Credit-Based Authorization for HIP Mobility

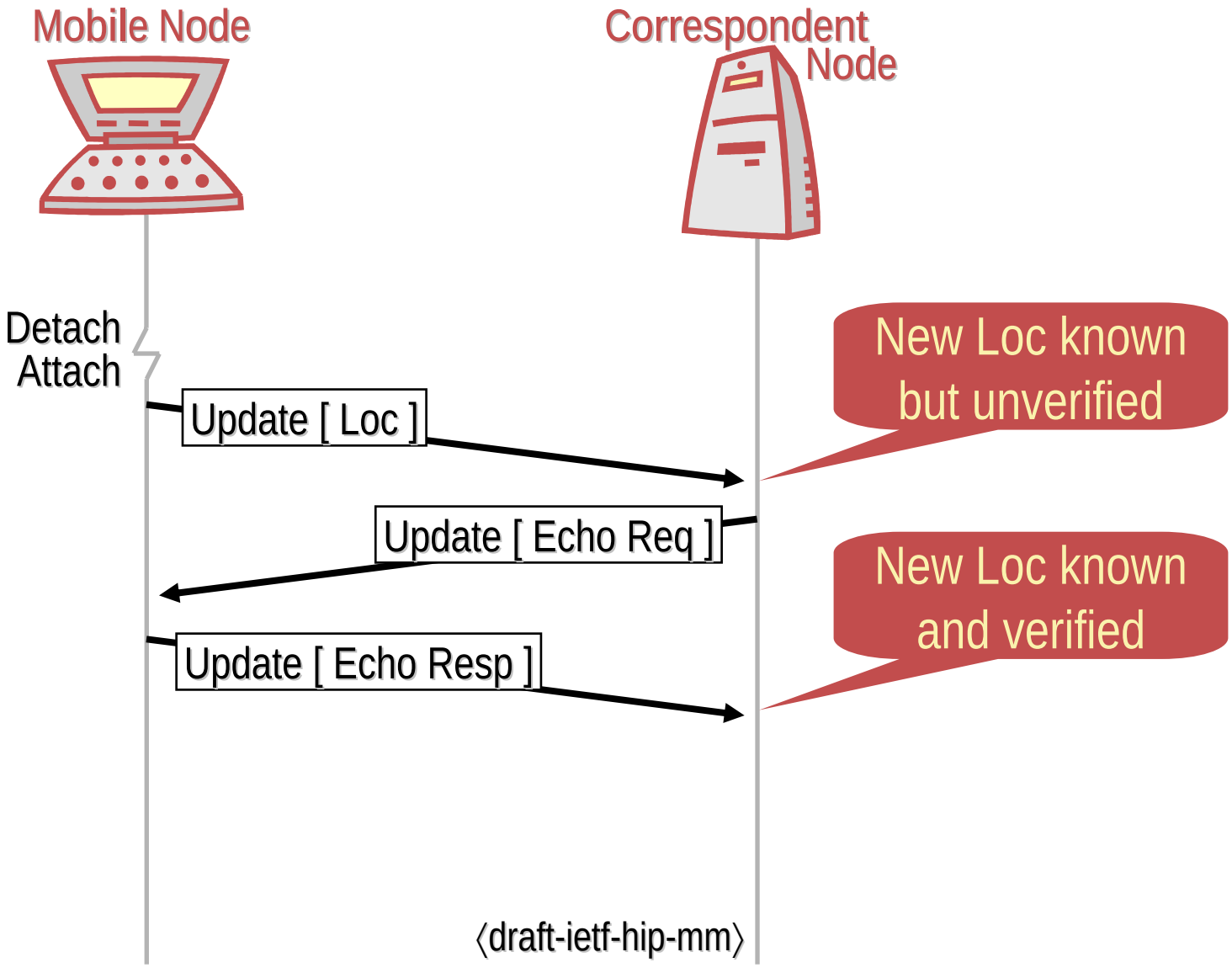
⟨draft-vogt-hip-credit-based-authorization⟩

Christian Vogt, chvogt@tm.uka.de

HIP Working Group Meeting, IETF 62

Minneapolis, MN, March 9, 2005

HIP Mobility Management



Why Do We Need Reachability Verification?

Because of redirection-based flooding attacks

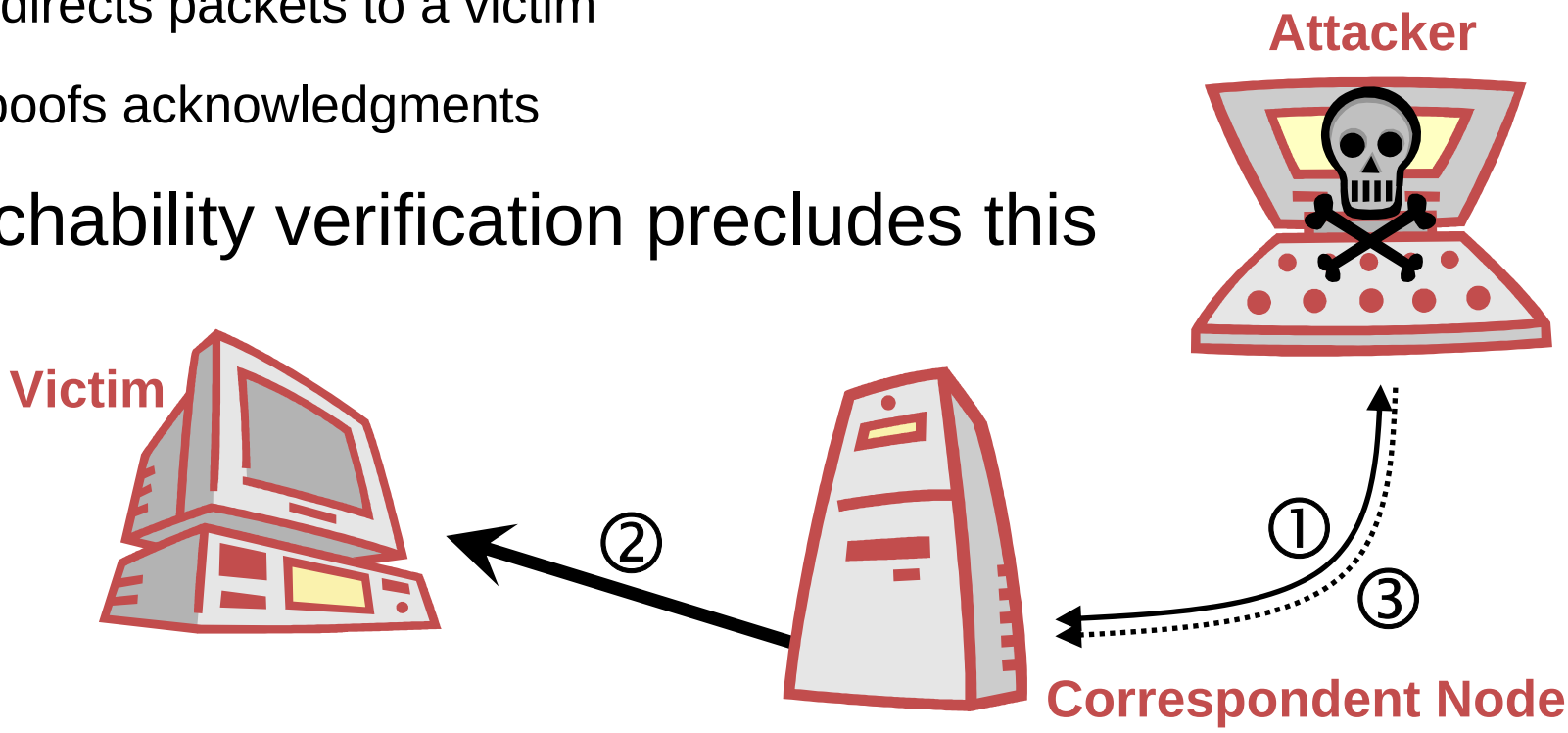
Here, the attacker…

① initiates download from CN

② redirects packets to a victim

③ spoofs acknowledgments

Reachability verification precludes this



Some Observations

What makes redirection-based flooding attractive?

- High potential for **amplification**
  (CN generates packets; attacker just spoofed Acks, if at all)
- **Any** IP node can be the **victim**
- Presumably **plenty** available **CN's**
  (that can be tricked into assisting in the attack)
- Easy set-up, no viral code distribution
  (in contrast to many conventional DoS attacks)

Some Observations

HIP provides authentication, but…

- Authentication does not imply security against flooding
  (Attacker can authenticate, because it redirects its own packets)
- Security against flooding not necessarily requires authentication
- ⇒ Authentication alone may not be a discouragement

Other Protection Mechanisms

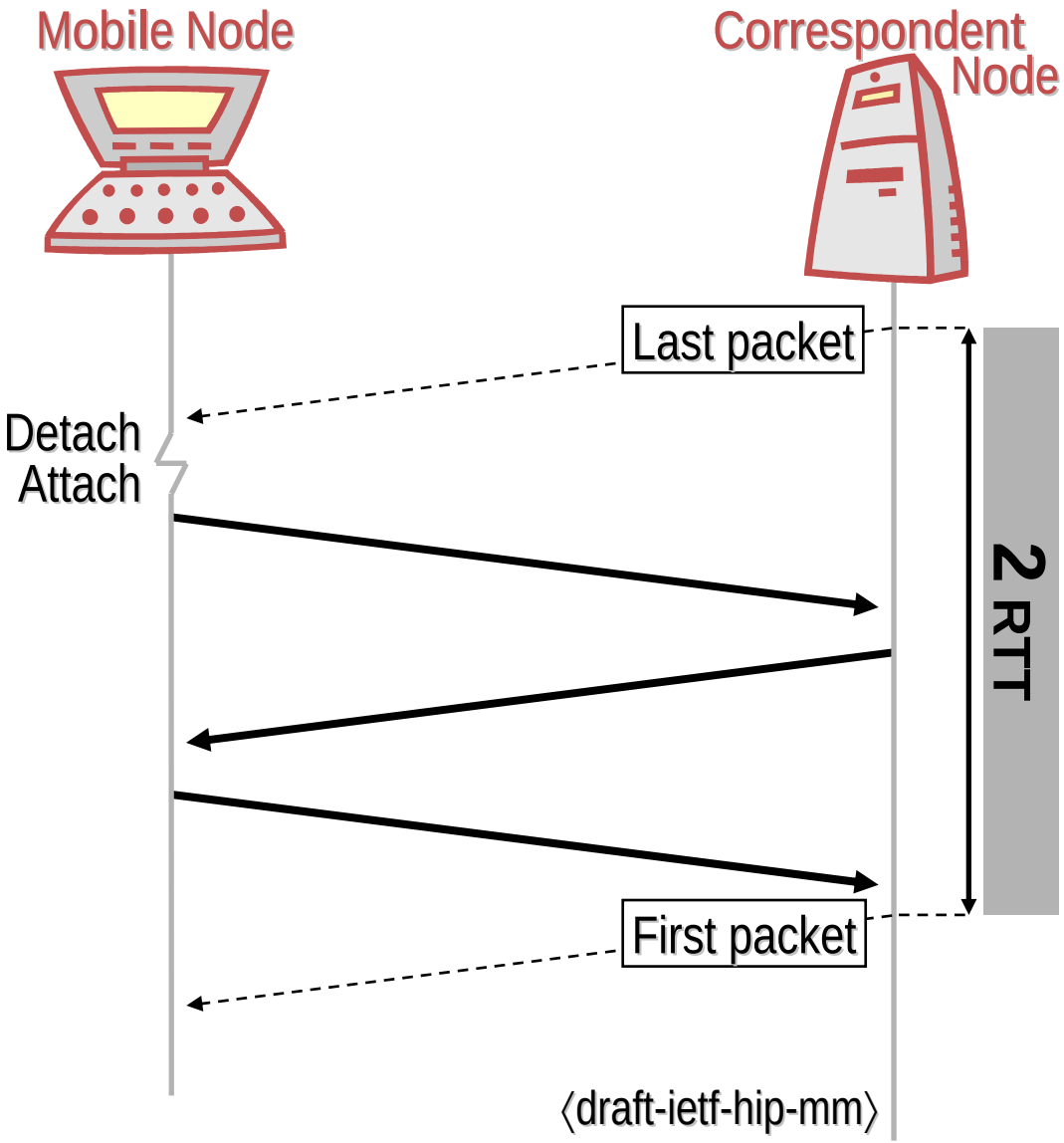
Trusting MN's

- Administrative relationship may imply trust
  (Home Agent in MIPv6, CN in MIPv6 with pre-computed binding keys)

Ingress filtering

- Does not protect a network from a flooding attack,
  but prevents initiation of a flooding attack from a certain network
- $\Rightarrow$ Depends on wide, preferably universal deployment
- Currently questionable whether this is the case today

How HIP Mobility Management Performs



How Can This Be Optimized?

Idea: CN uses address while unverified and protects period of vulnerability

Option 1: Lifetime restriction

- Disable unverified address after X seconds
- Easy to implement, but little secure
  (Attacker could re-register unverified address, or toggle btw. verified/unverified addresses)

How Can This Be Optimized?

Option 2: Heuristics

- must be rigid enough to recognize attacks early on,
  but must not cause immature sanctions on upright MN's
- Upright MN's may look like attackers from remote
  (E.g., new address may become stale before getting verified)
- ⇒ Appropriate heuristics may not be easy to find

Option 3: Credit-Based Authorization

- Recall: amplification makes redirection-based flooding attractive
- **CBA prevents amplification**, not misdirection per se
- Rationale: No amplification $\Rightarrow$ redirection-based flooding unattractive because other attack strategies…
  - are simpler
  - do not require authentication
  - may even have some amplification

  Examples are direct flooding, TCP-SYN spoofing

Credit-Based Authorization

Mobile Node

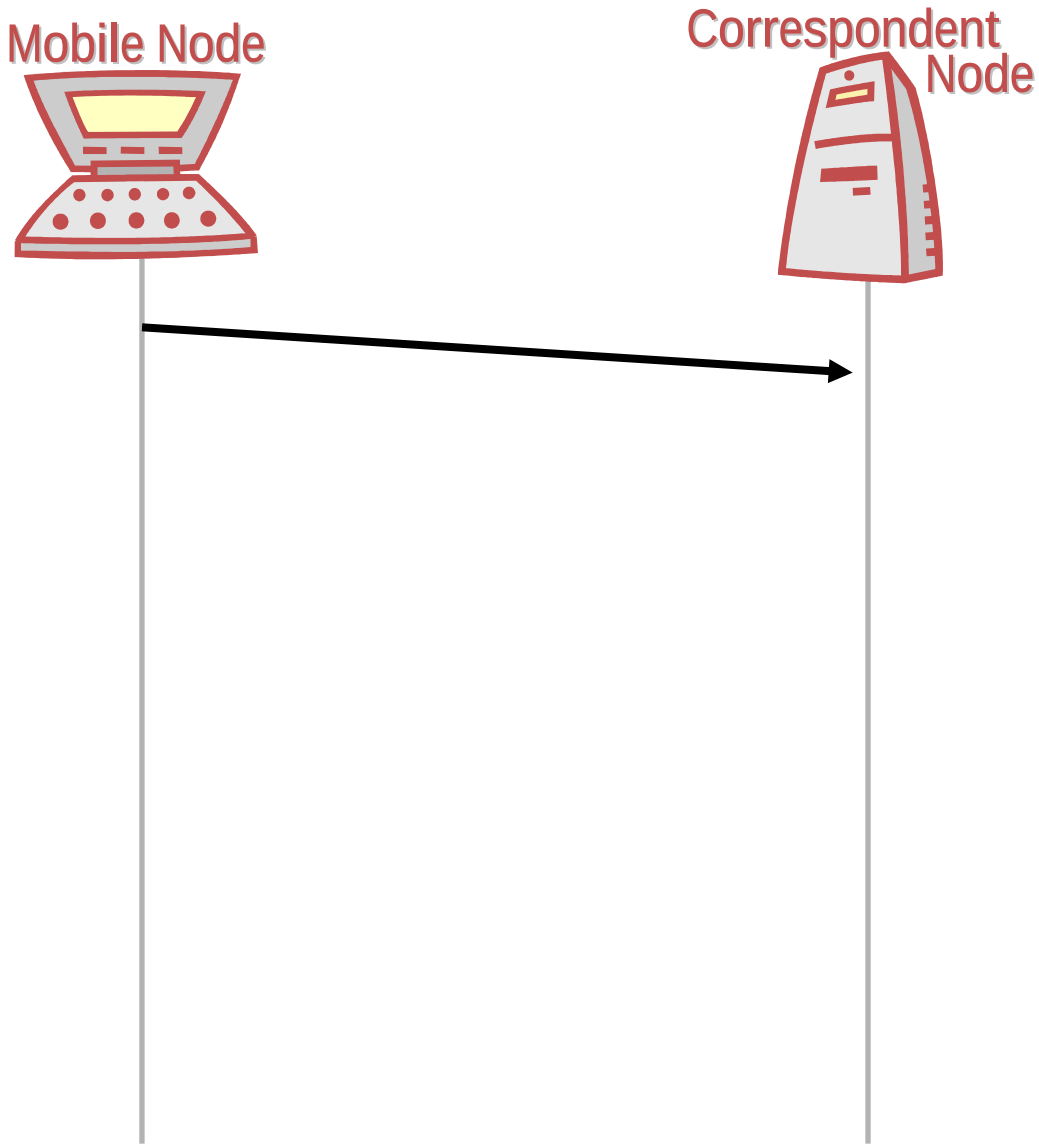
Correspondent Node

Acquires credit by sending pkts.

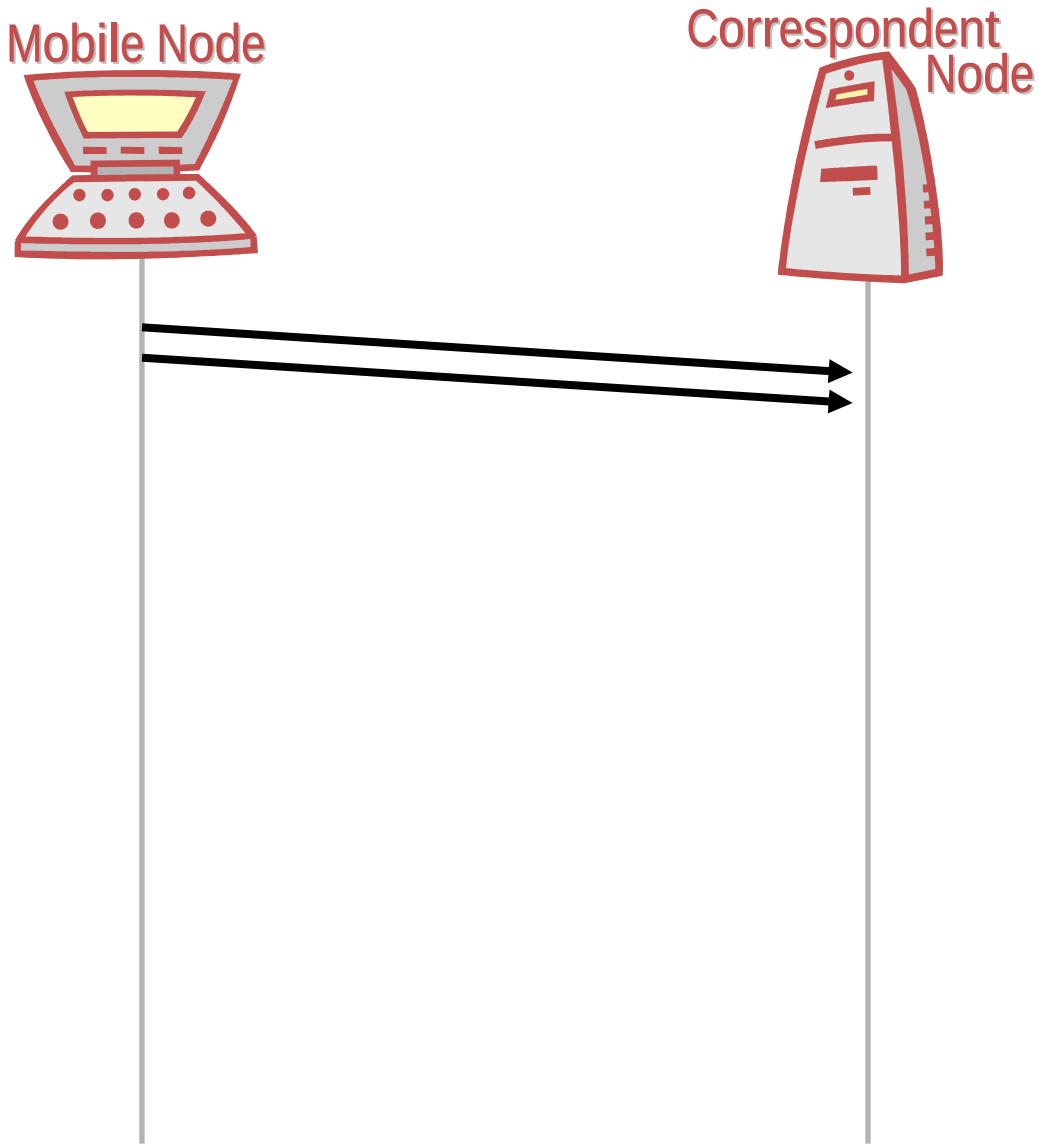
Consumes credit for being sent pkts. to unverified addr.

Maintains credit account

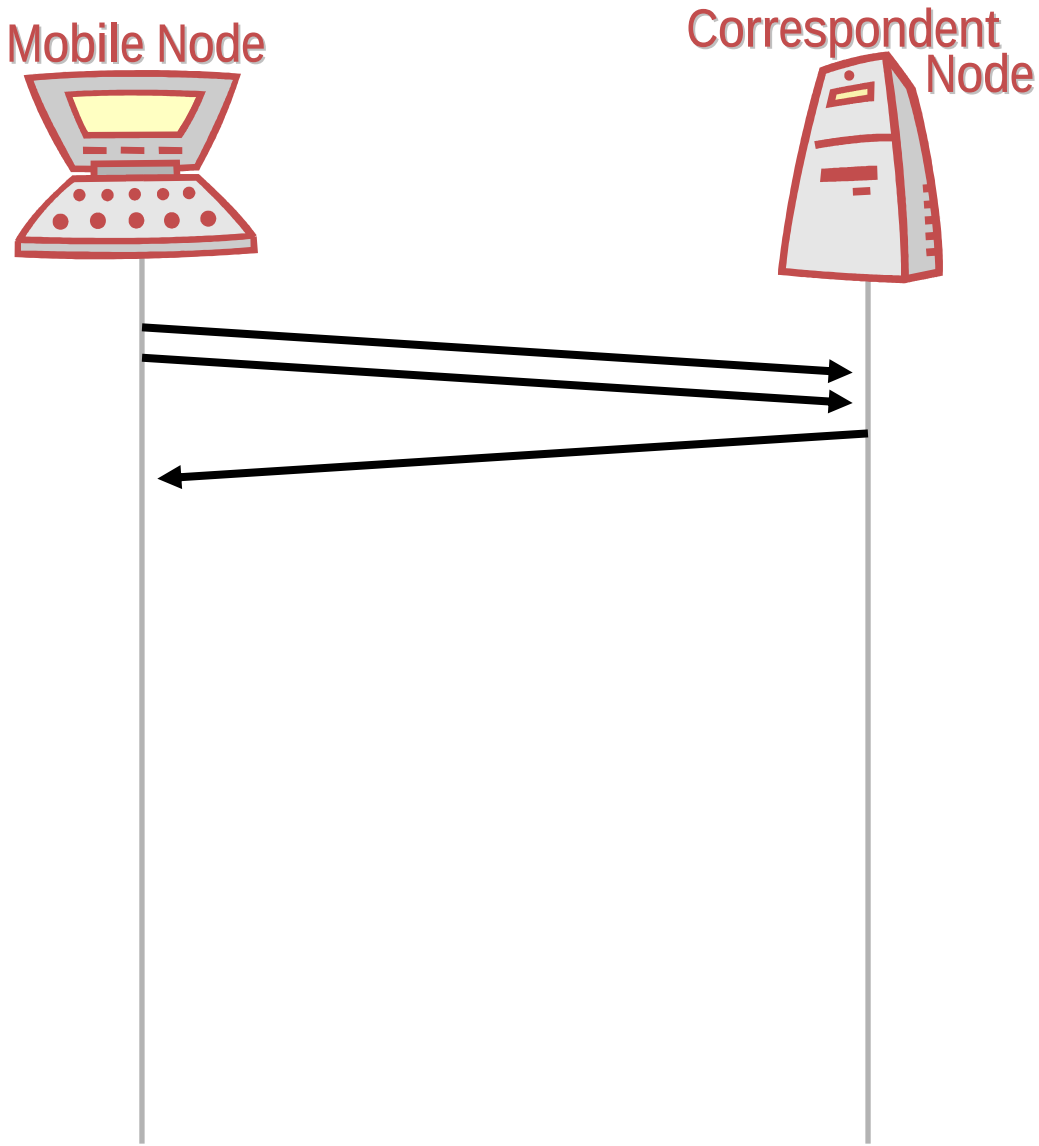
Credit-Based Authorization



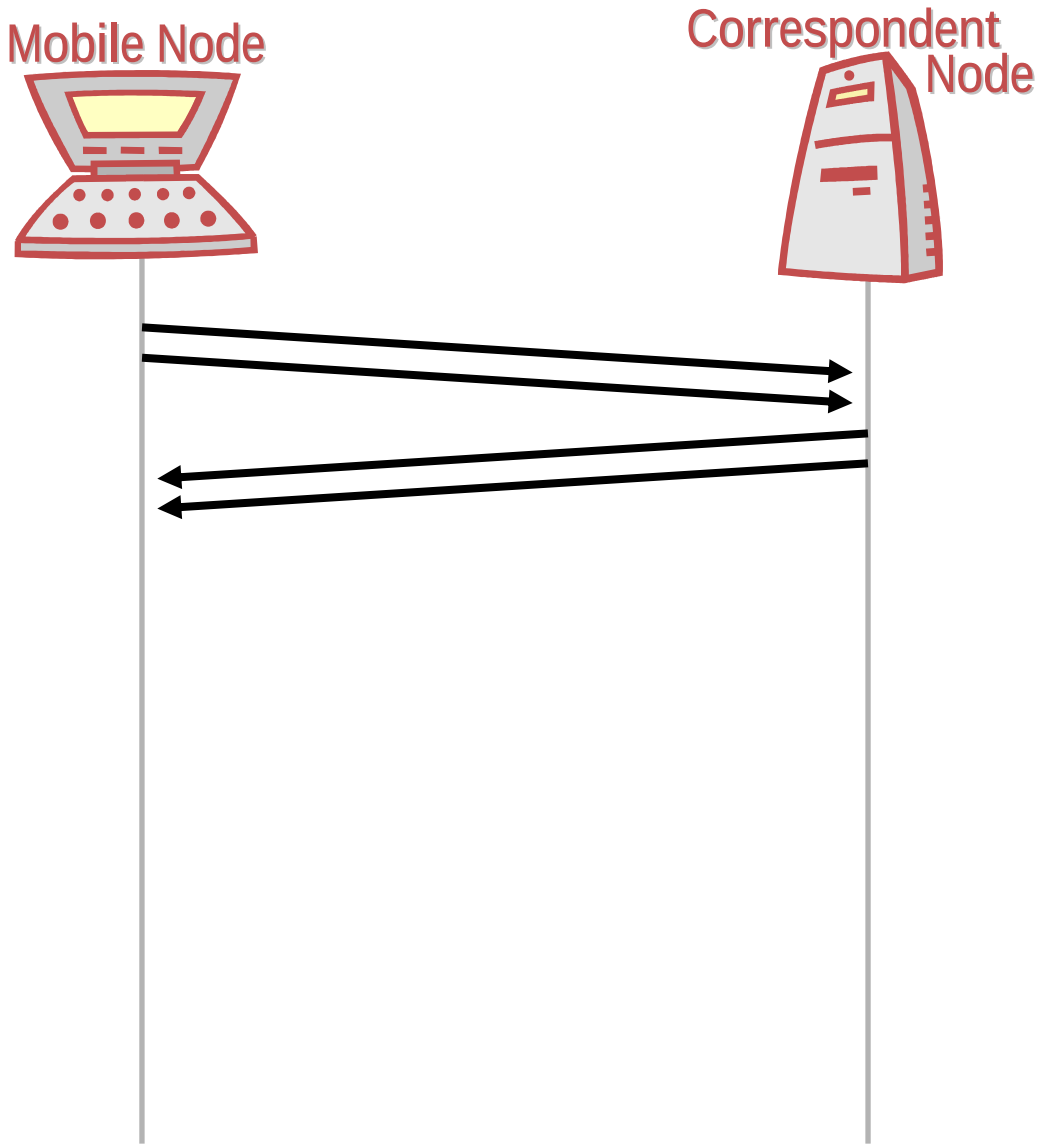
Credit-Based Authorization



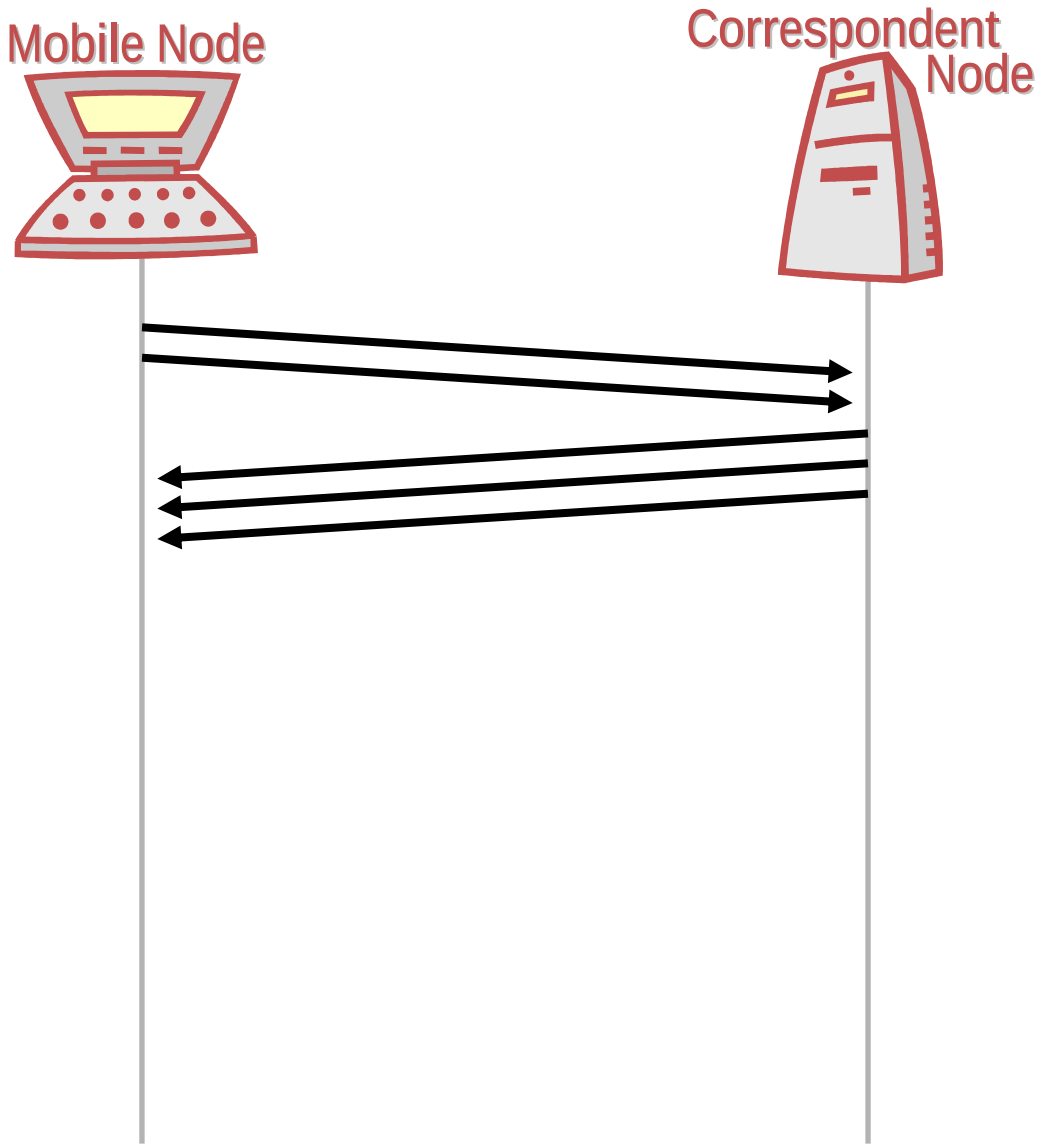
Credit-Based Authorization



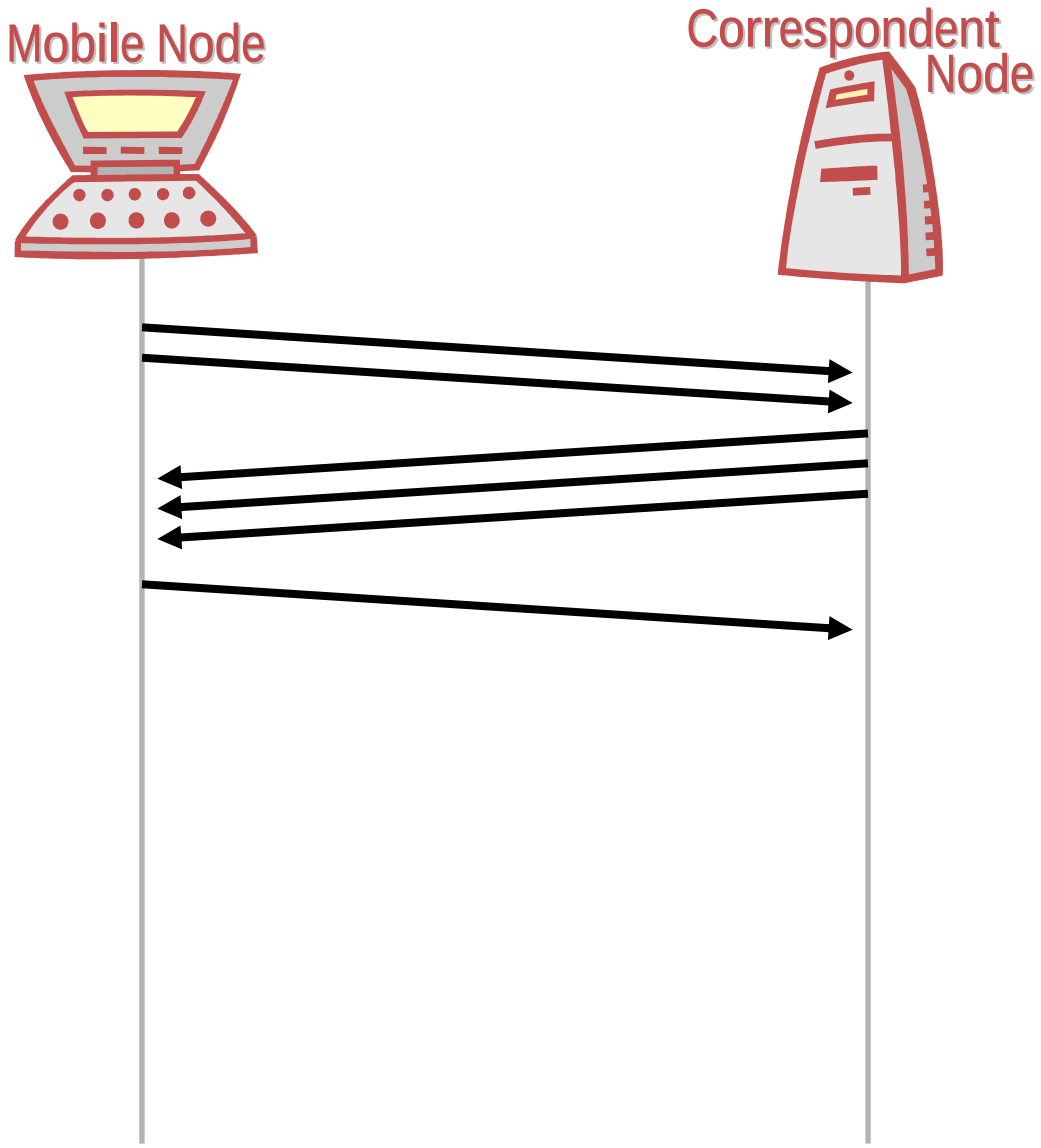
Credit-Based Authorization



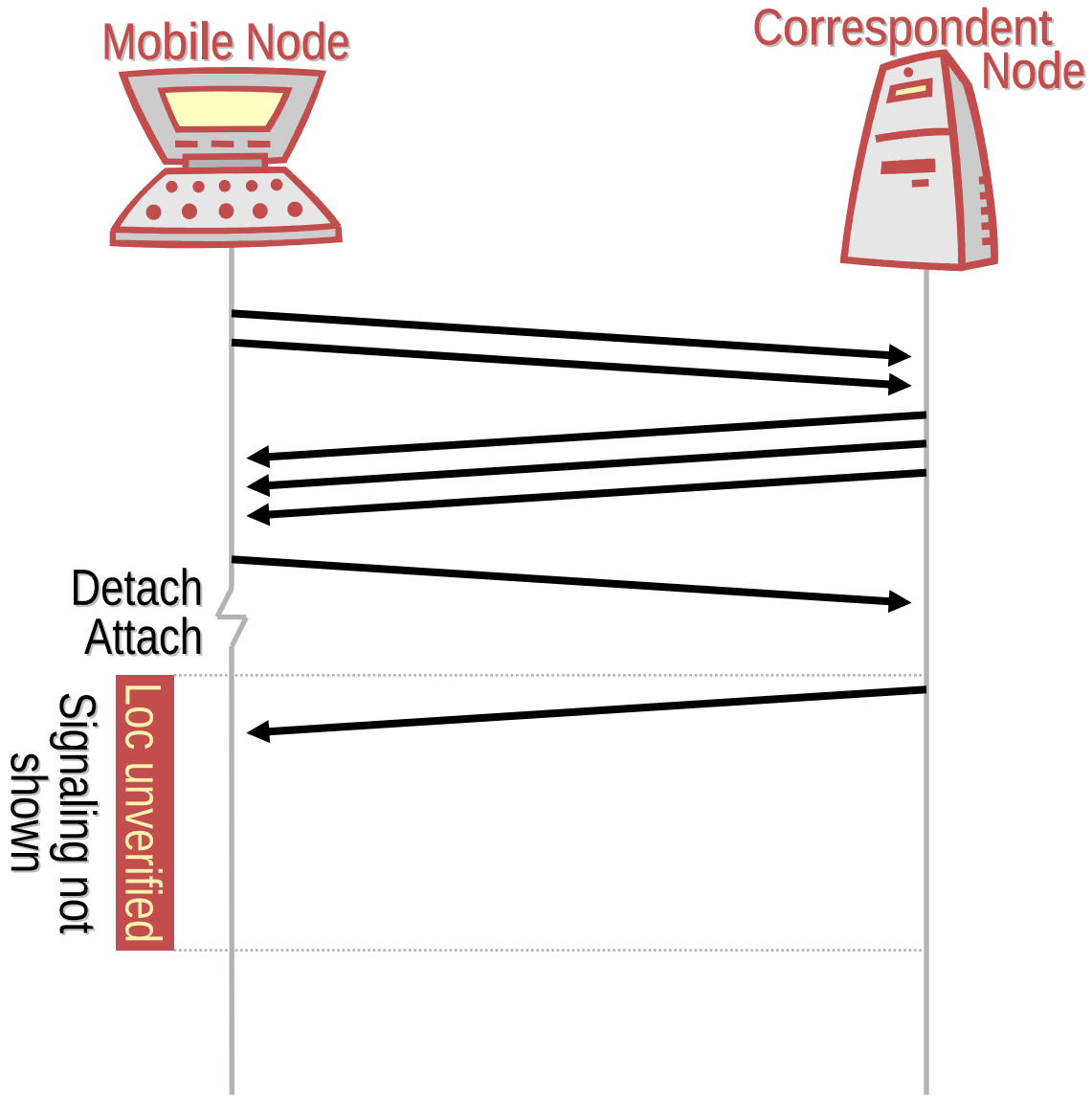
Credit-Based Authorization



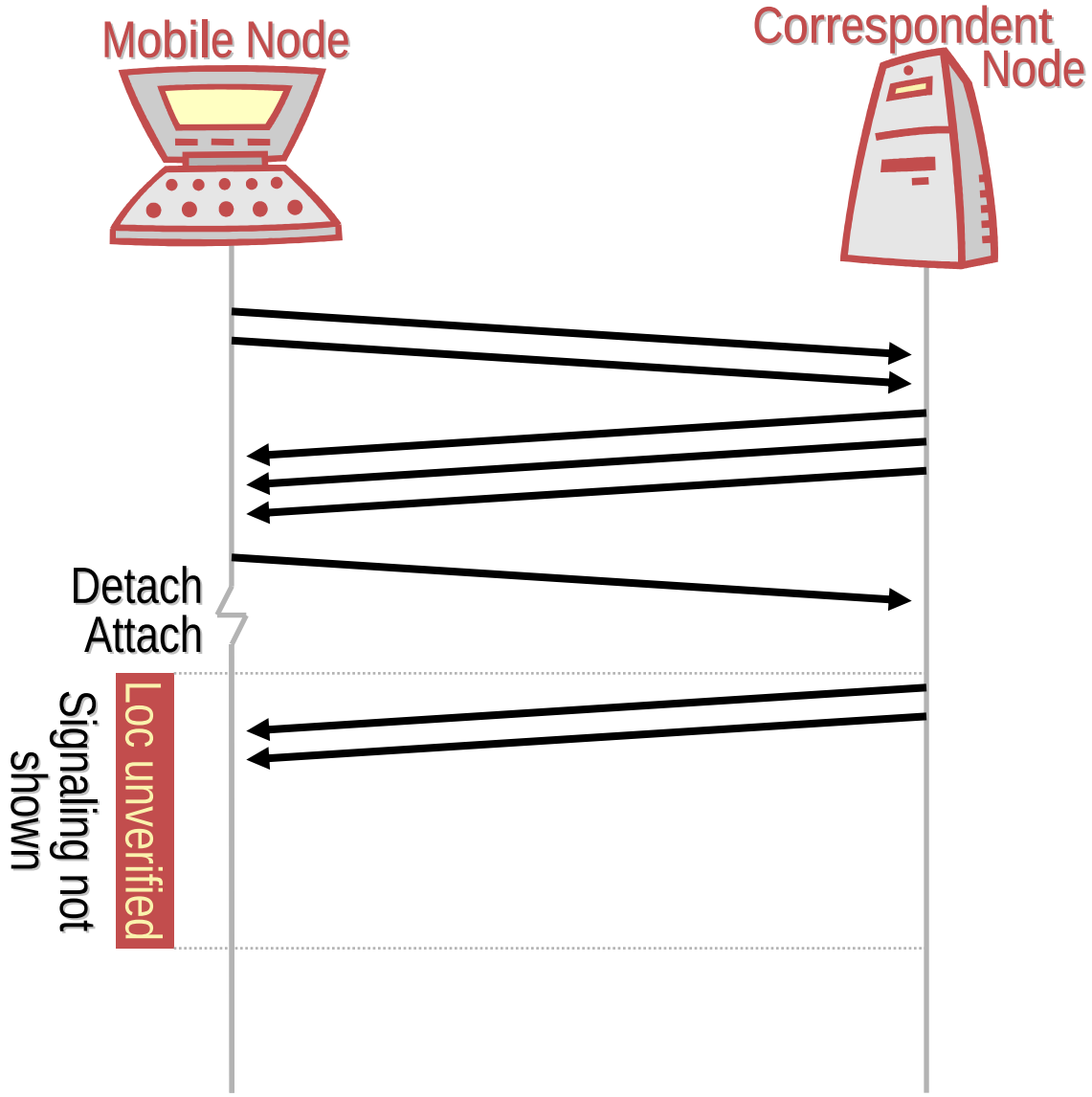
Credit-Based Authorization



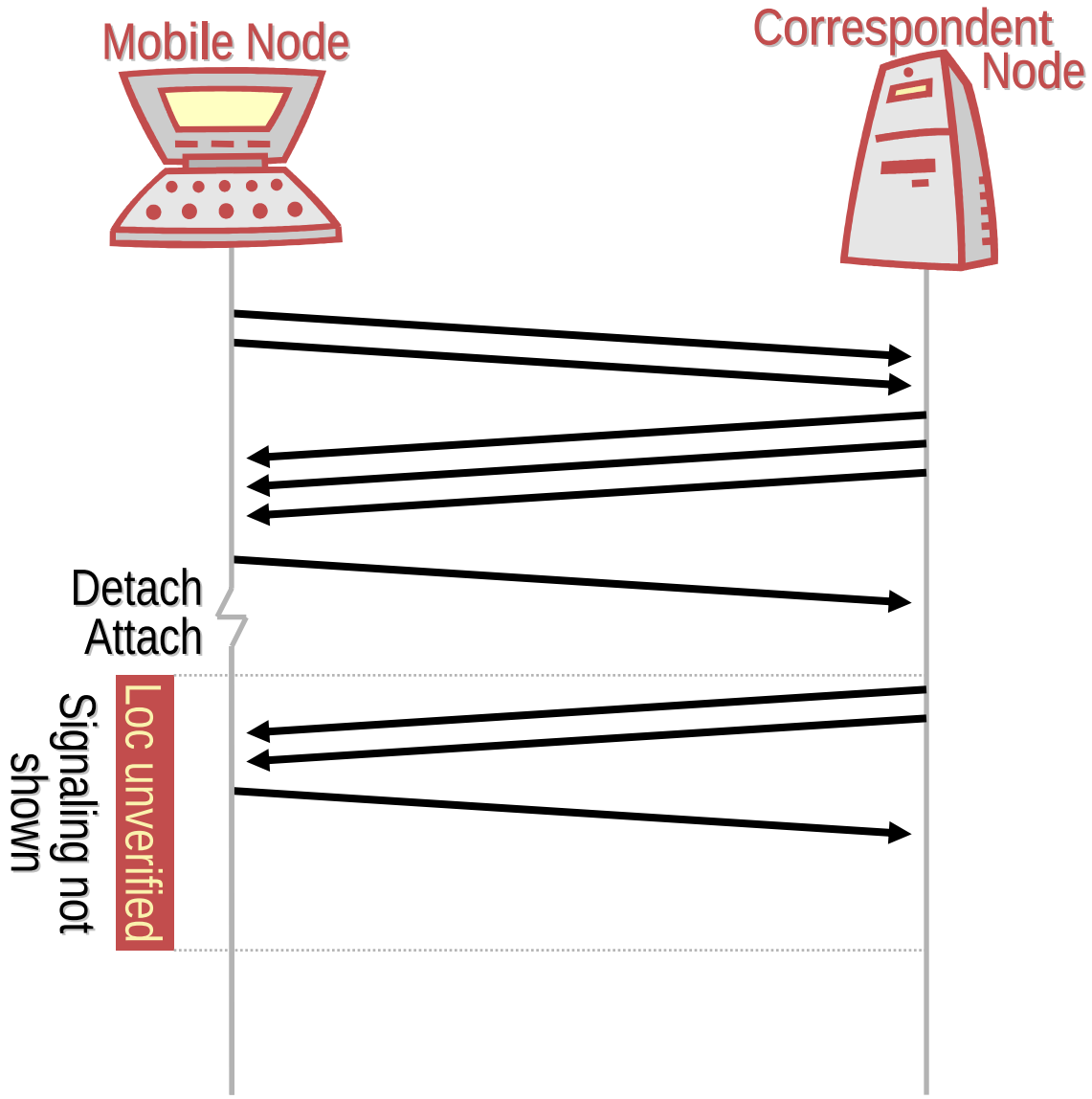
Credit-Based Authorization



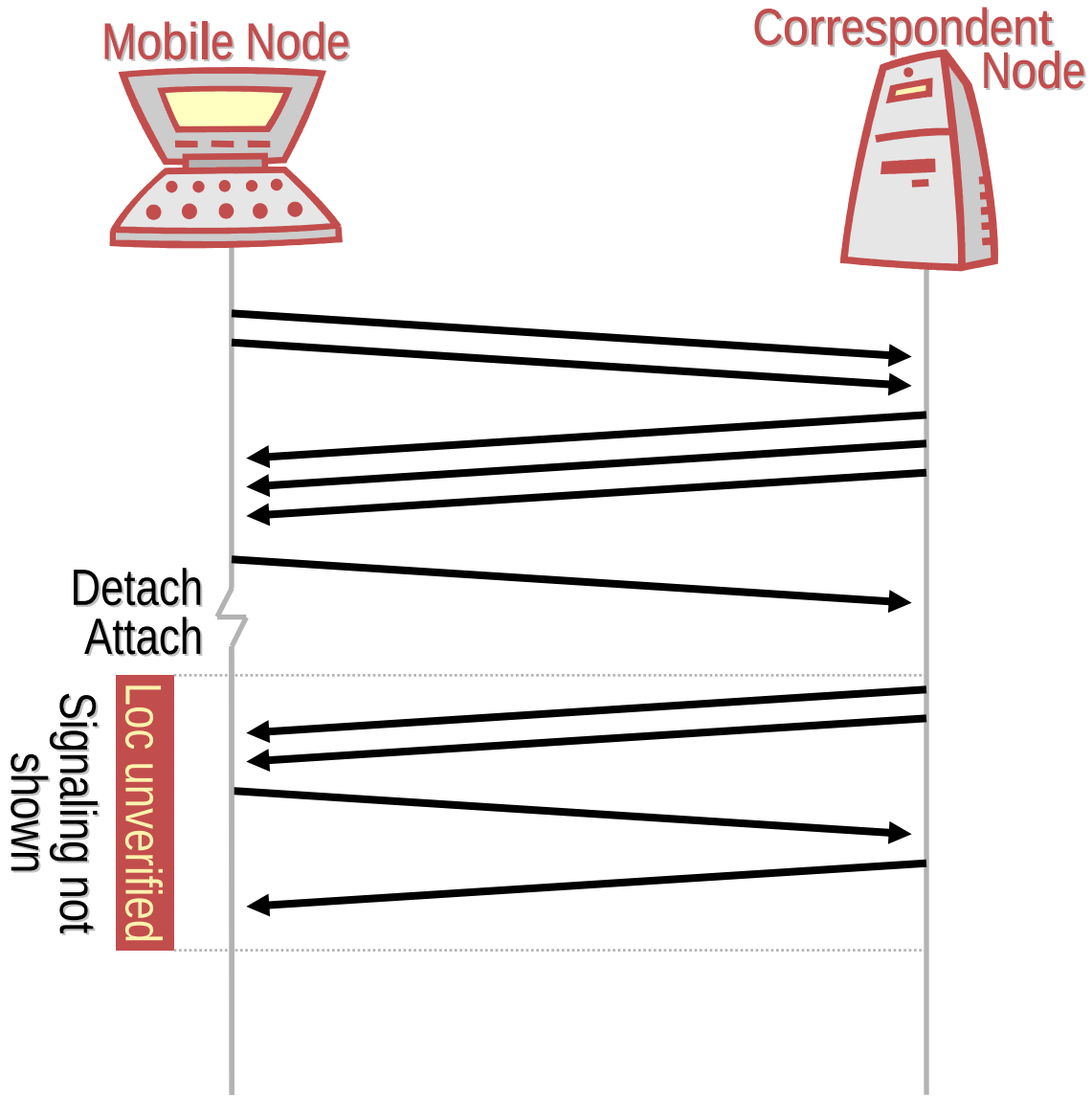
Credit-Based Authorization



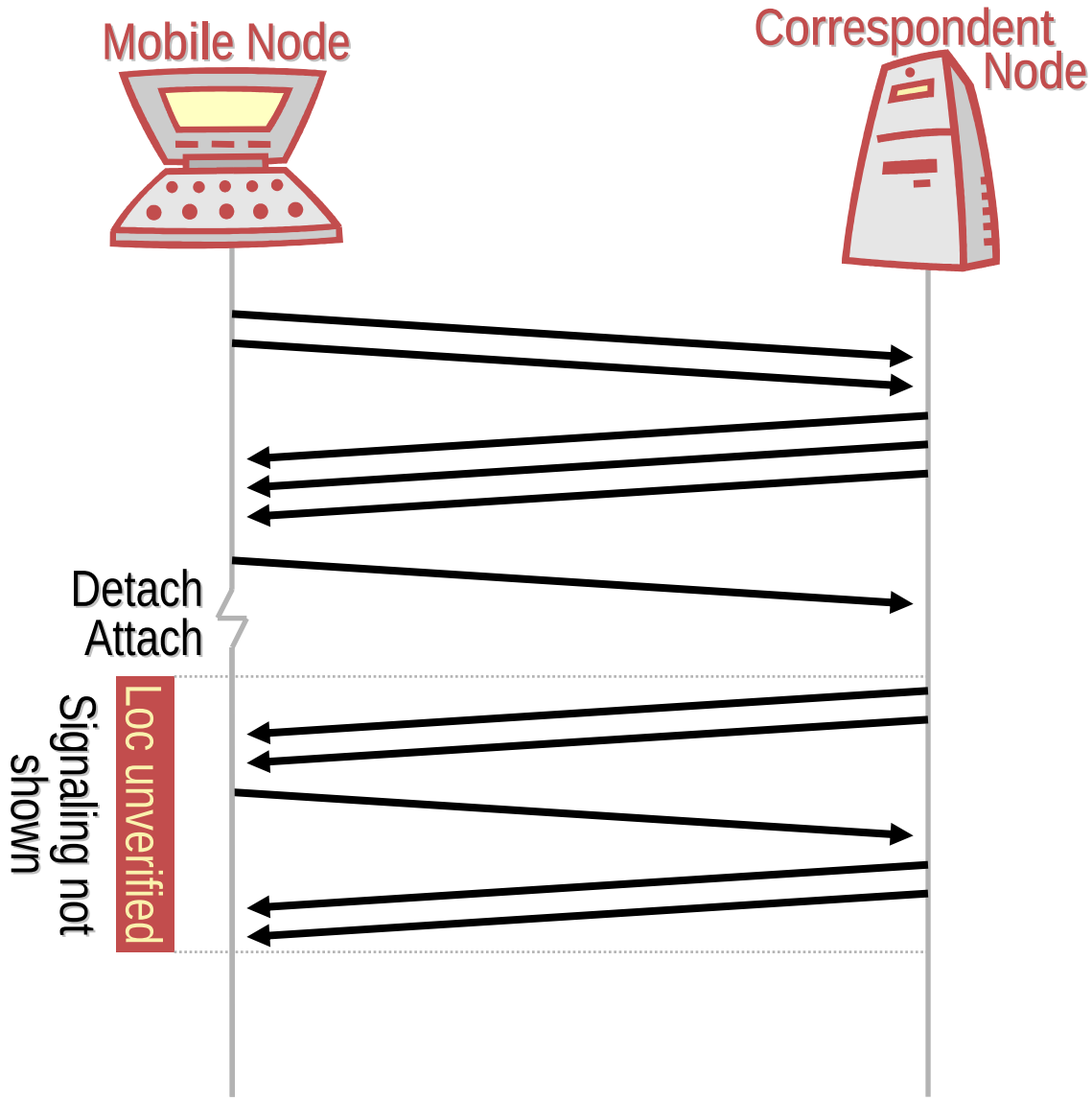
Credit-Based Authorization



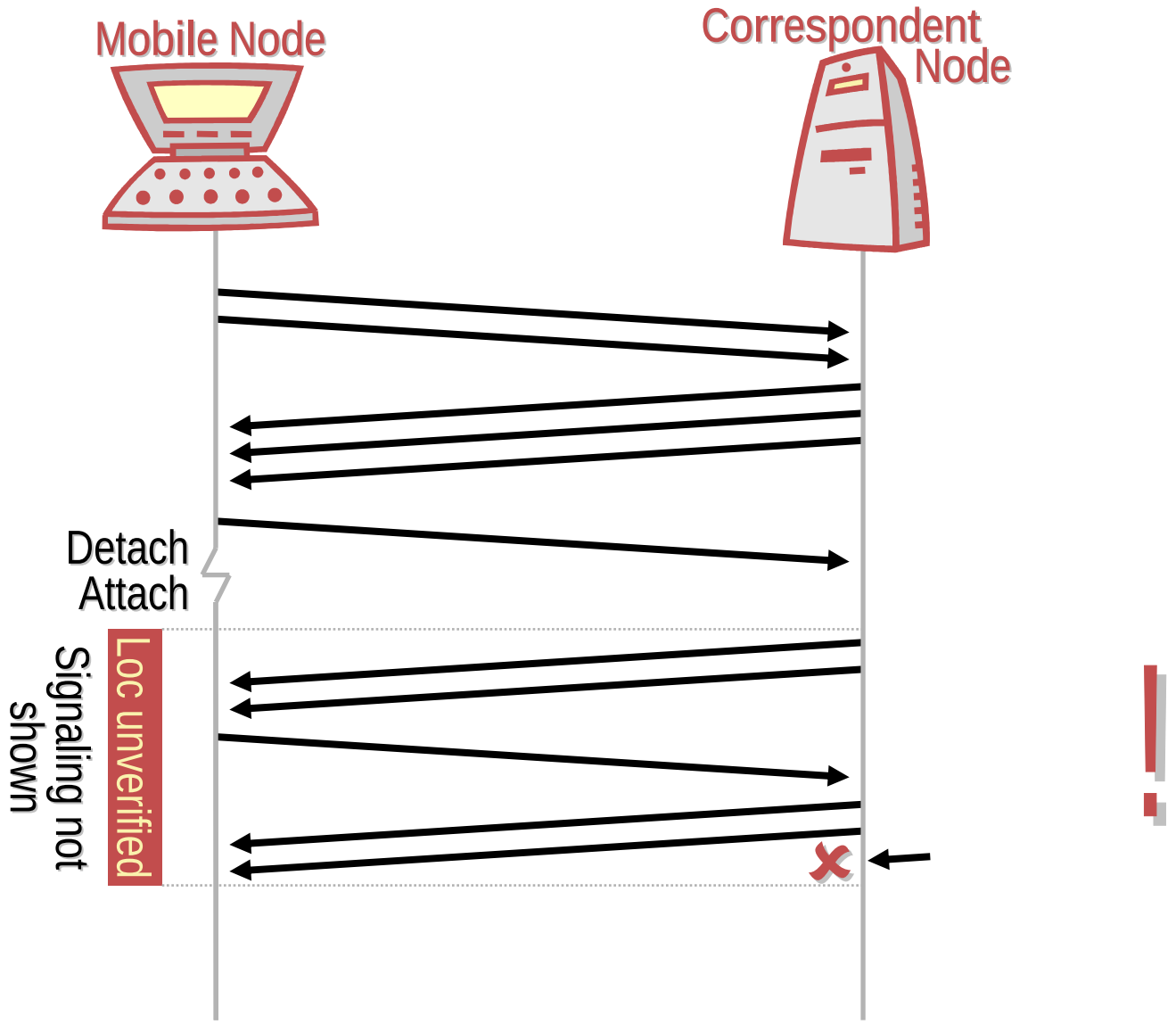
Credit-Based Authorization



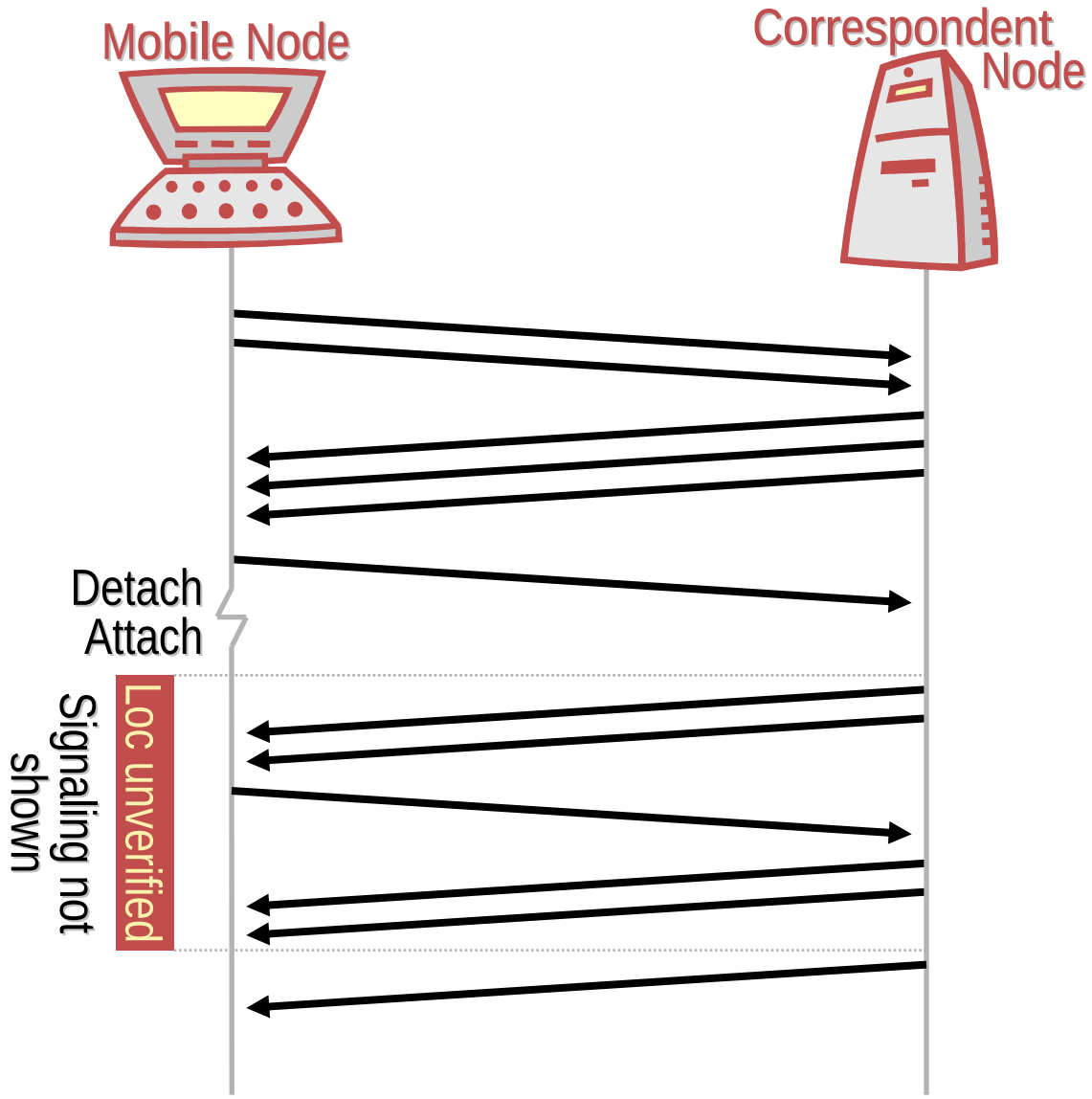
Credit-Based Authorization



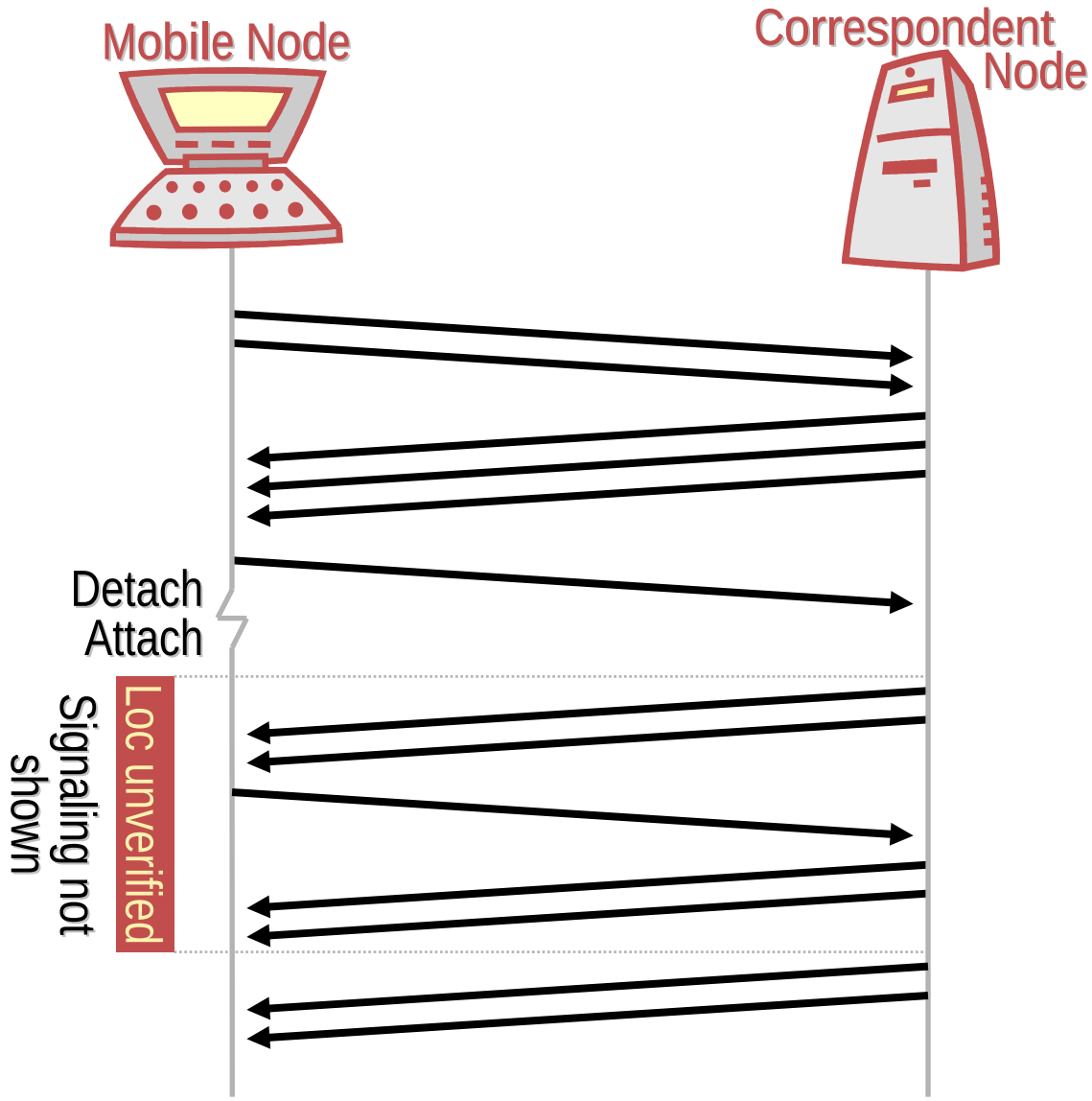
Credit-Based Authorization



Credit-Based Authorization



Credit-Based Authorization



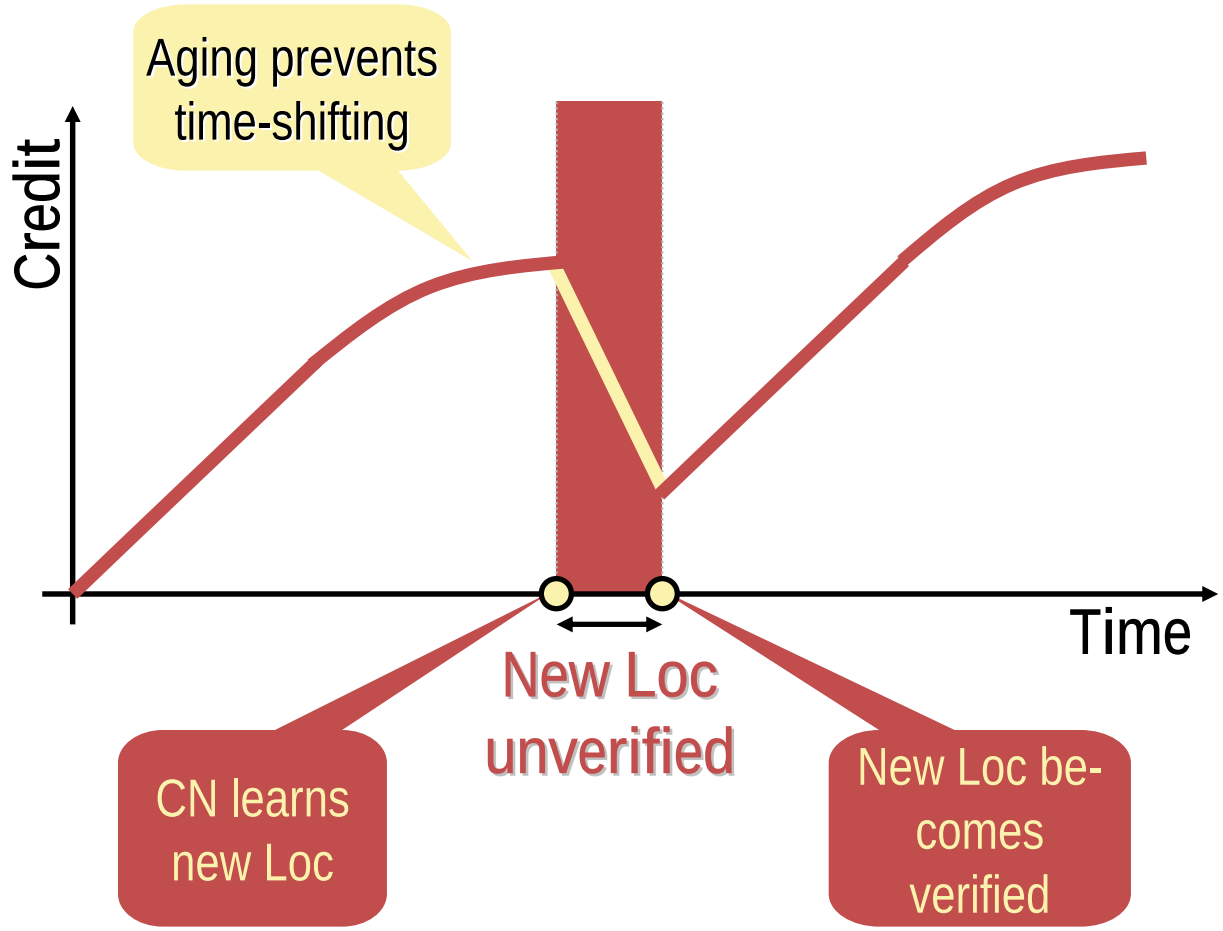
How About Time-Shifting Attacks?

How can an attacker prevented from…

- accumulating credit over a long time
- at a slow rate, and
- using this credit all at once

How About Time-Shifting Attacks?

Solution: Age existing credit ("negative interests")



How About Asymmetric Traffic?

Issue: Applications with asymmetric traffic patterns

- MN may not be able to collect sufficient credit

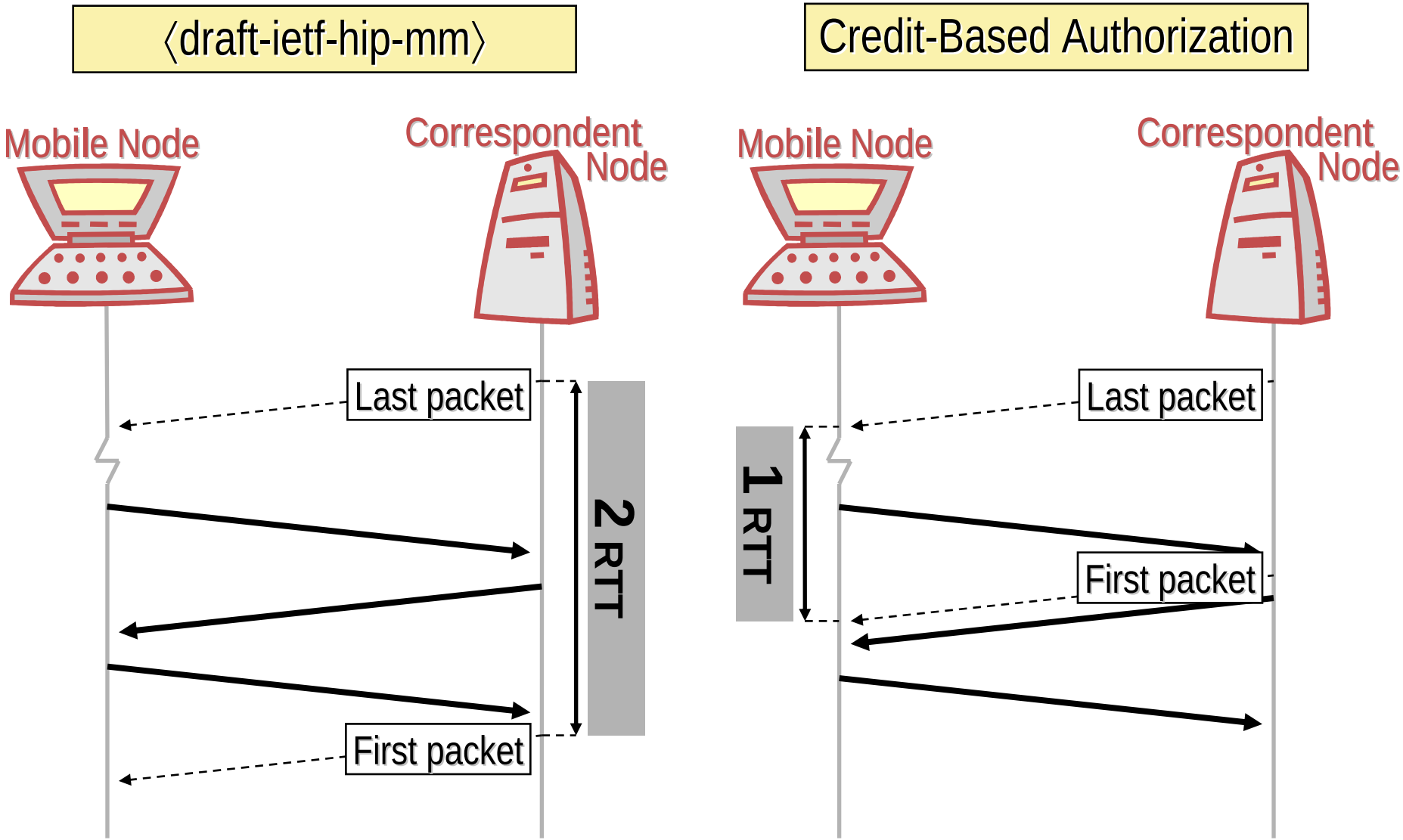
Option 1: Aging allows for asymmetry

- May limit supported applications

Option 2: Credit for packet reception and processing

- Requires feedback mechanism for CN
- $\Rightarrow$ IP-address spot checks (in-band reachability verification)
- Optional, not presented here

How Much Do We Benefit?



Conclusions

Credit-Based Authorization…

- prevents amplified, redirection-based flooding attacks
- allows CN to use unverified locators
- reduces handover-signaling delays by 1 RTT
- is transparent to MN

Implementation exists for Mobile IPv6

- Binding Cache holds per-MN variables
- $\Rightarrow$ Modifications only minor
- Similar integration possibilities in HIP

Conclusions

Interest to the WG?

- Possibly after base specification published?
- As part of the MM document?
  (Might make sense to optimize MM right away
  rather than through an optional extension…)