

Status update
New drafts
Implementation
Experimentation results

Early Binding Updates and Credit-Based Authorization

– A Status Update

Christian Vogt, chvogt@tm.uka.de

- Mobile IPv6 Route Optimization uses return-routability procedure to authorize binding between...
 - Home address == Who I am
 - C/o address == Where I am
- Idea: Verify MN's reachability at
 - home address for authentication
 - c/o address for binding authorization
- Handoff delays btw. 3 and 4 RTT
 - depends on degree of parallelism that implementation use
- Reduce this!

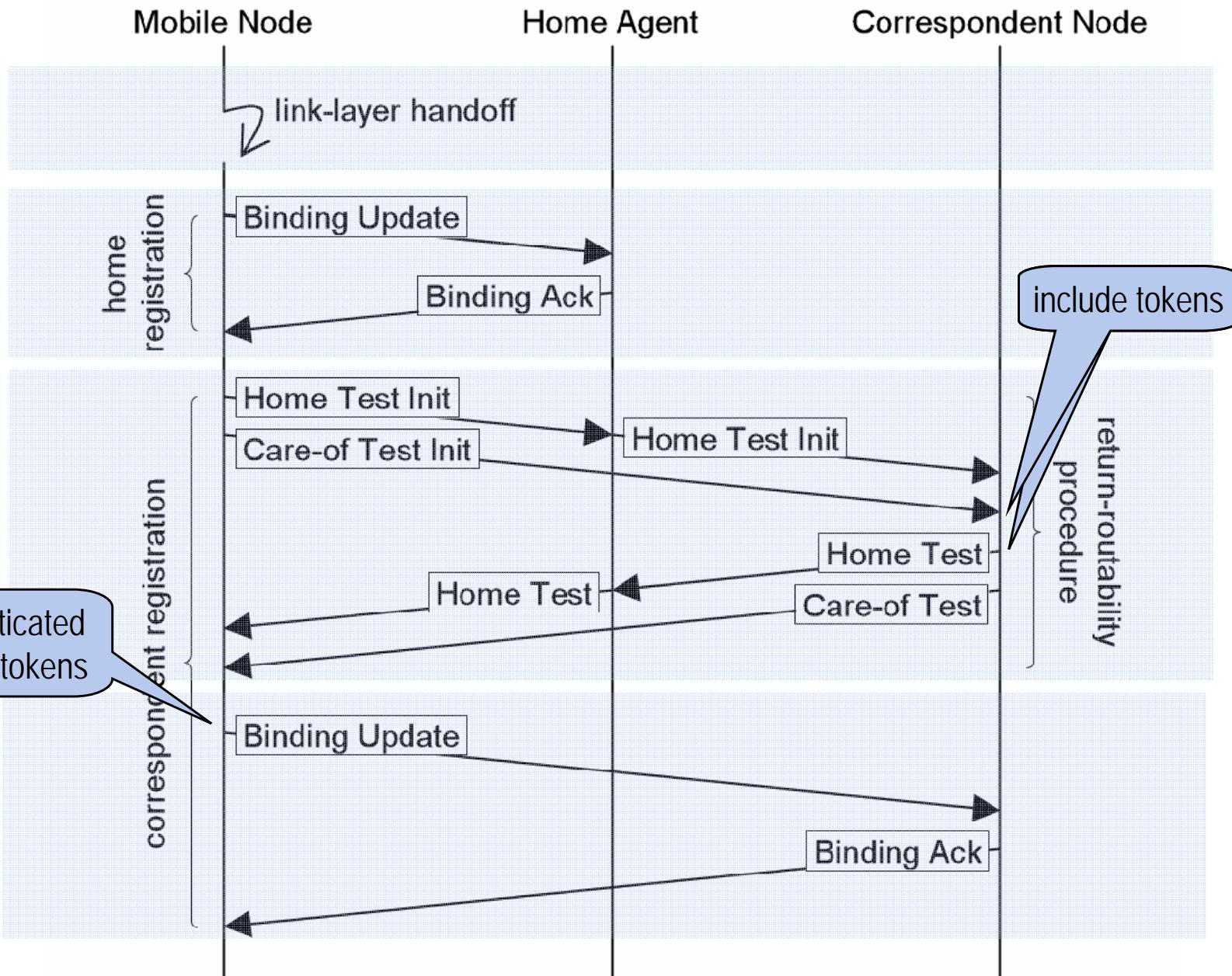
Early Binding Updates

- Modification to Mobile IPv6 binding-update procedure
 - Proactivity
 - Concurrency
 - Higher degree of parallelism
- Reduces handoff latency
 - to 1 RTT for reactive handoffs
 - to 0~1 RTT for proactive handoffs

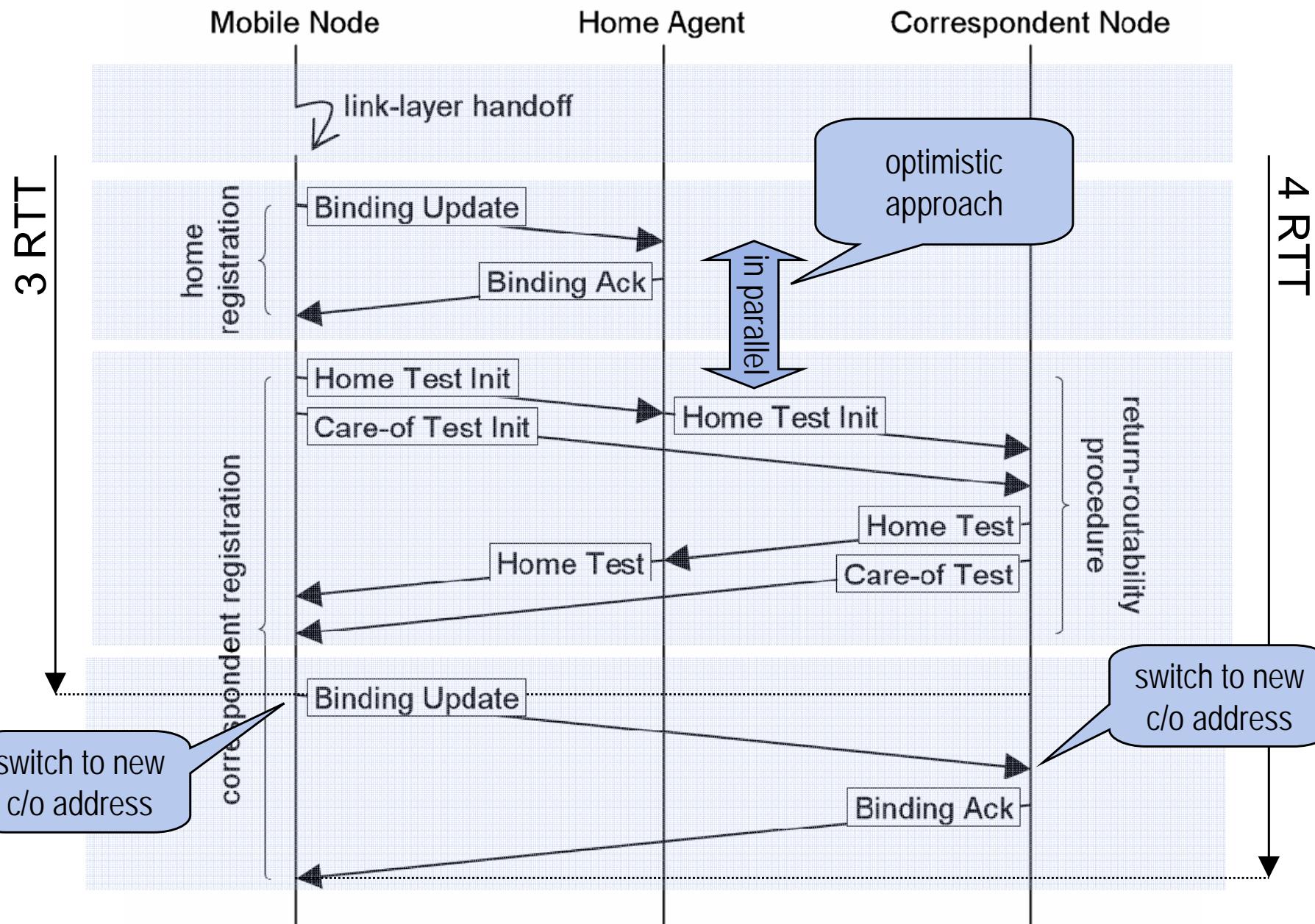
Credit-Based Authorization

- Strategy followed by CN
- Determines data that CN can securely send to MN before MN's reachability at new c/o address verified

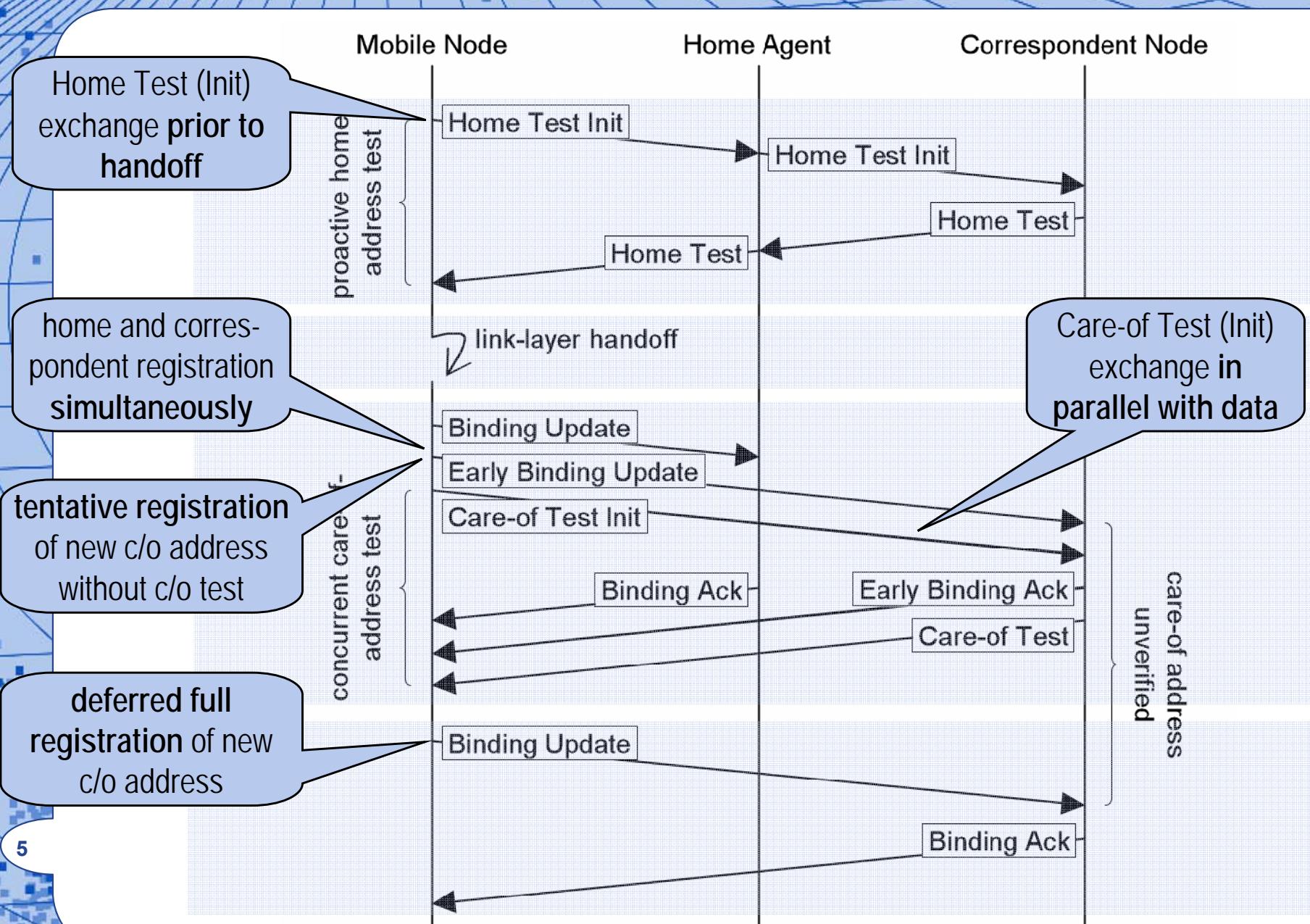
Standard Mobile IPv6



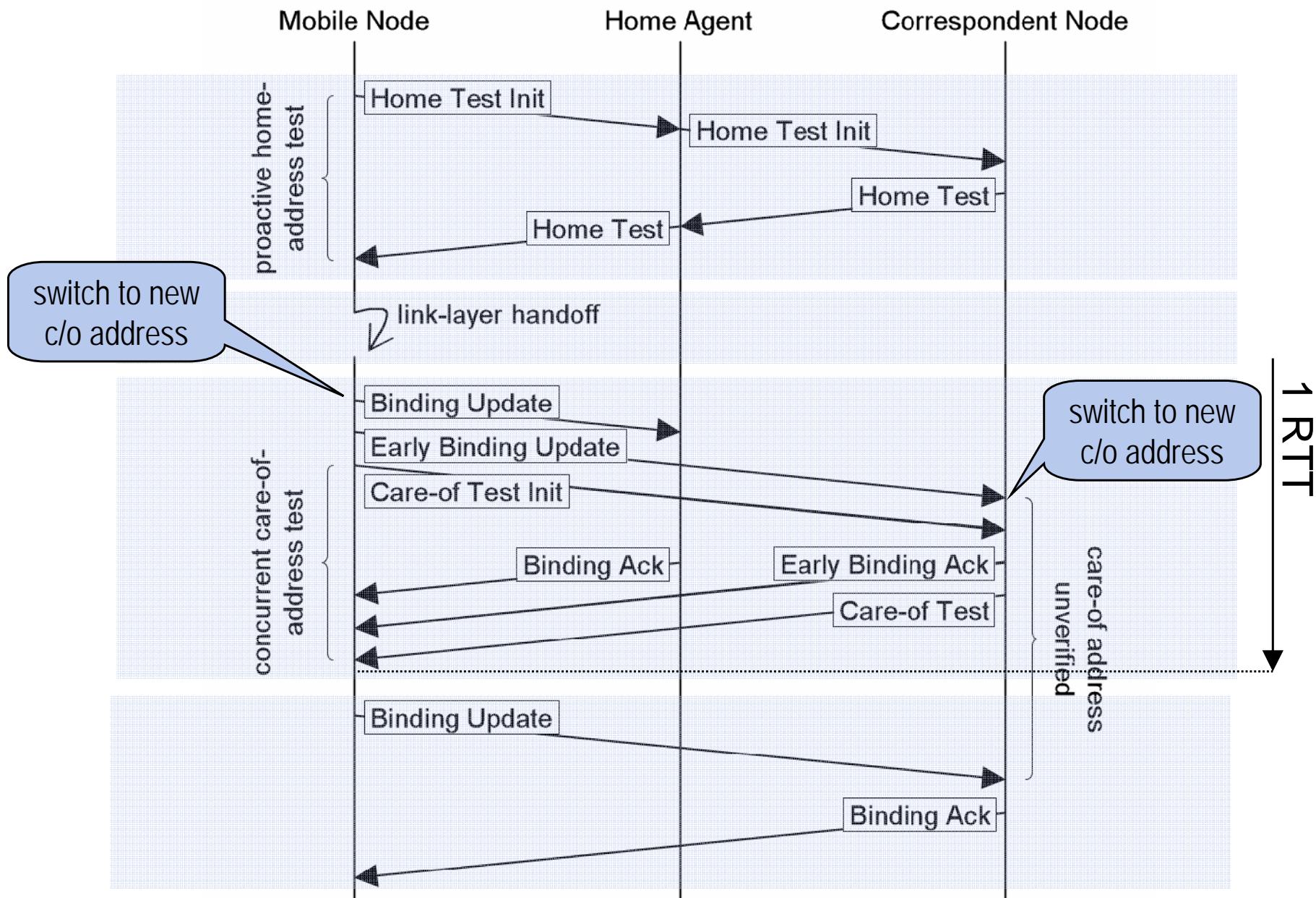
Standard Mobile IPv6



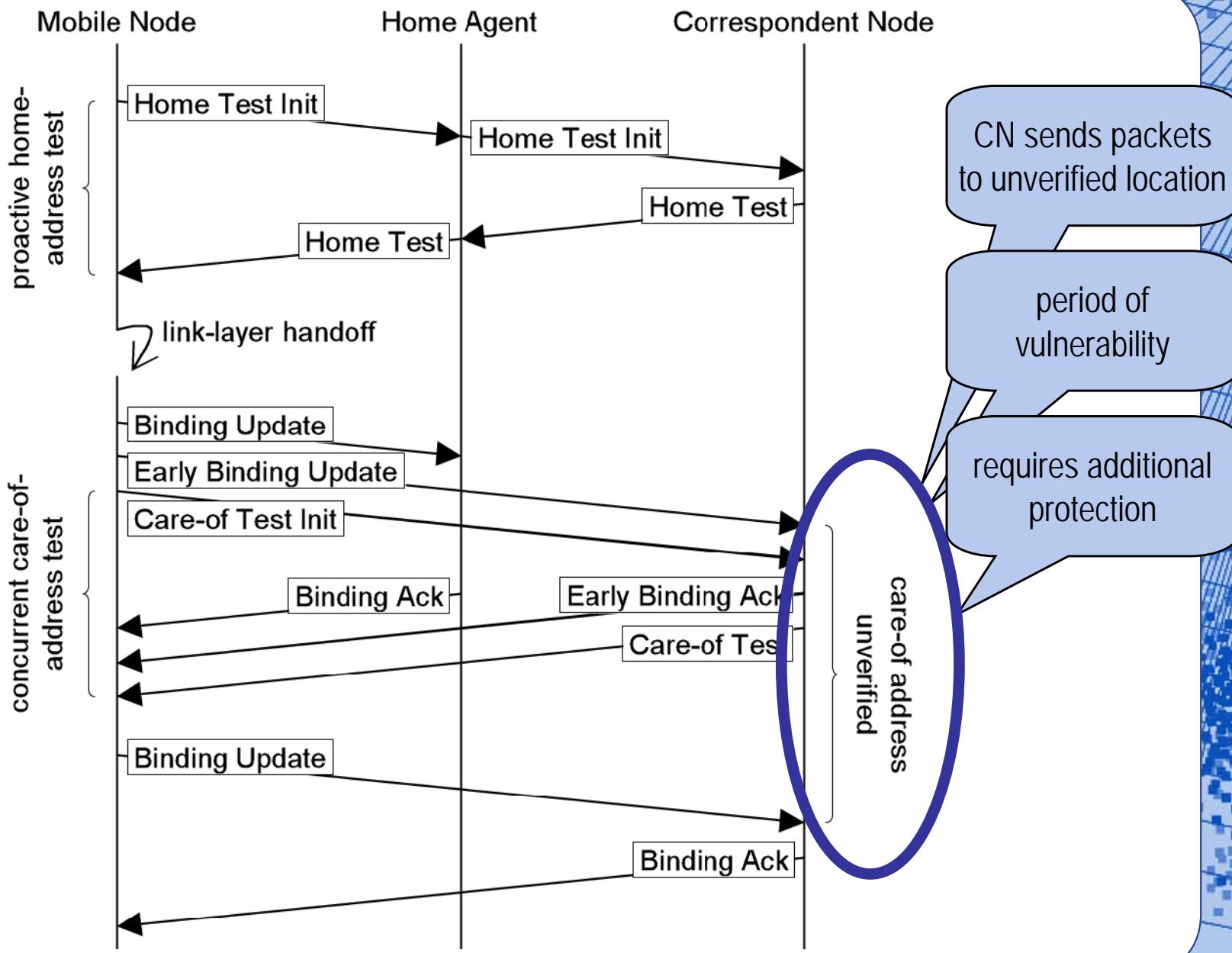
Mobile IPv6 + Early Binding Updates



Mobile IPv6 + Early Binding Updates



However...



Attacker could...

- establish a higher-layer connection (e.g., download)
- redirect packets to victim
- spoof TCP acknowledgments

Amplification!

- CN generates large data packets
- Attacker sends small ACKs

Without amplification...

- Flooding no more effective than direct flooding
- Direct flooding always possible

Idea

- Limit packets sent to unverified c/o address
so as to not cause amplification

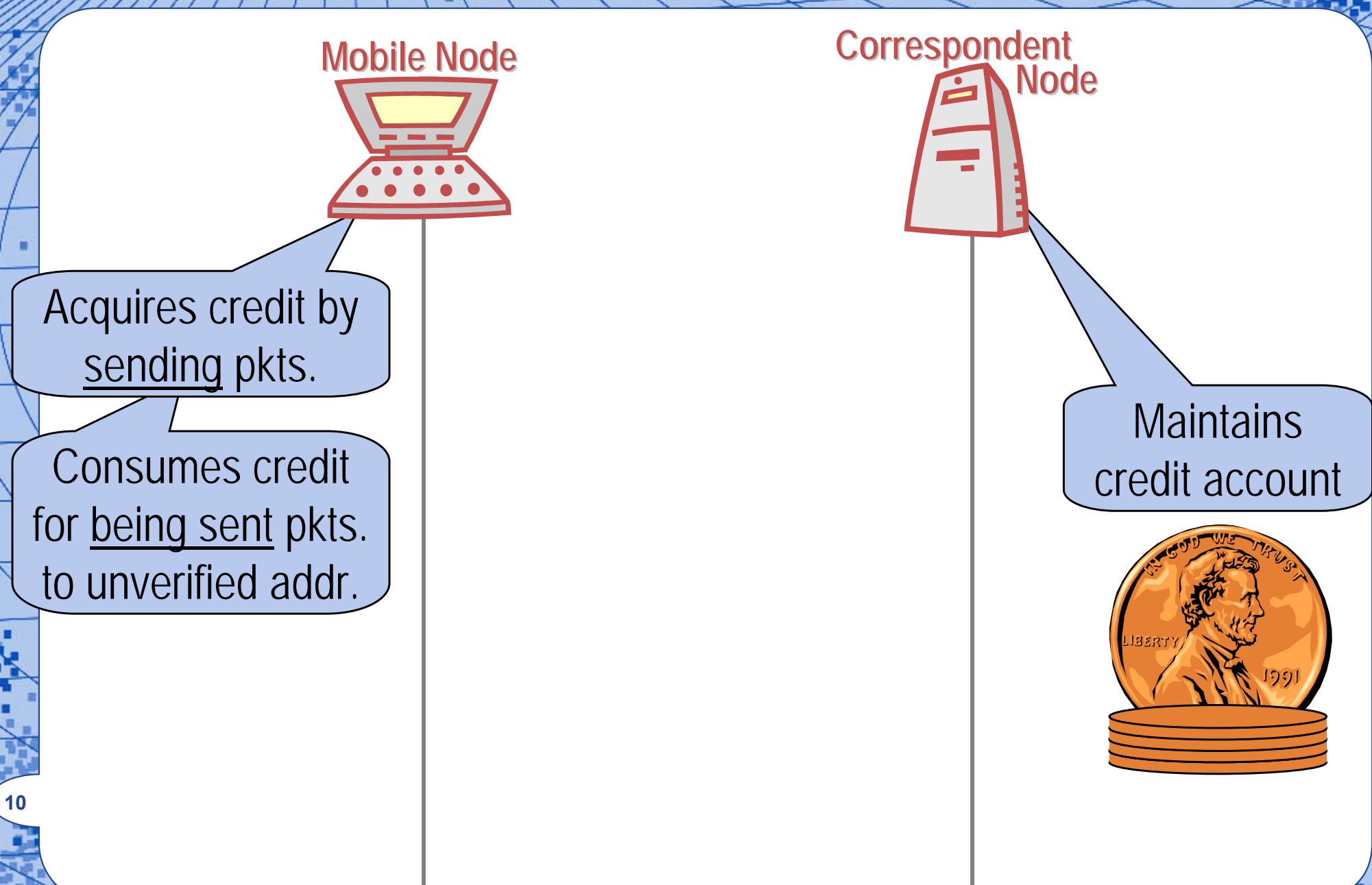
Solution

- Count the bytes received from MN/attacker
- Send no more bytes to unverified c/o address

Credit-Based Authorization

- Byte counter == "Credit account"

Credit-Based Authorization

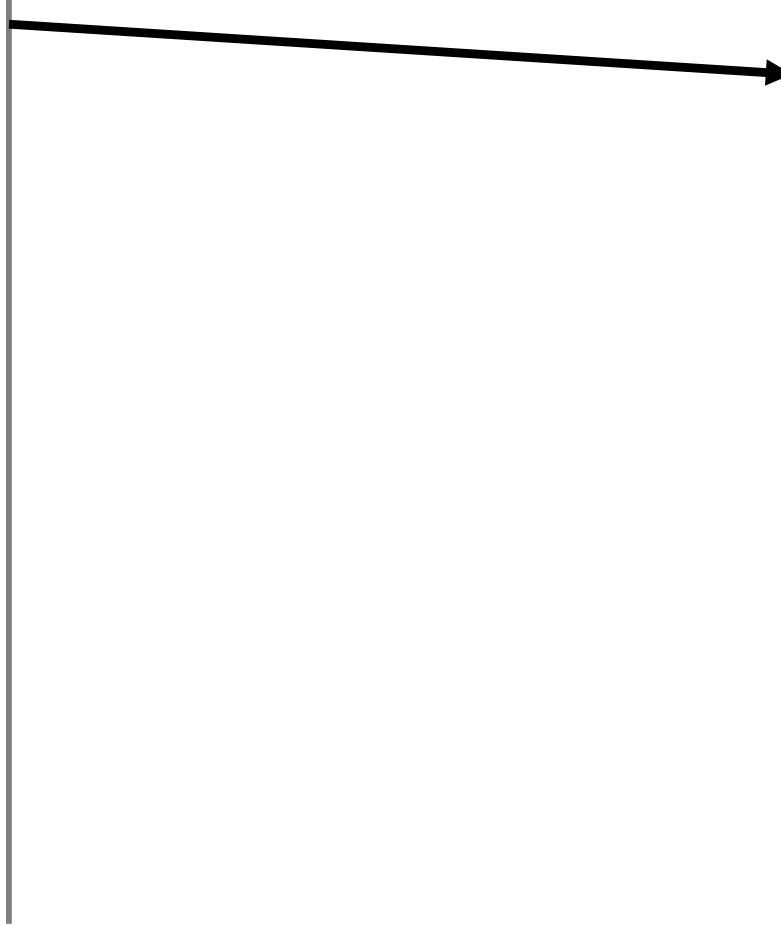
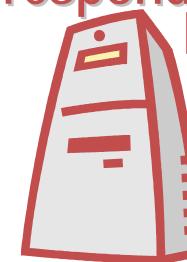


Credit-Based Authorization

Mobile Node



Correspondent Node



Credit-Based Authorization

Mobile Node



Correspondent
Node

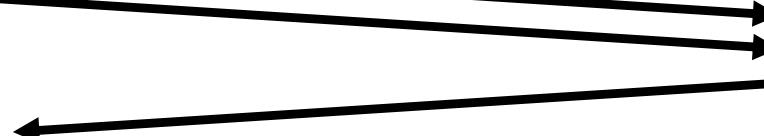


Credit-Based Authorization

Mobile Node



Correspondent Node

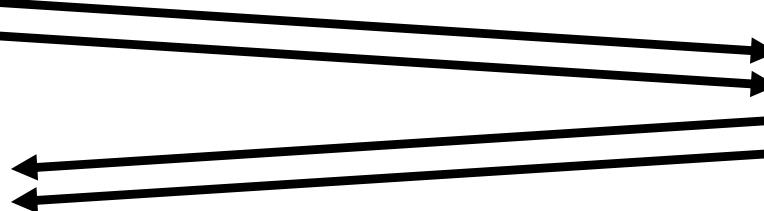


Credit-Based Authorization

Mobile Node



Correspondent Node

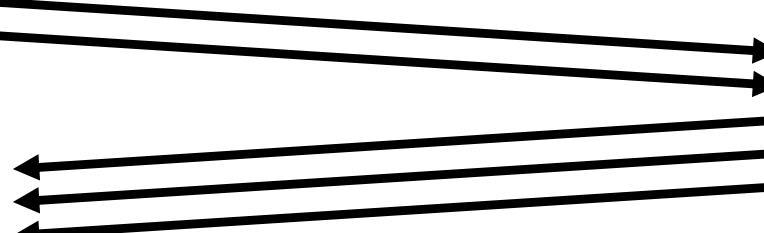


Credit-Based Authorization

Mobile Node



Correspondent Node

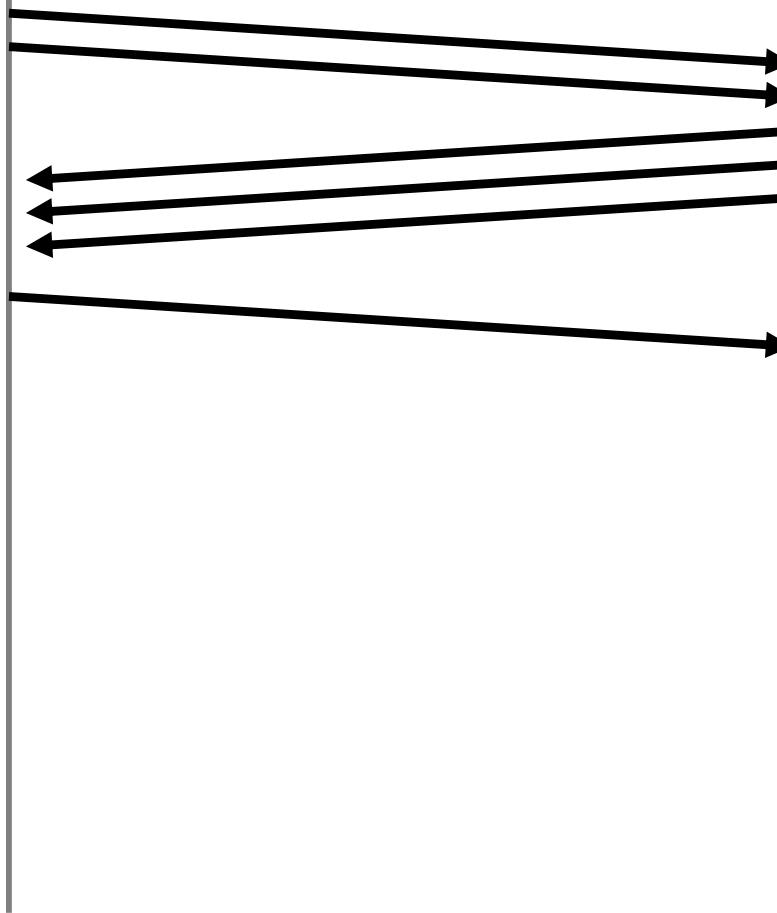


Credit-Based Authorization

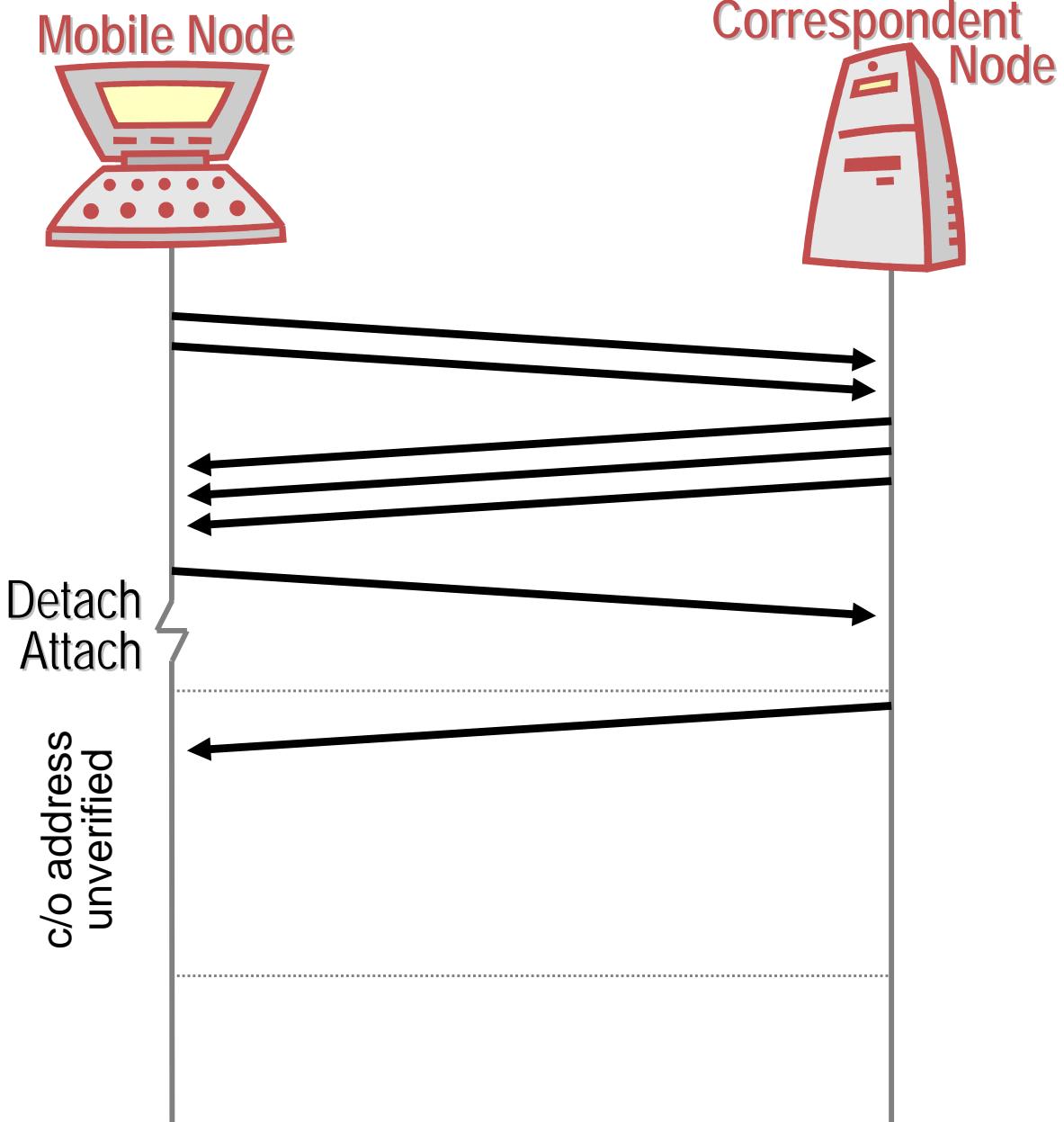
Mobile Node



Correspondent Node



Credit-Based Authorization



Credit-Based Authorization

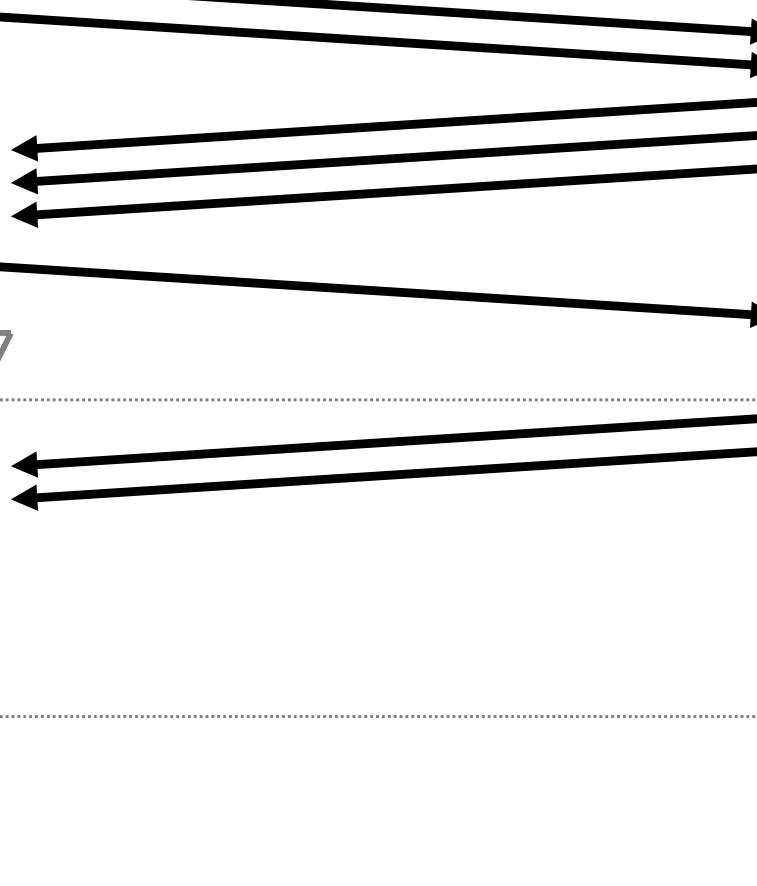
Mobile Node



Correspondent
Node



c/o address
unverified



Credit-Based Authorization

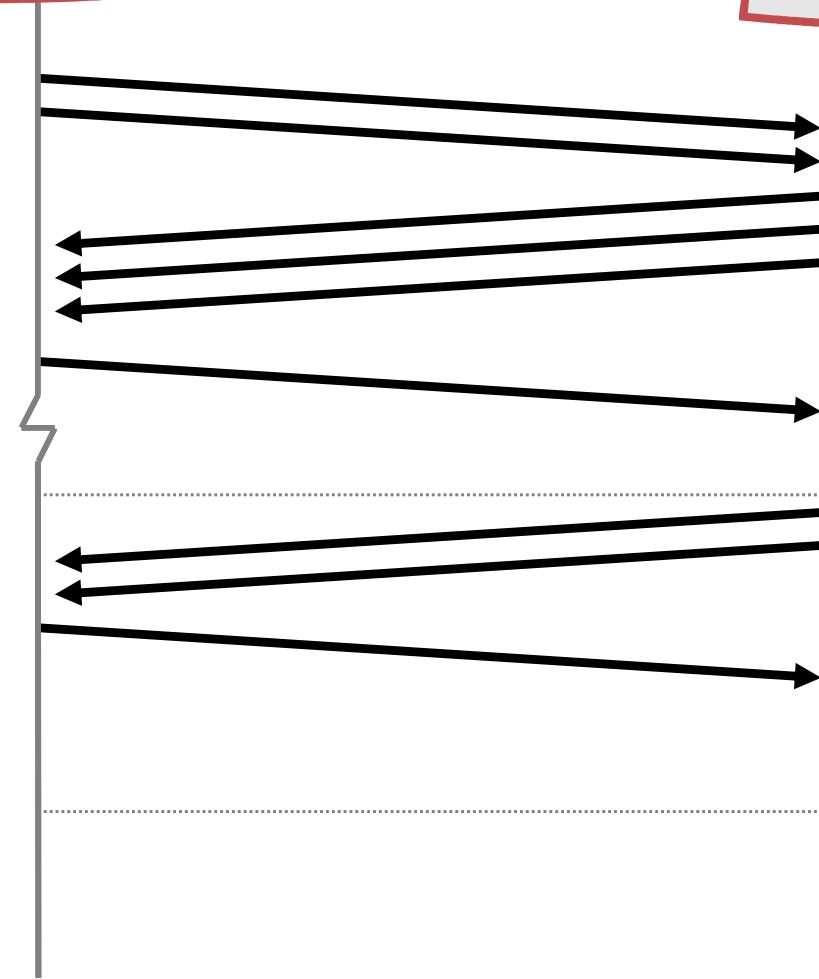
Mobile Node



Correspondent Node

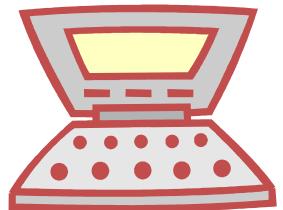


c/o address
unverified



Credit-Based Authorization

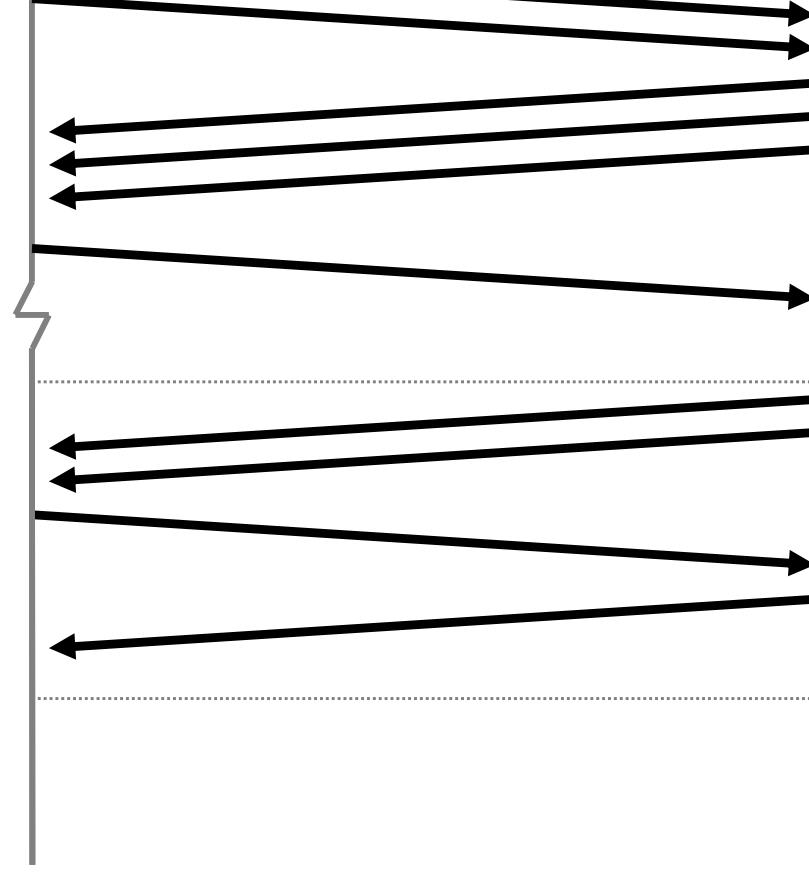
Mobile Node



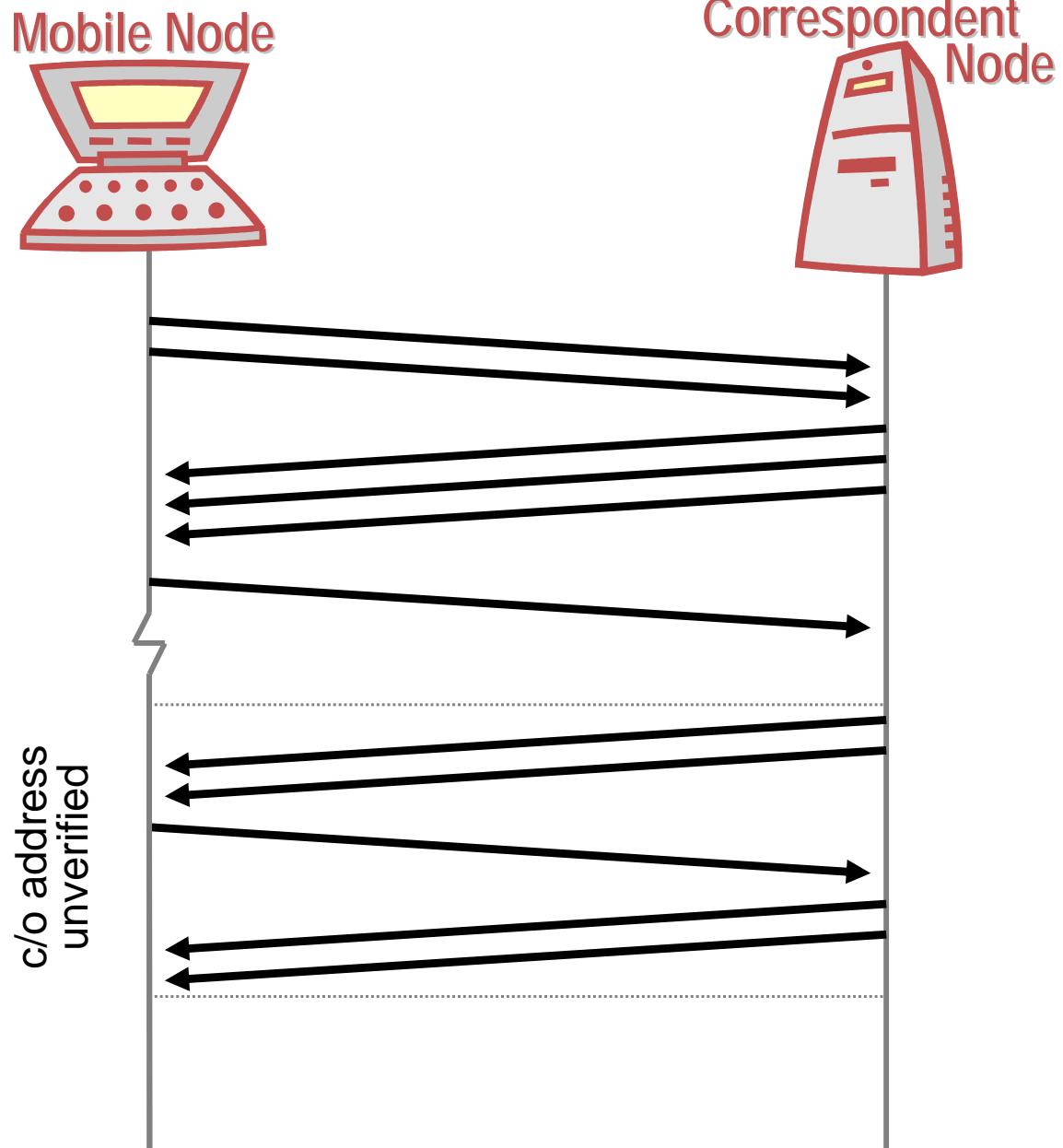
Correspondent Node



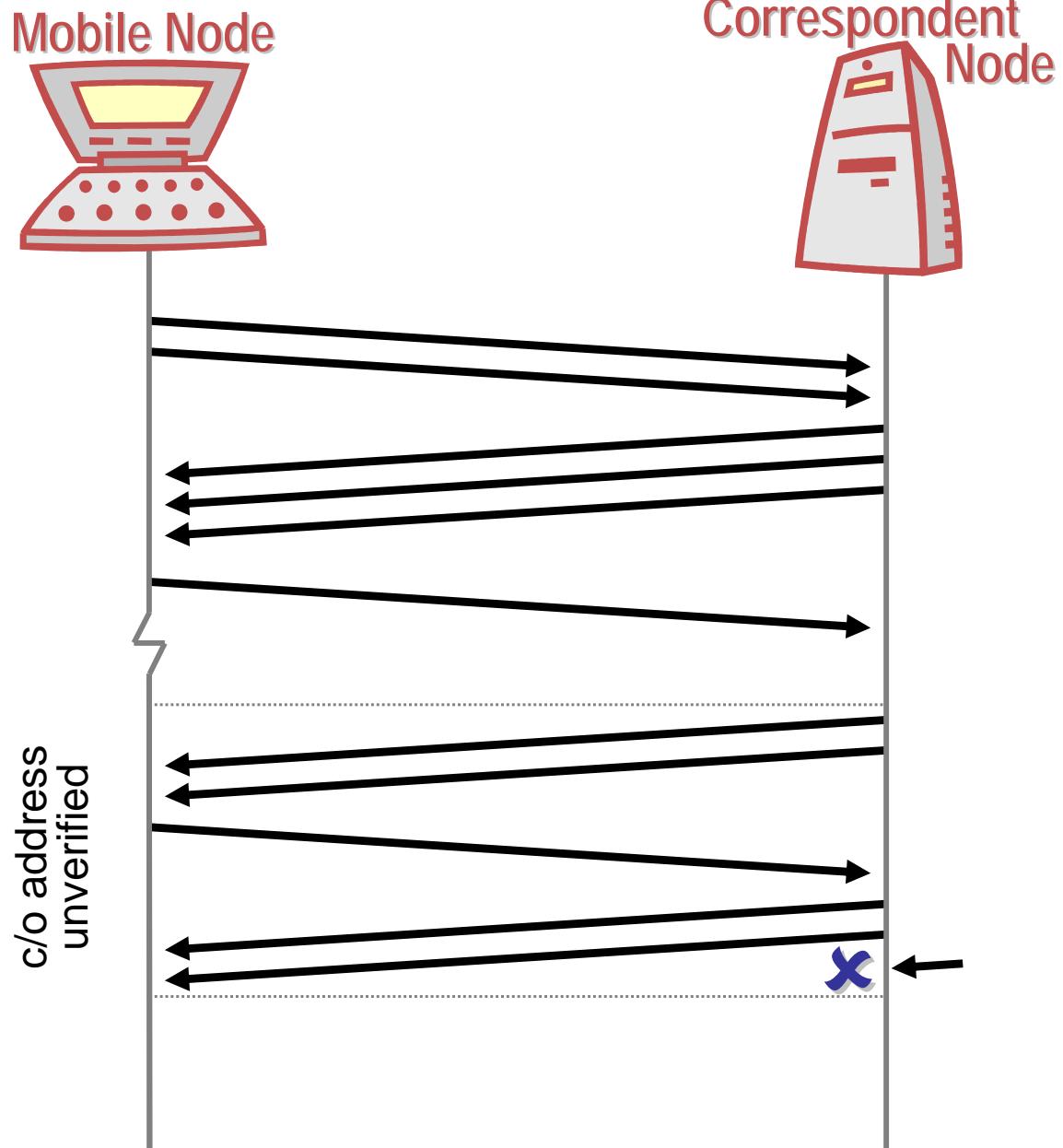
c/o address
unverified



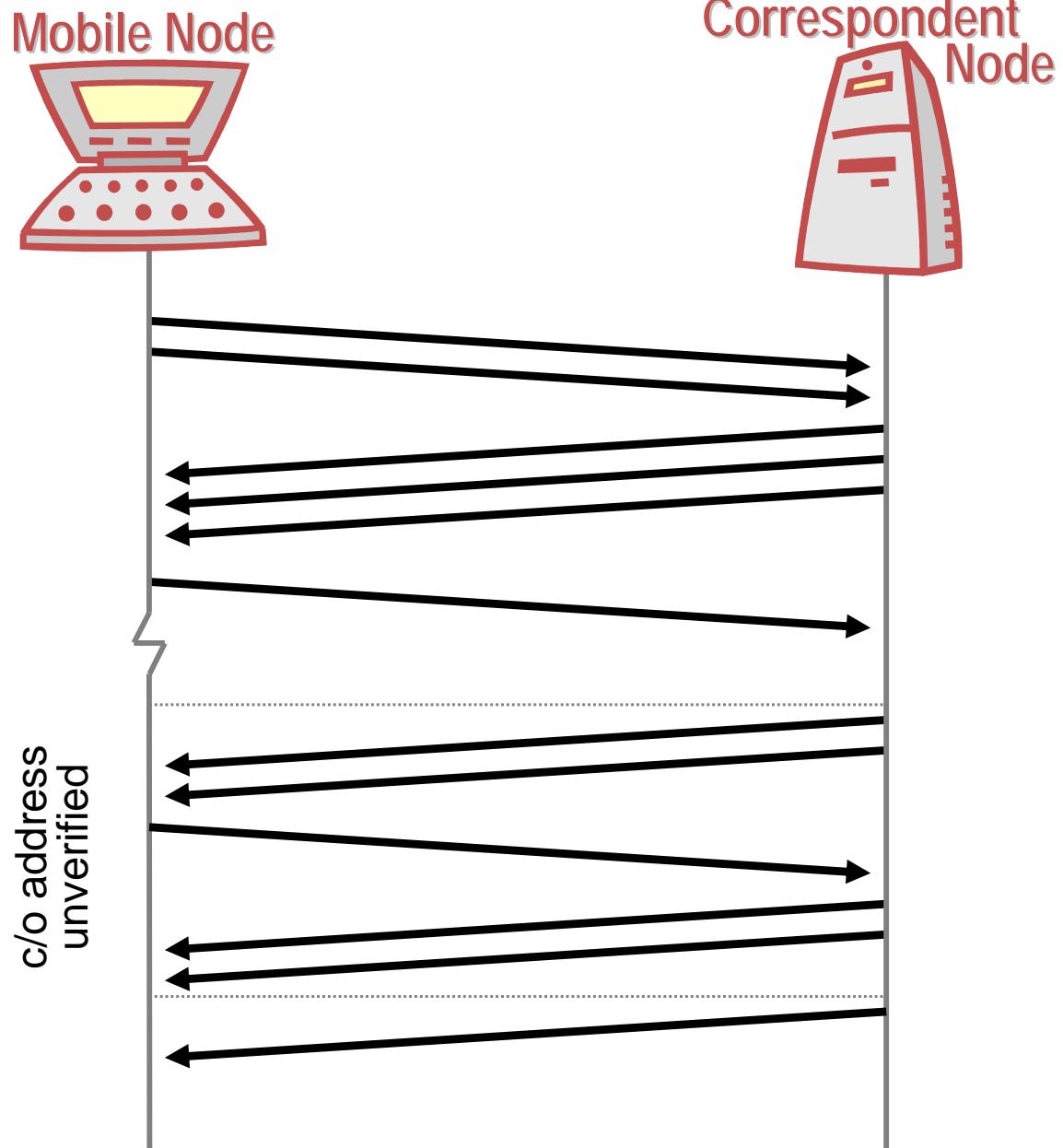
Credit-Based Authorization



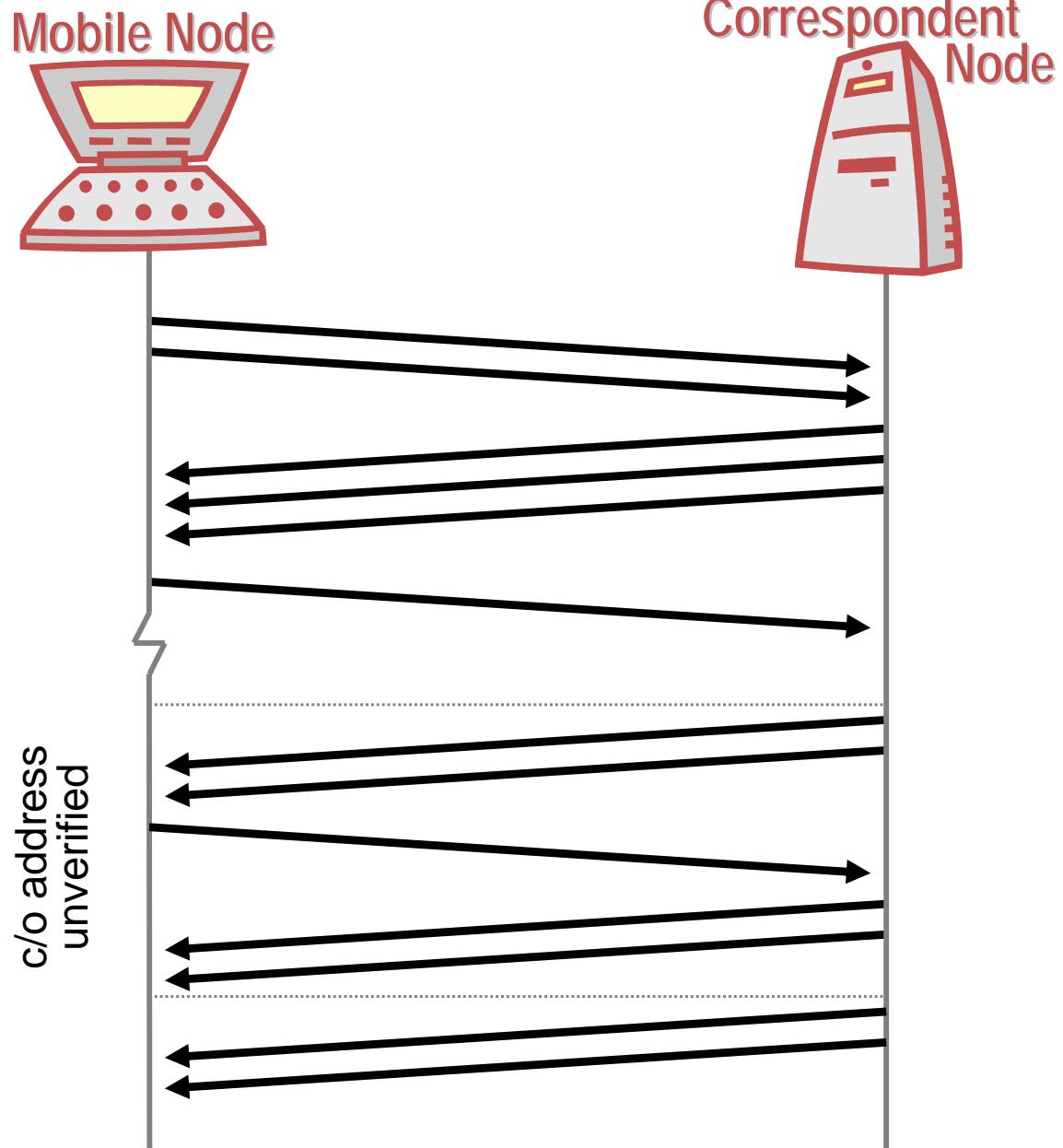
Credit-Based Authorization



Credit-Based Authorization



Credit-Based Authorization



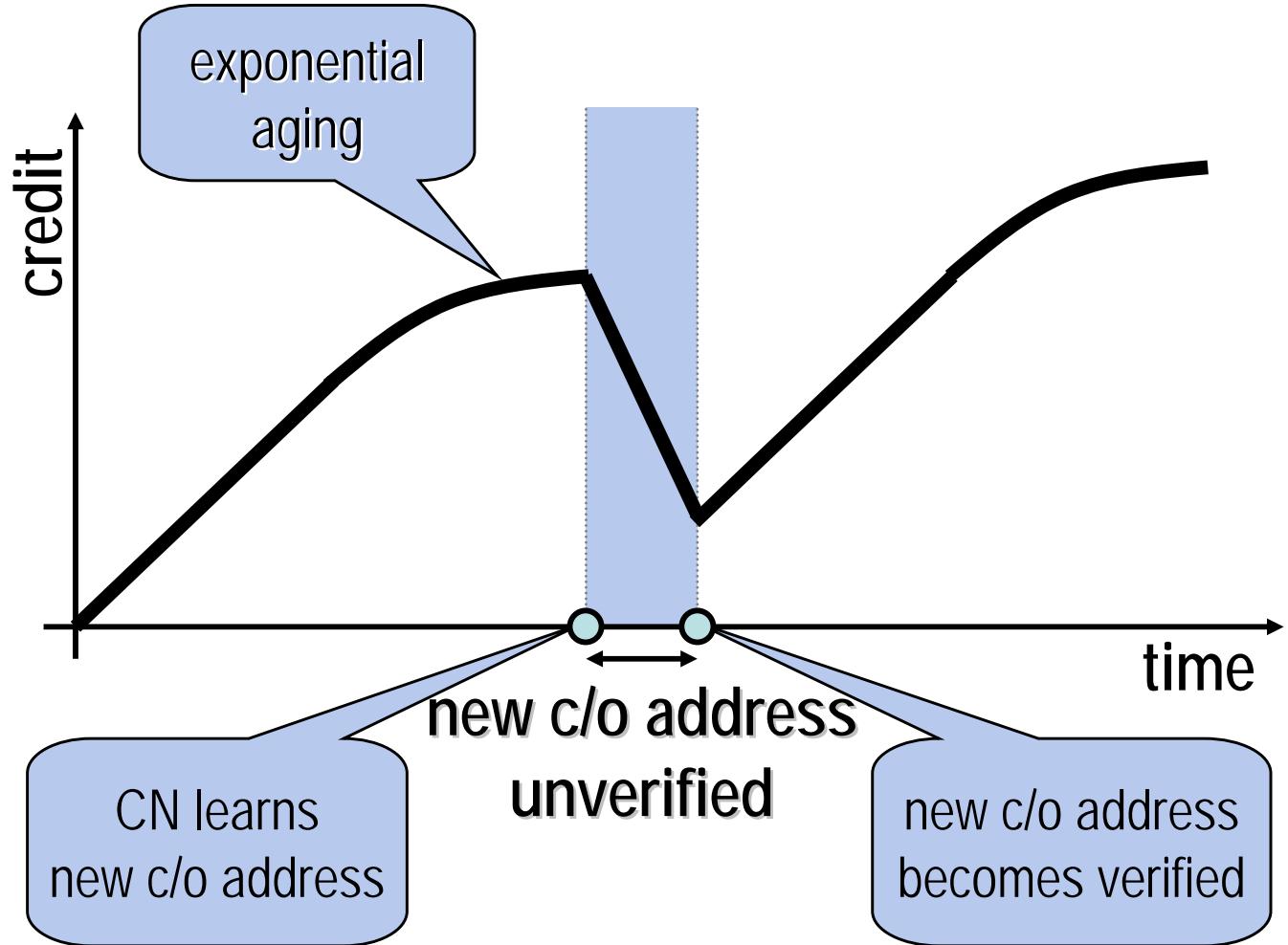
Credit account allows an attacker to...

- accumulate credit over a long time
- at a slow rate, and
- use this credit all at once

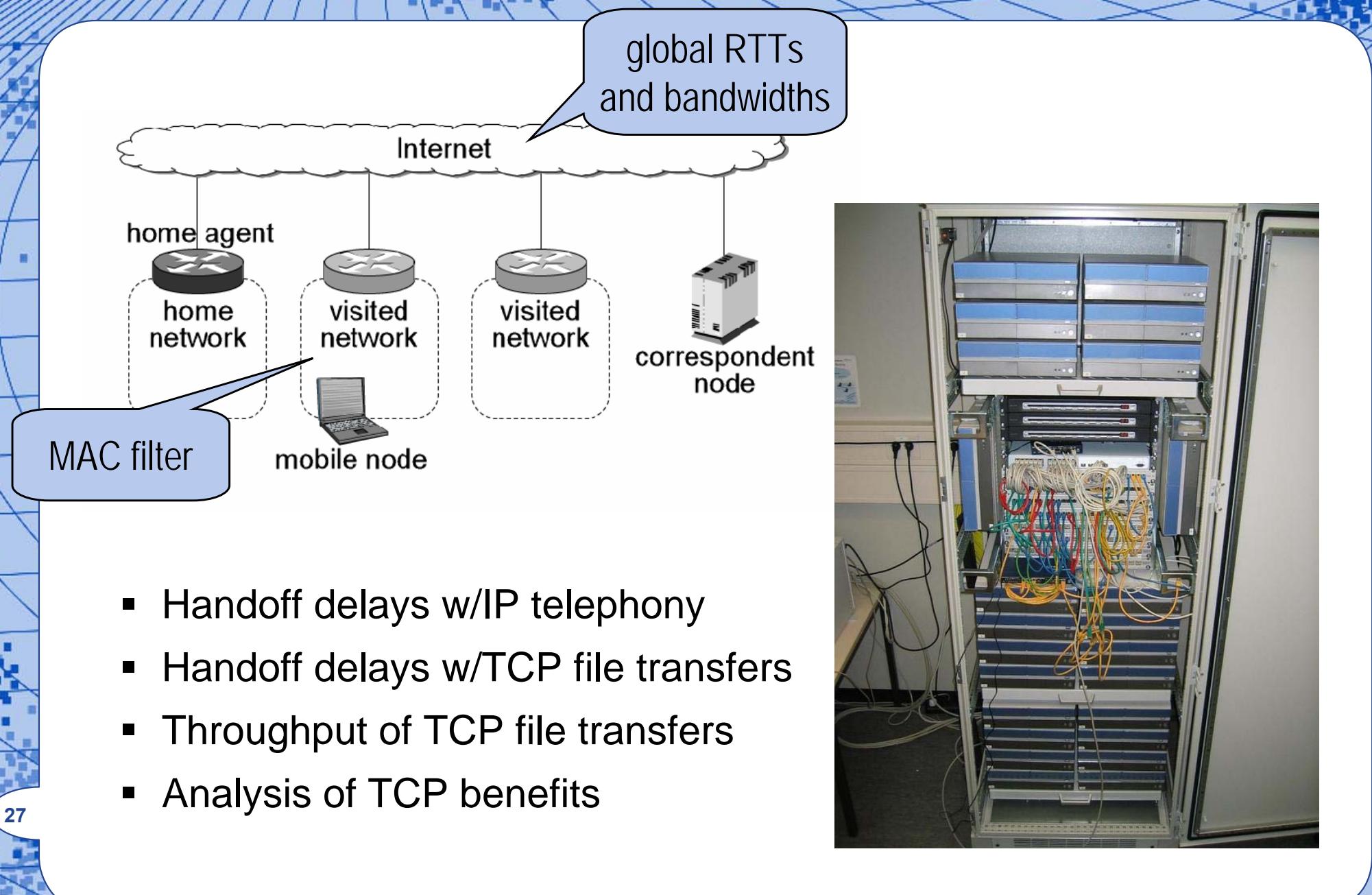
Facilitates large burst of packets from attackers
with low-bandwidth Internet access

Credit aging prevents this

Credit Aging



Experimental Evaluation



Application

- 64 kbps payload
- 10ms chunks
- 164B per packet (IPv6, extensions, UDP, RTP)
- bidirectional

Network

- 200ms round-trip time

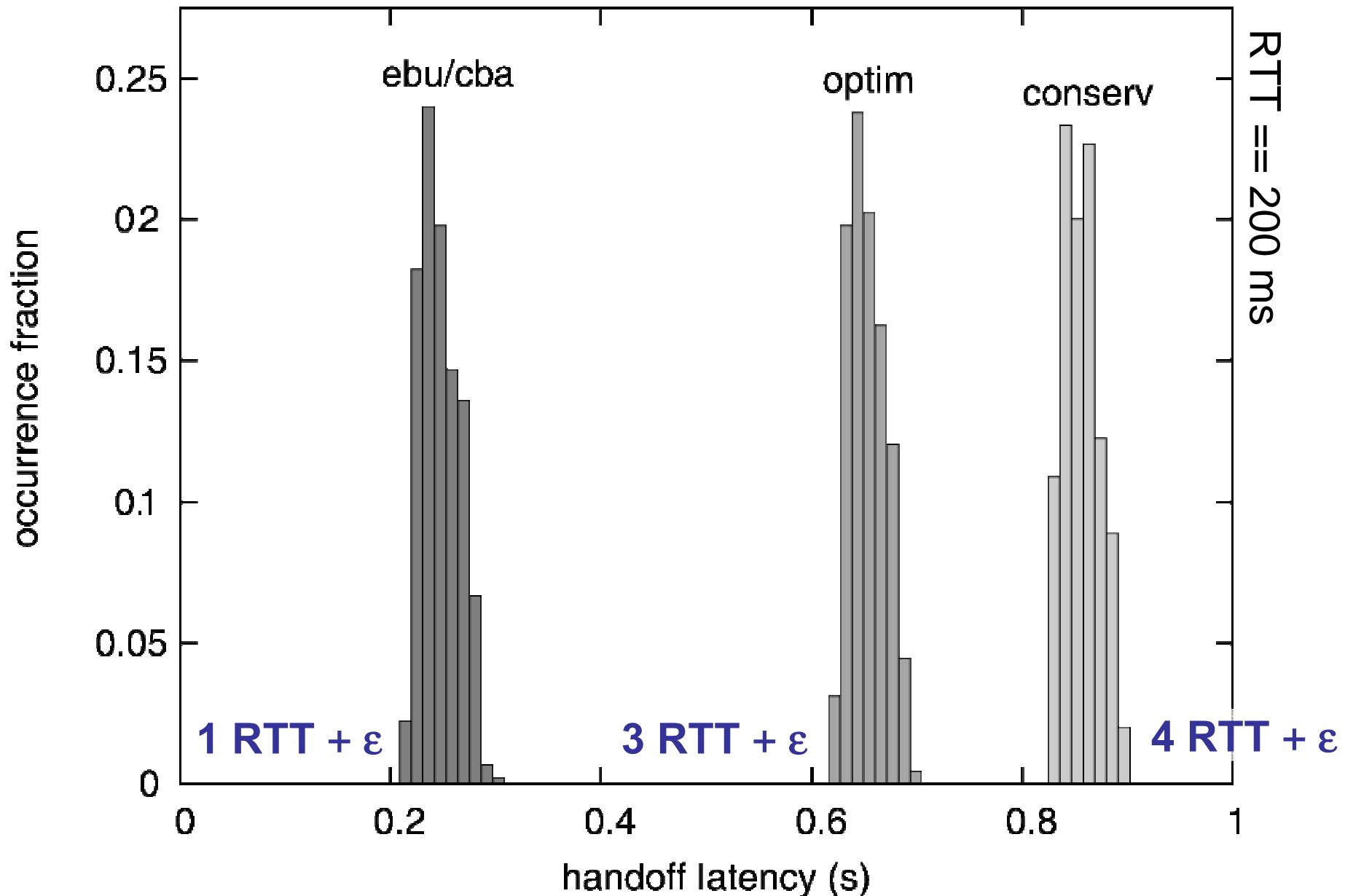
Mobility protocols

- standard (conservative) Mobile IPv6
- optimistic Mobile IPv6
- w/Early Binding Updates and Credit-Based Authorization

Confidence

- 500 handoffs per mobility protocol

Handoff Delay w/IP Telephony



Application

- 60s download (chargen-generated data)
- 1024 kbps bandwidth
- unidirektonal
- TCP Reno

Network

- 40ms to 200ms round-trip time

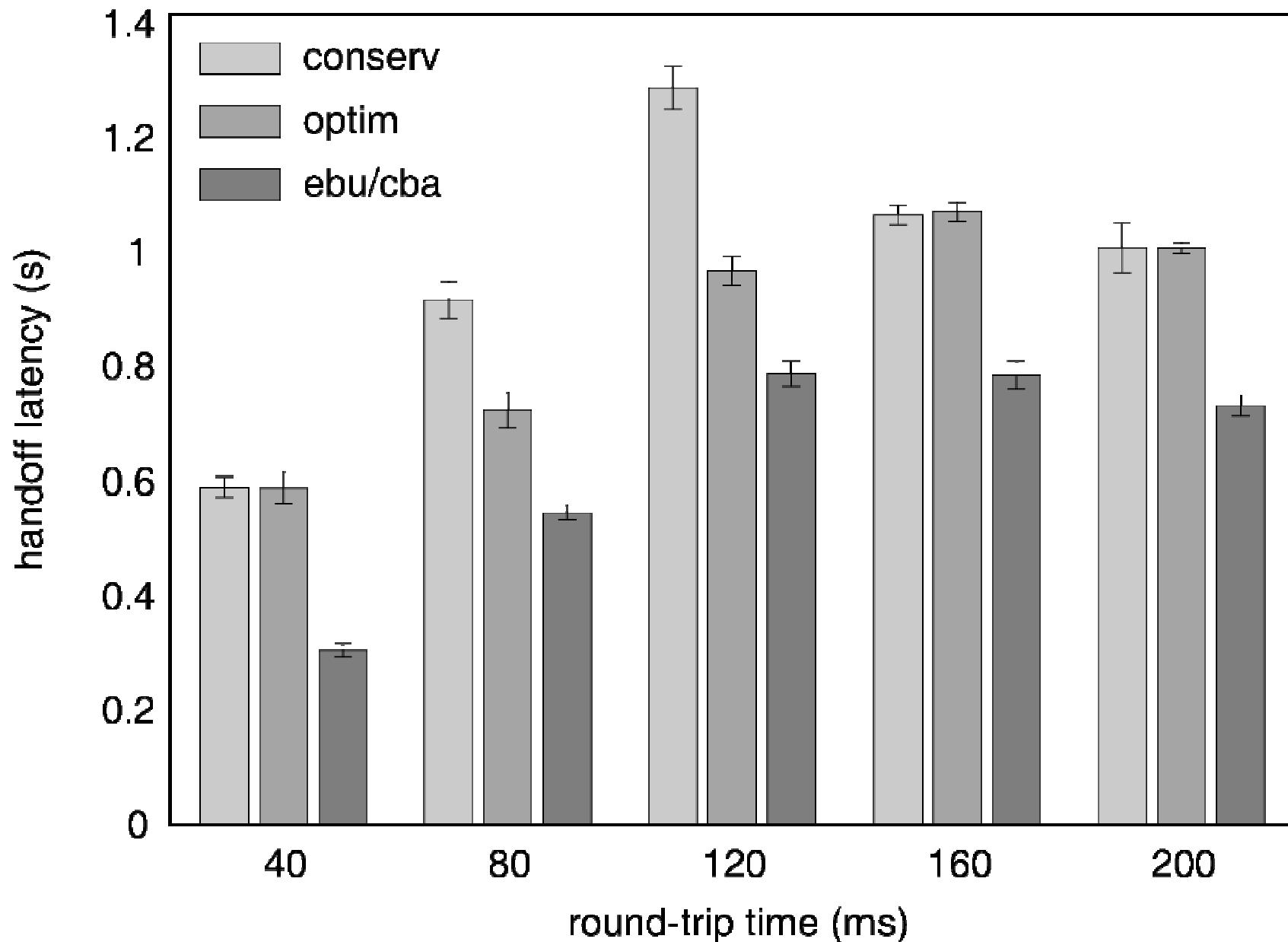
Mobility protocols

- standard (conservative) Mobile IPv6
- optimistic Mobile IPv6
- w/Early Binding Updates and Credit-Based Authorization

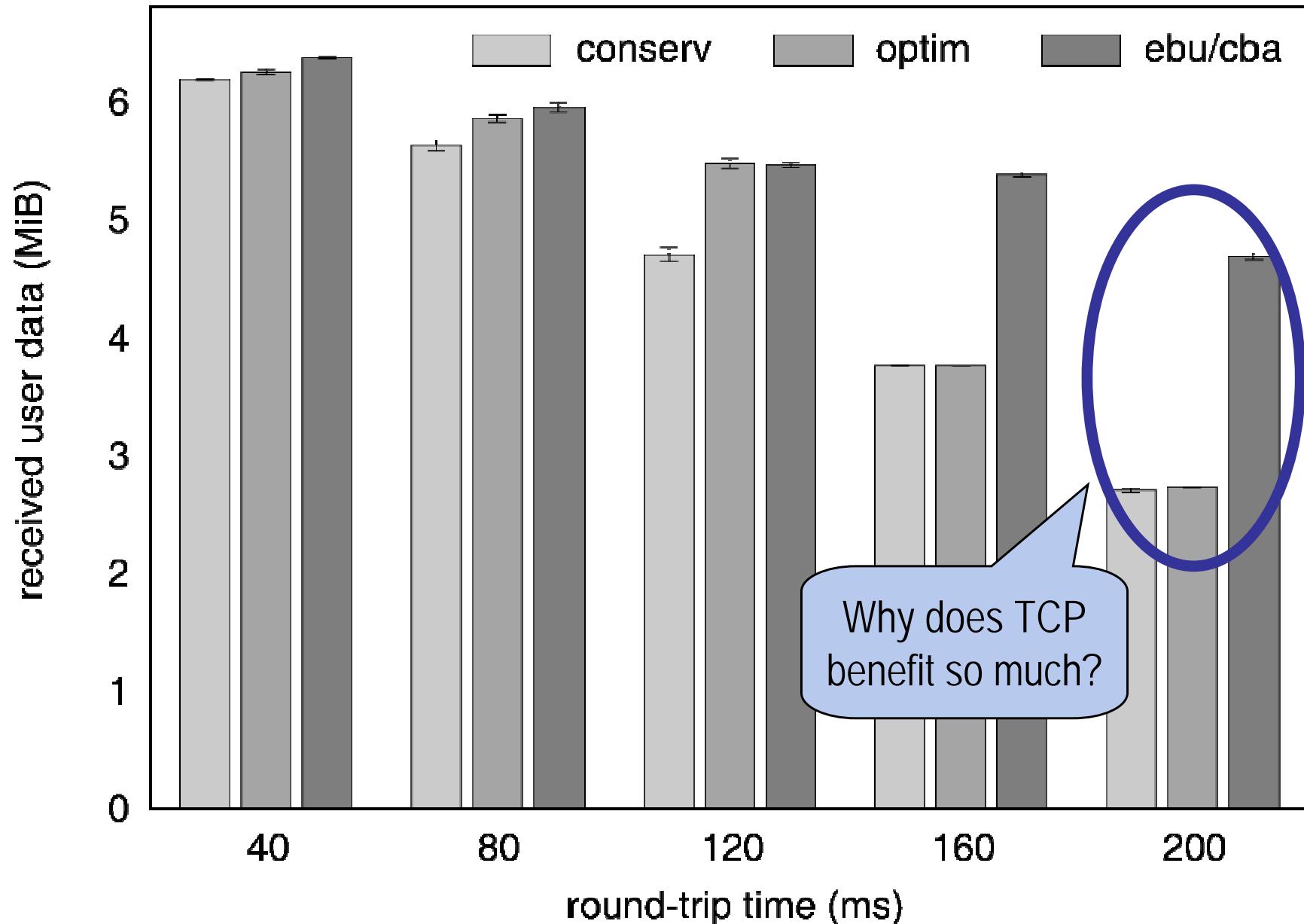
Confidence

- 20 experiments per mobility protocol per round-trip time
- 5 handoffs per experiment

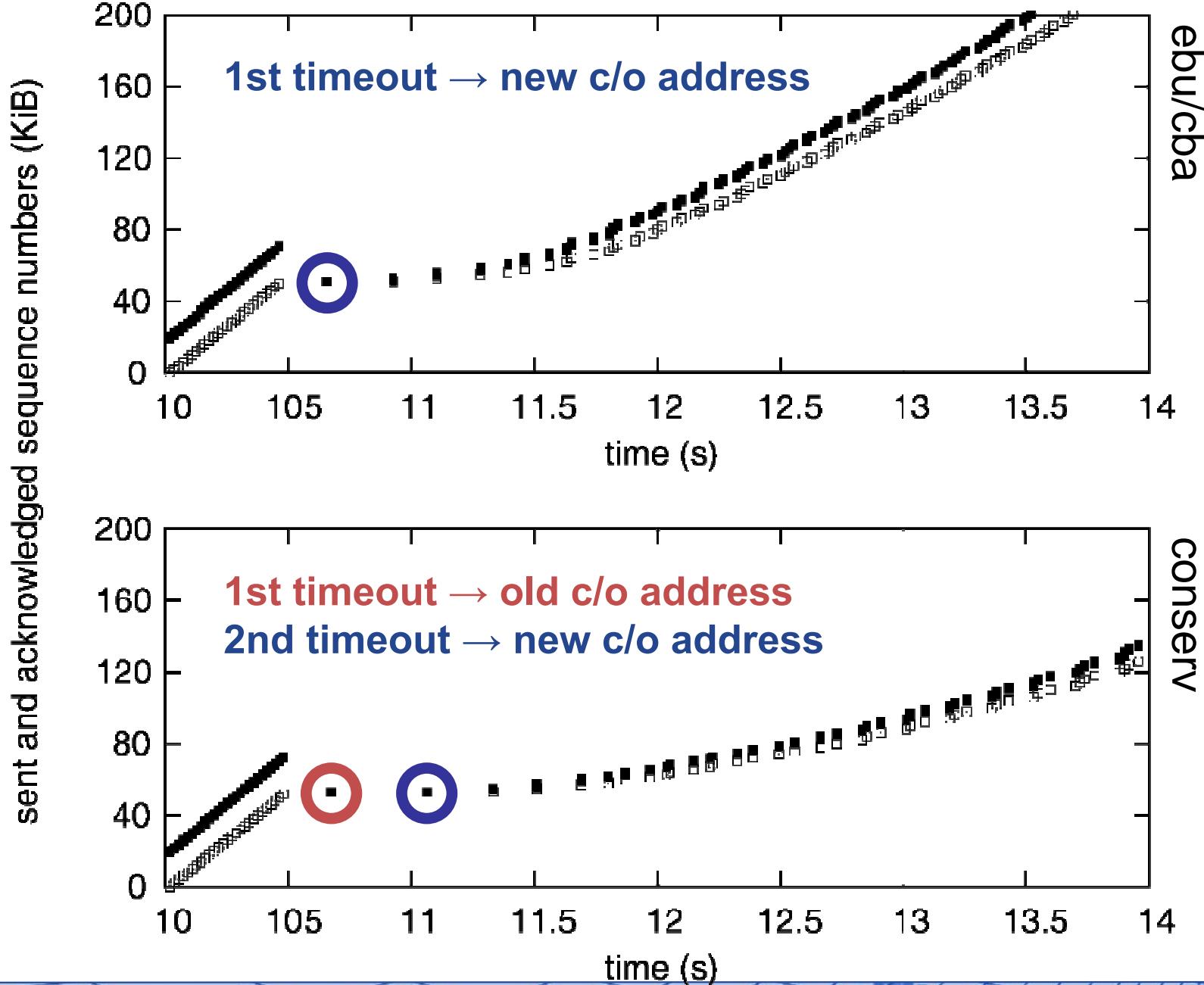
Handoff Delay w/TCP File Transfers



Throughput w/TCP File Transfers



Why TCP Benefits So Much



TCP behavior after 1st timeout

- set cwnd = 1
- set ssthresh = flightsize
- do Slow Start until $cwnd > ssthresh$

TCP behavior after 2nd timeout

- set cwnd = 1
- set ssthresh = 2 (minimum)
- effectively skip Slow Start

draft-vogt-mobopts-simple-ebu-00.txt

- includes diff's to RFC 3775
- specifies support for proactive handoffs
- no IANA requirements

draft-vogt-mobopts-simple-cba-00.txt

- transparent to MN
- no signaling
- no IANA requirements

- Early BU == BU where
 - Kbm == SHA1(home keygen token)
 - Care-of Nonce Index == 0
- Early BA accordingly
- CN w/EBU support
 - checks Nonce Indices option
 - Care-of Nonce Index == 0 ? \Rightarrow early Binding Update
 - Care-of Nonce Index != 0 ? \Rightarrow standard Binding Update
- CN w/o EBU support
 - sends BA w/status 137, "Expired care-of nonce index" or
 - sends no BA due to Authentication failure
- MN sets Acknowledge flag in early BU

Advantages of EBU/CBA

- Reduce handoff delays to 0~1 RTT (L3 only)
- Better accommodate TCP's retransmission algorithm
- No special network support required
- Applicable to inter-domain handovers

Drawbacks of EBU

- Additional signaling, especially for proactive home-address tests if done periodically
- Still 1 RTT latency for reactive handoffs
- Still 0~1 RTT latency for proactive handoffs

Many thanks to my students
for their eager and reliable co-operation:

- Ralf Beck
- Daniel Jungbluth
- Max Laier