End-to-End Mobility Support:

Combining Security and Efficiency

Christian Vogt, chvogt@tm.uka.de

NEC Europe, Network Laboratories, Heidelberg

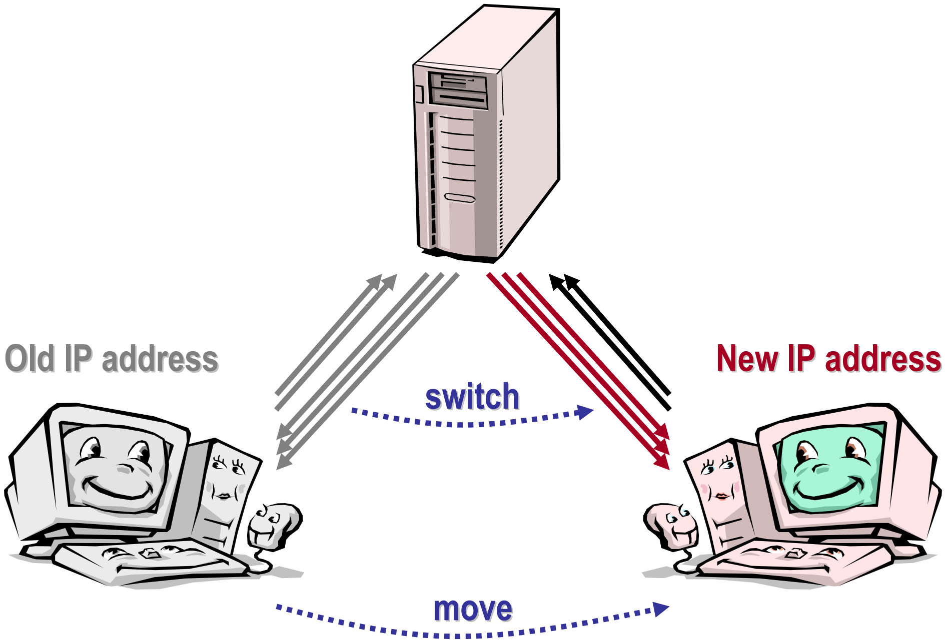
September 16, 2004

Outline

- **Mobility** scenarios, **security** threats
- **Flooding** attacks (will be our focus)
- **Protection** in Mobile IPv6 (induces latency…)
- **Latency**-oriented optimization (has three parts…)
  - Early Binding Updates
  - Credit-Based Authorization
  - IP-Address Spot Checks
- Open **issues**, future work
- Summary

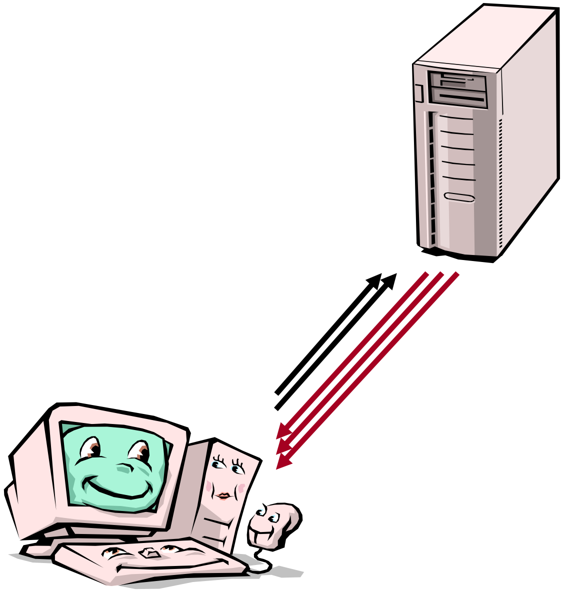
Mobility Scenario

- 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

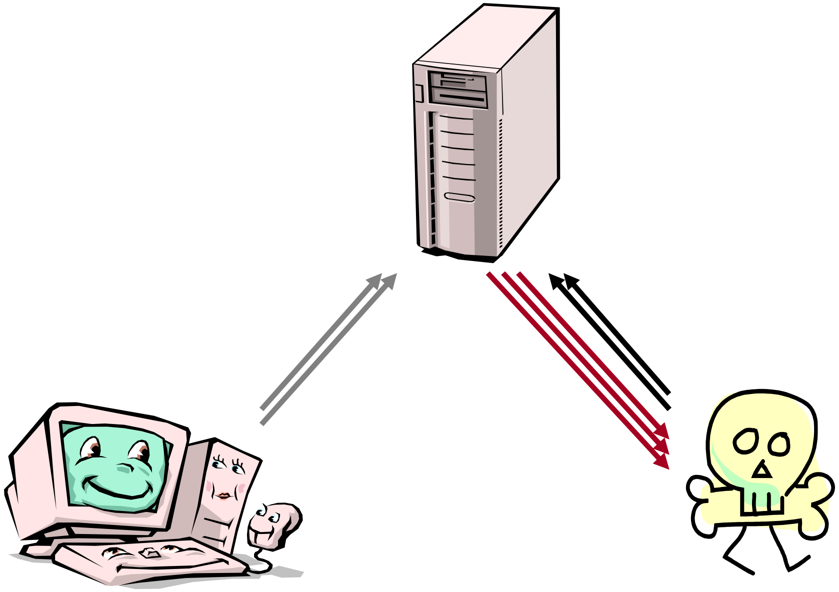


Security Threats: Impersonation

- 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**…

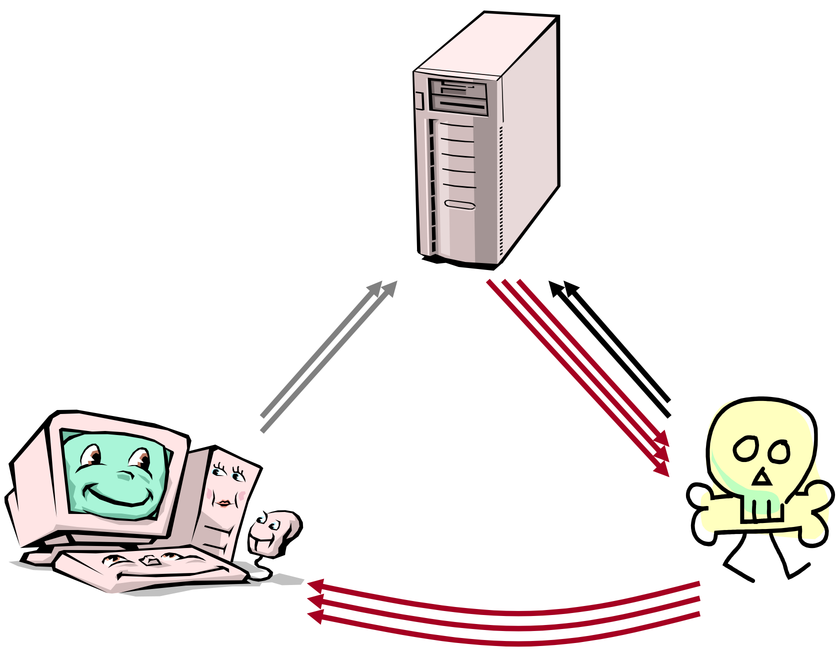


Before the attack…

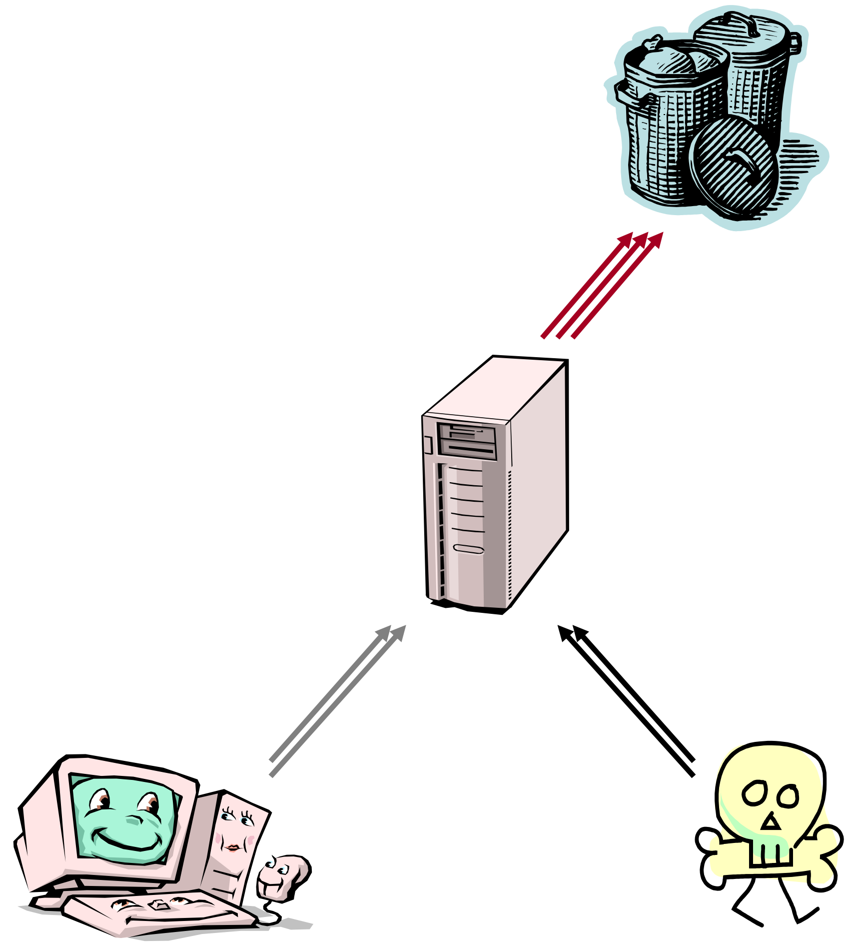


Connection high-jacking

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

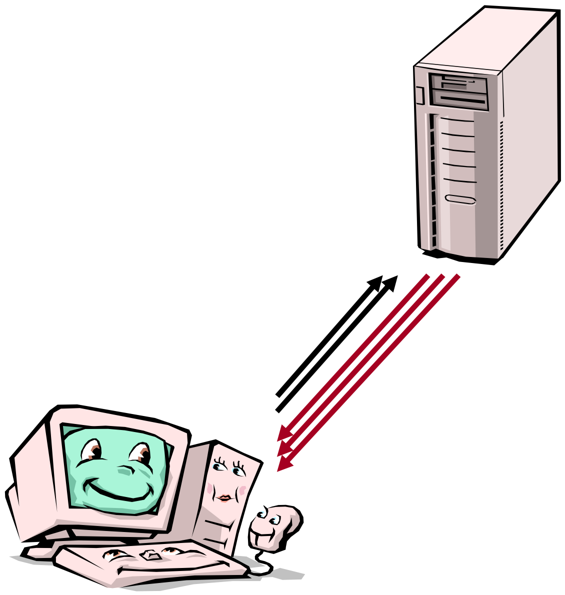


Eavesdropping or MiTM attack

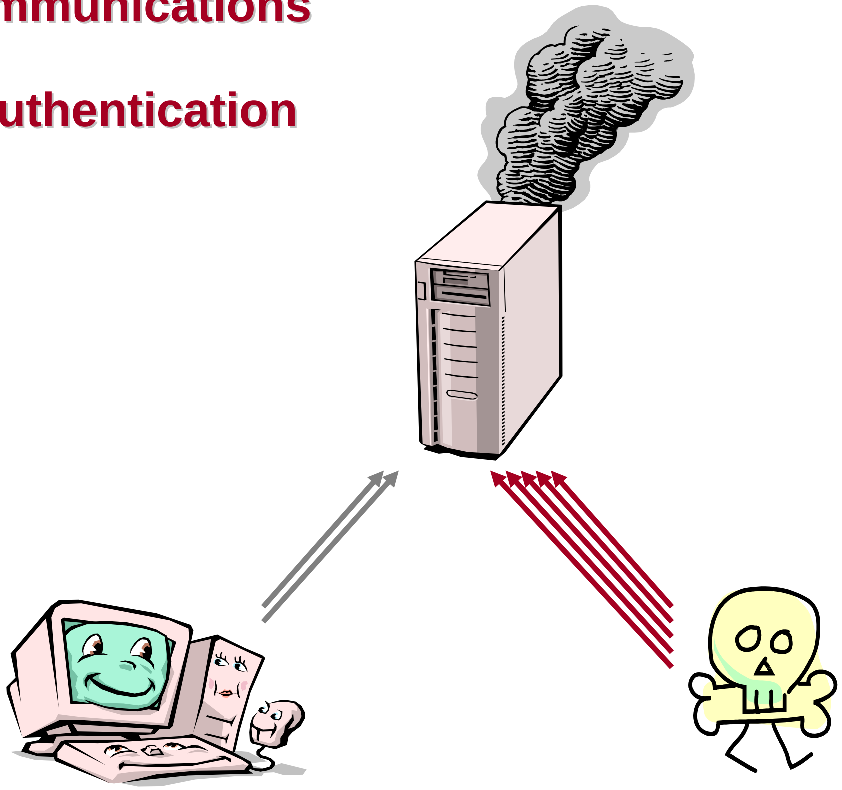


Dumping packets into random IP address

- 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**



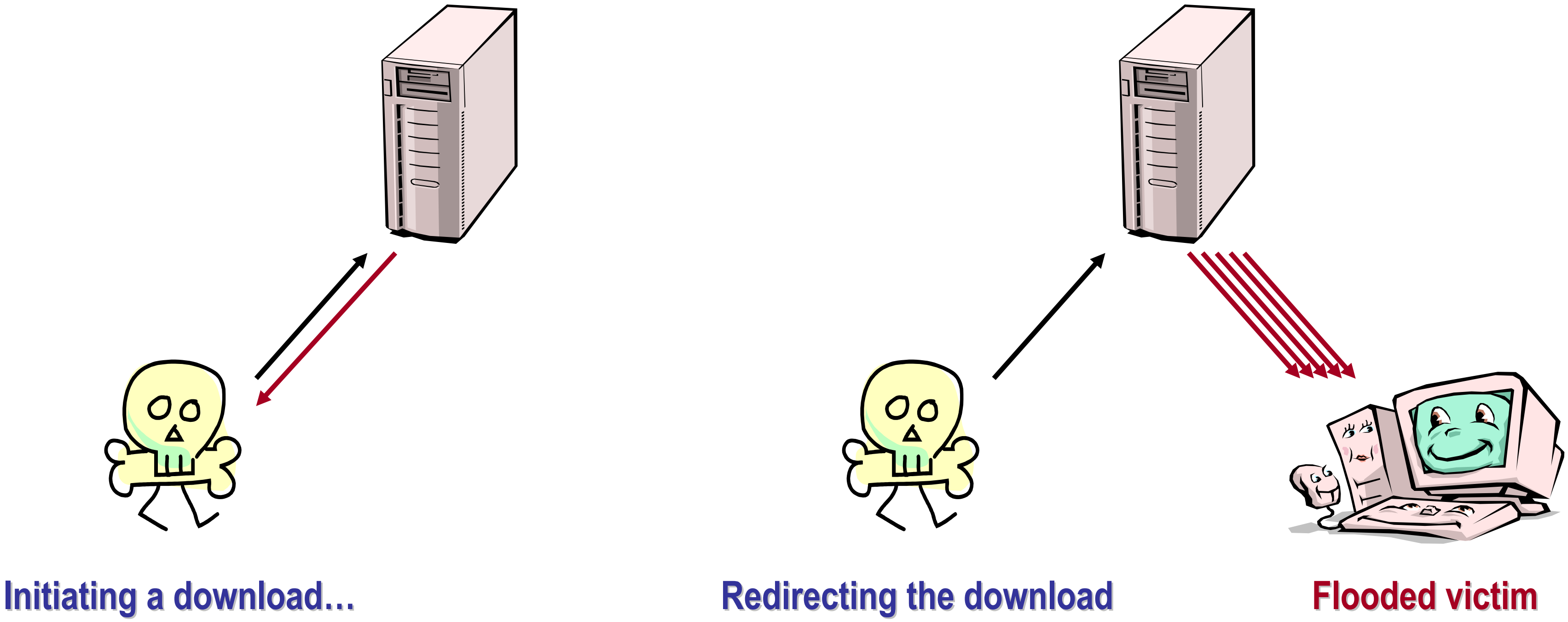
Before the attack…



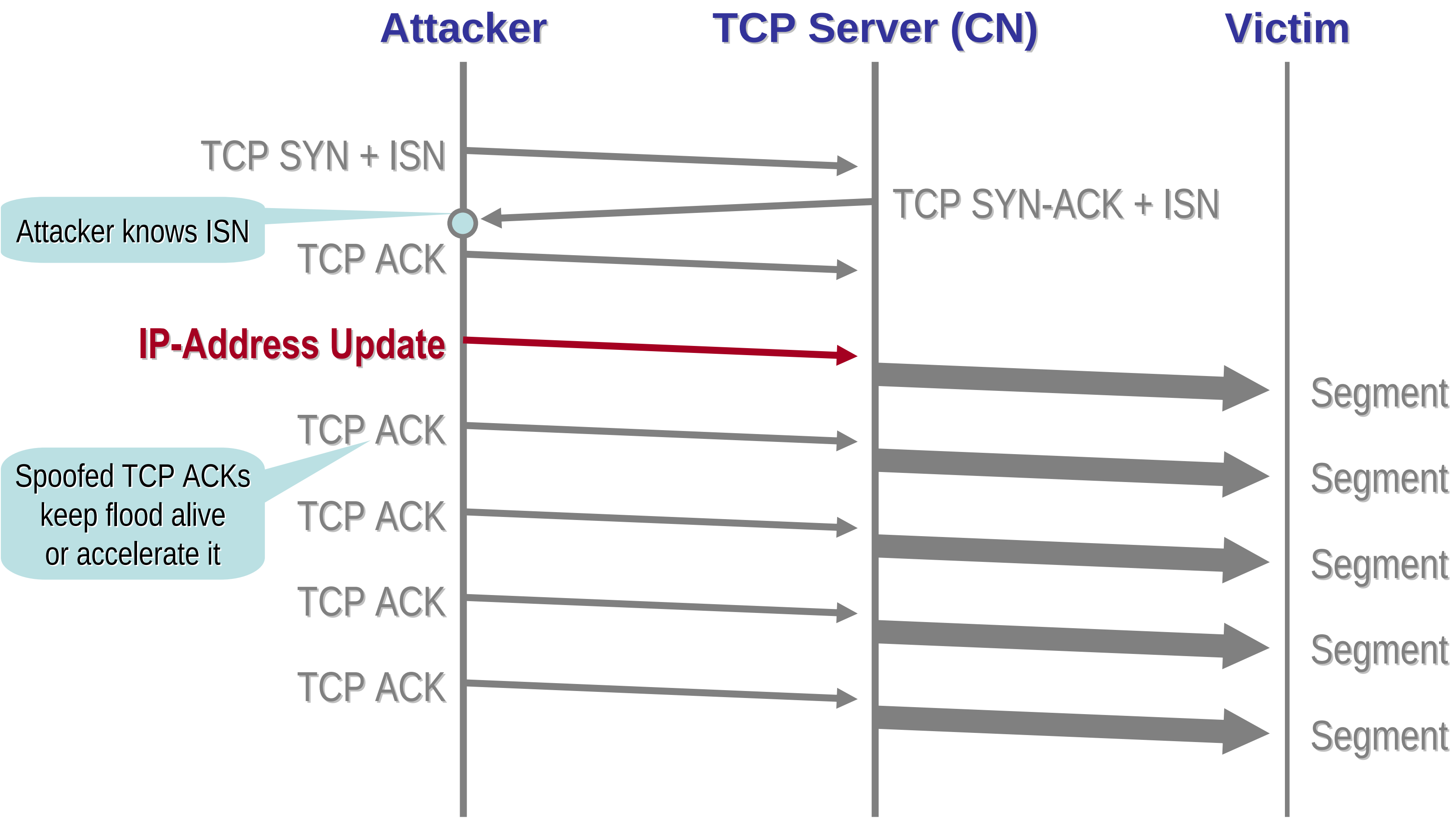
Blocking meaningful communications

Security Threats: 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**



Security Threats: Flooding (2)



- **Authentication** is what matters
- ⇒ **Check** a new **IP address** before using it

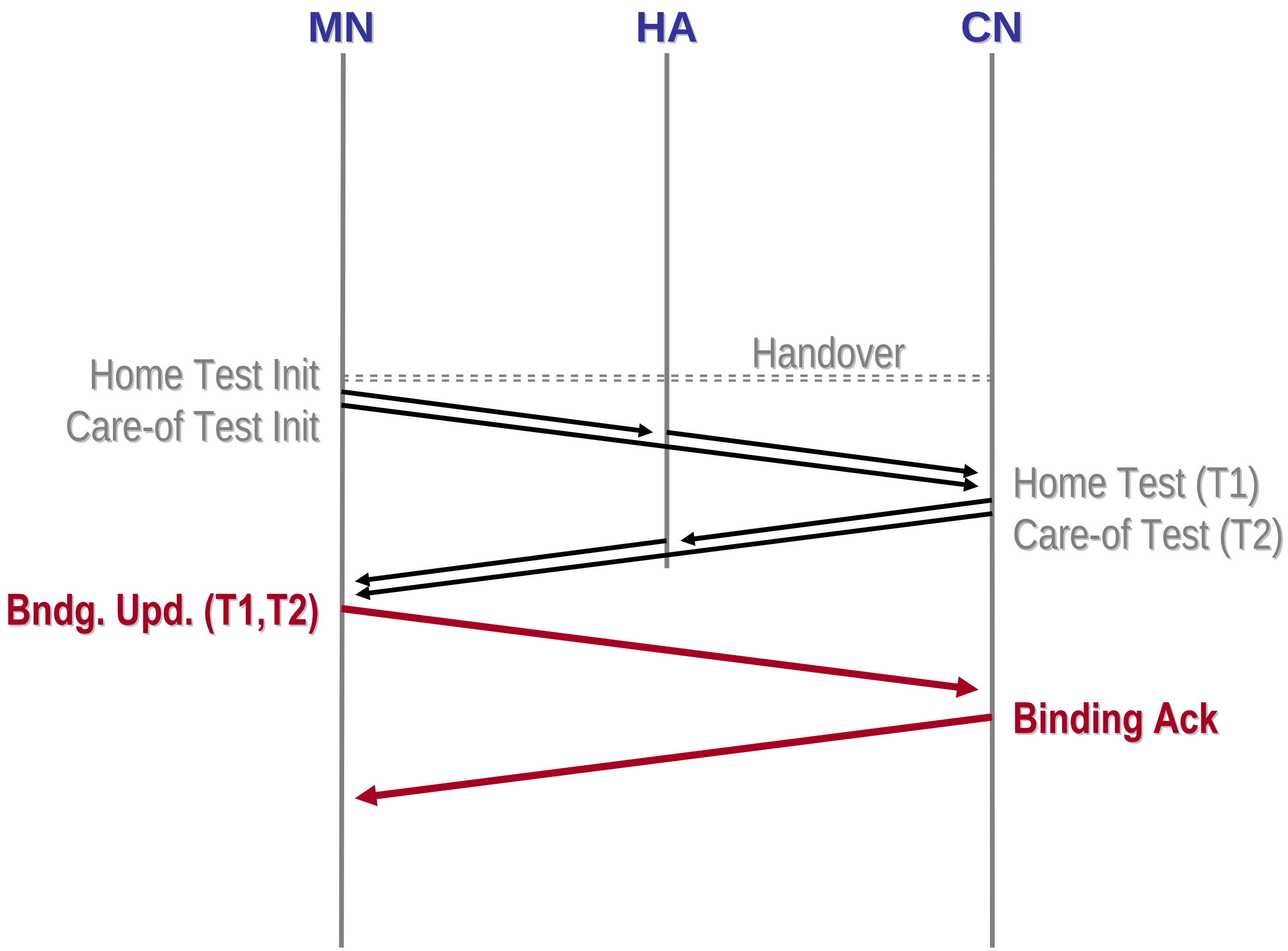
Focus on Flooding Attacks

Consider Mobile IPv6 as an example…

Mobile IPv6: An Overview

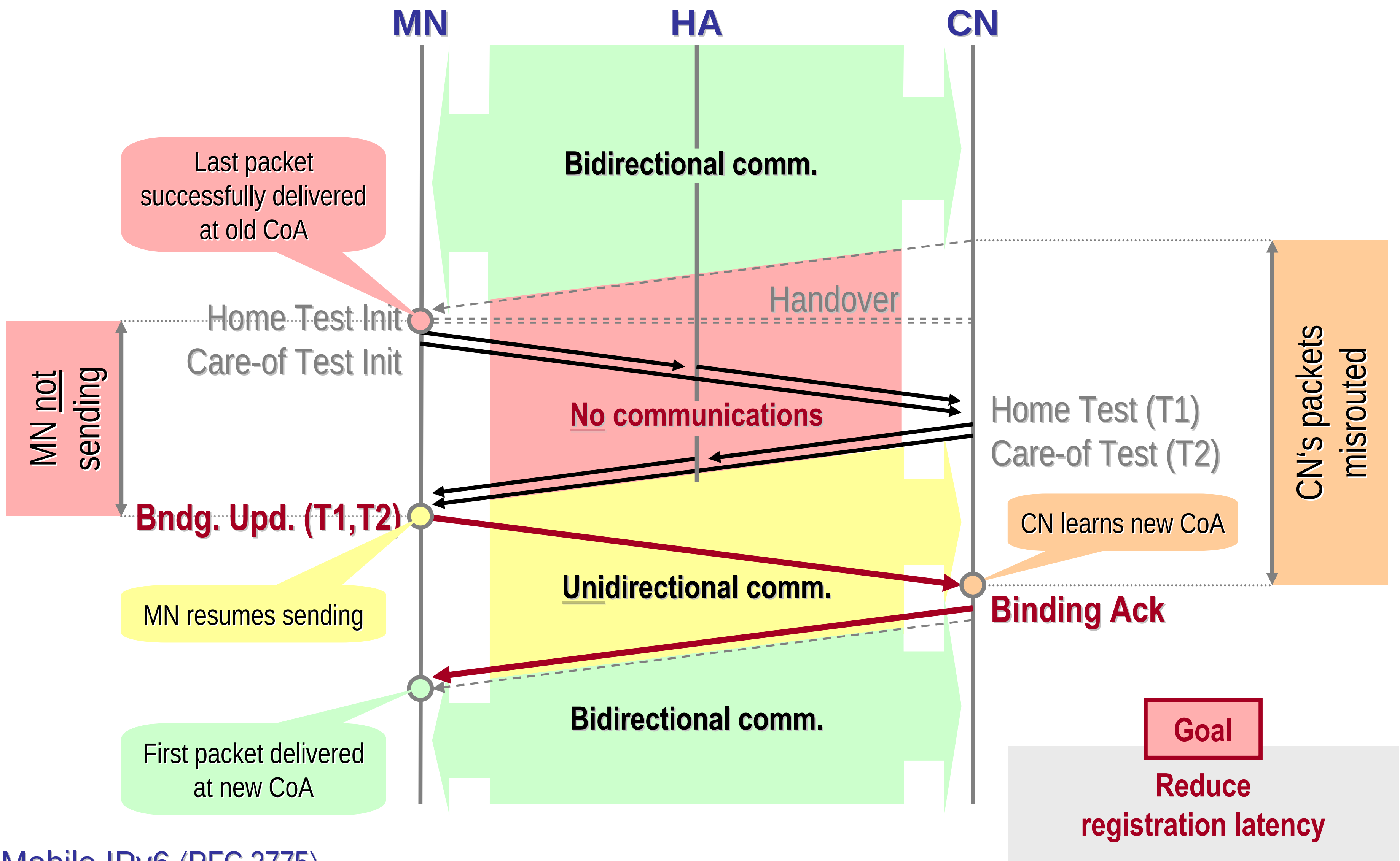
- MN has two IP addresses
  - **Care-of address** (CoA) from visited network
  - **Home address** (HoA) from Home Agent’s (HA) network
- **Home Agent** proxies MN (MN reachable at HoA)
- Mobile IPv6 swaps HoA, CoA (binding)
  - HoA for **upper layers**, signaling **authentication** (long-term significance)
  - CoA for **packet transportation** (topologically correct)
- **Correspondent registration** (binding update)
  - HoA test for signaling authentication
  - New-CoA test for flooding-attack prevention

Correspondent Registration



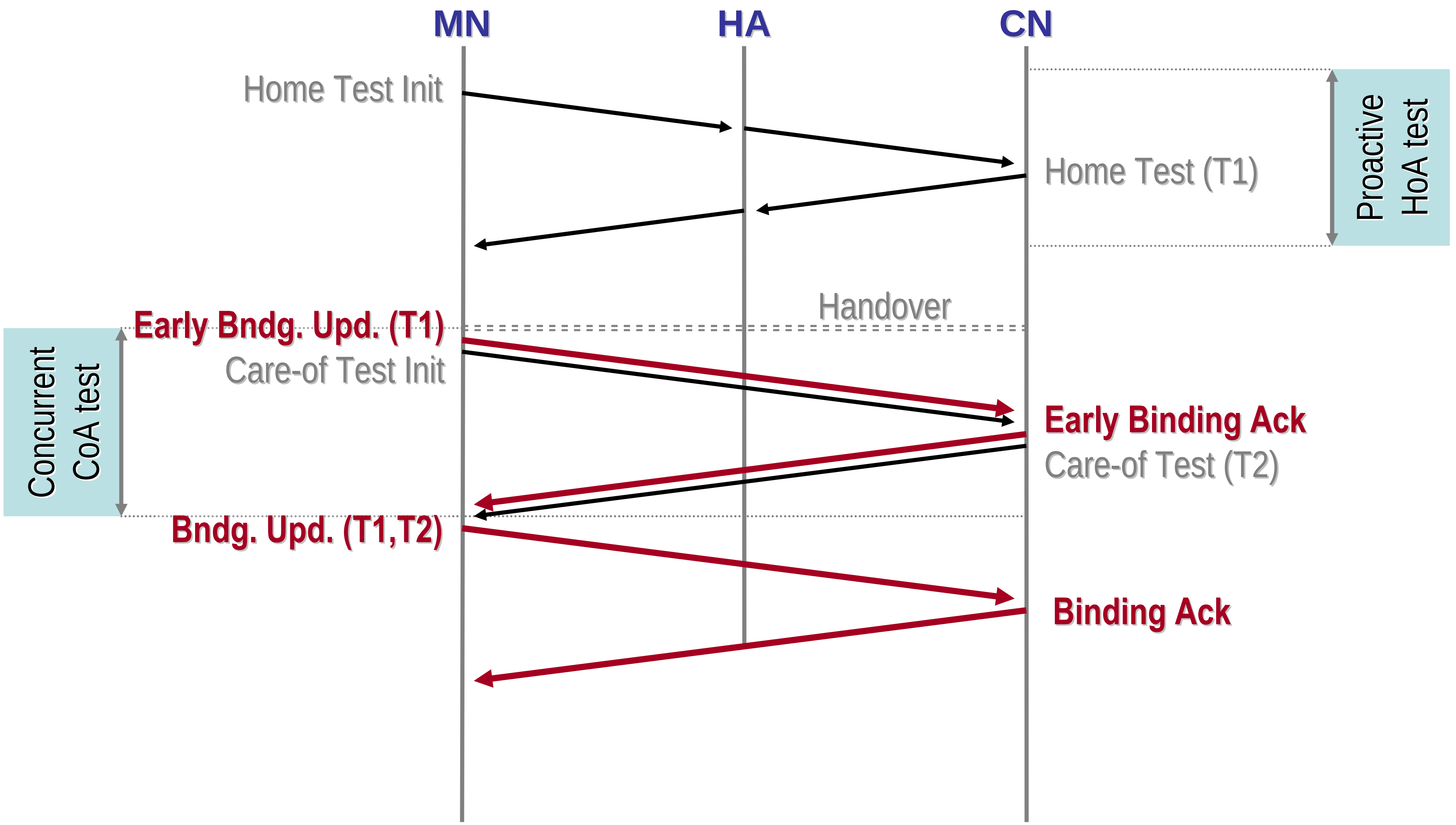
Mobile IPv6 ⟨RFC 3775⟩

Correspondent Registration (2)



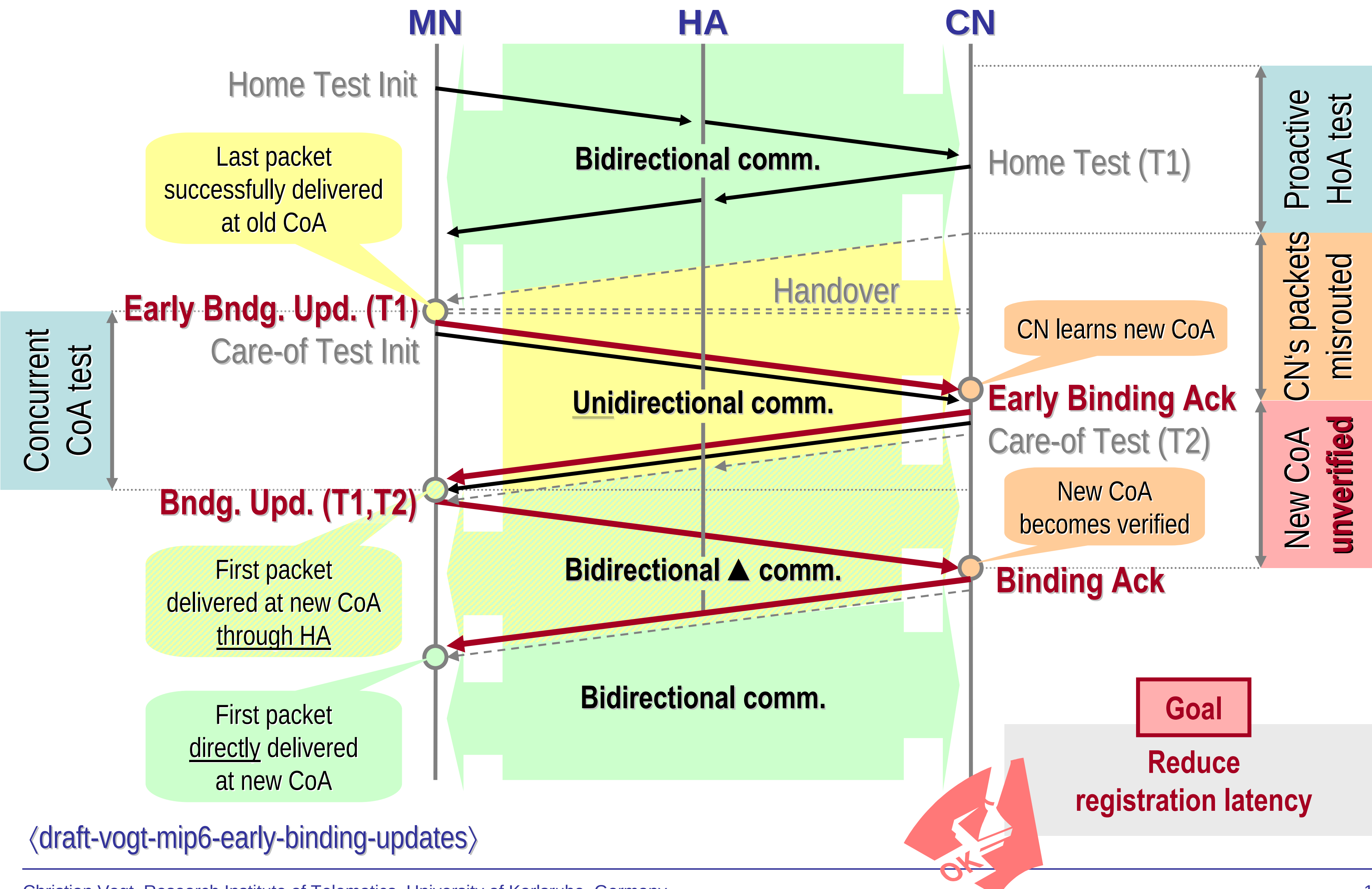
Mobile IPv6 ⟨RFC 3775⟩

Early Binding Updates



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

Early Binding Updates (2)



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

Temporarily routing through the HA is sub-optimal.

Can we enable direct bidirectional communications

even while the new CoA is unverified?

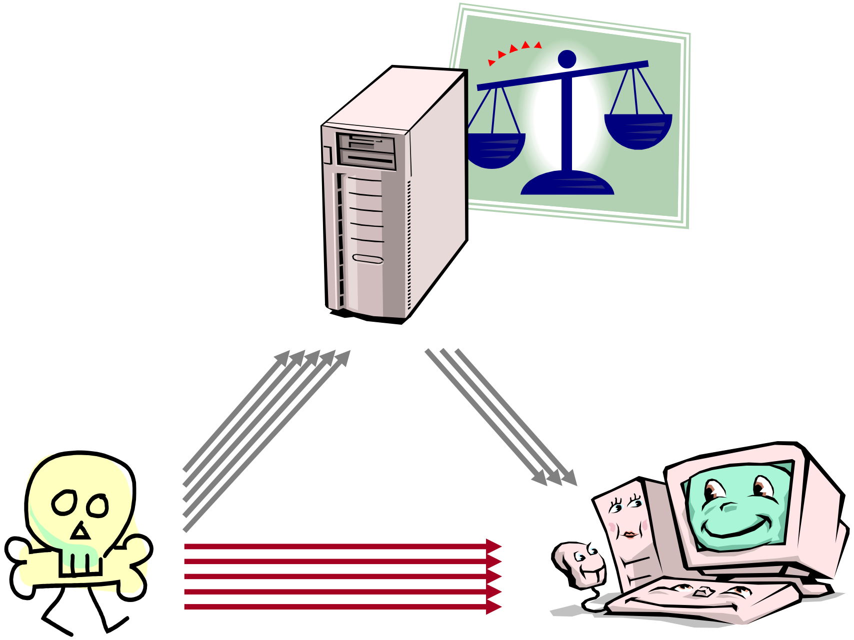
Yes, we can…

Credit-Based Authorization

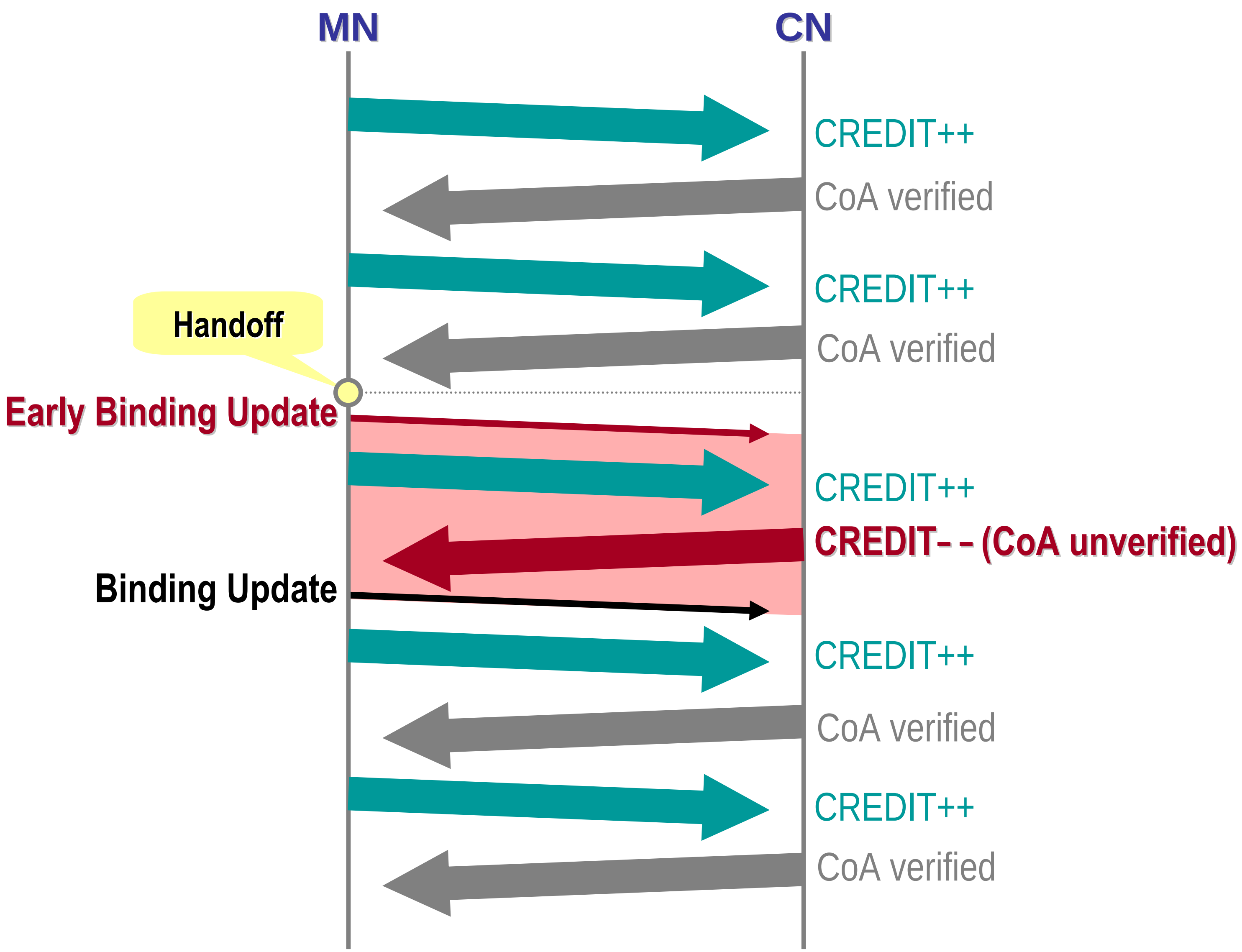
- CN does **send** packets **to an unverified CoA**, but…
- **Not more than** recently **received** from MN
- ⇒ **No amplification**
- **Redirection** possible, but **little attractive** (direct flooding is easier)

Goal

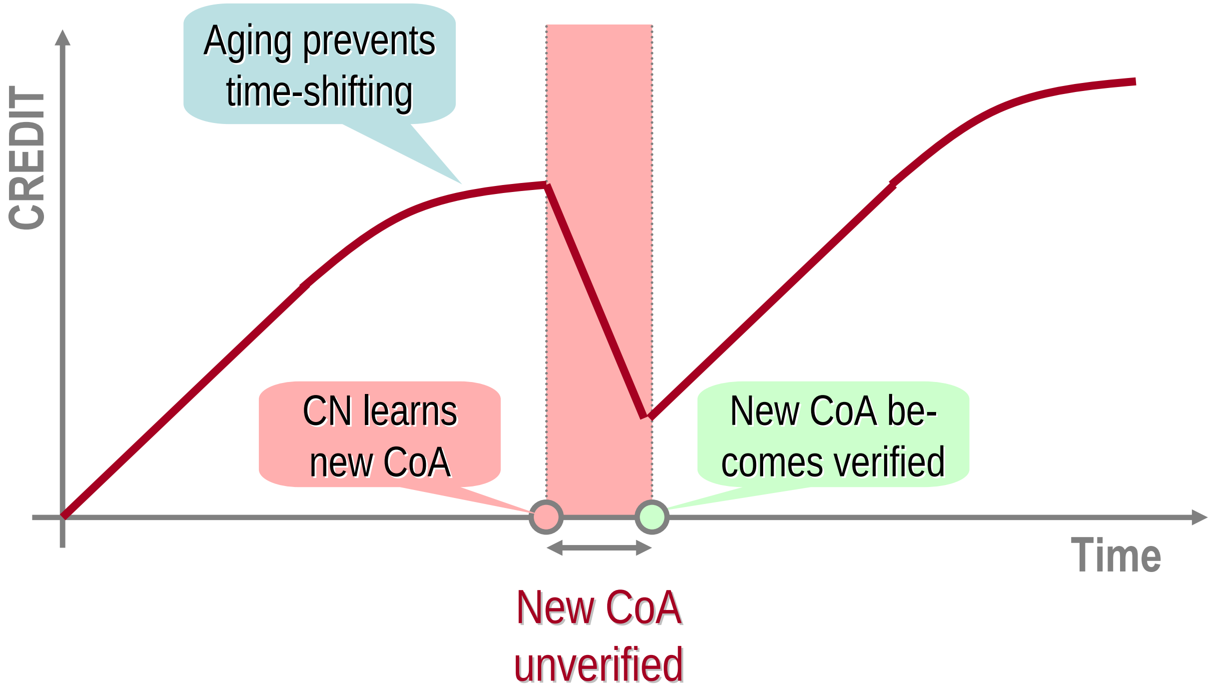
Direct bidirectional comm. while new CoA unverified



Credit-Based Authorization: An Example

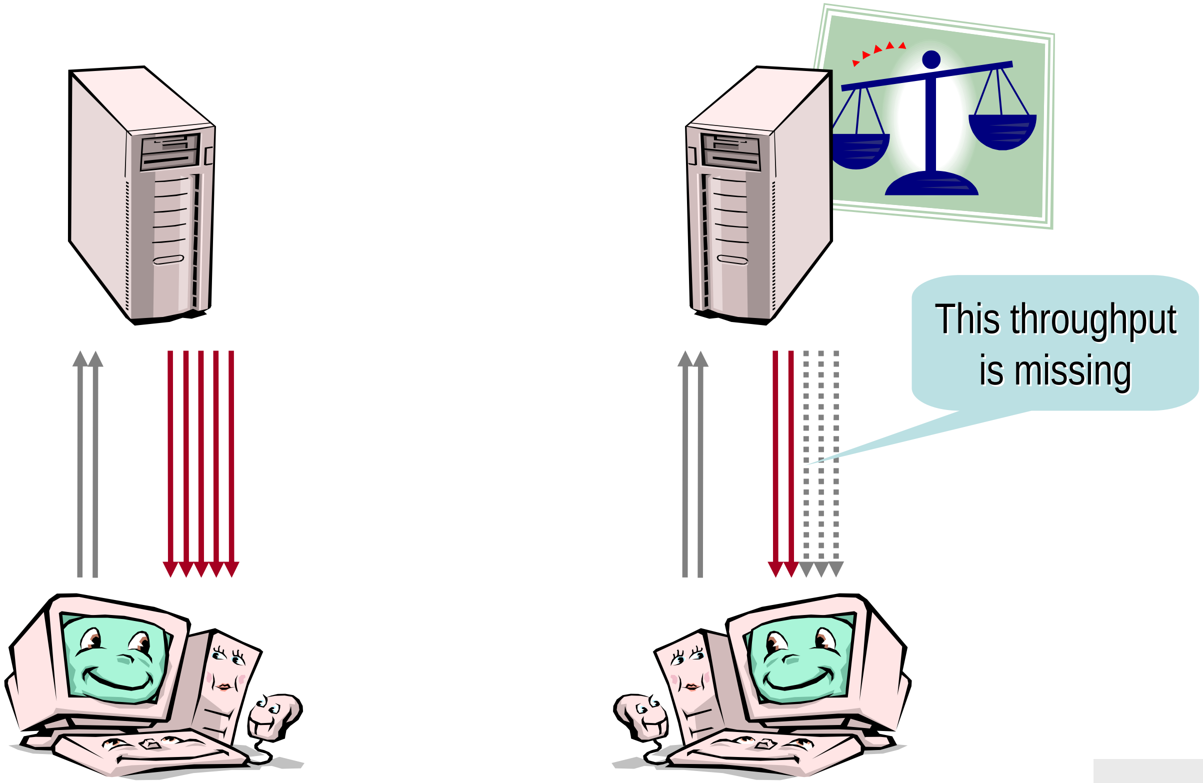


Credit-Based Authorization: An Example (2)



Supporting Asymmetric Traffic

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



While CoA is verified… | **While CoA is <u>un</u>verified…**

Goal

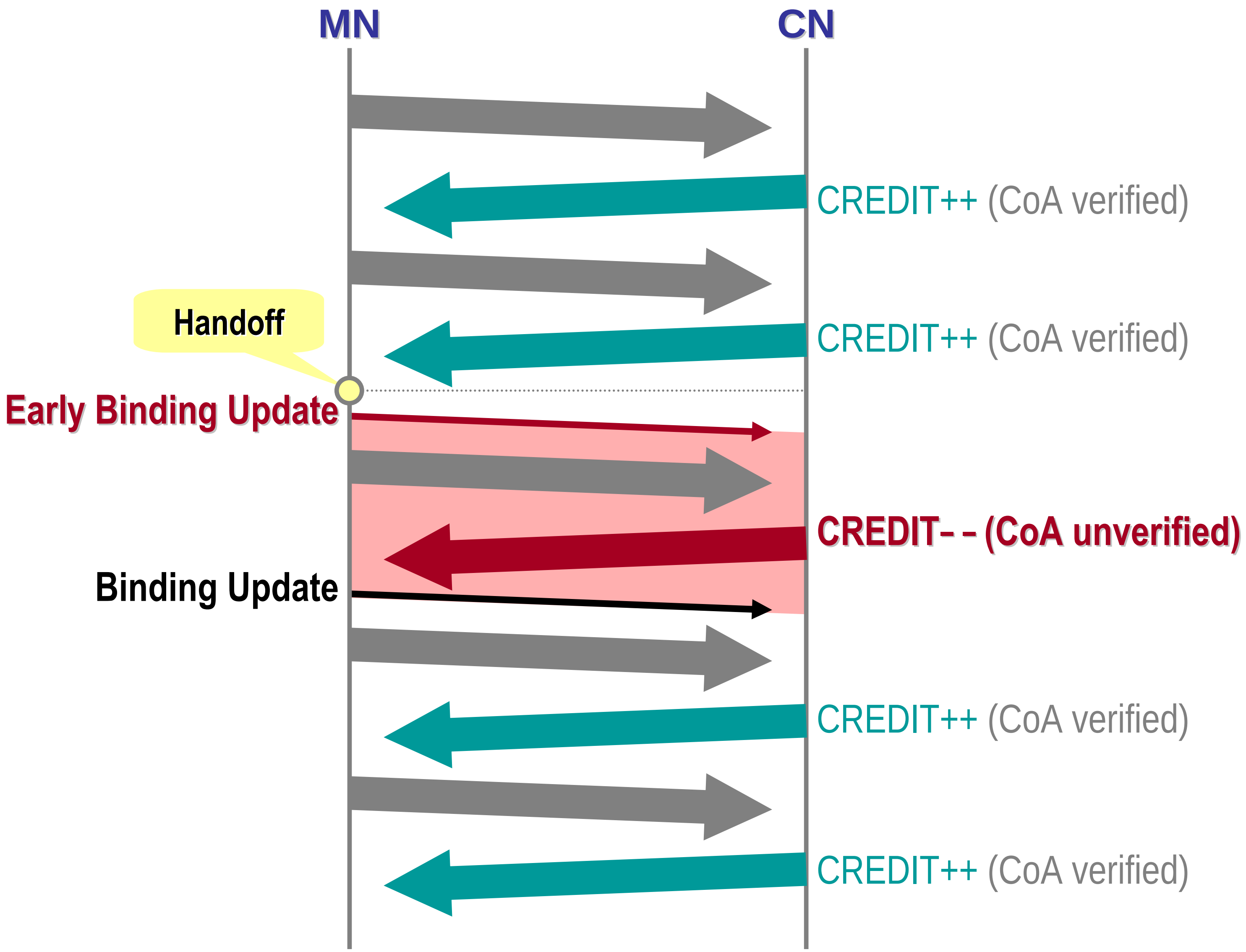
Support applications with asymmetric traffic, too

Supporting Asymmetric Traffic (2)

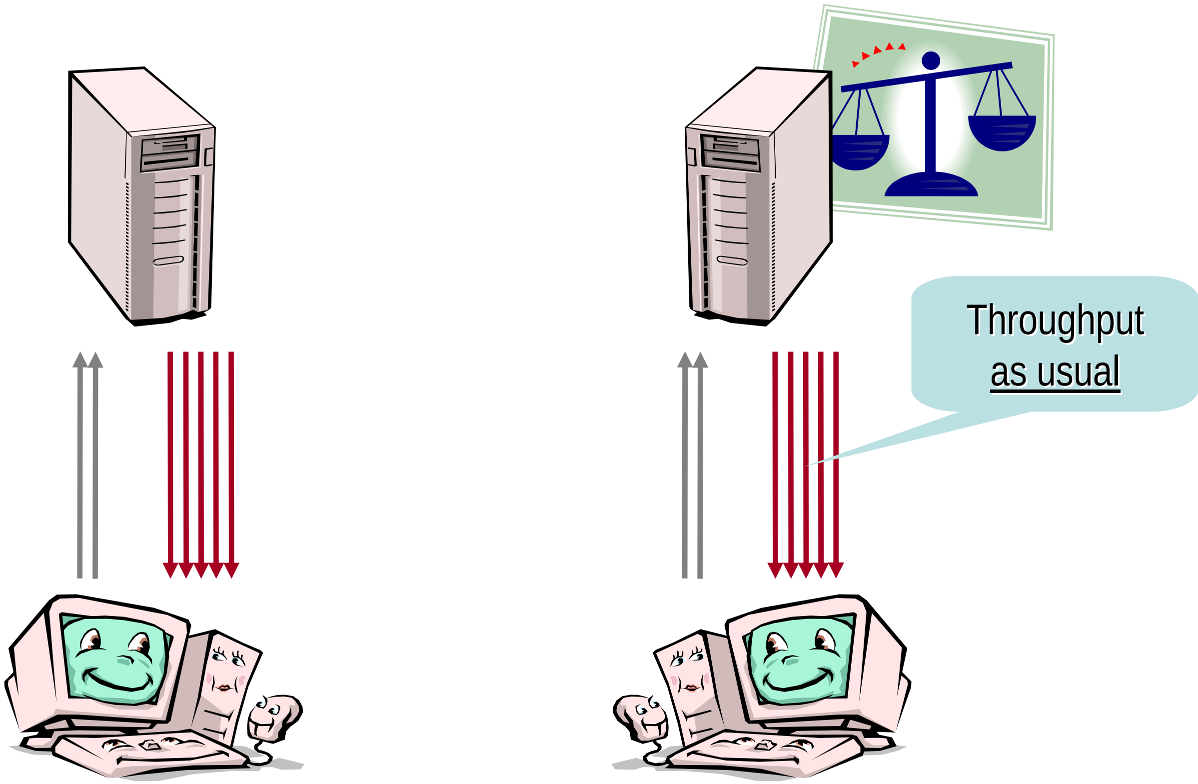
- If we can give a MN credit for packets that it sends…
- …then we could also give the MN **credit for packet reception**
- The MN spends **comparable resources**

  on receiving packets as on sending packets

Supporting Asymmetric Traffic (3)



Supporting Asymmetric Traffic (4)

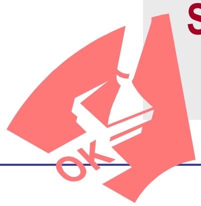


While CoA is verified…

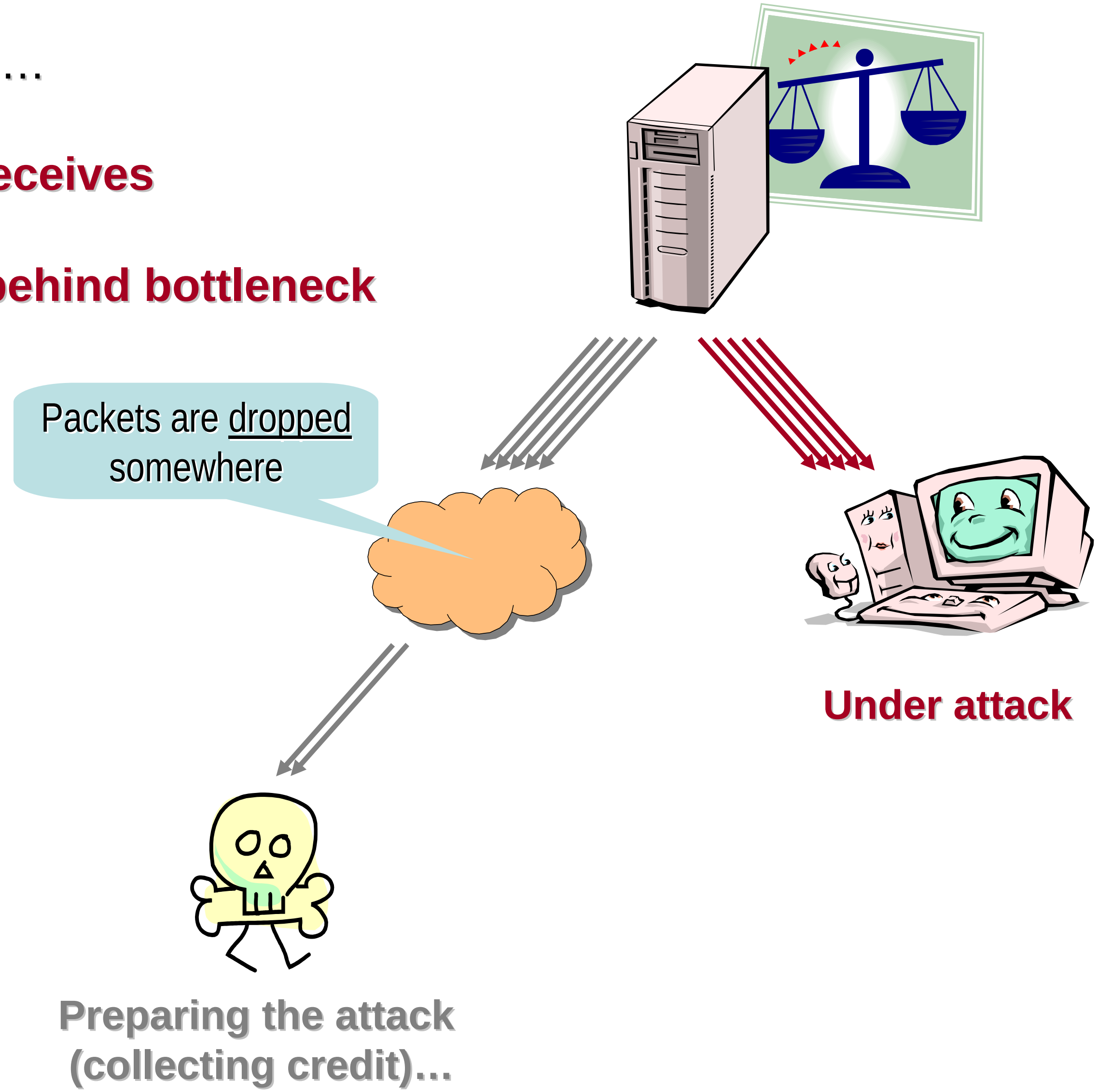
While CoA is <u>un</u>verified…

Goal

Support applications with asymmetric traffic, too



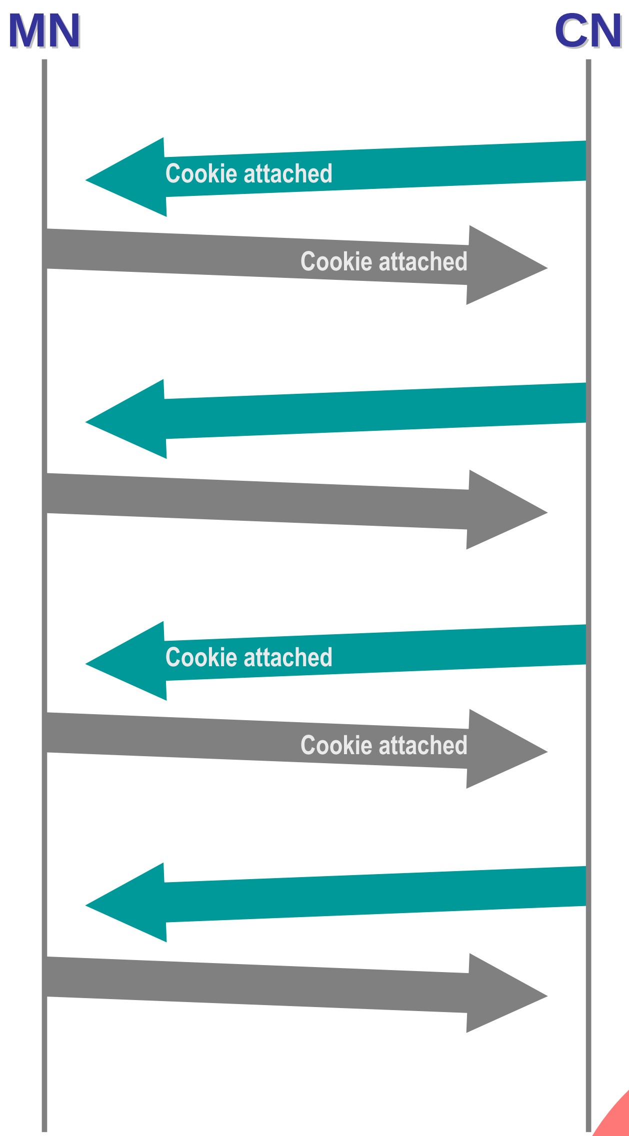
- CN knows what it **sends**…
- …but not what the MN **receives**
- An attacker may locate **behind bottleneck**



Goal

Credit received packets, not sent packets

Care-of Address Spot Checks

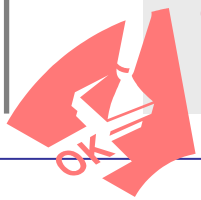


CREDIT ~

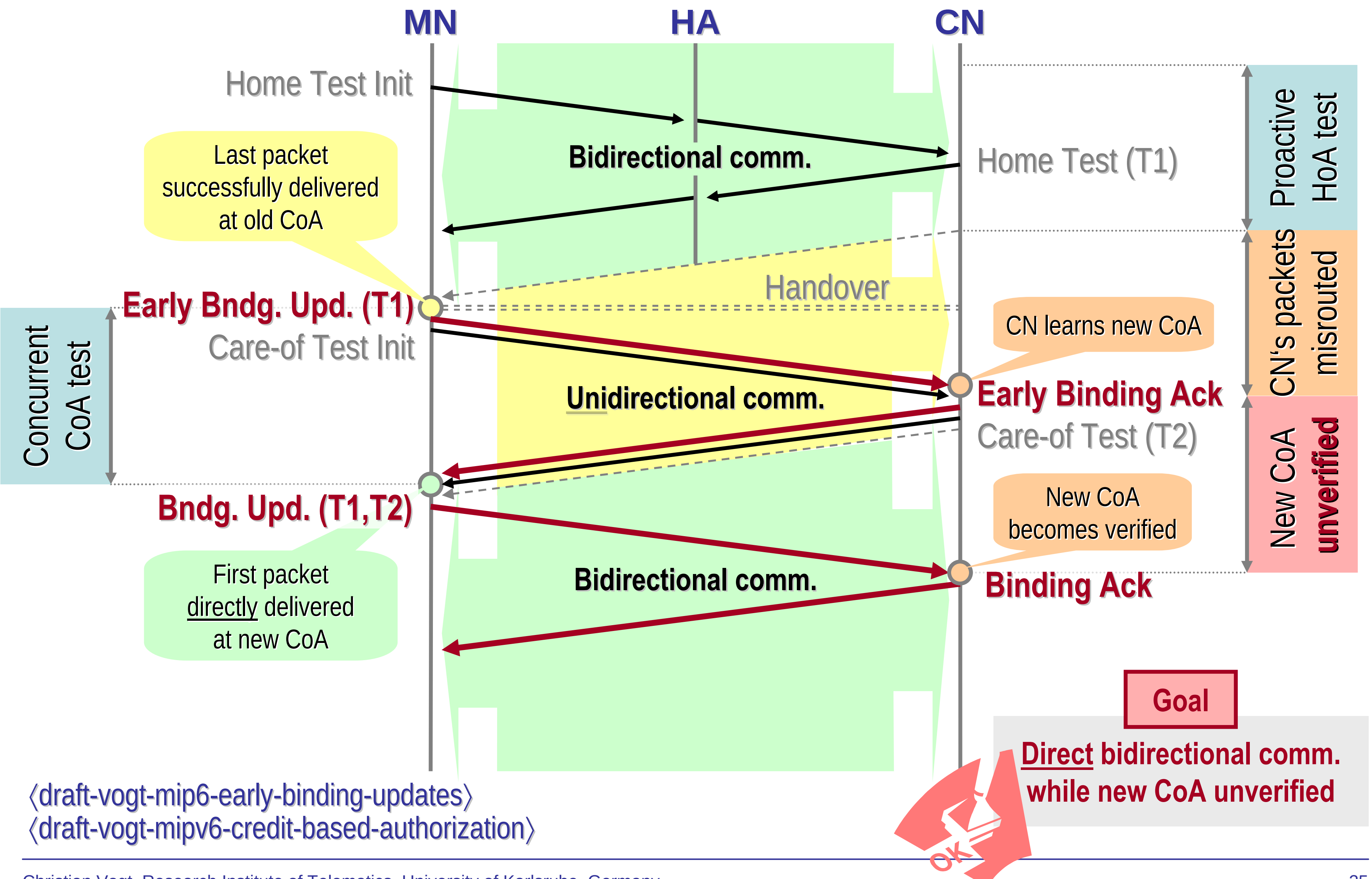
$$\frac{\text{\# Cookies returned}}{\text{\# Cookies sent}}$$

Goal

Credit <u>received</u> packets, not sent packets



The Big Picture



⟨draft-vogt-mip6-early-binding-updates⟩
⟨draft-vogt-mipv6-credit-based-authorization⟩

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 (w/o Spot Checks) 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**

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 (**Spot Checks**)