Mobile IPv6 – Base Status & Open Issues

Jari Arkko, Charlie Perkins

Mobile IP WG meeting

IETF 55

Status

- Draft-ietf-mobileip-ipv6-19.txt
- Progress:
  - Has gone through WG last call
  - Issues raised during (and after) WG last call
  - All issues resolved
  - Additional draft created and referenced for HA-MN IPsec details
  - Reviewed by ADs; IETF last call not to be initiated yet
  - AD comments have been posted to the list
  - Two closed issues discussed after posting draft 19
- Plan:
  - Resolve AD comments, publish new version, go to IETF last call

Statistics

- Issue filing / solving process used

  http://www.piuha.net/~jarkko/publications/mipv6/MIPv6-Issues.html

- Statistics for issues filed after start of WG last call on July 2
  - 102 issues filed
  - 12 issues rejected
  - 90 adopted:
    - 6 issues classified as major
    - 30 issues classified as medium
    - 30 issues classified as minor
    - 24 issues classified as editorial

Main Modifications

- 53 - No longer require HAO for all IPv6 nodes
- 72 - Forwarding from previous CoA moved out of base
- 69 - rules on how to use IPsec MN-HA have been provided
- 117 - Home RR token (cookie) is now sufficient for de-reg
- 123 - Prefix security has been included as a SHOULD
- 144 - Unsolicited MPAs are acked by MPSes.

Currently Discussed Issues (1/2)

- 150 - De-registration failure when returning home
- 146 - Preshared Kbm as an optional scheme in addition to RR
- 155 - Editorial comments (AD)
- 154 - ND constant tuning (AD)
- 156 - Conflicts with ND specifications e.g. on DAD (AD)
- 157 - Address collision action (AD)
- 158 - When to start RO (AD)
- 159 - 'D' bit semantics (AD)
- 160 - HA discovery single address woes (AD)
- 161 - MIPv6 and DHCP (AD)
- 162 - Site local issues (AD)
- 163 - Run MLD (AD)

Currently Discussed Issues (2/2)

- 164 - Sequence number update / authorization order
- 165 - HA address in DHAAD response always
- 166 - Allow DHAAD in home
- 167 - MLD source on foreign link
- 168 - L bit is not worth the trouble

159 – 'D' bit semantics (AD)

- Someone needs to keep track of when DAD needs to be run. Current draft puts this responsibility on the MN.
- The question is whether this is right, or if the HA could do this easier.
- Proposal: Remove 'D' bit and let home agent initiate DAD unless:
  - De-registration
  - Already defending the home address
- Agreement on list

163 - Run MLD (AD)

- How does the home agent know which multicast groups the mobile node has joined?
- Proposal: Run MLD
  - The home agent MUST be capable of receiving tunneled multicast group membership control information from the mobile node in order to determine which groups the mobile node has subscribed to.
  - (Does not mention MLD directly.)
- Agreement on list

156 - Conflicts with ND and DAD (AD)

- Current specification says DAD can be skipped or addresses can be optimistically taken to use while DAD is running
- Conflict with ND specifications. Also ongoing work in IPv6 to create optimistic DAD scheme.
- Proposal: Produce a complete, separate optimistic DAD specification.
- Agreement on list?

146 - Preshared Kbm (old)

- Proposed addition of preshared Kbm as an optional scheme in addition to RR for route optimization authorization
- Chairs requested that the feature be pulled out of the base specification
- Current status is that feature is to be located in a separate specification

158 - When to start RO (AD)

- Text suggests that mobile typically starts Return Routability immediately so that optimal routing can be achieved.
- Complaint: Mobile IPv6 does not have deployment experience to substantiate that this is needed. For some applications, it may not produce significant benefit.
- On the other hand, routing is typically not application controlled. RO produces at least some degree of improvement except when there is no traffic or just few packets.
- Proposal: Relax the current rules in the specification to say that RR/RO MAY be started. Leave it to implementers, future experience to determine exact right starting time.
- Note: RO is still a SHOULD in the specification, just that the exact time to start it is left as a MAY.

160 - HA discovery single address (AD)

- Current specification returns just one address of a single HA in DHAAD.
- Problem: this is not inline with the general IPv6 approach of allowing multiple addresses.
- Proposal: Let DHAAD return all addresses of each HA. Show which addresses belong to which HA.
- Need to work on the details.

150 - Failed de-reg when returning home

- An old problem: if de-registration fails, how is the BA routed to the node? HA is still defending the home address.
- Draft 19 solved this by requiring BAs in this case be sent to the link layer address the BU came from.
- Complaint on the list: shouldn't require tracking link layer addresses. We already require MN to respond to NS while it is waiting for BA.
- Solution: just require sending to the MN's link layer address, either tracked through the stack or queried from the MN in the usual manner.
- Agreement on list?

157 - Address collision action (AD)

- Collisions could happen due to real IID problems or DoS attacks
- RFC 2462 says disable interface & wait for reconfiguration
- We agree that this is too drastic in many cases. The question is where to document proper actions? Issues with including it in the current spec:
  - Does not appear just with MIPv6, also a general problem
  - Defense against attacks is only partial until SEND has a solution
  - Perhaps the real collision case is too infrequent to warrant immediate standard?
  - OTOH, MIPv6 could have an immediate (even if temporary) cure for this
  - Temporary cure avoids permanently disabled interface
- Proposal: Let Secure ND WG deal with the attack problem, and IPv6 deal with an update to the too drastic action in 2462
- Counter proposal: Just keep the simple protection now in Mipv6.
- No agreement on list yet

154 - ND constant tuning (AD)

- Mobile IPv6 specification lowers certain IPv6 ND constants in order to make it possible to have a higher frequency and smaller delays for RAs.
- This is an IP-layer solution to high performance movements:
  - Detection of movement
  - Getting the parameters for the new network
- Can we make a separate specification for this, and leave the constant modifications out from Mobile IPv6 base specification?
- Alternative ways ahead:
  1. Specify new constant values in Mipv6 spec. End of story.
  2. Specify new constant values in Mipv6 spec, but start also an activity to come up with a separate constant adjustment document (either in MIP or IPv6 WGs).
  3. Remove constant modifications from Mipv6 specification, and start an activity to come up with a separate constant adjustment document.

154 (Continued)

- The constants in draft 19 might delay Mipv6 specification.
- Need to agree with the ADs that the constants belong here.
- The creation of a separate document will take time.
- Some implementers want solutions now for their products.
- Lower layer indications more efficient than beacons.
- Not all link layers and driver firmware support indications.
- Lower layer does not help the effect of the RA rate limitation.
- The constant modifications are really needed for all routers.
- A separate specification easier updated with new optimizations
- Existing concerns easier to incorporate if not in Mipv6 base.

161 – MIPv6 and DHCP (AD)

162 - Site local issues (AD)

155 – Editorial comments (AD)

- Mostly, just adopted – but:
  - Should there be ranges of types (< 128 vs. >= 128)?
  - Should upper layer protocols know about Home Address Option?
  - What does mobile do if it gets a sequence number error from CN?
  - Should CN send some kind of error message instead of ever silently dropping Binding Updates?
  - Renumbering vs. behavior when 'S' == 0?
    - Proposal: special error code from Home Agent when prefix lifetime < 120 minutes.
  - How does a home agent know which prefixes make its global IP addresses admissible for the Home Agent Reply message?
  - When does a home agent allow incoming advertisements to override existing information contained in PrefAdvList?
  - Why would MN delete a binding cache entry in response to Binding Request? (proposal – it shouldn't except maybe for privacy reasons?)
  - Constants in alphabetical order?
  - Retransmission philosophy?
  - Values for constants?

168 - L bit is not worth the trouble

167 - MLD source on foreign link

166 - Allow DHAAD in home

165 - HA address in DHAAD response always

164 – Sequence number update / authorization order

MIPv6 – IPsec issues

Vijay Devarapalli and Jari Arkko

Mobile IP WG meeting

IETF 55

Status of Draft

- Draft-ietf-mobileip-mipv6-ha-ipsec-01.txt
  - Informational category
- Status
  - Gone through WG last call
  - A couple of open issues
  - A few comments from the IPsec mailing list (Cheryl Madson)

Resolved Issues

- Support for dynamic key establishment
  - SHOULD/MAY?
  - MAY in the draft. Manual key establishment a MUST
- MIPv6 - VPN interactions
  - Postponed to a later date.
  - Depends a lot on where the VPN gateway and HA are located. If VPN gateway and HA are co-located, it is very easy. Otherwise, needs some more work.....
- When to update end point (CoA) of tunnel in the SADB?
  - At MN, as soon as it acquires a new primary CoA
  - At HA, as soon as it successfully processes the BU for the new CoA

Resolved Issues (contd.)

- IKE is run using CoA but still negotiate SA for home address
  - (Jari, more here?)

- MN returning home
  - CoA<->HA tunnel torn down
  - SPD entries for tunneled traffic become inactive
  - SAD entries based on tunnel interface. Can be stored and used later if created manually
  - BU/BA security association pair SHOULD NOT be deleted

Tunneled Packet Format

- Non-Optimal Format

IPv6 Hdr (src = CoA, dst = HA)

Dst Opts Hdr

HAO

ESP hdr

IPv6 Hdr (src = HoA, dst = CN)

Mobility Hdr

HoTi

- Optimal Format

IPv6 Hdr (src = CoA, dst = HA)

ESP hdr

IPv6 Hdr (src = HoA, dst = CN)

Mobility Hdr

HoTi

- Pros of Optimal Format
  - Avoids an overhead of 24 bytes for HAO/Rt Hdr
  - MIPv6 tunnels treated as IPsec tunnels
  - CoA – HoA mapping checked when IPsec check done
  - Manages only one tunnel CoA<->HA

Tunneling Packet Format (contd.)

- Cons of Optimal format
  - Per-Interface IPsec support need. RFC 2401 says IPsec is always per inteface. Nothing new
  - An API to the SA databse needed to update the tunnel gateway address whenever the MN changes its CoA
- Cons of non-optimal format
  - Need to manage two tunnels. CoA<->HA and degenerate HoA<->HA
- SA_Update
  - SADB in the kernel. MIPv6 in the kernel too
  - Update could also be delete/add SA, if API not available. New SA has the same fields as the old SA except for one of the tunnel gateway addresses.
  - When to do it?
    - At MN, as soon as it acquires a new primary CoA
    - At HA, as soon as it successfully processes the BU for the new CoA.

Auth-in-App approach

- Authorization is done in the App, while authentication is done by IPsec
- IPsec needs to inform MIPv6 module the SPI – HoA mapping everytime a new SA is created
  - setsockopt()?
- MIPv6 module checks to see if the SPI present in the Ipsec header is authorized to change a mobility binding
- Pros
  - A single SA pair for BU/BACK, Tunneled HoTi/HoT, MPS/MPA (traditional approach – 3)
- Cons
  - A new approach
  - Difficult handling tunneled HoTi and payload packets
    - The authorization check done in forwarding module?
    - Cant be done in forwarding module, because outer header is lost when the packet reaches the forwarding module.

    (Jari, should we talk about possible attacks if authorization check not done?)
  - How does IPsec know that a newly created SA is for an app which does its own authorization?

IPsec WG comments

- Are MIP tunnels being replaced by IPsec tunnels?
  - (yes?)
- More details related to the change of tunnel end points needed
  - When?
  - What happens when end point changes during a re-key?
- Any requirements on IKE?
  - More info needed
- What is the granularity of a "user" relative to an MN?
  - Can a MN support more than one user?
  - If yes, do they get separate home addresses?
  - Do they share a home address?

  (we don't have an answer yet)

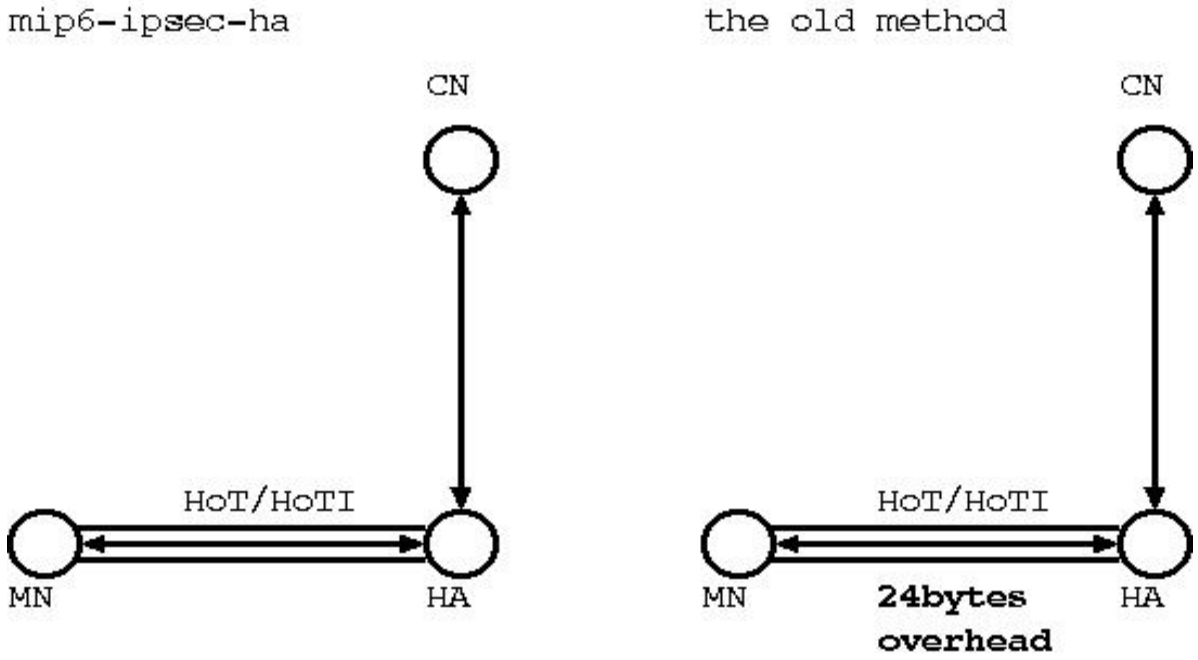
Comparison bewteen the optimized format and the non-optimized format

Header overhead

- There are three cases
  - HoT/HoTI case
  - non-IPseced traffic case
  - IPseced traffic case

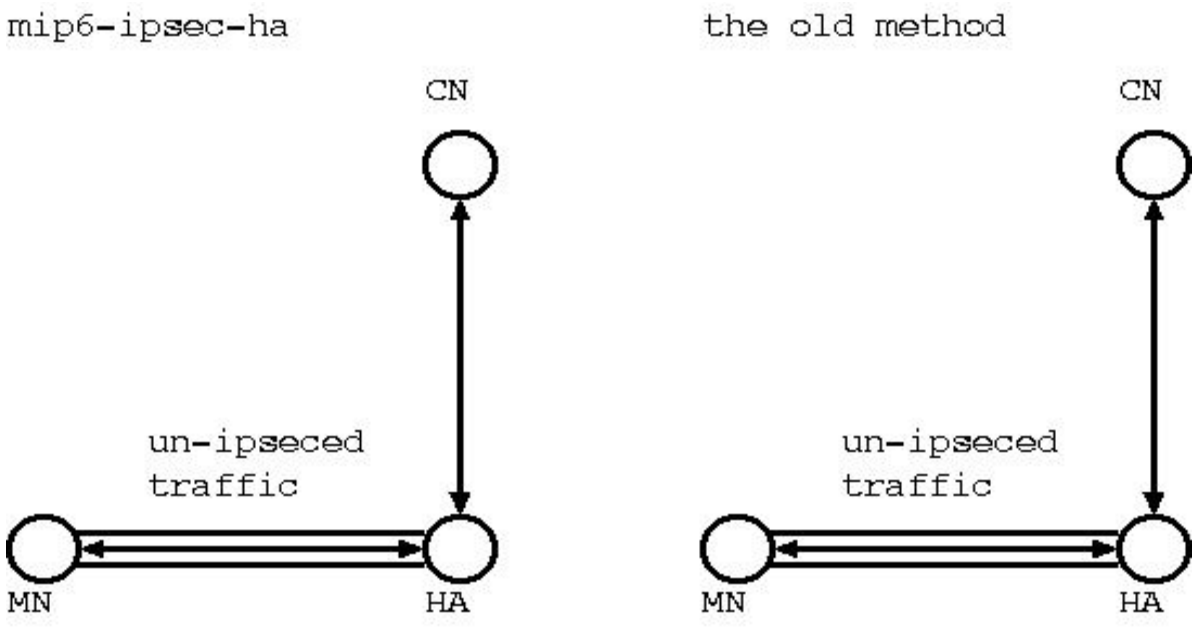
Detail for each case (1/3)

- HoT/HoTI case
  - Optimized ... no overhead
  - Non-optimized ... 24 bytes overhead



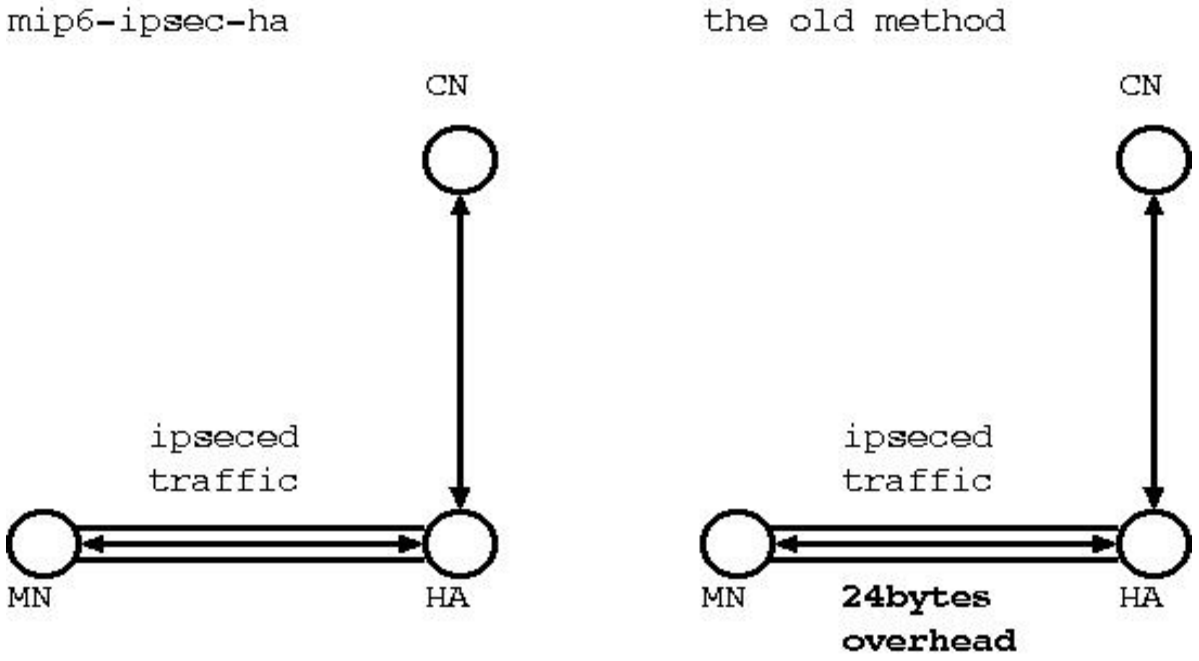
Detail for each case (2/3)

- Non-IPseced traffic case
  - Optimized ... no overhead
  - Non-optimized ... no overhead



Detail for each case (3/3)

- IPseced traffic case
  - Optimized ... no overhead
  - Non-optimized ... 24 bytes overhead

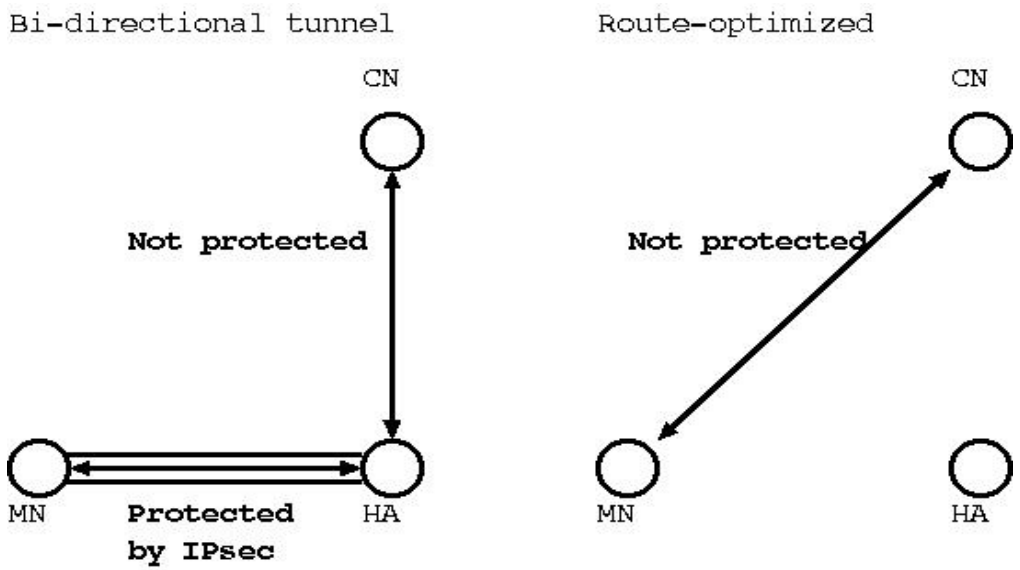


Header overhead conclusion

- The optimized fotmat has advantages in two cases
  - 1) HoT/HoTI case
  - 2) IPseced traffic case
- Case 1) is not significant because it produces relatively small amount of traffic
- How important 2) is? (see following slides)

Protecting MN-HA tunnel

- We can protect MN-HA tunnel, but ...
  - HA-CN path is not protected
  - In Route-optimized case, there is no protection at all



Observation(1/2)

- The optimized format has advantages in some cases
  - HoT/HoTI case
  - IPseced traffic case
- In non-IPseced traffic case, there is no difference between the two formats
- Even in IPseced traffic case, we can't protect
  - HA-CN path
  - the entire path when RO is used

Observation(2/2)

- In both cases, IPsec stack need not be modified
  - The optimized format needs to add some APIs to modify IPsec SAD (in some implementations, SPD also)
  - In non-optimized format, there are no need to add APIs