On Efficient and Secure End-to-End Mobility Support

Christian Vogt, chvogt@tm.uka.de

Security Group, Institute of Telematics, University of Karlsruhe

January 19, 2005

Outline

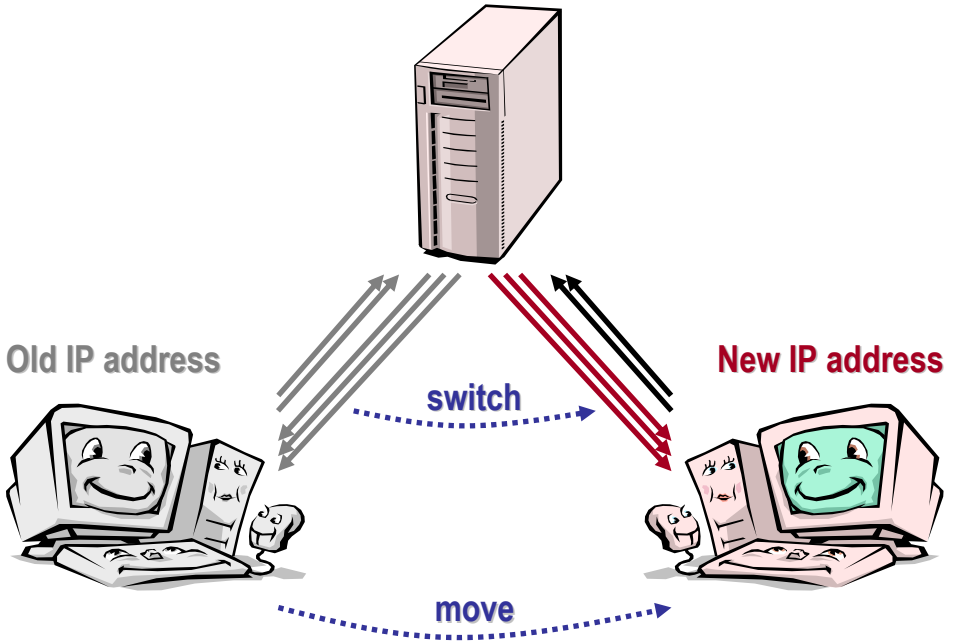
- **Mobility** scenario, **security** threats
- **Mobile IPv6**: How does it protect?
- **Latency**-oriented optimizations
  - Early Binding Updates
  - Credit-Based Authorization
  - Care-of Address Spot Checks
- Discussion, open **issues**, future work, testbed
- Summary

Mobility-Related Security Threats

What makes a mobile Internet different from today's?

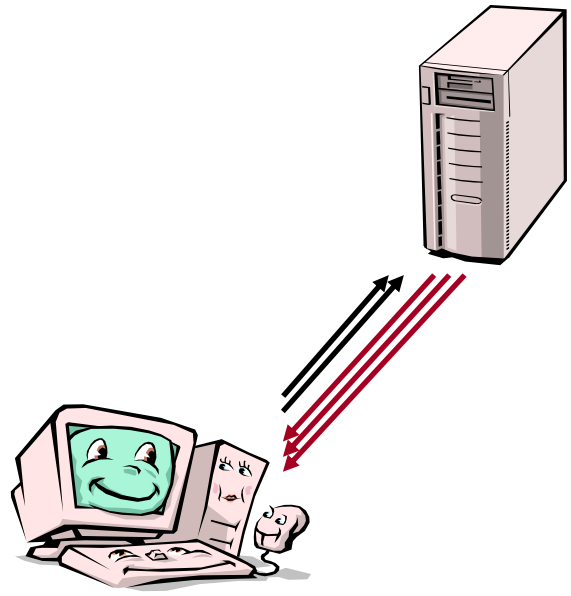
Mobility Scenario

- Mobile Node (MN) **moves** through IP sub-networks
- MN **configures** new IP addresses
- MN **registers** new IP addresses with Correspondent Node (CN)
- CN and MN **switch** to new IP address
- Mobility-management protocol **screens** IP-address changes from upper layers

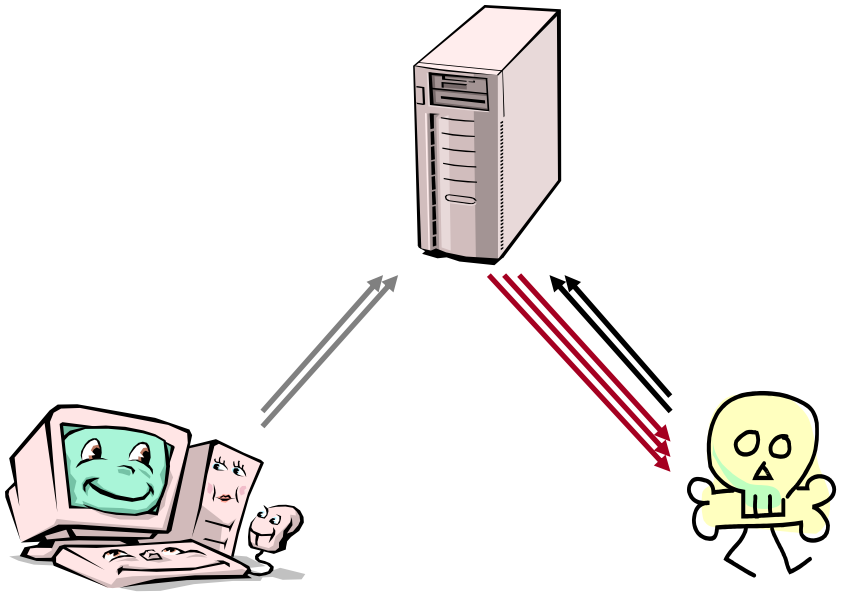


Impersonation

- If a MN can change its own IP address…
- …then an attacker might be able to **redirect** packets **on behalf** of a victim
- The attacker could be a **connection high-jacker**…



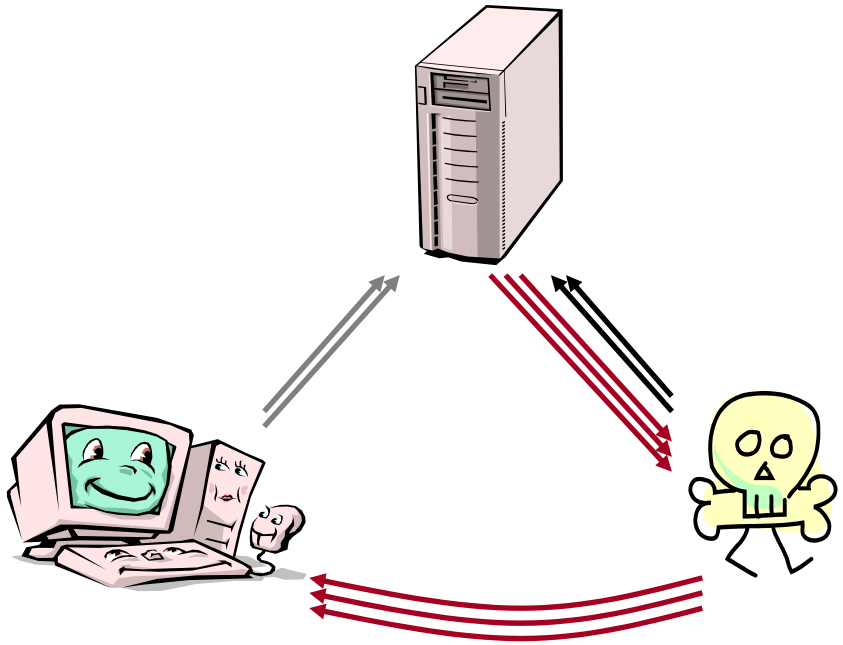
Before the attack…



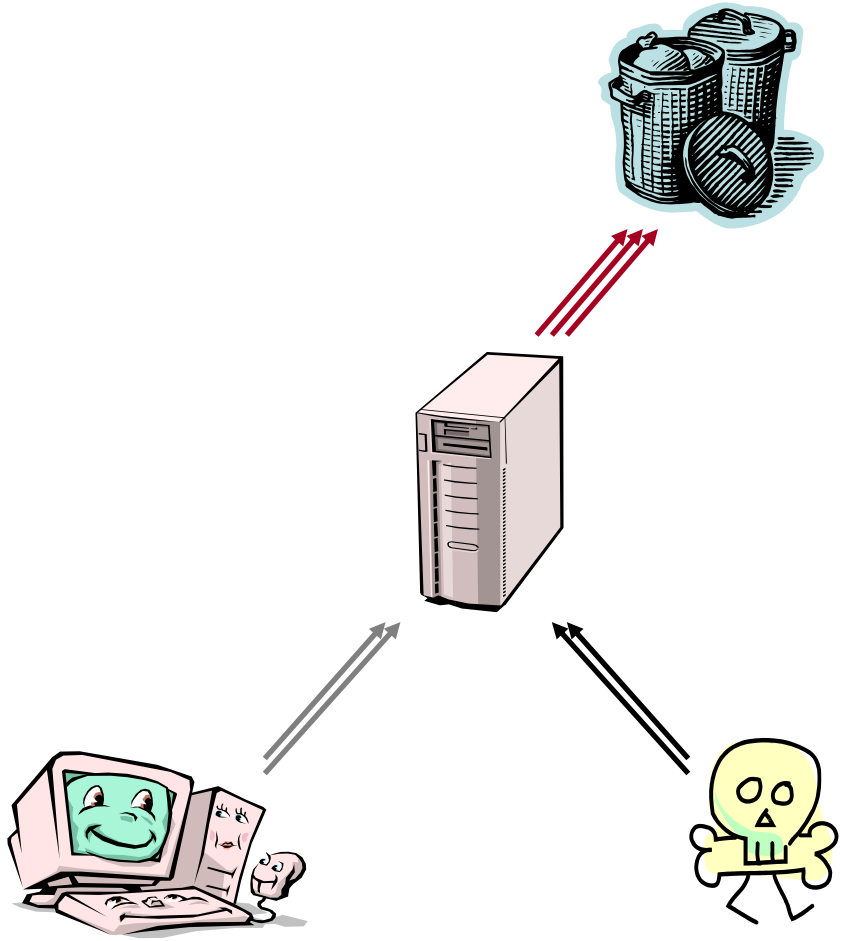
Connection high-jacking

Impersonation (2)

- …an **eavesdropper** or **MiTM**…
- …or it could simply cause havoc
- ⇒ **Authentication** before redirection



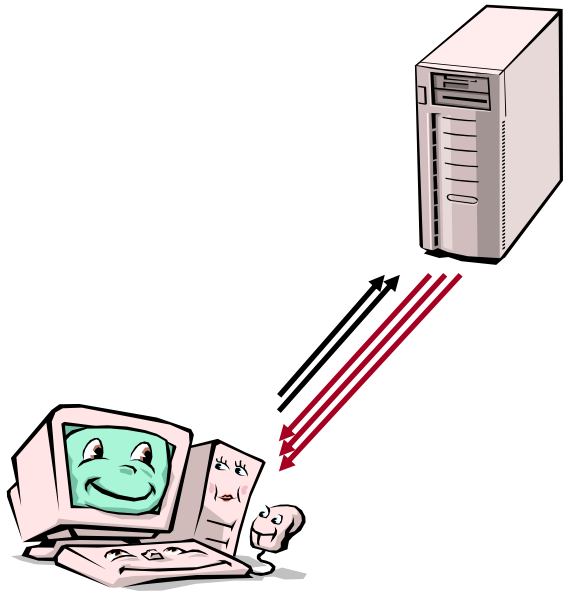
Eavesdropping or MiTM attack



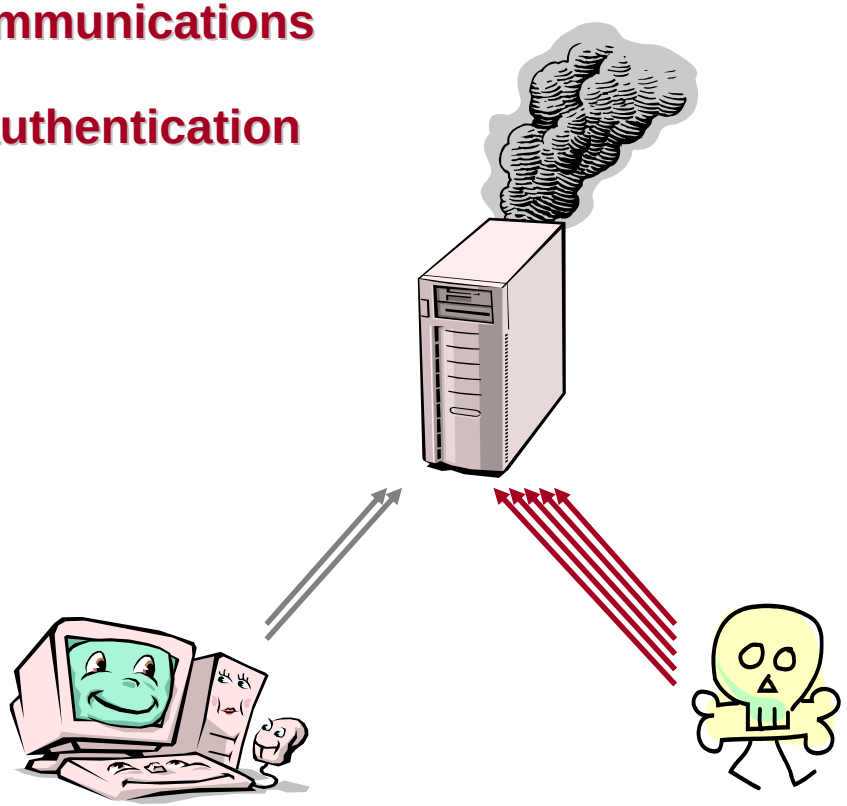
Dumping packets into random IP address

Resource Exhaustion

- If it takes the CN a lot of resources to process an IP-address registration…
- …then an attacker might massively **register spoofed IP-addresses**
- CN can **no** longer have **meaningful communications**
- ⇒ **Commit** resources only **after** MN's **authentication**



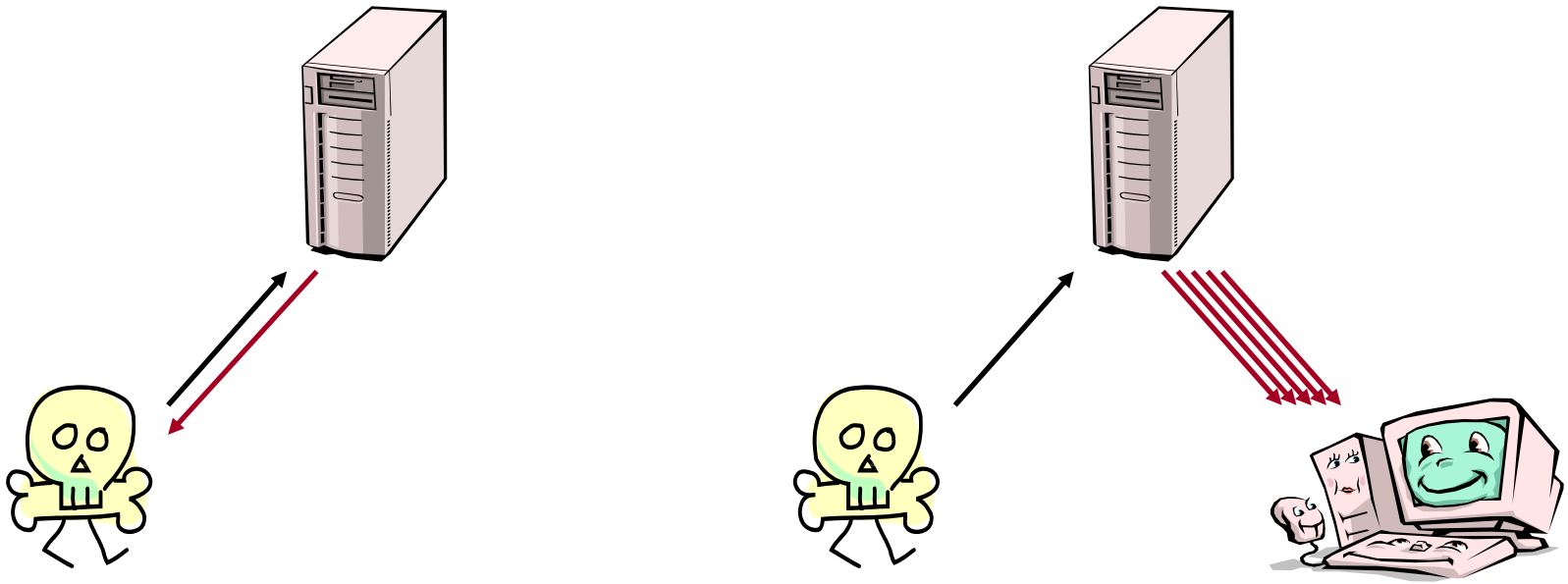
Before the attack…



Blocking meaningful communications

Flooding

- If a MN can redirect its packets to a new IP address…
- …then an attacker might **redirect** a high load of **traffic** to a victim
- Victim can be **any** IP **node**

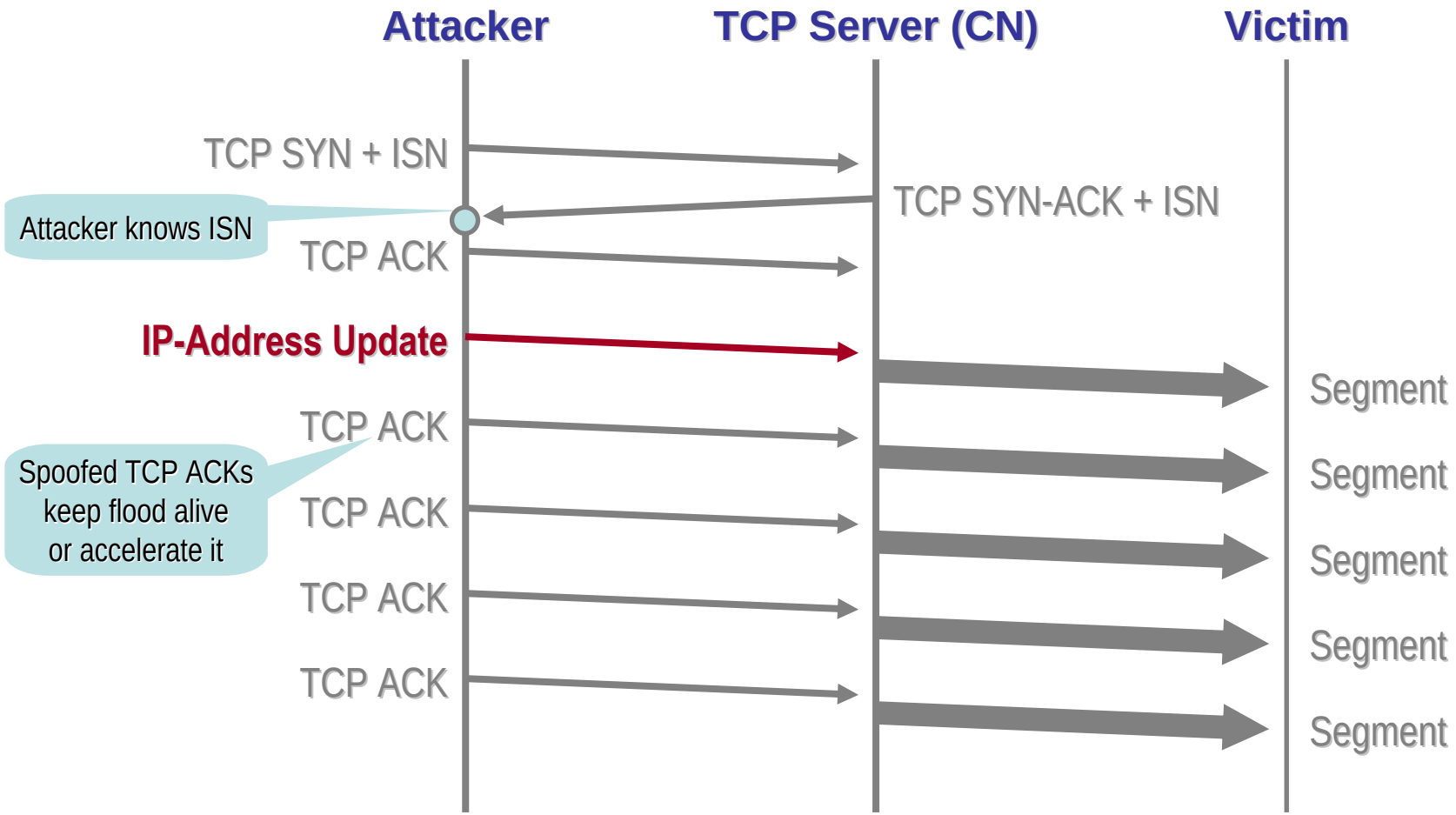


Initiating a download…

Redirecting the download

Flooded victim

Flooding (2)



- **IP-address ownership** is what matters here, not authentication
- ⇒ **Check** a new **IP address** before using it

Mobile IPv6

How does it solve the problems?

MN uses two IP addresses

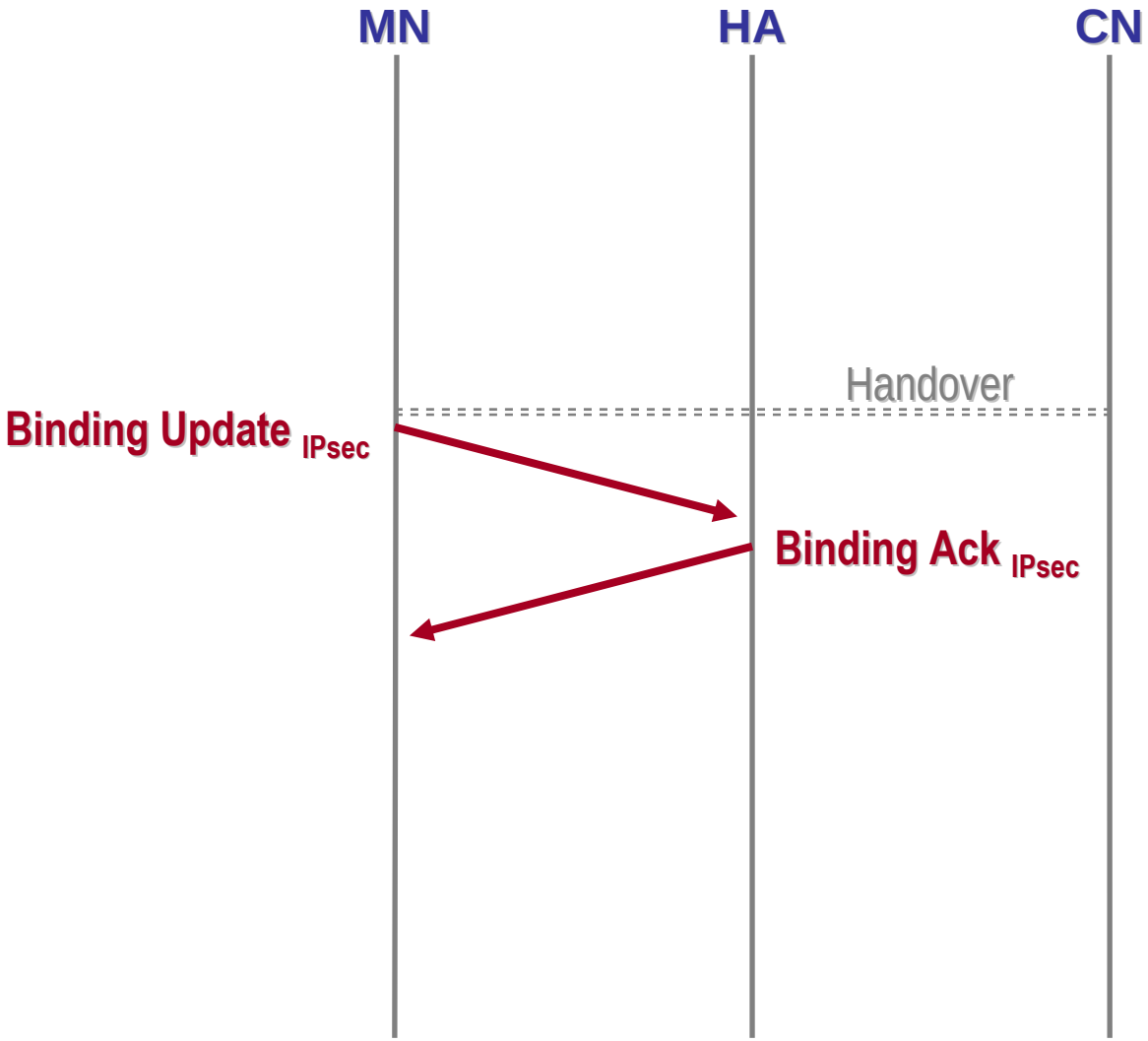
- **Care-of address** (CoA) from visited network
  - For routing
  - Is topologically correct
- **Home address** (HoA) from a “home” network
  - Has long-term significance
  - For Mobile IPv6 signaling authentication
  - For end-point identification at upper layers
- Mobile IPv6 protocol swaps CoA and HoA

Overview on Mobile IPv6 (2)

When away from home, the MN does a…

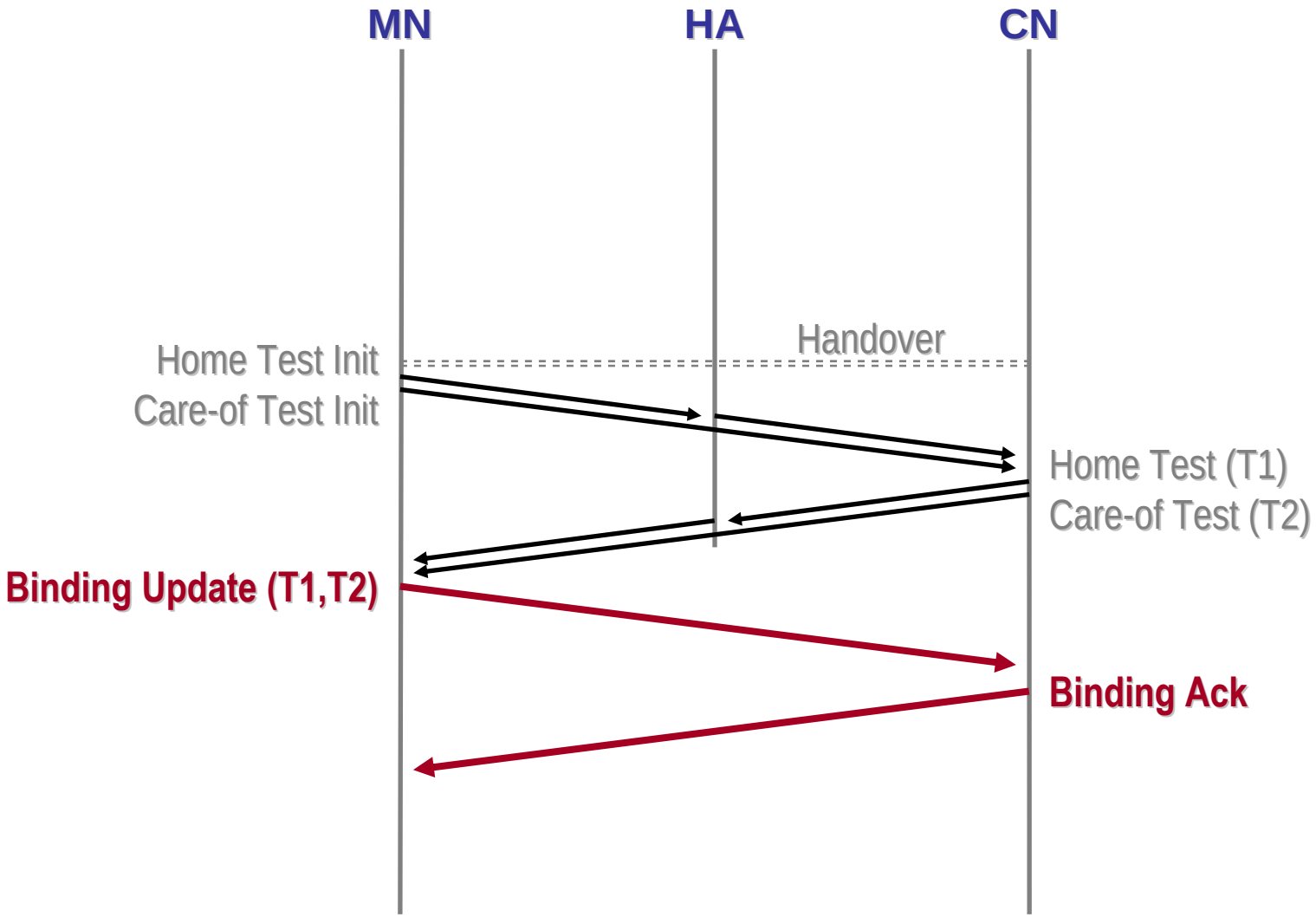
- **Home registration**
  - Registration with Home Agent (HA), the MN's proxy in the home network
    - MN is reachable at the HoA. Tunnel btw. HoA and CoA
  - Pre-configured security relationship btw. MN and HA
  - Authentication, authorization through IPsec
- **Correspondent registration**
  - Registration with CN
  - Typically no a-priori security relationship
  - Authentication, authorization through a routing property
    - Secret-token exchange through the HoA (HoA test)
    - Secret-token exchange through the CoA (CoA test)

Home Registration

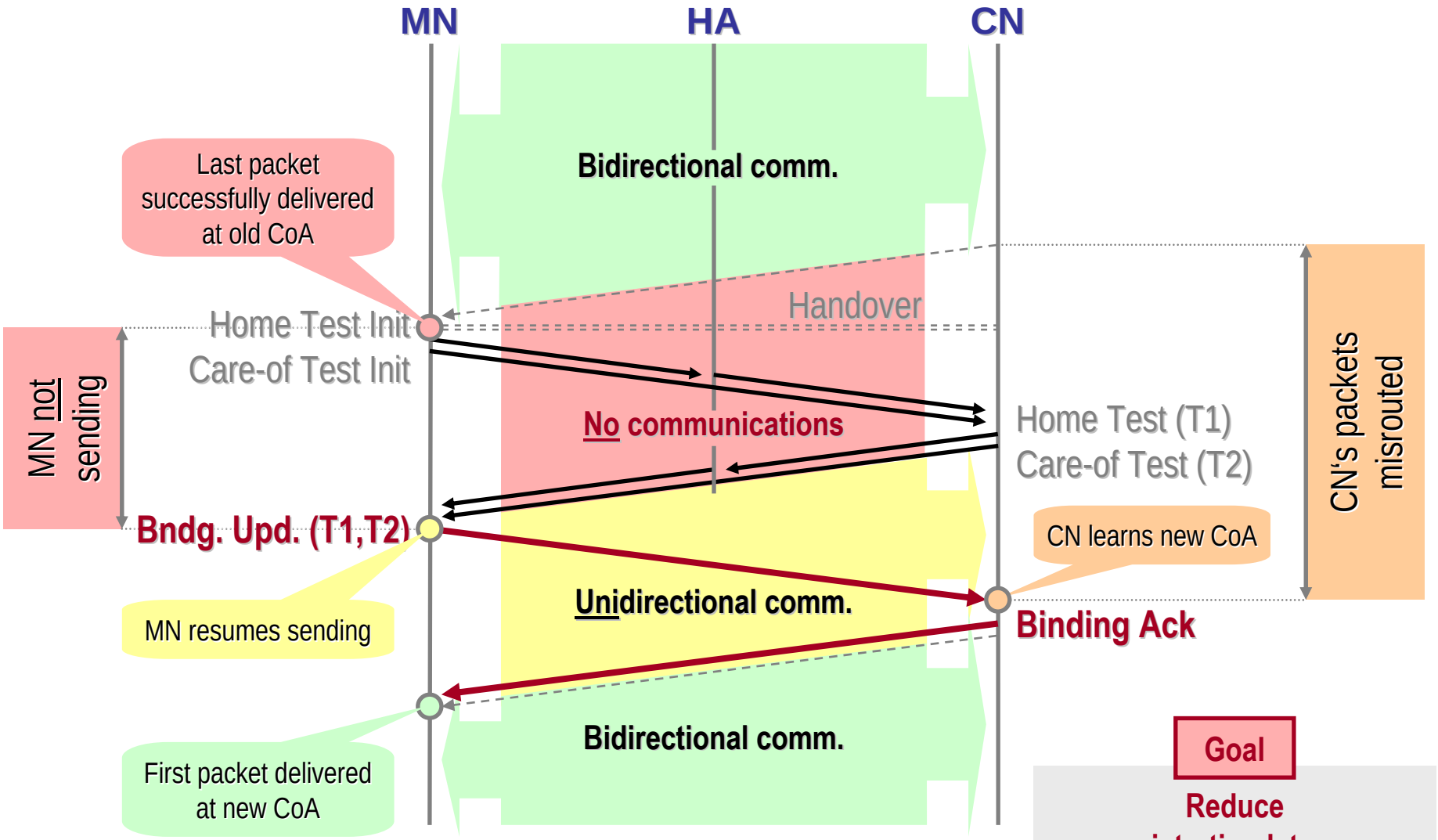


Mobile IPv6 ⟨RFC 3775⟩

Correspondent Registration



Mobile IPv6 ⟨RFC 3775⟩

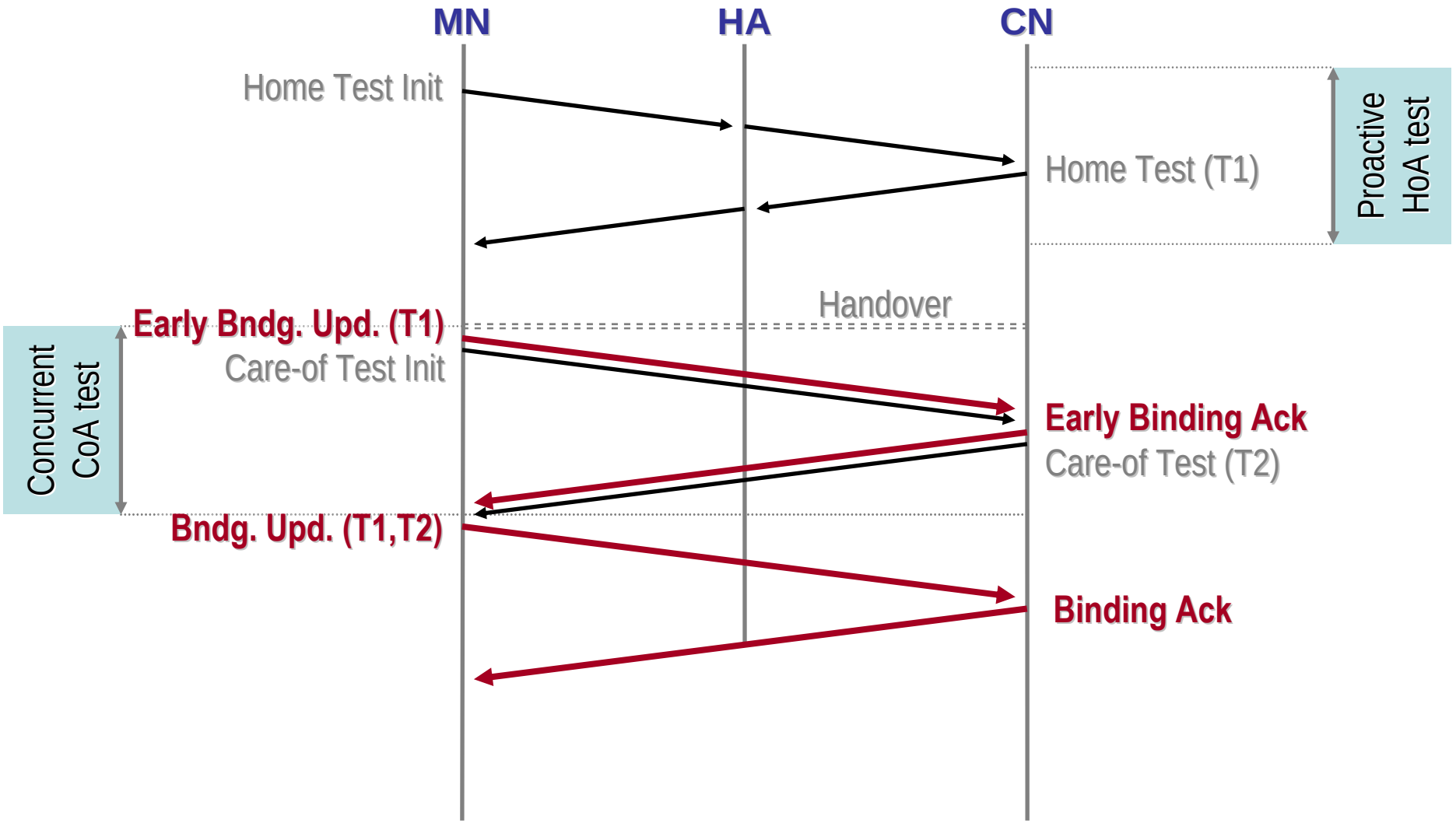


Mobile IPv6 ⟨RFC 3775⟩

Early Binding Updates

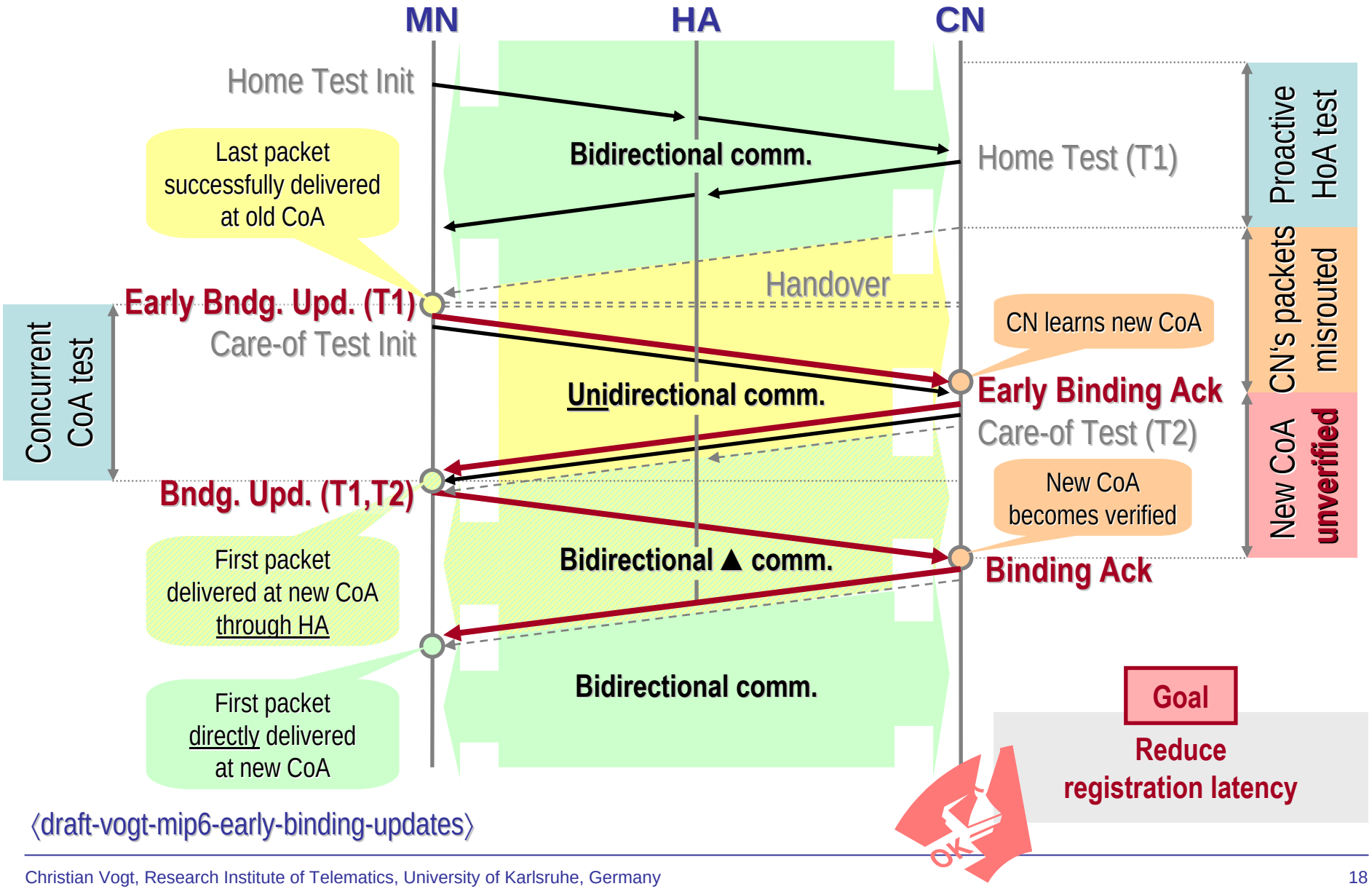
Making Mobile IPv6 more efficient…

Early Binding Updates: The Idea



⟨draft-vogt-mip6-early-binding-updates⟩

Analysis of Early Binding Updates



⟨draft-vogt-mip6-early-binding-updates⟩

Temporarily routing through the HA is sub-optimal…

Credit-Based Authorization

Care-of Address Spot Checks

Enabling direct bidirectional communications,

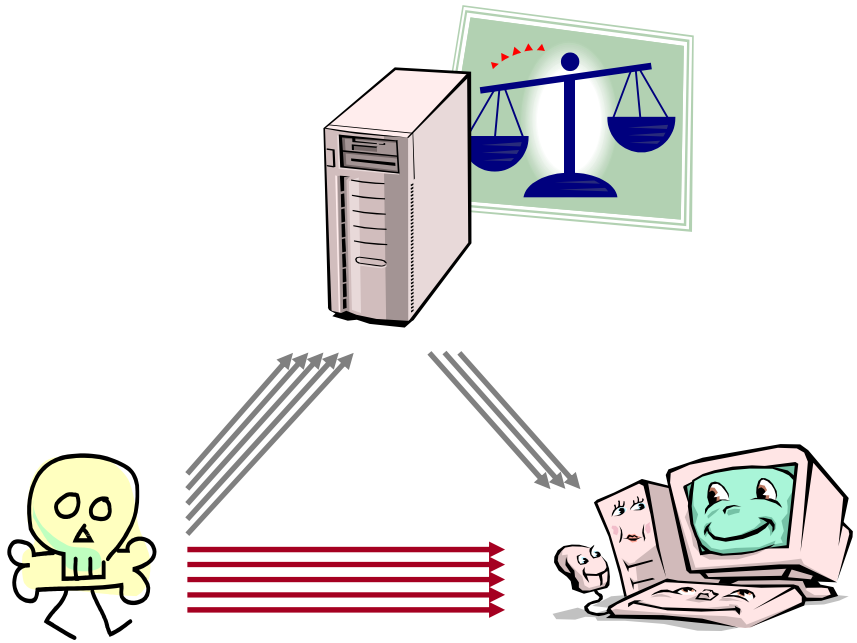
even while a CoA is unconfirmed

Credit-Based Authorization: The Idea

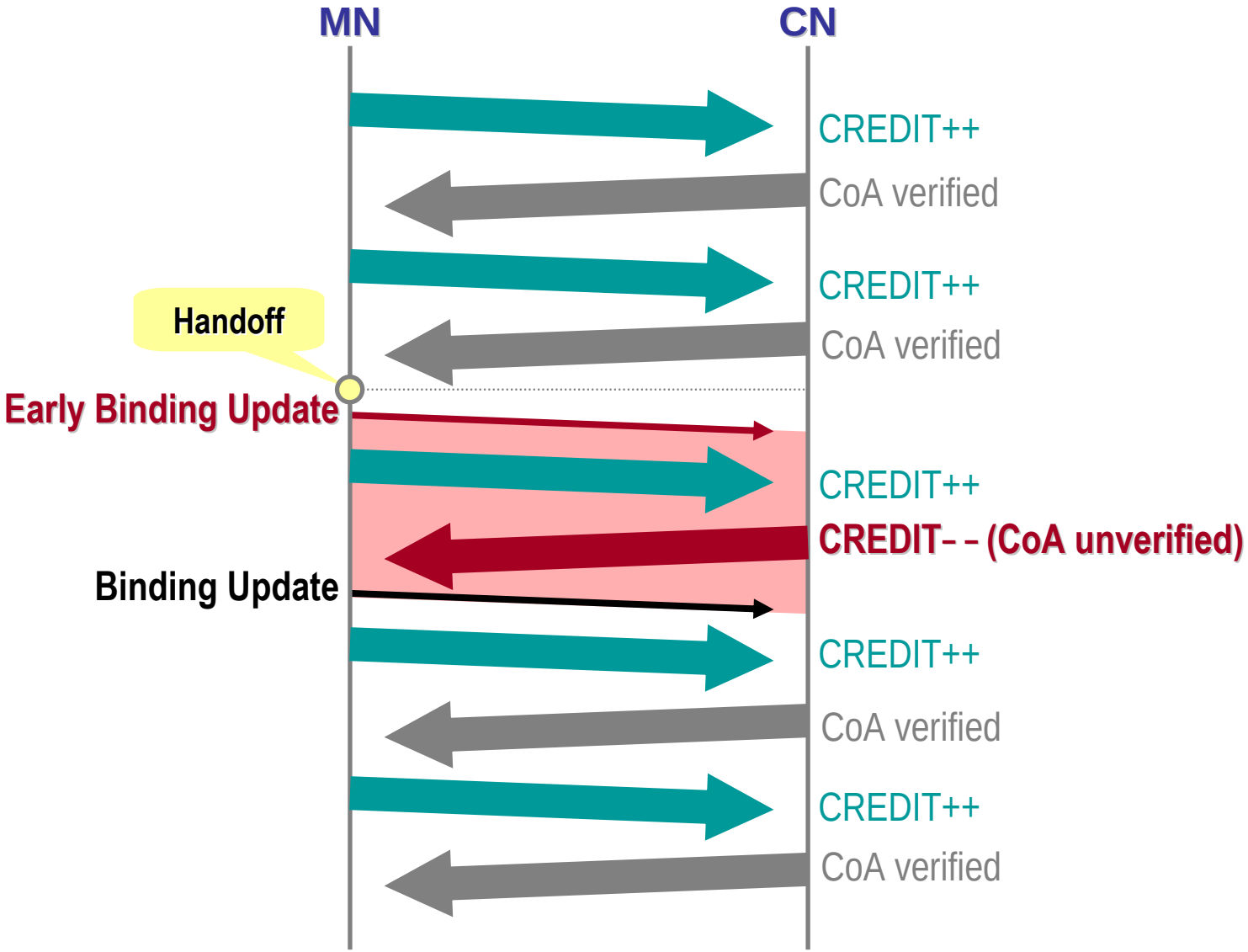
- CN does **send** packets **to an unverified CoA**, but…
- **Not more than** recently **received** from MN
- ⇒ **No amplification**
- **Redirection** possible, but **little attractive** (direct flooding is easier)

Goal

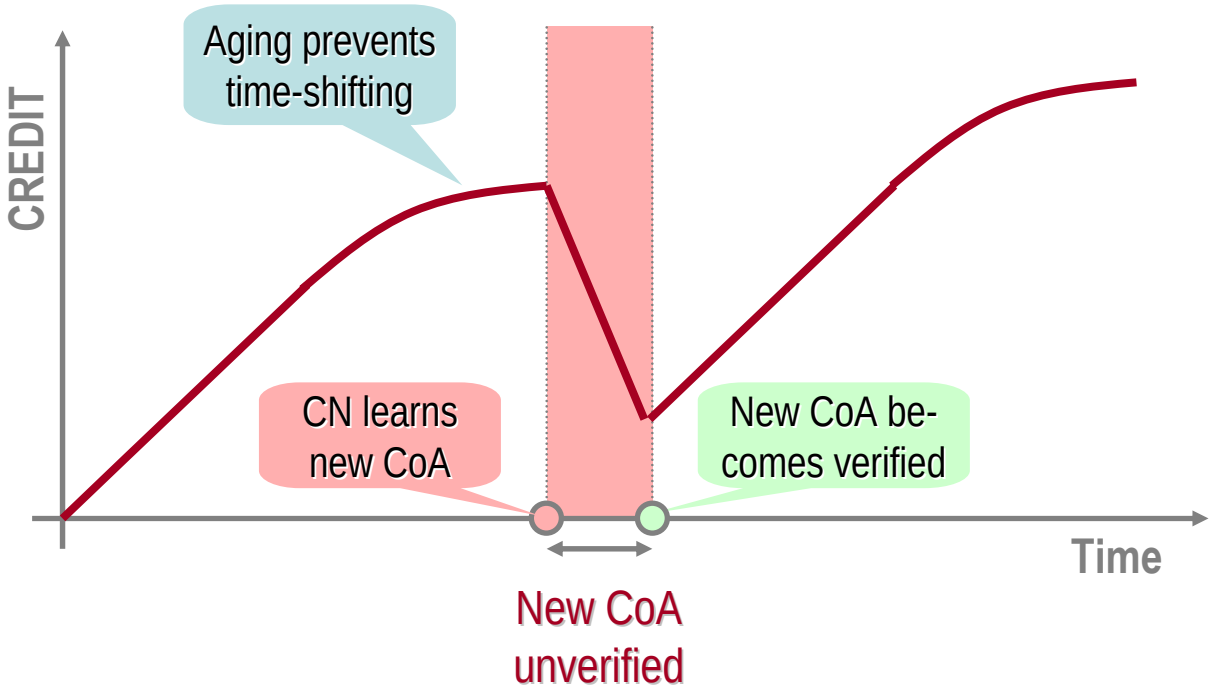
Direct bidirectional comm. while new CoA unverified



Example (1)

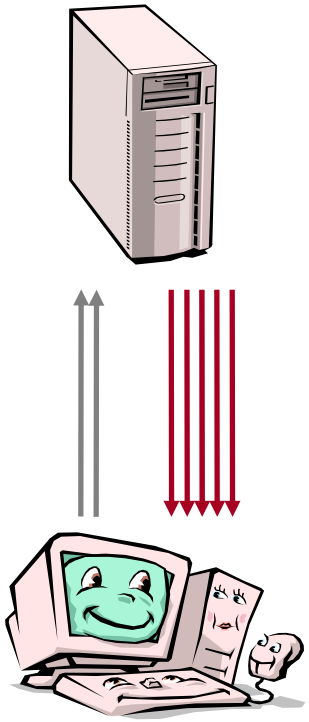

MN
CN
CREDIT++
CoA verified
CREDIT++
CoA verified
Handoff
Early Binding Update
CREDIT++
CREDIT– – (CoA unverified)
Binding Update
CREDIT++
CoA verified
CREDIT++
CoA verified

Example (2)

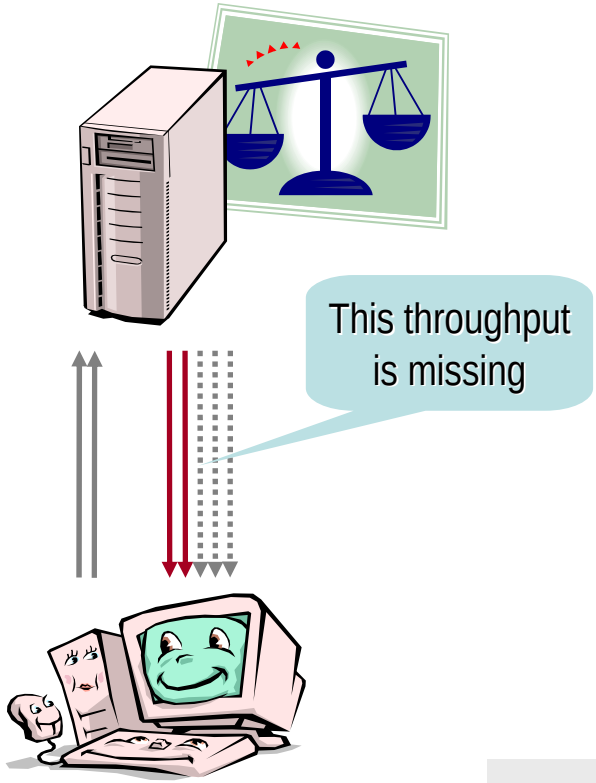

Aging prevents time-shifting
CREDIT
CN learns new CoA
New CoA be-comes verified
Time
New CoA unverified

Supporting Asymmetric Traffic

- **MN** usually **sends less** than CN
- MN may **not** get **enough credit**



While CoA is verified…



While CoA is unverified…

Goal

Support applications with asymmetric traffic, too

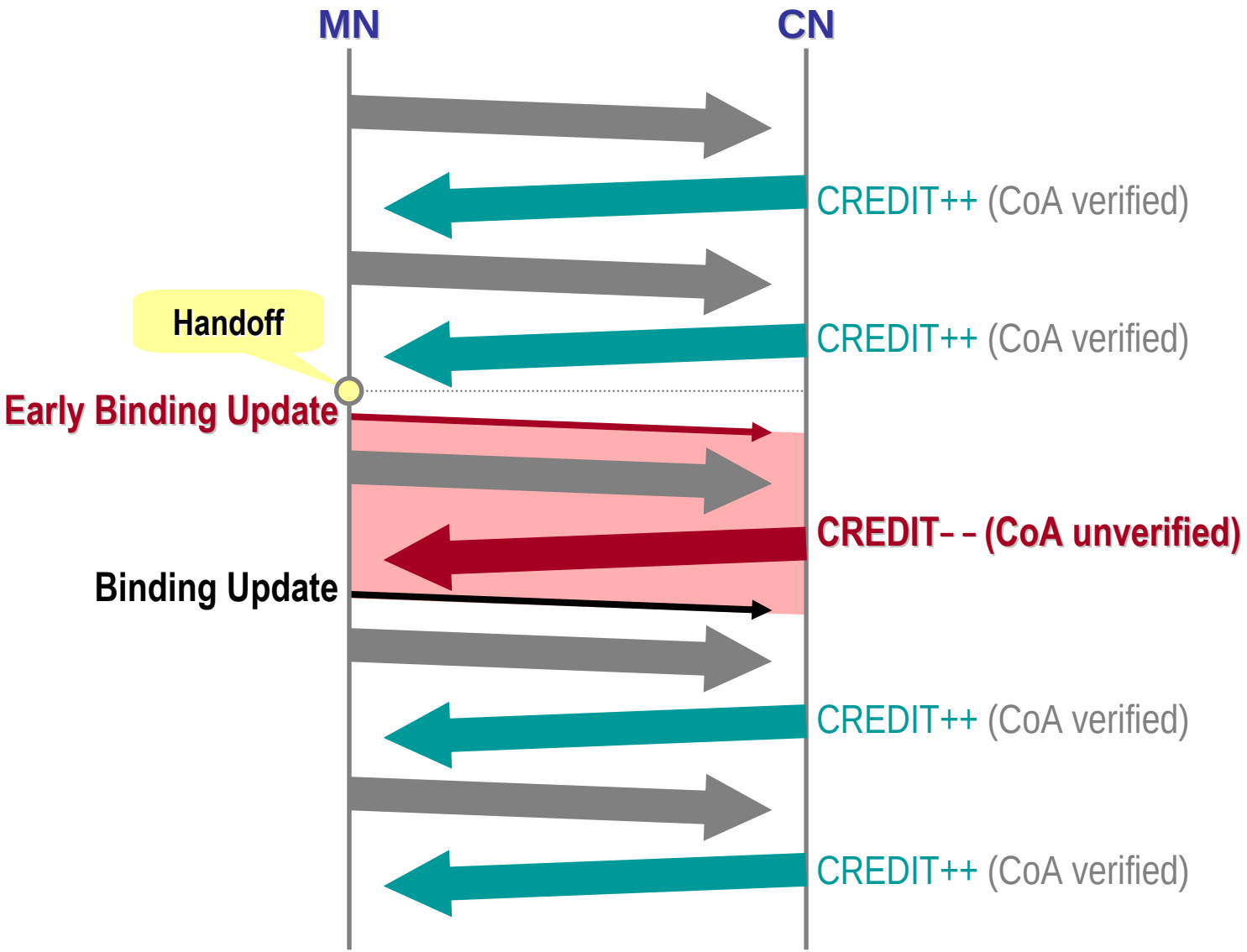
Supporting Asymmetric Traffic (2)

- If we can give a MN credit for packets that it sends…
- …then we could also give the MN **credit for packet reception**
- The MN spends **comparable resources**

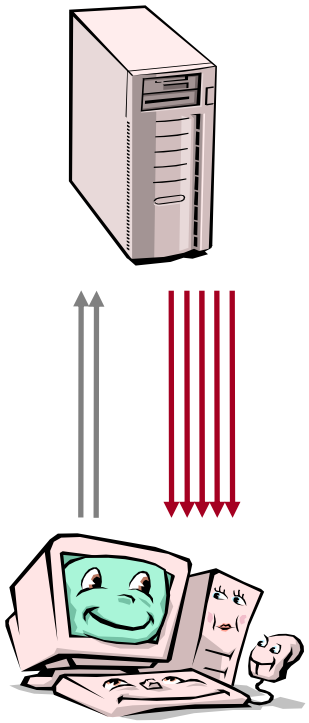
  on receiving packets as on sending packets

  in terms of bandwidth, processing capacity, memory

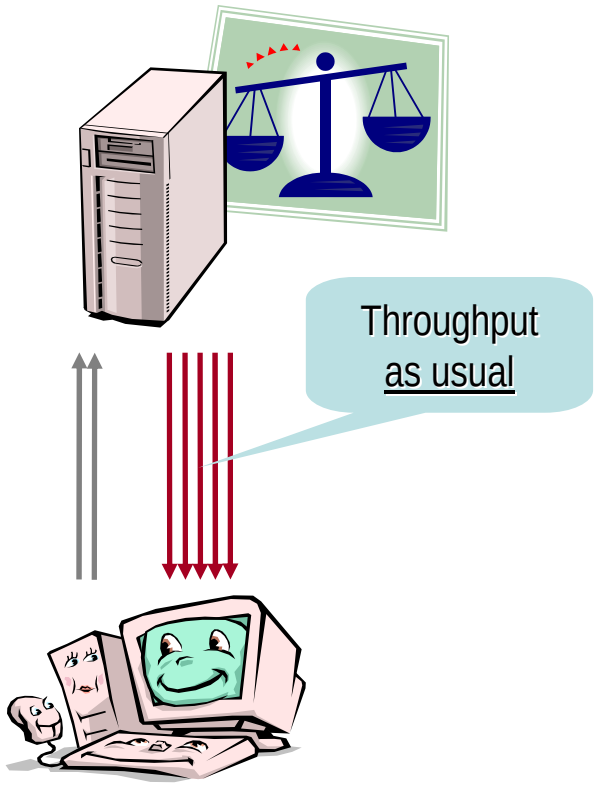
Supporting Asymmetric Traffic (3)



Supporting Asymmetric Traffic (4)



While CoA is verified…



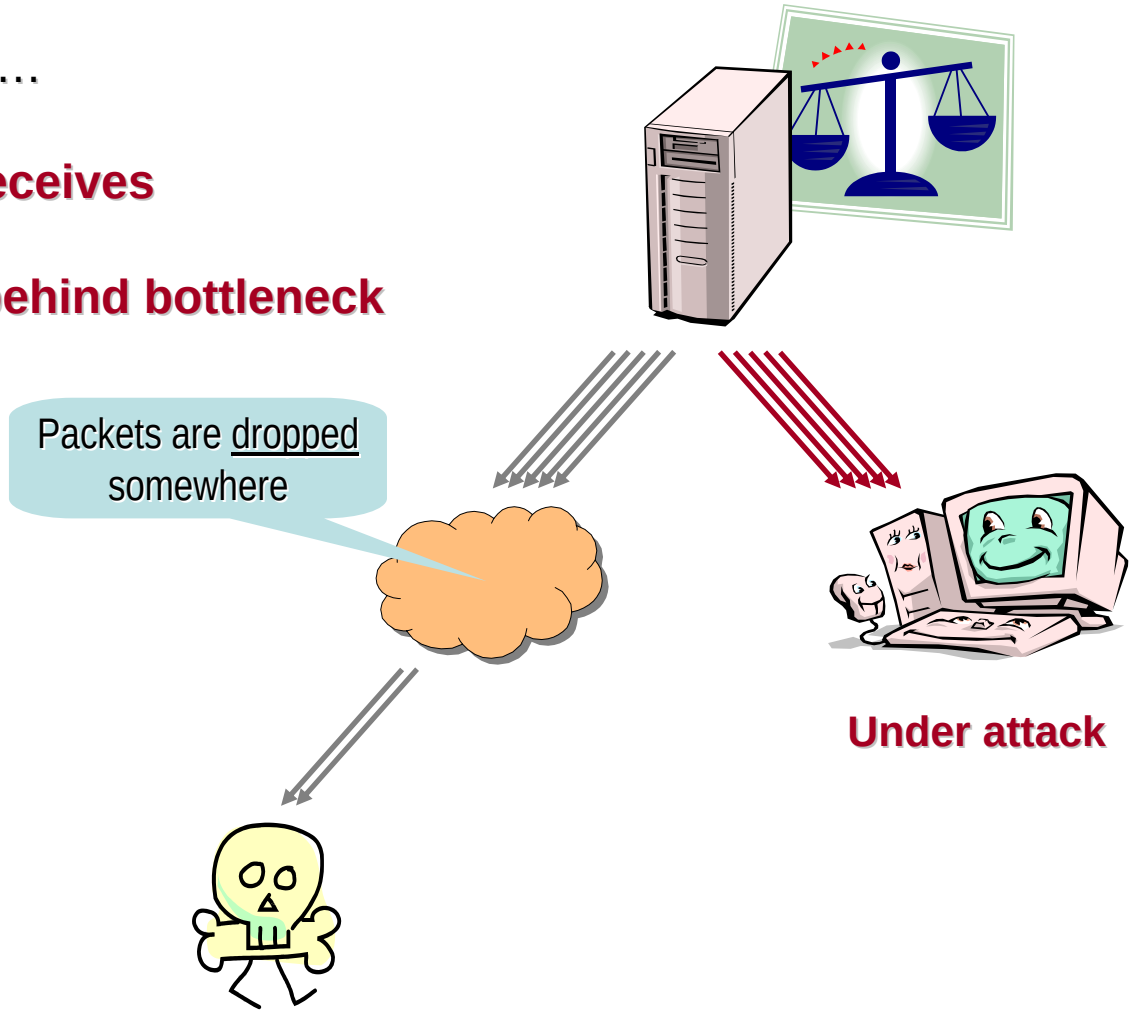
While CoA is unverified…

Goal

Support applications with asymmetric traffic, too

Supporting Asymmetric Traffic, more…

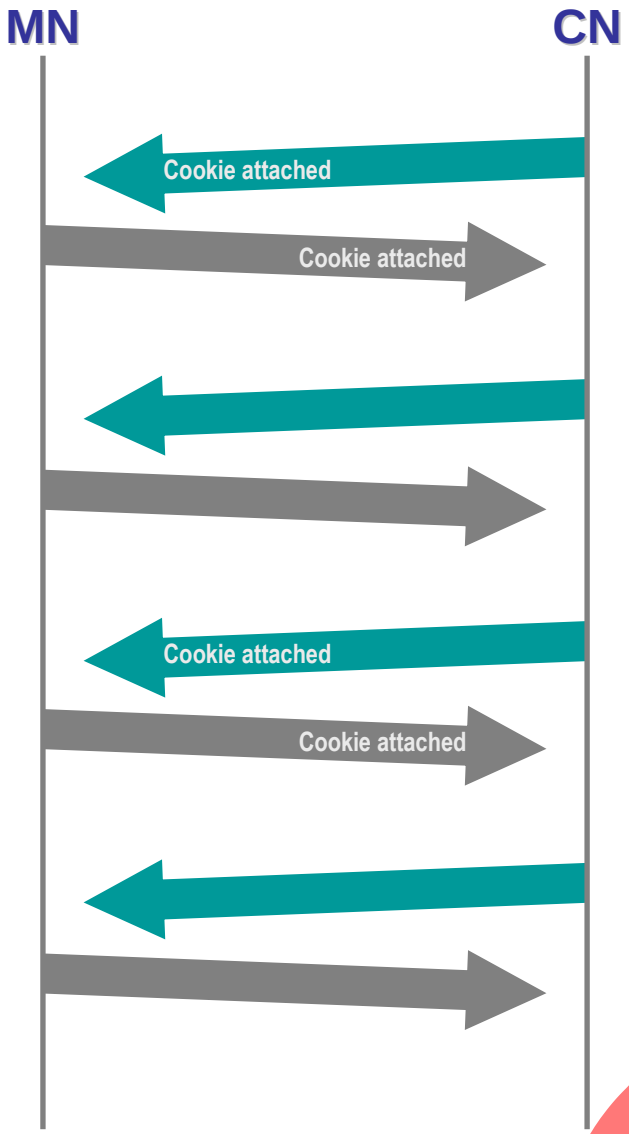
- CN knows what it **sends**…
- …but not what the MN **receives**
- An attacker may locate **behind bottleneck**



Goal

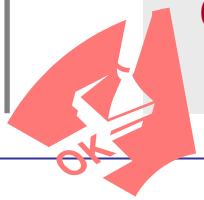
Credit received packets, not sent packets

Care-of Address Spot Checks: The Idea



CREDIT ~

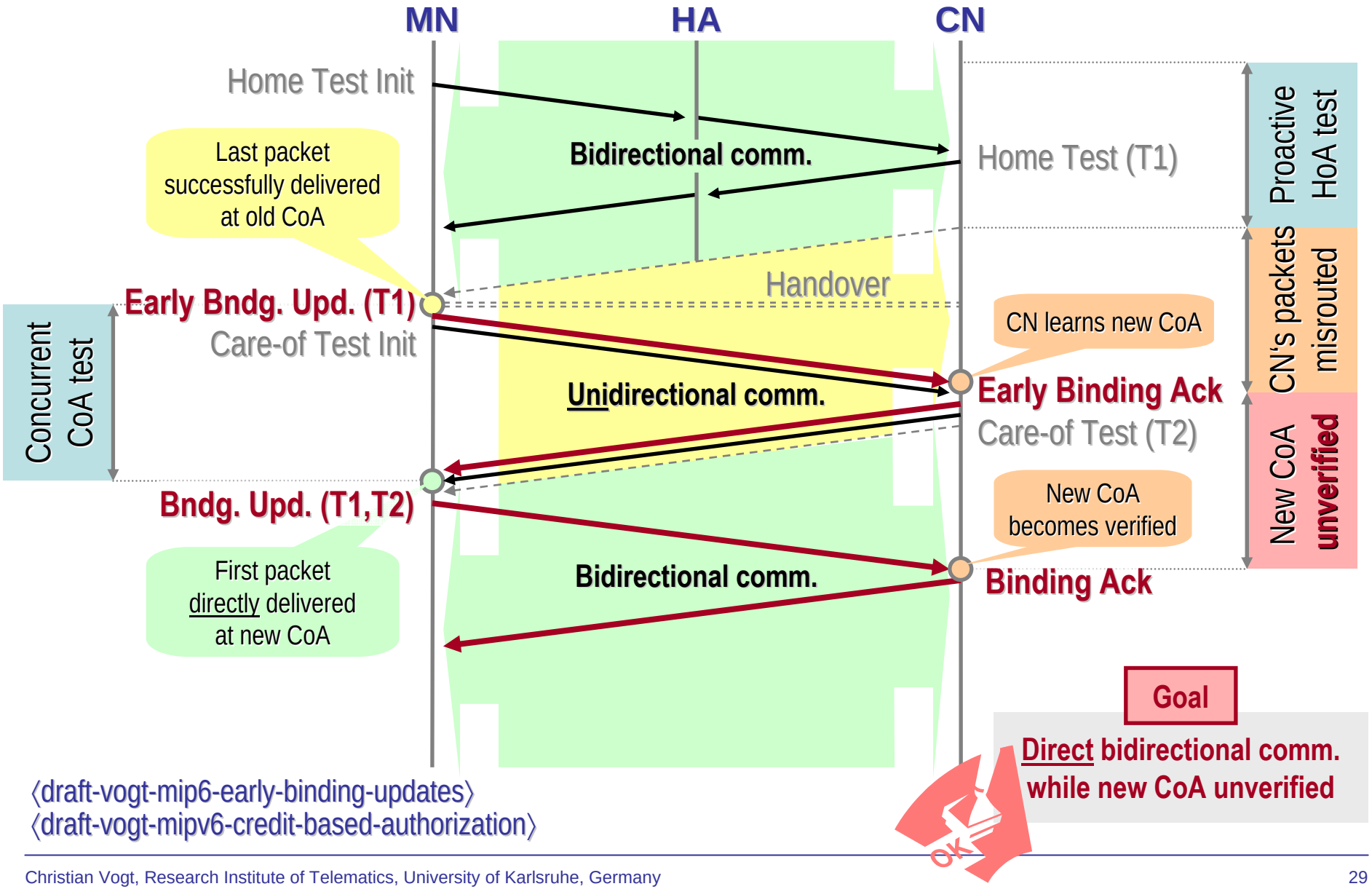
$$\frac{\text{\# Cookies returned}}{\text{\# Cookies sent}}$$



Goal

Credit received packets, not sent packets

The Big Picture



Discussion

- Early Binding Updates are specific to Mobile IPv6, but…
  - Concurrent IP-address tests
  - Credit-Based Authorization
  - IP-address spot checks

  …are also **applicable to other MM protocols** (e.g., HIP, Mobike, SCTP)
- Credit-Based Authorization is **transparent** to MN
- **End-to-end** vs. local
  - Fast and Hierarchical Mobile IPv6 are faster…
  - …but do not work across administrative domains

Open Issues

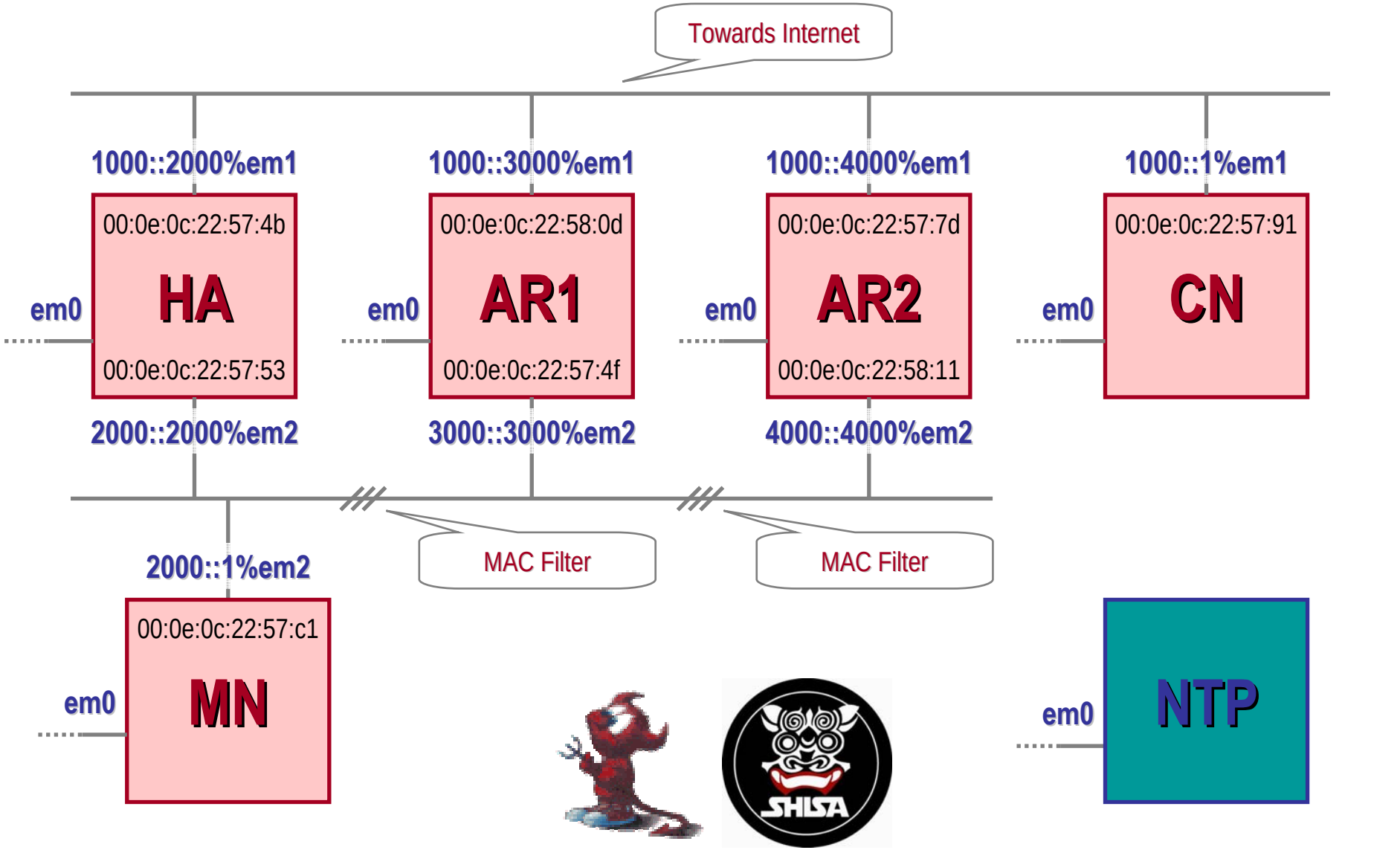
- How do these optimizations perform in a **real scenario**?
- What are the **impacts on applications**?
- Credit **sent or received** packets?
- What protocol **parameters** are best? (Aging, tentative binding lifetime)
- How **complex** is an implementation?

Future work

- MN may anticipate movement and proactively configure new IP address

  $\Rightarrow$ Credit-Based Authorization allows for **anticipated** IP-address **registration**

Testbed


Towards Internet
1000::2000%em1
1000::3000%em1
1000::4000%em1
1000::1%em1
00:0e:0c:22:57:4b
HA
00:0e:0c:22:57:53
00:0e:0c:22:58:0d
AR1
00:0e:0c:22:57:4f
00:0e:0c:22:57:7d
AR2
00:0e:0c:22:58:11
00:0e:0c:22:57:91
CN
em0
em0
em0
em0
2000::2000%em2
3000::3000%em2
4000::4000%em2
MAC Filter
MAC Filter
2000::1%em2
00:0e:0c:22:57:c1
MN
em0
NTP
em0
SHISA
FreeBSD 5.3, Kame-Shisa Mobile IPv6

Summary

- Mobility causes security **threats**
  - Impersonation
  - Resource exhaustion
  - Flooding
- Solution: HoA/CoA-address test (in Mobile IPv6)
  - Trade security for **latency**
- Optimization: **Early Binding Updates**
  - Proactive HoA test
  - Concurrent CoA test
- CN still cannot send to unverified CoA ⇒ **Credit-Based Authorization**
  - Credit packets received from MN
  - …or packets sent to MN…
  - …or packets received by MN