NEMO Working Group
Internet Draft
Expires: March 2004

Jong
Seon
Chongk
Seoul National Uni
Sun
Hyunjeo
Chang
Samsung Elec
Septemb

Secure Nested Tunnels Optimization using Nested Path Info
draft-na-nemo-nested-path-info-00

Status of this Memo

Abstract

This document addresses how to securely achieve the nested
optimization using nested path information that reflects th
optimized path from Top Level Mobile Router(TLMR) to Mobile
Router(MR) in nested mobile networks. The solution is base
Reverse Routing Header(RRH) idea and the concern of securit

problem in RRH. By carefully taking a look at the simplicit
Routing Header Type 2 routing mechanism and the complexity
Access Router Option(ARO) based solution to get rid of the
of possible attack for RRH, the proposed solution has been
considered to preserve the efficiency of RRH without the la
security.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHA
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONA
this document are to be interpreted as described in RFC-211

Table of Contents

1. Introduction

NEMO Basic Support Solution[15] would suppose to support transparent mobility to mobile network nodes(MNNs) in mobil networks by using MR-HA bi-directional tunneling. However, multiple mobile networks are nested, that brings an routing overhead to us which is well known as "pinball" routing pro So, it needs to avoid routing overhead like this because we easily imagine the applications of nested mobile networks s NEMO in public transportations e.g. train, bus, airplane. I and [5], the nested routing problem has been broadly touche general still not acceptable we think.

To get generally acceptable solution for this problem, this document addresses how to securely achieve the nested tunne optimization using nested path information that reflects th optimized path from Top Level Mobile Router(TLMR) to Mobile Router(MR) in nested mobile networks. The solution is base Reverse Routing Header(RRH)[4] idea and the concern of spoo attack(or redirect attack) from [5]. By carefully taking a the simplicity of Routing Header Type 2 routing mechanism a complexity of Access Router Option(ARO) solution to get rid threat of possible attack for RRH, the proposed solution ha considered to preserve the efficiency of RRH without the la security.

In proposed solution, MR uses Nested Path Information(NPI)

inform the optimized routing path of its HA. It discovers N
sent from its Access Router(AR) and deliver that informatio
HA through BU. Unlike RRH of [4], NPI cannot be modified or
by the intermediate ARs. In case of the existence of fake A
nested path, Of course, false NPI information may be used b
It's impossible that there is unauthenticated fake AR if on
network access control properly applied. But, although it's
possible, the fake AR would not get any reward for such an
impersonating if the HA-MR tunnel could be protected by IPS
the integrity of NPI also additionally protected by Authent
Header[8]. In section 6, the security considerations will b
mentioned.

2. Terminology

It is assumed that readers are familiar with NEMO terminolo
described in [2][14], and the terms described in [4][5]. In
addition, we define a few of terms used in describing the o
of our solution.

Nested Path Information (NPI)

A form of array of IPv6 global addresses that are th
addresses of Mobile Routers on the nested path which
from TLMR to any nested MR in nested mobile networks

RO-enabled

That is a similar with "NEMO-enabled" used in [ARO].
any tunnel that applied with the scheme of route
optimization proposed by this document is referred t
enabled" tunnel.

Nested Path Option (NP Option)

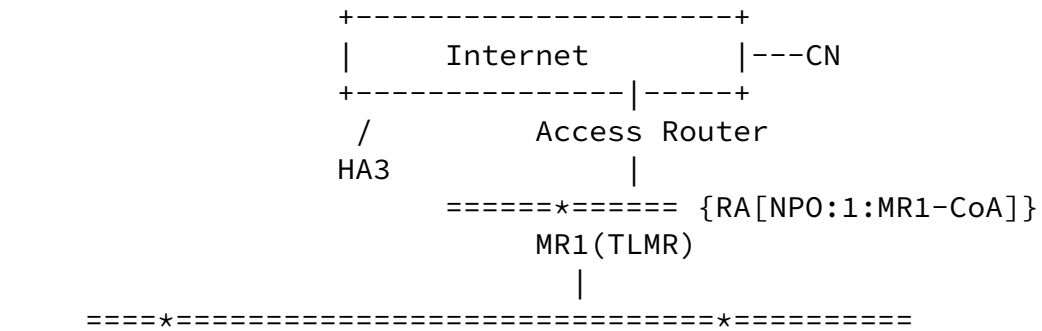
New type of option added in Router Advertisement to
NPI in nested mobile networks. That information is f
from TLMR to downward by relaying of each AR.

Nested Routing Path Option (NRP Option)

New type of mobility option used in BU message. That
NPI to Home Agent(HA).

3. Overview of Operation

We use the nested mobile network example as following Fig.1



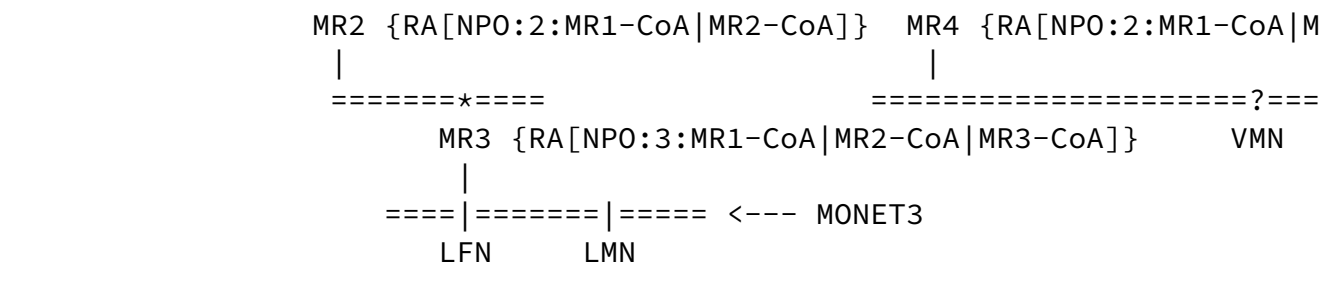
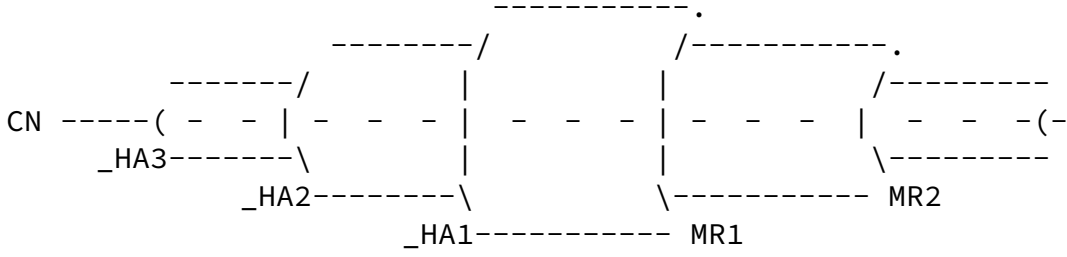
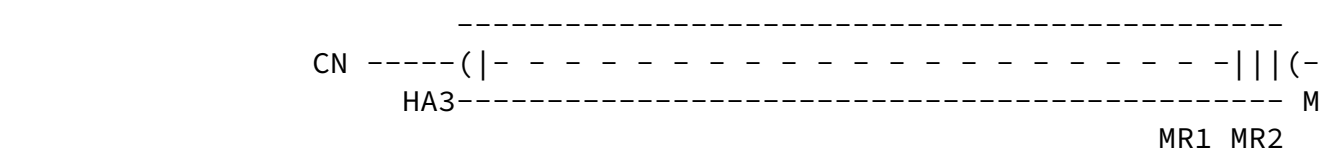


Fig.1 An example nested Mobile Network

In this example, we would have three bi-directional nested
by using NEMO Basic Solution if any nested tunnel optimizat
applied.



With the proposed solution, we can get one optimized tunnel
follows. From the following optimized tunnel, we can see th
solution's optimized result is same with one in [4].



No receiving RA with NP Option in the access link gets MR1
that it is TLMR of nested mobile networks. As in Fig.1, MR1
periodically RA with NP Option to its ingress link. MR2 and
each relays its RA with modified NP Option, in which IPv6 g
address of the egress interface is appended, to ingress lin

Through the NP Option relay of MRs, MR3 results in getting
nested path such like MR1-CoA->MR2-CoA->MR3-CoA, the path t
from MR3.

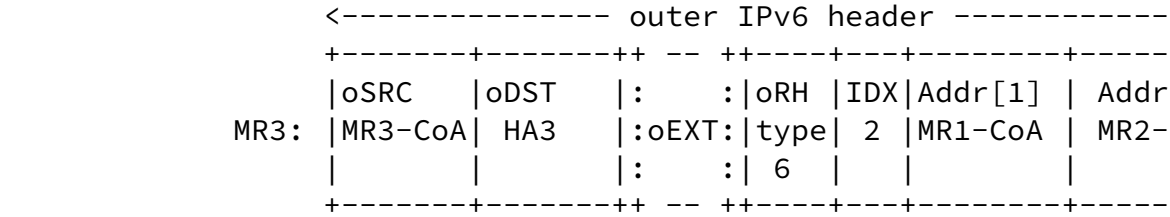
MR3 can start extended Binding Update(BU) with HA3 for the
optimization after getting NPI from RA with NP Option. MR3
Option, newly introduced mobility option to securely carry

HA3. This kind of BU with NRP Option makes it possible that
nested tunnels optimization between MR3 and HA3. Basically,
message is exchanged to HA3 through normal nested tunnels.
receiving BU with NRP Option makes new Binding Cache(BC) en
NPI and RO-enabled tunnel-interface for forward tunneling.
receiving successful BACK, MR3 also sets up the RO-enabled
interface for reverse tunneling. In RO-enabled tunnel inter
each created in MR3 and HA3 through MIPv6 BU/BACK exchange,
effectively used in routing that optimizing the nested tunn

After the establishment of RO-enabled bi-directional tunne
can forward the packets from its ingress interfaces to RO-e
reverse tunnel interface and HA3 can do the packets destine
MONET3 to RO-enabled forward tunnel interface. For details,
following subsections describe the procedure of reverse and
packet delivery using the RO-enabled tunnel.

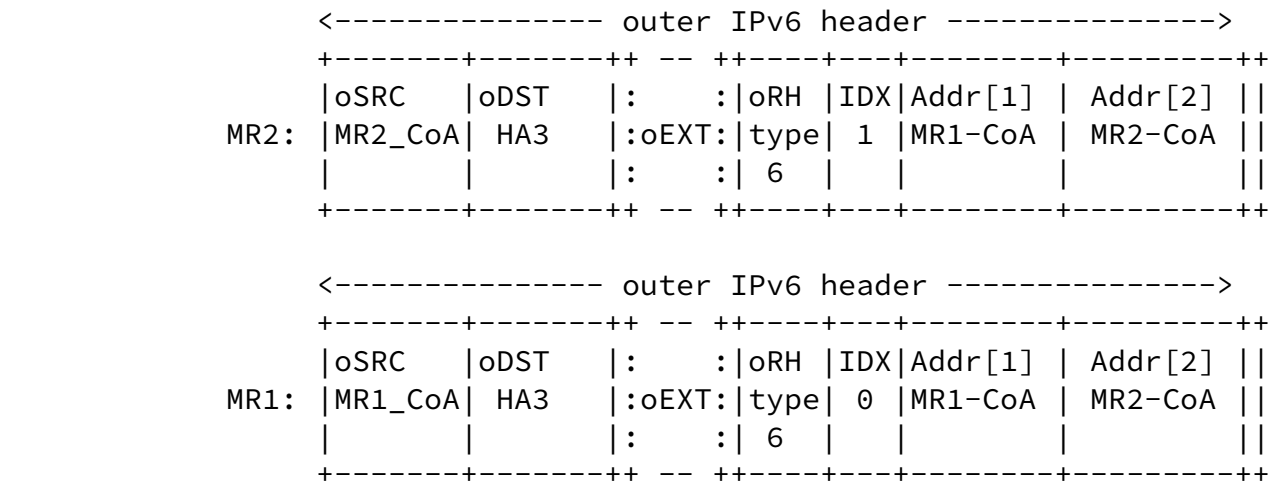
3.1 Reverse Packet Delivery(MR3 -> HA3)

In order to forward the packets sent from ingress side to H
makes sure that the correspondent tunnel interface is alrea
established by both MR3 and HA3. If that tunnel interface m
with RO-enabled and NPI available in Binding Update List(BU
MR3 builds the tunneling packet like below and forwards to
MR on the nested path. In the outer IPv6 header, Type 6 Rou
Header(RH) needs to be used to indicate next-hop MRs that t
tunneling packet can be delivered to the Home Agent through
nested tunnels optimization using NPI.



In the example, MR2 does not forward packets to HA2 via def
reverse tunnel(nested tunnel) if they have RH Type 6 option
header. Instead of reverse tunneling, MR2 refers to the add
Addr[IDX] indexed by IDX field, and makes sure that it is M
address. If the indexed address matched with any of address
its egress interfaces, MR2 forwards the packet, for which t

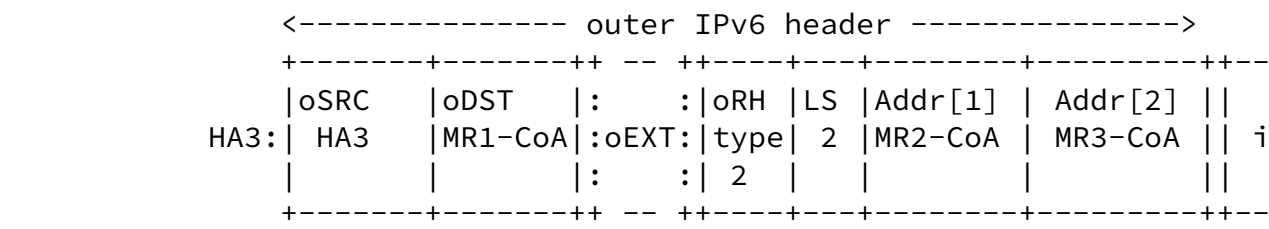
source address and IDX field in outer IPv6 header are only
as below, to that interface. Otherwise, the packet will be
discarded. As like MR2's operation, MR1 does the same thing
below.



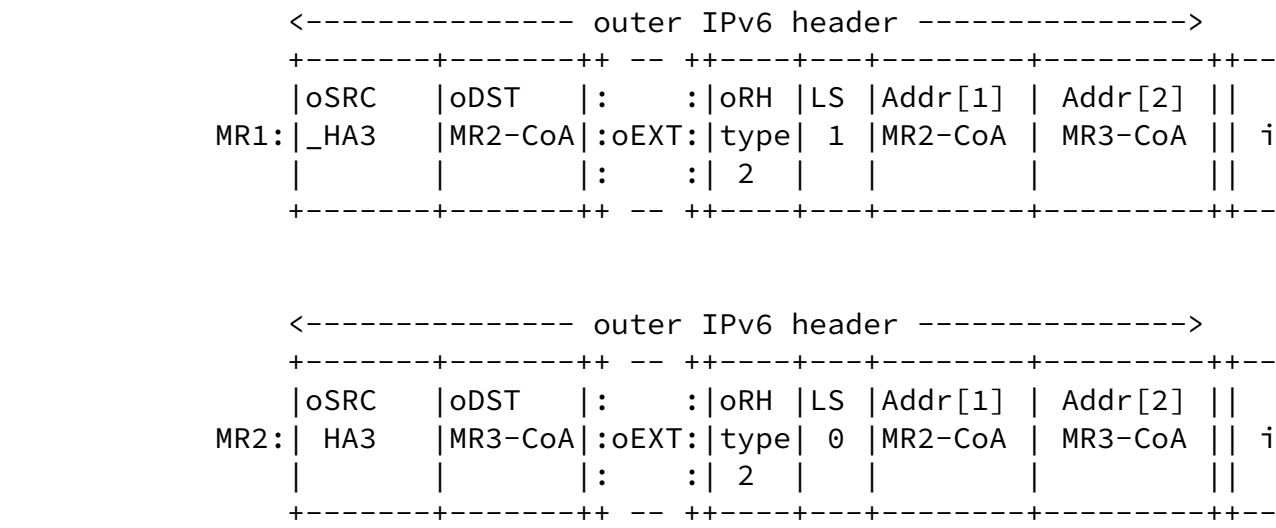
The packet sent from MR1 through the RO-enabled tunnel is d
to HA3. HA3 detects the existence of Type 6 RH optional hea
searches a BC entry with NPI that has TLMR on the nested pa
is exactly matched with the source address of the packet. I
entry is valid and the correspondent RO-enabled tunnel inte
exists, the packet is forwarded to the interface so that it
properly decapsulated. As a result of the MR3-HA3 tunneling
inner packet properly routed to the original destination by

3.2 Forward Packet Delivery(HA3 -> MR3)

The packet destined to the LFN in MONET3 is intercepted by
delivered by the procedure as follows. HA3 gets know that M
tunnel is RO-enabled. Therefore, the packet is forwarded to
with encapsulated as below via RO-enabled tunnel interface.



MR1 does routing with extended semantics for the packets th
RH Type 2 optional header as in [4]. The packets with RH Ty
header sent from HA3 properly delivered to MR3 by MR1 and M
the nested path as follows:



The packets with LS=0 are no more routed in MR3, therefore processed by MR3 as if sent from nested forward tunneling b MR3 and HA3. In the end, the packets decapsulated, and forw LFN.

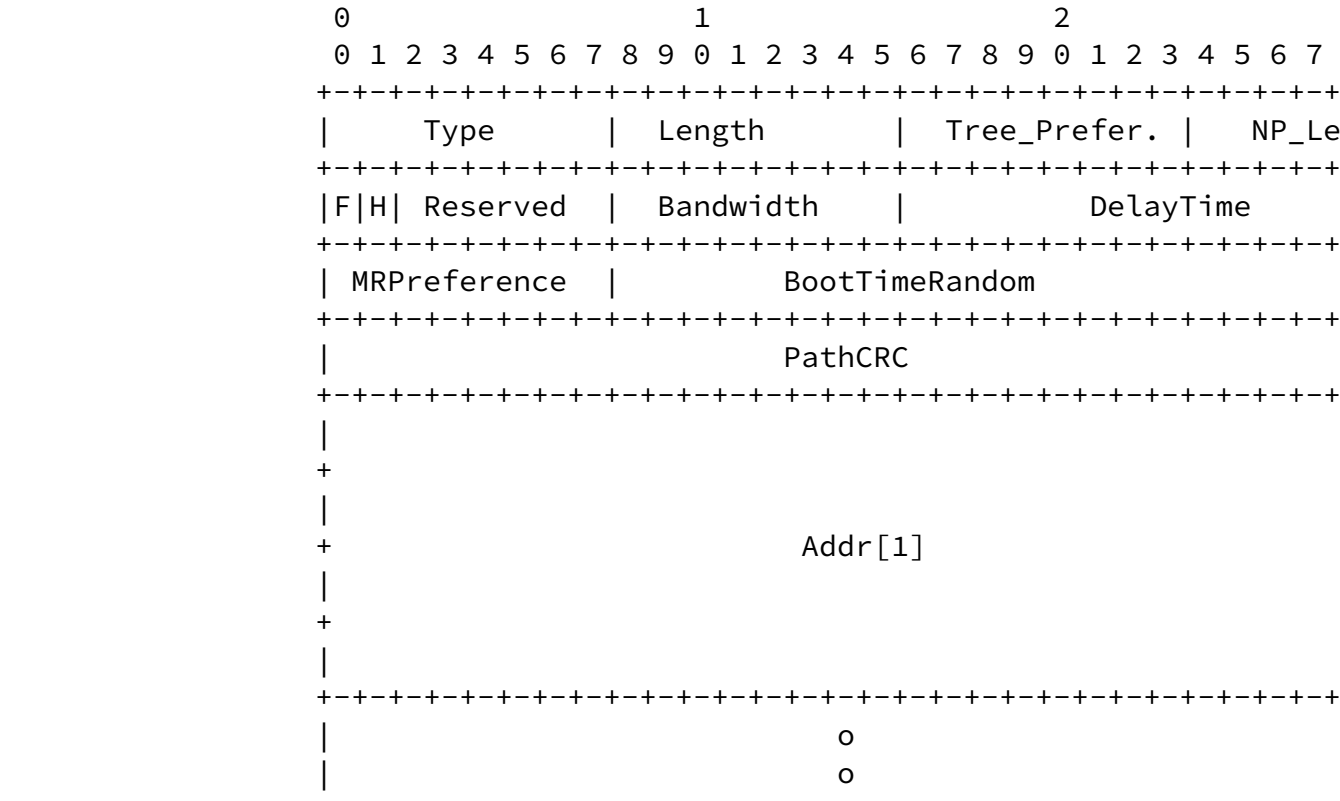
4. Extensions

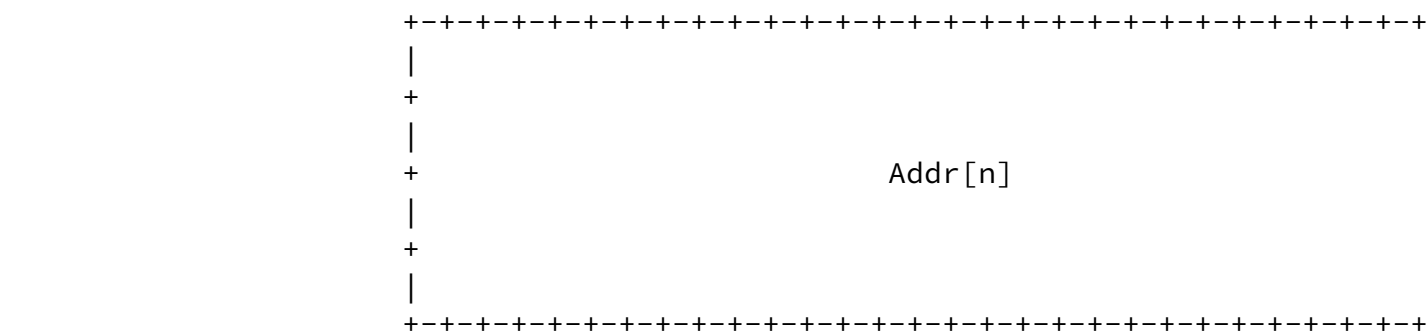
The proposed solution requires some extensions for existing
and IPv6 protocols.

4.1 Neighbor Discovery Extensions

4.1.1 Nested Path Option(NP Option)

Basically, we use the same RA format used in [4] section 6.
also, the format of additional NP Option inherits most of f
Tree Information Option used in [4] section 6.2 because of
similarity of usage. The format of NP Option is as follows:





This format represents the following changes over the ori
specified for Tree Information Option in [4]:

Type

8-bit unsigned integer set to the assigned value by
TBD.

Length

8-bit unsigned integer updated by each MR on the nes
The length of the option (including the type and len
fields) in units of 8 octets.

NP_Length

4.1.2 8-bit unsigned integer set to 1 by the TLMR. That ind
the size of Addr[] array.

Addr[1]

TLMR's IPv6 global address, set by the TLMR. Identi
the tree.

Addr[n]

IPv6 global address of n-th MRs on the way, set by n

The TLMR MUST include this option in its Router Advert

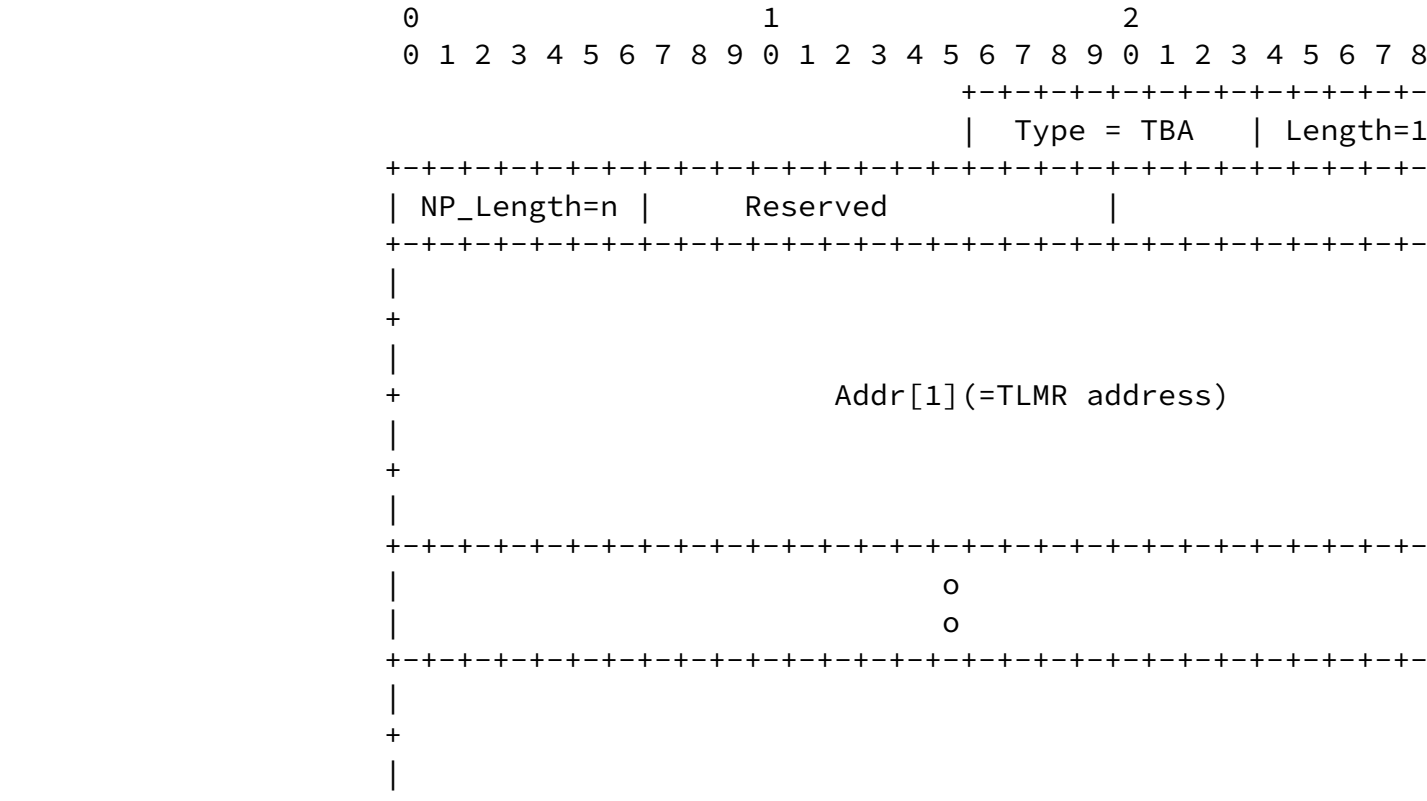
A MR receiving this option from its Attachment Router MUST
the Length, TreeDepth, MRPreference, BootTimeRandom and Pat

fields,and addtionally MUST append its IPv6 global address
Addr[n] slot if it is n-th MR on the path, and MUST propaga
its ingress interface(s). The alignment requirement of the
Option is 8n.

4.2 MIPv6 Extensions

4.2.1 Nested Routing Path Option(NRP Option)

MR adds new mobility option, NRP Option in BU message to se
RO-enabled tunnel with its HA. The format of this option is
follows:



```
+                            Addr[n]
|
+
|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Type

8-bit identifier of the Mobility Header option type. value that identifies an Access Router Option is yet assigned.

Length

8-bit unsigned integer that specifies the length of mobility option in octets, excluding Type and Lengt

NP_Length

8-bit unsigned integer that indicates the number of slots.

Addr[1..n]

Vector of IPv6 global addresses of MRs on the nested numbered 1 to n.

NRP Option is only valid in a Binding Update message. The p of this option is to inform HA that it can do optimize the tunnels overhead. Using this information, HA can route pack the sender via the MRs on the nested path by extended Type optional header.

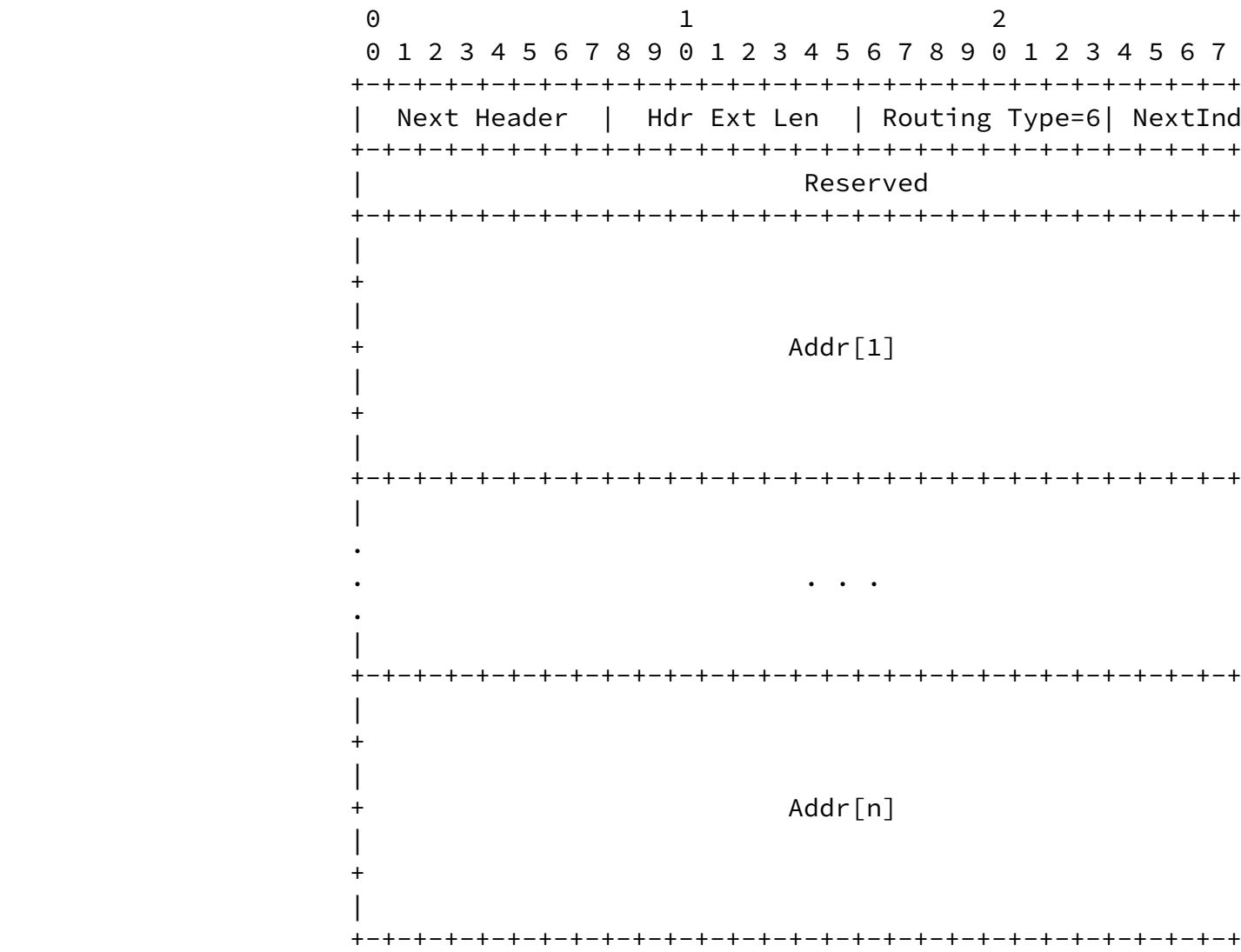
4.2.2 Extended Type 2 Routing Header(RH)

The format and semantics of Type 2 Routing Header is perfec with one defined in [4] section 4.1.

4.2.3 Type 6 Routing Header

Type 6 Routing Header is newly defined to enable the NPI-aw

routing by MRs on the nested path. the format of this heade
follows:



Next Header

8-bit selector. Identifies the type of header immed
following the Routing Header. Uses the same value a
IPv6 Next Header field [10].

Hdr Ext Len

8-bit unsigned integer. Length of the routing heade

octet units, not including the first 8 octets. This is always equal to twice the number of addresses in Address vector.

Routing Type

8-bit unsigned integer that contains the value 6. Th type value unconfirmed by IANA. TBD.

NextIndex

8-bit unsigned integer. This value identifies the i address vector. The forwarder needs to make sure th indexed address is same with its address. If yes, it the source address of the packet to its address and the packet. By hop-by-hop, the mobile router that understands this type of routing header MUST decreme NextIndex by 1 at forwarding. If NextIndex is 0, ign option.

Address[1..n]

Vector of 128-bit addresses, numbered 1 to n.

4.3 MR Extension

According to MIPv6 Spec.[1], MR MUST maintain Binding Updat List(BU List). In managing BU List, the following informati be maintained additionally to use RO-enabled MR-HA tunnel d in this proposed solution.

Nested Tunnels Optimization(NTO) flag :

When set indicates that the associated BU entry is R enabled for nested tunnels optimization.

Nested Path Information(NPI) Address Vector :

The path vector information transferred in Nested Ro Path Option at BU.

The successful BU with NRP Option allows the ready of RO-en
tunnel interface that would be associated with the correspo
entry of BU List. That tunnel interface is set up to add Ty
optional header at the encapsulation of tunneled packets. A
enabled BU, all packets through RO-enabled reverse tunnel h
6 RH optional header in tunnel extension header so that the
properly delivered to HA through the optimized nested path.

For packets sent from HA through Type 2 RH, MR decapsulates
outer packet, and forwards the inner packet to the ingress
There is no difference with normal packets routed via neste
because source address is HA and destination address is MR.

4.4 HA Extension

According to MIPv6 Spec.[1], HA MUST maintain Binding Cache
Like MR extension, HA MUST maintain additionally the follow
information in associated BC entry in case of receiving BU
Option.

Nested Tunnels Optimization(NTO) flag :

When set indicates that
enabled for nested tunnels optimization.

Nested Path Information(NPI) Address Vector :

The path vector information carried in Nested Routin
Option during BU.

With the success of BU, HA has to add new entry in tunnel i
table. At that time, the tunnel interface is being marked w
enabled so that Extended Type 2 RH[4] inserted into Tunnel
Extension Header[16] at processing packet tunneling encapsu
As a result of applying Type 2 RH based on NPI, all packets
destined to mobile networks are forwarded to TLMR on the ne
path through the RO-enabled forward tunnel.

For the packets forwarded via RO-enabled reverse tunnel by
decapsulates them, and checks the validity of Type 6 RH. th
conditions are as follows:

(1) NextIndex MUST be zero.

(2) There is at least one entry registered by BU wit
which TLMR address matches the source address of inc
outer packet.

(3) CareOf address of the BC entry MUST match the la
address(e.g. MR3) which is the result of subtracting
NPI address vector(e.g. MR1->MR2->MR3) to the addres
Type 6 RH(e.g. MR1->MR2) in order.

If above conditions are all satisfied, inner packets are fo
by MIPv6 specification. Otherwise, they are discarded by HA

5. Further Route Optimization

5.1 MN-HA Tunnel Optimization in Mobile Networks

In Fig.1, VMN can do RO-enabled binding update with MR4_HA nested path MR1_CoA->MR4_CoA. VMN-VMN_HA tunnel can be opti VMN follows faithfully extension of the operation like MR d section 4.4.

5.2 MN-CN Route Optimization in Mobile Networks

MIPv6 Route Optimization can be considered in nested mobile networks. To apply our solution, the following extensions a required to MN and CN.

(1) MN and CN MUST use the nested routing path optio doing BU.
(2) RH Type 6 optional header MUST be applied to the sent from MN to CN.
(3) Extended RH Type 2 optional header MUST be appli the packets sent from CN to MN.

We see the possibility and detailed protocol design of MN-C optimization using NPI will be next our work item.

6. Security Considerations

Basically, MR-HA bi-directional tunneling is protected by IPSEC[7][8][9]. However, we can suspect that the part of NP untrustworthy by itself or can be modified by the intermedi that be fake. In case of [4], the vulnerability for spoofin by an attacker on the nested path has been known. Those kin attack can be avoided in the proposed solution as the integ NPI is guaranteed on the fly.

6.1 NPI Authenticity

We need to assure that NPI is an available path and intact. the assurance, there MUST be any security mechanism to auth AR on access link by MR each other. That would be implement some types of Network Access Control(NAC) or domain-specifi authentication method. Due to out of scope of this document details for those mechanisms will not be described in here, solution needs to assume pre-established security associati between visited AR and visiting MR for NPI authenticity.

6.2 How to avoid the spoofing attack

The integrity of information chunks of RH Type 6/2 used in solution can be guaranteed by using AH[8]. It means that th intermediate forwarders on the nested path for RH Type 6/2 modify any part of NPI. Unlike RRH, NPI is immutable except NextIndex so that it can be protected by AH. Any attacker t doesn't know secret key used in MR-HA tunnel cannot forge N protected by AH for its own benefit.

6.3 The existence of fake MR

There may be a fake MR acting as a forwarder on NPI path. Inadvertently or not, it's possible because of the lack of access security mentioned in section 6.1. Although in this NPI in RH Type 6/2 cannot be modified because of AH protect Any contents through MR-HA tunnel cannot be disclosed becau can be protected by ESP[9]. Merely, the possible attack is passive denial-of-service that means the denial of routing However, as these types of attacks can be easily detected, cannot be an effective attack in itself.

References

[1] Perkins, C., Johnson, D. and J. Arkko, "Mobility Supp IPv6", draft-ietf-mobileip-ipv6-18 (work in progress) 2002.

[2] Ernst, T. and H. Lach, "Network Mobility Support Term draft-ietf-nemo-terminology-00 (work in progress), Ma

[3] Ernst, T., Castelluccia, C., Bellier, L., Lach, H. an Olivereau, "Mobile Networks Support in Mobile IPv6 (P Scope Binding Updates)", draft-ernst-mobileip-v6-netw (work in progress), March 2002.

[4] Thubert, P., and Molteni, M., "IPv6 Reverse Routing H and Its Application to Mobile Networks", Internet Dra draft-thubert-nemo-reverse-routing-header-01 (work in progress), Oct 2002.

[5] Chan-Wah Ng, and Takeshi Tanaka, "Securing Nested Tun Optimization with Access Router Option", Internet Dra -ng-nemo-access-router-option-00(work in progress), O

[7] Kent, S. and R. Atkinson, "Security Architecture for

Internet Protocol", RFC 2401, November 1998.

[8] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[9] Kent, S. and R. Atkinson, "IP Encapsulating Security (ESP)", RFC 2406, November 1998.

[10] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1

[11] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Di for IP Version 6 (IPv6)", RFC 2461, December 1998.

[12] Conta, A. and S. Deering, "Internet Control Message P (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.

[13] Reynolds, J., "Assigned Numbers: RFC 1700 is Replaced an On-line Database", RFC 3232, January 2002.

[14] Thubert, P., and Molteni, M., "Taxonomy of Route Opti Models in the NEMO Context", Internet Draft: draft-th nemo-ro-taxonomy-00(work in progress), Oct 2002.

[15] vijay, D., Ryuji, W., Alexandru, P., Pascal, T., "NEM Support Protocol", draft-ietf-nemo-basic-support-00(w process), June 2003.

[16] A. Conta, S. Deering, "Generic Packet Tunneling in IP Specificiation", RFC2473, December 1998.

Acknowledgments

Authors would like to thank you the authors of [4] and [5] fruitful comments on this problem area.

Authors' Addresses

Jongkeun Na
Information Networking & Computing Lab.
School of Computer Science and Engineering,
Seoul National University, Seoul Korea
EMail: jkna@popeye.snu.ac.kr

Sungho Cho
Information Networking & Computing Lab.
School of Computer Science and Engineering,
Seoul National University, Seoul Korea
EMail: shcho@popeye.snu.ac.kr

Chongkwon Kim
Information Networking & Computing Lab.
School of Computer Science and Engineering,
Seoul National University, Seoul Korea
EMail: ckim@popeye.snu.ac.kr

Sungjin Lee
Telecommunication R&D Center,
Samsung Electronics
Dong Suwon P.O. BOX 105
416, Maetan-3Dong, Paldal-Gu
Suwon-City, Gyunggi-Do, 442-600
KOREA
EMail : steve.lee@samsung.com

Hyungjeong Kang
Telecommunication R&D Center,
Samsung Electronics
Dong Suwon P.O. BOX 105
416, Maetan-3Dong, Paldal-Gu
Suwon-City, Gyunggi-Do, 442-600
KOREA
EMail : hyunjeong.kang@samsung.com

Changhoi Koo
Telecommunication R&D Center,

Samsung Electronics
Dong Suwon P.O. BOX 105
416, Maetan-3Dong, Paldal-Gu
Suwon-City, Gyunggi-Do, 442-600
KOREA
EMail : chkoo@samsung.com