MIP6 Route Optimization Enhancements

⟨draft-arkko-mip6-ro-enhancements-00⟩

Jari Arkko, jari.arkko@ericsson.com

Christian Vogt, chvogt@tm.uka.de

IETF 61, Washington D.C.

Mobopts Meeting, November 10, 2004

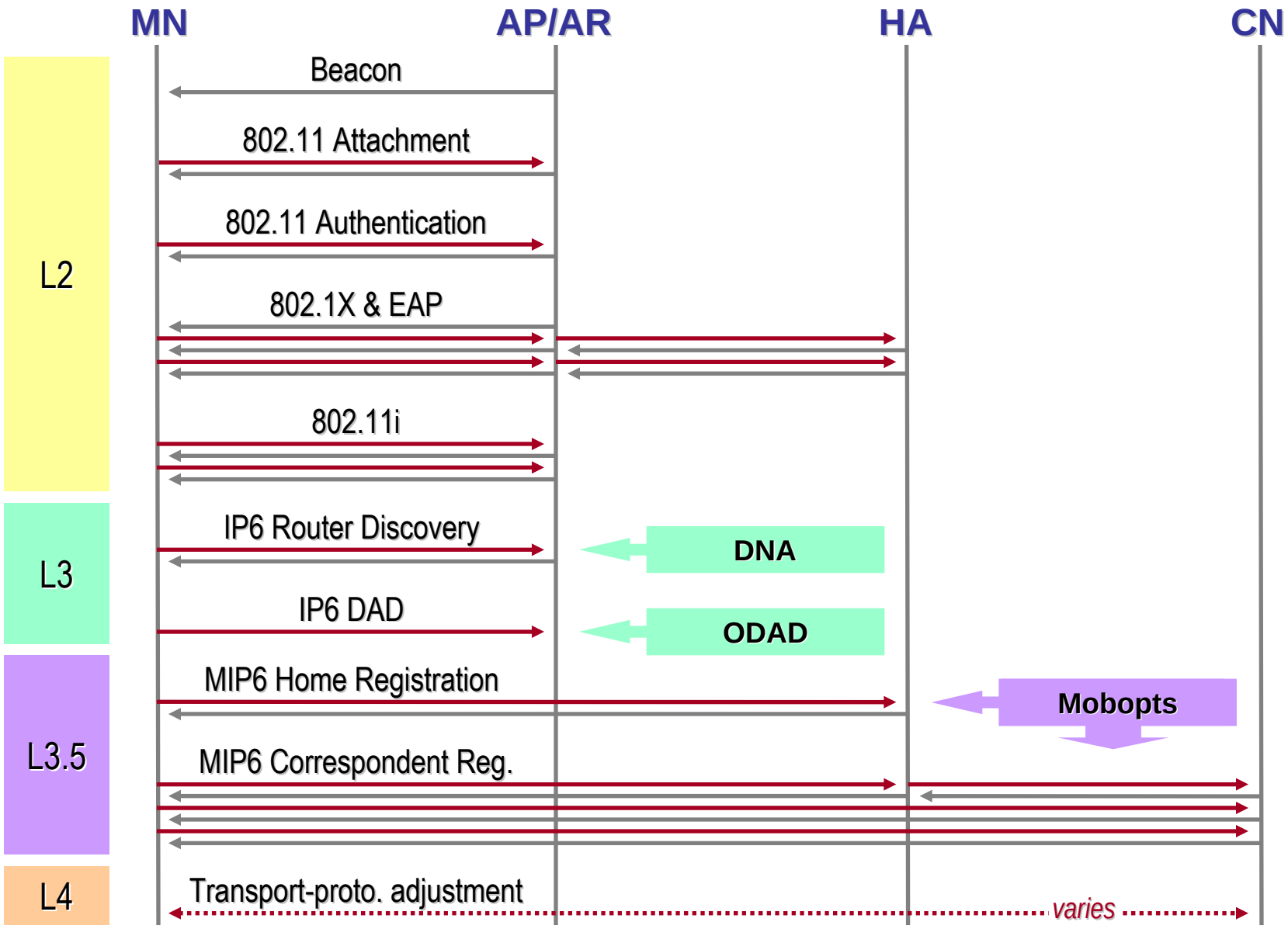
Outline

- Where we are
- Goals
- Toolbox
- Categorization
- Analysis
- Conclusion and future work

Where We Are

MIP6 as part of the entire stack

Where We Are: The Big Picture



Where We Are: MIP6 Route Optimization

Registration issues

- Prove MN's ownership of HoA (authentication)
- Verify MN's presence at new CoA (flooding-attack prevention)
- Register new CoA

No problem with home registration

- Security association ⇒ authentication ⇒ HoA ownership
- Trust relationship supersedes CoA test

But how about correspondent registration?

- No security association ⇒ How to authenticate unknown principals?

  (Certificates bind ID to public key, but ID typically ≠ HoA)
- No trust relationship ⇒ How to ensure presence at CoA?
- Solution adopted in MIP6: Return Routability

Where We Are: Return Routability

RR is a compromise…

- Efficiency
- Security

…under the pre-condition of universal applicability (low requirements, zero-configurability)

RR may not be optimal in all scenarios

- Real-time applications ⇒ reduce latency
- Confidential communications ⇒ increase security
- Resource constraints ⇒ relax signaling, processing overhead

Goals

Improving and enhancing MIP6 RO

Goals

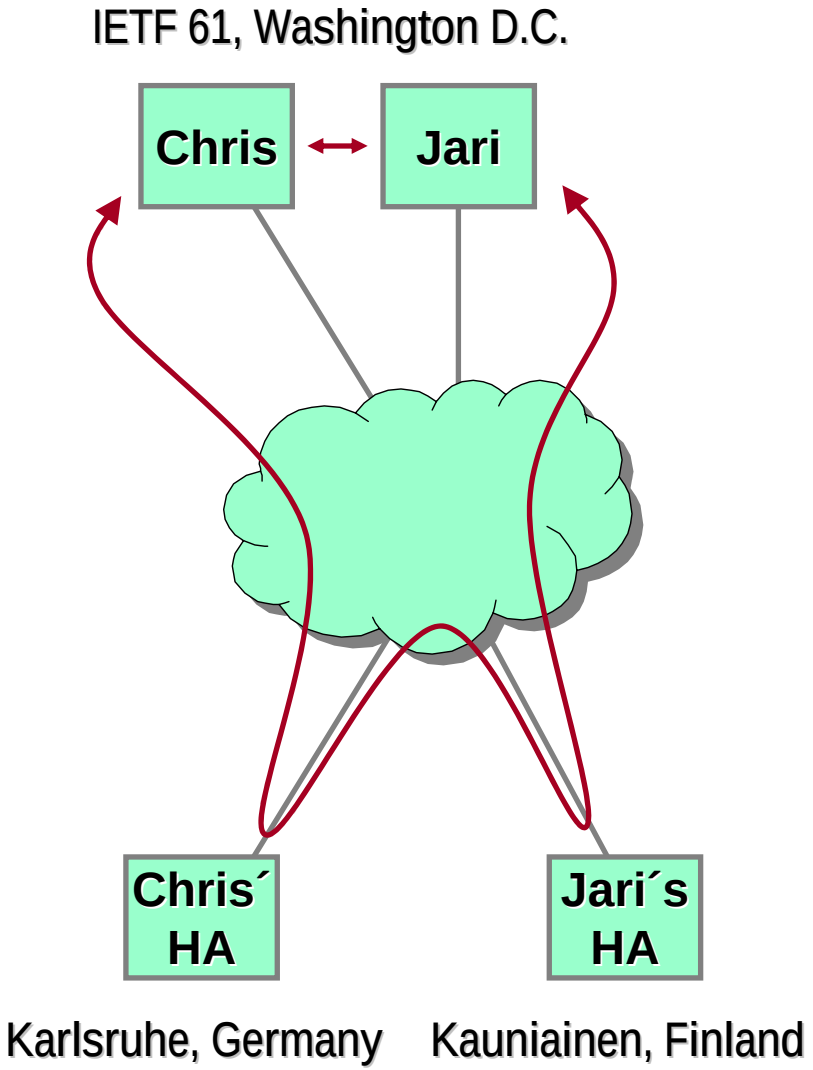
- Latency optimizations
- Security enhancements
- Signaling optimizations
- Applicability enhancements

Goals: Latency Optimizations

4 msg. exchanges

- Register w/ HA
- Prove HoA ownership
- Verify presence at new CoA
- Register w/ CN

2 end-to-end paths (longest governs delay)



Goals: Security Enhancements

RR narrows the windows of vulnerability to on-path, on-time attackers

- Off-path attacker cannot impersonate MN
- Off-path attackers cannot flood 3rd parties (through faked data-stream subscriptions)
- On-path attacker must be present constantly

RR raises security level of mobile Internet to that of today's Internet

But we may still want to have a stronger, cryptographic mechanism

Goals: Signaling Optimizations

3 out of 4 msg. exchanges pertain to correspondent registration…

- In HO case and periodically

  (Prevent time/space-shift attacks; limit attack to on-path, on-time)

- Overhead is not a problem for a communicating, moving MN…
- …but may be an issue for an idle, temporarily non-moving MN
- Overhead issue in core network providing HA functionality?

Goals: Applicability Enhancements

Since HoA and CoA are carried in each packet, pseudonymity, anonymity, and location privacy are not provided.

Reducing processing overhead at MNs by using cheaper authentication algorithms (Be careful of bidding-down attacks!) or delegation.

Toolbox

Strategies used in existing proposals

Toolbox: Latency Optimization

- Optimistic home registration

  (= Parallel home registration, correspondent reg. = Don't wait for HA's Ack)

- Optimistic correspondent reg.

  (= Parallel correspondent reg., data exchange = Don't wait for CN's Ack)

- Parallel HoA, CoA tests (send HoTI, CoTI simultaneously)
- Proactive HoA test (periodically, in anticipation)
- Proactive CoA test (requires 2 I/F)
- Diverting packets through HA (intermediate binding cancellation)

RFC-3775-conformant

- Anticipated registration (new CoA through external mechanism)
- Concurrent CoA test (Heuristics, Credit-Based Authorization)

Modifications

Toolbox: Security Enhancements

- Encrypted tunnel secures signaling close to the MN

  Links close to the MN are likely to involve wireless links

- Stateless HoA, CoA tests

  Make the CN resilient to resource-exhaustion attacks

- Cryptographically bound identifiers

  Bind MN's identity to public key (routable MIP6 HoA, CGA, or non-routable HIP HI)

- Pre-configuring shared keys

  MN and CN must know each other

Adopted in RFC 3775

Modifications

Toolbox: Signaling Optimization

- Local mobility management

  Spare global signaling (plus the associated latency)

- Gradual binding-lifetime extension

  Relax binding-refreshment interval for non-moving MNs

Toolbox: Applicability Enhancements

- Reducing processing through alternative cryptographic algorithms…

  E.g., use MD5 instead of SHA-1, ECC instead of RSA

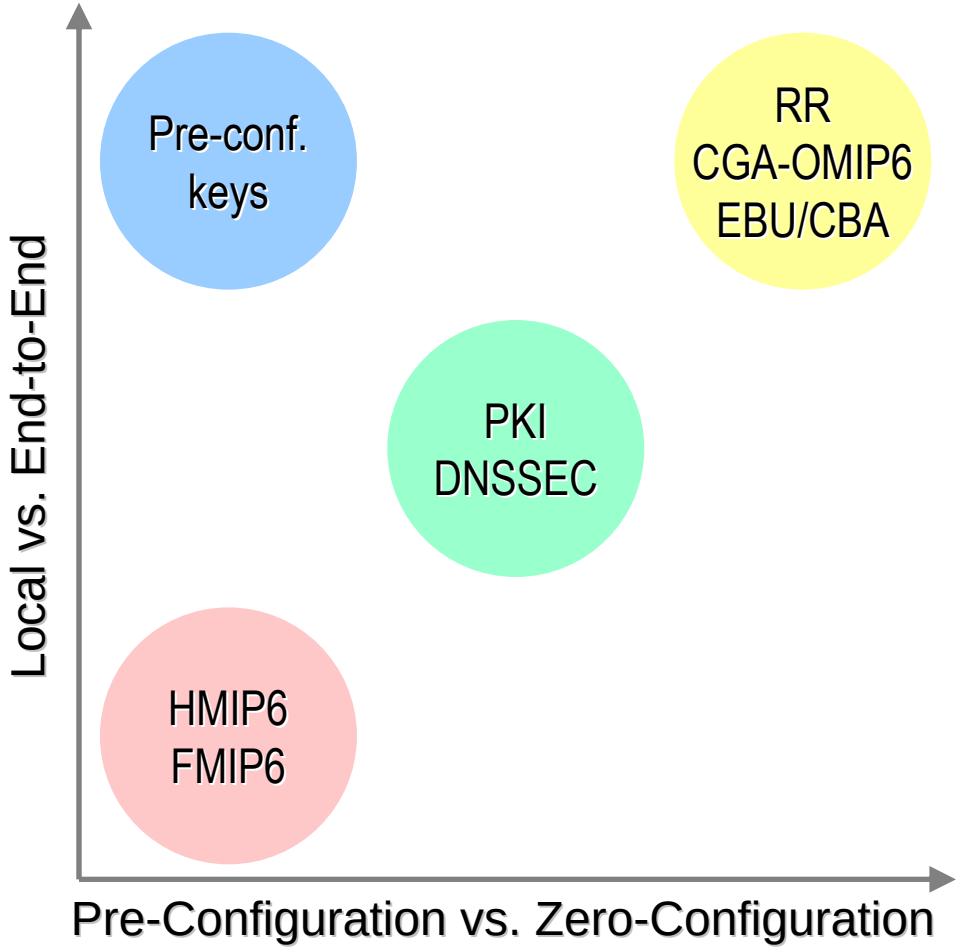
- …or through delegating authentication and vouching

  HA is less constrained than MN and may do expensive processing or signaling

Categorization and Analysis

Looking at existing proposals…

Categorization



- Local support eliminates global signaling…
- …but implies investments in the access network…
- …and does not support cross-domain handovers

- Pre-configuration eliminates signaling and latency, too…
- …but limits applicability

- End-to-end approaches are cost-effective…
- …and work w/ any access network…
- …but require longer RTTs

Analysis

- Reasonable relationship btw. efficiency, security gain and deployment cost
- Proposals usually use more than one strategy from the toolbox
- Community analysis is paramount for any new proposal

  E.g. early RR, CGA, EBU had no sufficient protection against 3rd-party flooding

  Early BUB, OMIP6 were subject to Kilroy-was-here-first attack
- Many of the existing proposals are mature

Conclusion and Future Work

Lots more remains to be done…

Conclusion and Future Work

- RR is the default; enhancements mainly for special usage scenarios

  (Fast movements, real-time applications, MNs in stand-by mode)

  ⇒ No single enhancement, but a variety

- Future work
  - Local enhancements w/o network support
  - CoA verifications using lower-layer assistance or SEND
  - Further enhancements that increase the cost for a particular attack to an unacceptable level (like CBA)
  - Combining mobility and multi-homing
  - Applying enhancements to other mobility protocols
- Experimental data (How usable are proposals as part of the complete stack?)
- Publication as RFC (Wider deployment can yield more insight as well)