n * MAX\_NPT\_DELAY \quad \text{(Eq 4)}$$

where

T_rtt is the round-trip time taken for a packet to be sent from the mobile router to the correspondent node and back again, via the home agent, and

n is a number of Mobile Network Prefix options included in the HoTI message.

This a best estimate assuming there is no congestion in the network. A more conservative value can be given by

$$timer = 2 * T\_rtt + n * MAX\_NPT\_DELAY \quad \text{(Eq 5)}$$

In addition, once the mobile router has received the Home Test message, it will know from the Number of Prefixes option how many network prefixes the correspondent node is willing to accept. The

mobile router can then adjust the timer value accordingly.

Once the mobile router has received the Home Test message, Care-of Test message, and all the Network Prefix Test messages (as specified

by the Number of Prefixes option) or when the timer expires, it can proceed to complete the return routability procedure by sending the Binding Update message. This is described in the next sub-section (Section 5.5).

There are several sanity checks the mobile router can perform when receiving the Home Test, Care-of Test, and Network Prefix Test messages. Firstly, the mobile router can verify that the Home Init Cookie and Care-of Init Cookie are the same as those it has sent in the Home Test Init and Care-of Test Init messages. Secondly, it can check that the Network Prefix Test message specifies the same Home Init Cookie. Thirdly, it can verify that the Network Prefix Test message specifies the same Home Nonce Index as that specified in the Home Test message.

5.5 Sending the Binding Update

To complete the return routability procedure, the mobile router will have to send the Binding Update message to the correspondent node. In the Binding Update message, the mobile router should include the nonce indices in the Nonce Indices option. In addition, a Mobile Network Prefix option should also be included for every network prefix that the mobile router has received a Network Prefix Test message. Furthermore, the mobile router should include a cryptographic checksum in the Authenticator field of a Binding Authorization Data option. To generate the checksum, the mobile router must first obtain the binding management key, Kbm, given by

$$Kbm := SHA1\ (HoK \mid CoK \mid NPK\_1 \mid \ldots \mid NPK\_n) \qquad \text{(Eq 6)}$$

where

SHA1(m) is the result of applying the Secure Hash Algorithm [5] on the message m,

HoK is the Home Keygen Token from the HoT message,

CoK is the Care-of Keygen Token from the CoT message, and

NPK_i is the Network Prefix Keygen Token from the i-th NPT message.

This gives the Kbm as a 20 octets (160 bits) long value. It is used by both the mobile router and the correspondent node to generate the

Authenticator value. For the Binding Update message, the Authenticator value is given by

```
Authenticator := First(96,
      HMAC_SHA1(Kbm, (CoA | correspondent | BU))        (Eq 6)
```

where

CoA is the care-of address of the mobile router,

correspondent is the address of the correspondent node, and

BU is the entire Binding Update message except the Authenticator field itself.

When generating the Authenticator value, the Checksum field of the Mobility Header is first initialized as zero. Before sending the Binding Update message, the Binding Authorization Data option is appended as the last option, and the Checksum is finally calculated, including the Authenticator field in the calculation. If there are multiple Mobile Network Prefix options, the mobile router must be careful to ensure that the order of the Mobile Network Prefix options is the same as the order the corresponding Network Prefix Keygen Token is concatenated in (Eq 6) to generate the Kbm. The packet contents of the Binding Update message is shown below:

```
IPv6 Header {
    Source = care-of address of mobile router
    Destination = correspondent node
```

```
    }
    Mobility Header {
        MH Type = Binding Update
        Flags = H,K must be cleared, R should be set
        Nonce Indices Option {
            Home Nonce Index
            Care-of Nonce Index
        }
        Mobile Network Prefix Option {
            Prefix Length = length of prefix
            Mobile Network Prefix = prefix of the mobile network
        }
        Binding Authorization Data Option {
            Authenticator = calculated as per (Eq 7)
        }
    }
```

It must again be noted that the correspondent node need not maintain

any state information before the receipt of the Binding Update message. Using information contained in the Binding Update message, it is sufficient for the correspondent node to generate the Home Keygen Token, Care-of Keygen Token, and Network Prefix Keygen Token(s) to derive the binding management key independently and verify the Authenticator value.

5.6 Error Handling

This section outlines some of the possible error conditions that might occur during a RRNP procedure.

- Failure to receive HoT/CoT message

  When a mobile router fails to receive a HoT or CoT message after

sending the HoTI and CoTI message, the mobile router must not proceed with sending of binding update. If a pre-determined time period, possibly determined by (Eq 5), has elapsed, the mobile router may assume that some packets are lost, and re-initiate the RRNP procedure. The mobile router may give up after consecutive failed attempts.

- Failure to receive NPT message

  If the mobile router failed to receive any NPT message, even though the HoT message indicates that the correspondnet node has accepted one or more Mobile Network Prefix options, the mobile router may choose to proceed with sending normal Binding Update message (without any Mobile Network Prefix options) or to re-initiate the RRNP procedure. It makes sense to proceed with sending normal Binding Update message only if the mobile router itself is communicating with the correspondent node. If the mobile router choose to re-initiate the RRNP procedure, it may give up after consecutive failed attempts.

- Correspondent node does not support RR procedure

  If the correspondent node does not support the original return routability procedure, it will respond to the HoTI and CoTI messages with an ICMP parameter problem code 1. The mobile router should take such messages as indication of the correspondent node not supporting the RR procedure.

- Correspondent node does not support RRNP procedure

  If the correspondent node supports the original return routability procedure, but not the RRNP extension, it will silently ignore the Mobile Network Prefix option in HoTI message. This will result in

the correspondent node returning a HoT message without any Number of Prefixes option. The mobile router should take the absence of Number of Network Prefixes option as an indication of the correspondent node not supporting the RRNP procedure, and either proceed with the normal RR procedure, or give up the RRNP procedure. It makes sense to proceed with the normal RR procedure only if the mobile router itself is communicating with the correspondent node.

6. Security Considerations

The RRNP procedure described is designed to minimize the possible security threats mobile routers and correspondent nodes are exposed to when attempting to achieve route optimization. The RRNP procedure described here is an extension of the original RR procedure described in Mobile IPv6. This extension has been carefully designed to retain all the beneficial features of the original RR procedure [7].

Firstly, keys and nonce used are never transmitted in clear. For an attacker to independently derive the binding management key, the attacker must be able to intercept all the Home Test, Care-of Test and Network Prefix Test messages sent by the correspondent node. It is especially difficult for the attacker to intercept the Network Prefix Test message since the destination is a randomly selected address.

Secondly, the correspondent node is not required to maintain any state information before accepting the binding update. This reduces the possibility of the correspondent node being exposed to denial-of-service attack.

Thirdly, replay attacks are diverted since the Binding Update/Acknowledgment message is protected by the Authenticator data, so a replay attack staged by simply changing the sequence number of previously snooped Binding Update/Acknowledgment message and re-calculating the mobility header checksum will not work since the cryptographic hash value in the Authenticator data will not tally.

The only relaxation in terms of security this RRNP procedure has is that the correspondent node will need to send more than one packets for every HoTI message received. It is thus possible for an attacker to make use of this amplification effect to launch a distributed denial-of-service attack against a victim, by having the correspondent node send large number of HoT and NPT messages to the victim. As mentioned in the earlier text, the correspondent node can somewhat ameliorate this by adding random delays before sending the

NPT messages. In addition, the correspondent node can also refuse to process subsequent HoTI messages when it has received a large number of HoTI messages in a short span of time. Finally, the option of whether to respond to route optimization should be made configurable in implementations of correspondent node, and the default configuration should be set to not perform route optimization.

7 References

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

[2] Devarapalli, V., "Network Mobility (NEMO) Basic Support Protocol", draft-ietf-nemo-basic-support-03 (work in progress), June 2004.

[3] Thubert, P., Molteni, M. and C. Ng, "Taxonomy of Route Optimization models in the Nemo Context", draft-thubert-nemo-ro-taxonomy-02 (work in progress), February 2004.

[4] Ernst, T. and H. Lach, "Network Mobility Support Terminology", draft-ietf-nemo-terminology-01 (work in progress), February 2004.

[5] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-1, April 1995, <http://www.itl.nist.gov/fipspubs/fip180-1.htm>.

[6] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[7] Nikander, P., "Mobile IP version 6 Route Optimization Security Design Background", draft-ietf-mip6-ro-sec-01 (work in progress), July 2004.

[8] Wakikawa, R., "Optimized Route Cache Protocol (ORC)", draft-wakikawa-nemo-orc-00 (work in progress), July 2004.

Authors' Addresses

Chan-Wah Ng
Panasonic Singapore Laboratories Pte Ltd
Blk 1022 Tai Seng Ave #06-3530
Tai Seng Industrial Estate
Singapore 534415
SG

Phone: +65 65505420
EMail: cwng@psl.com.sg

Jun Hirano
Matsushita Electric Industrial Co., Ltd. (Panasonic)
5-3 Hikarino-oka
Yokosuka, Kanagawa 239-0847
JP

Phone: +81 46 840 5123

EMail: hirano.jun@jp.panasonic.com

Appendix A. Applicability of RRNP

Although this memo assumes route optimization to be achieved by binding network prefixes to care-of address at the correspondent node, the same principle behind RRNP can be used as long as a node needs to verify if prefixes are indeed owned by some other node that claims to own them.

For instance, in [8], correspondent router is performing route optimization in proxy of correspondent node. The correspondent router can then use RRNP to verify that mobile router owns the mobile network prefix it claims to own. In addition, if the correspondent router sends to the mobile router one or more network prefixes that the correspondent router claims to be able to perform route optimization on behalf of, the mobile router can use the same principle behind RRNP to test the validity of such a claim.

In the latter case, there is no need to send the CoTI message if the correspondent router is a fix node. The correspondent router can simple send the HoTI message to the mobile router with network prefix information. To test the validity, the mobile router responds with HoT and NPT messages. The mobile router only accepts the correspondent router as a valid proxy for the correspondent nodes the correspondent router claims to manage when the RRNP procedure is succesfully completed.

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

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