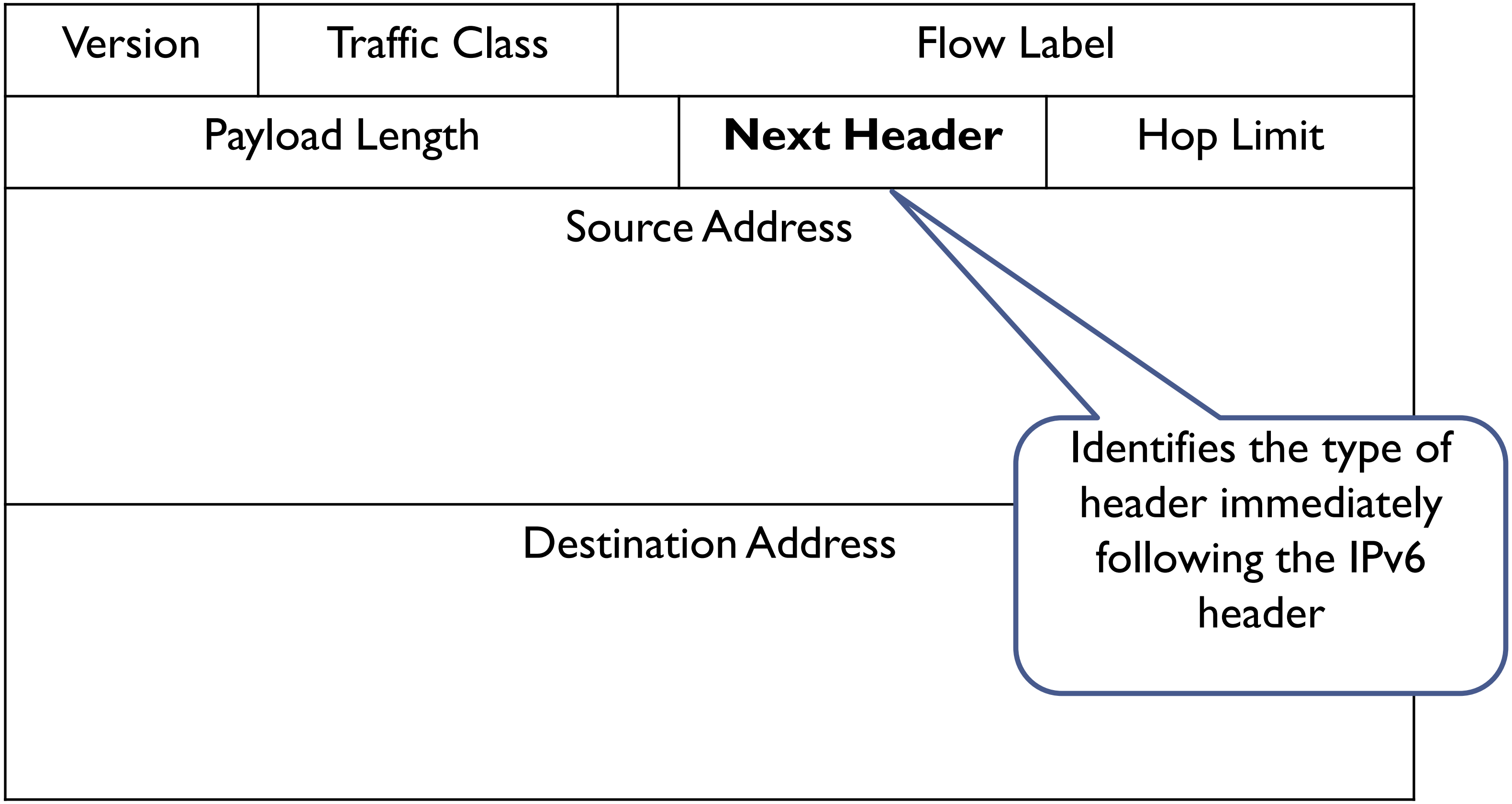
Security of Mobile IPv6

Lei Qin

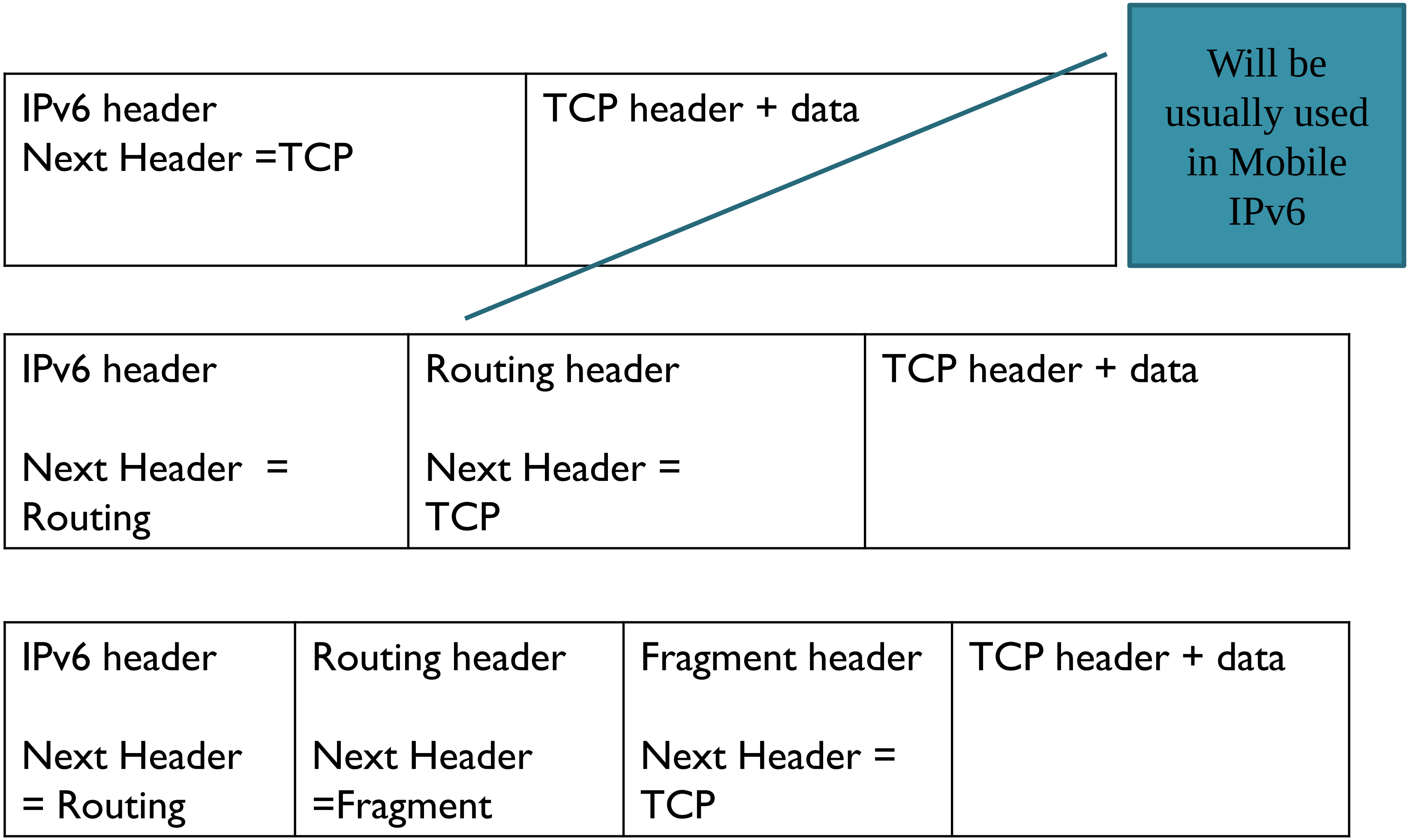
IPv6 Header Format



<table>
<tr><td>Version</td><td colspan="2">Traffic Class</td><td colspan="2">Flow Label</td></tr>
<tr><td colspan="2">Payload Length</td><td colspan="2"><b>Next Header</b></td><td>Hop Limit</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
</table>

Identifies the type of header immediately following the IPv6 header

IPv6 Extension Headers



IPv6 header Next Header =TCP	TCP header + data

Will be usually used in Mobile IPv6

IPv6 header Next Header = Routing	Routing header Next Header = TCP	TCP header + data

IPv6 header Next Header = Routing	Routing header Next Header =Fragment	Fragment header Next Header = TCP	TCP header + data

Why we need Mobile IP

- What if a host were disconnect from one network and connected to another network?

- Two kinds of problem

1. Existing connections: become invalid
2. New connections: unreachable

Problem 1: important for stateful protocols

Problem 2: concerns servers but not clients

Both problems are important for some peer to peer applications, e.g., instant messaging and VoIP.

Aim of Mobile IP

- Solve both kinds of problems introduced by mobility

1. All higher-level connections between **mobile node (MN)** and its **correspondent** should work well upon address changing
2. The mobile node should be reachable anywhere

- It should also be transparent to higher level protocols (Modifies only IP layer)

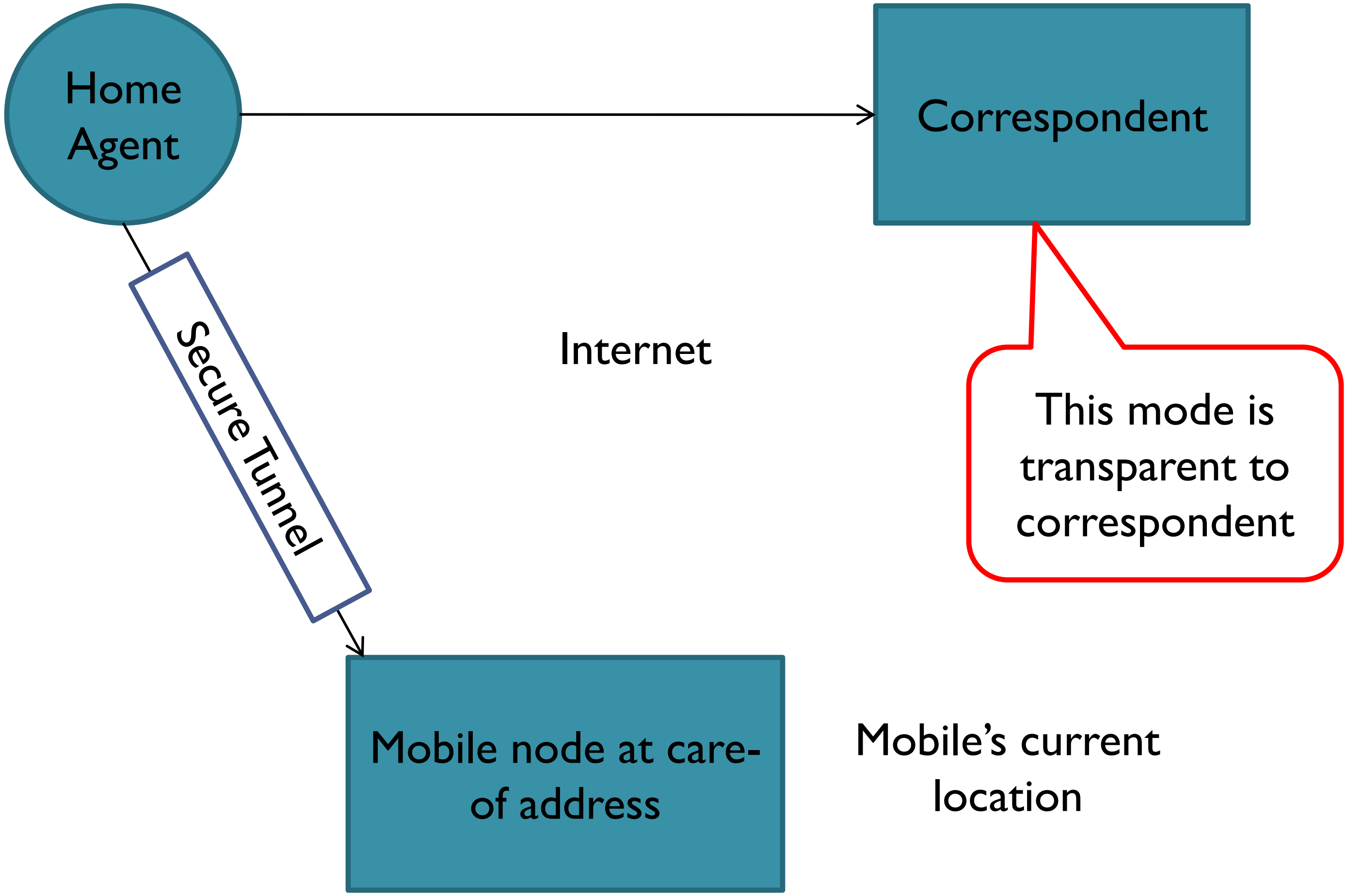
Infrastructure of Mobile IP

- Every mobile node has a home network: its original network
- Special relationship between home network and the mobile
- Home address: mobile's original address
- Home agent: a trusted router at home network
- Correspondent node (CN): a host communicates with mobile; can be any internet node; does not have any relation with mobile or home agent in advance.

Mobile IP continued

- Care-of address (CoA): mobile's current IP address
- Every time mobile connects to a new network: send binding update (BU) to home agent to inform its new care-of address
- Again, mobile IP implementation depends on the secure communication tunnel (IPsec) between mobile and its home agent

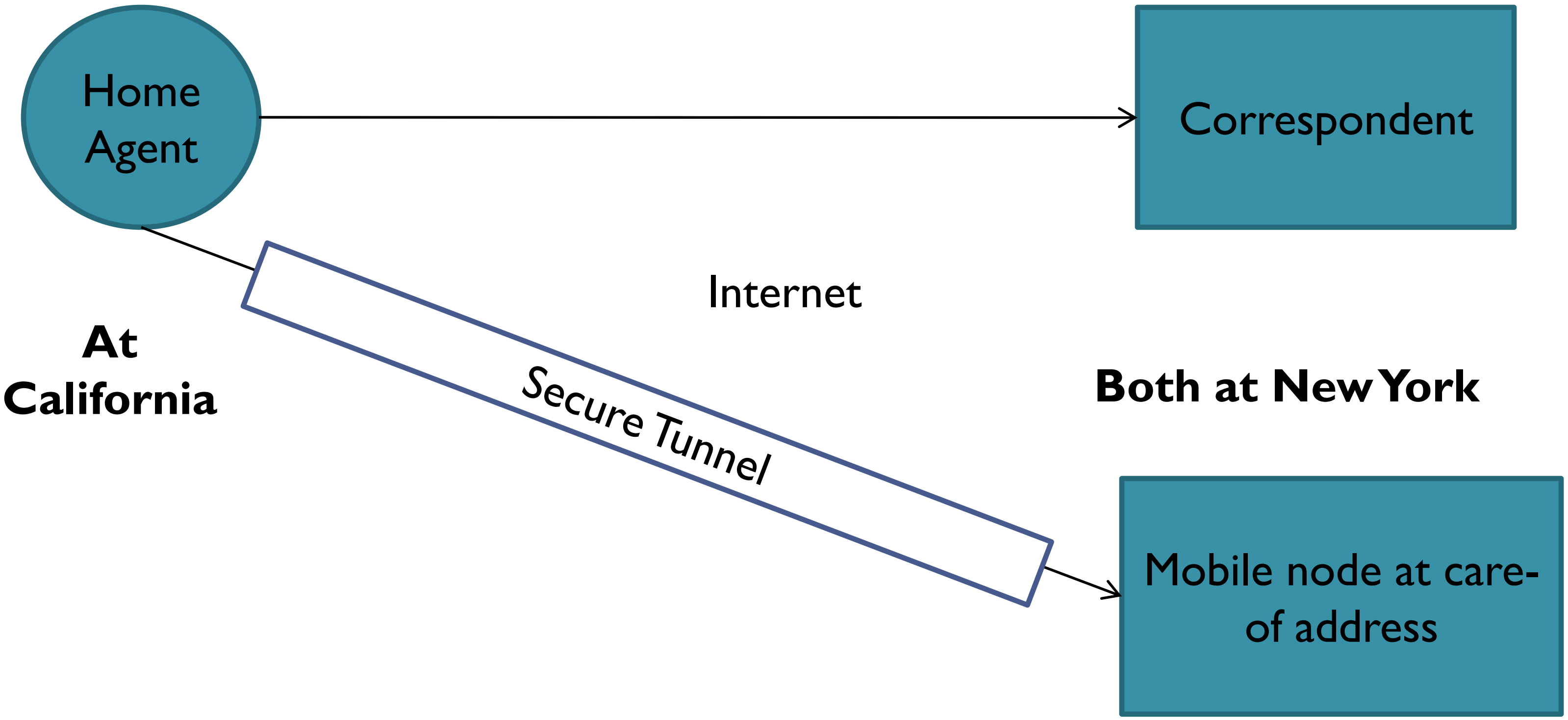
Transparent mode of Mobile IPv6



This mode is transparent to correspondent

Problem of transparent mode

- The routing is far from optimal



Home Agent

Correspondent

Internet

At California

Secure Tunnel

Both at New York

Mobile node at care-of address

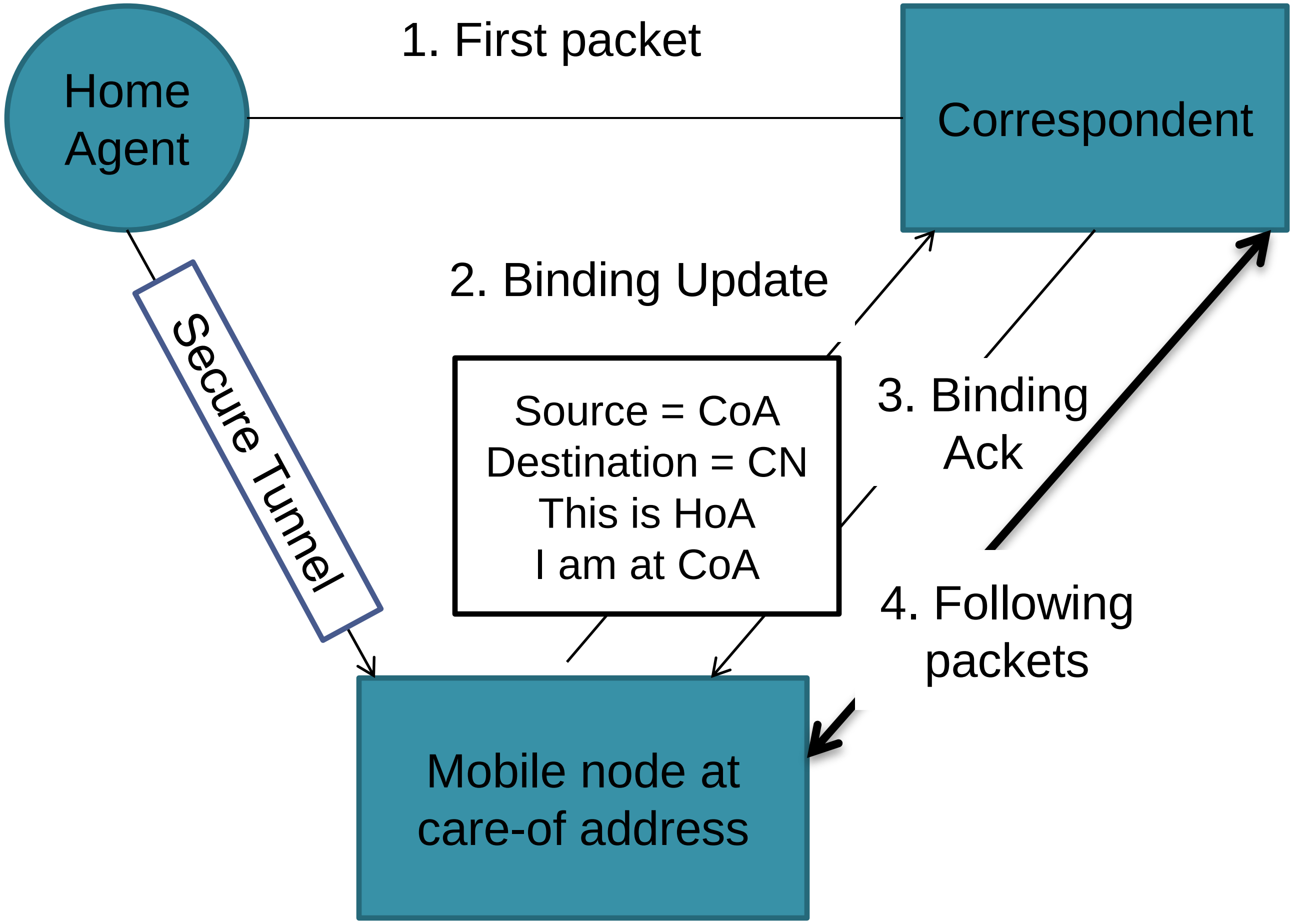
Solution: route optimization (RO)

- The optimization requires the configuration of correspondent (simple)
- **Important: binding update (BU),** contains home address and new care-of address
- When mobile's address is changed, it sends binding update (BU) to all its correspondents

Route optimization (RO)

- Correspondent acknowledges the BU and store address information of mobile in a binding cache
- Mobile: refresh the binding every few minutes even if it's address is not changed
- If cache entry (binding) expires or is deleted, correspondent will send packets to home address again

Route optimization protocol



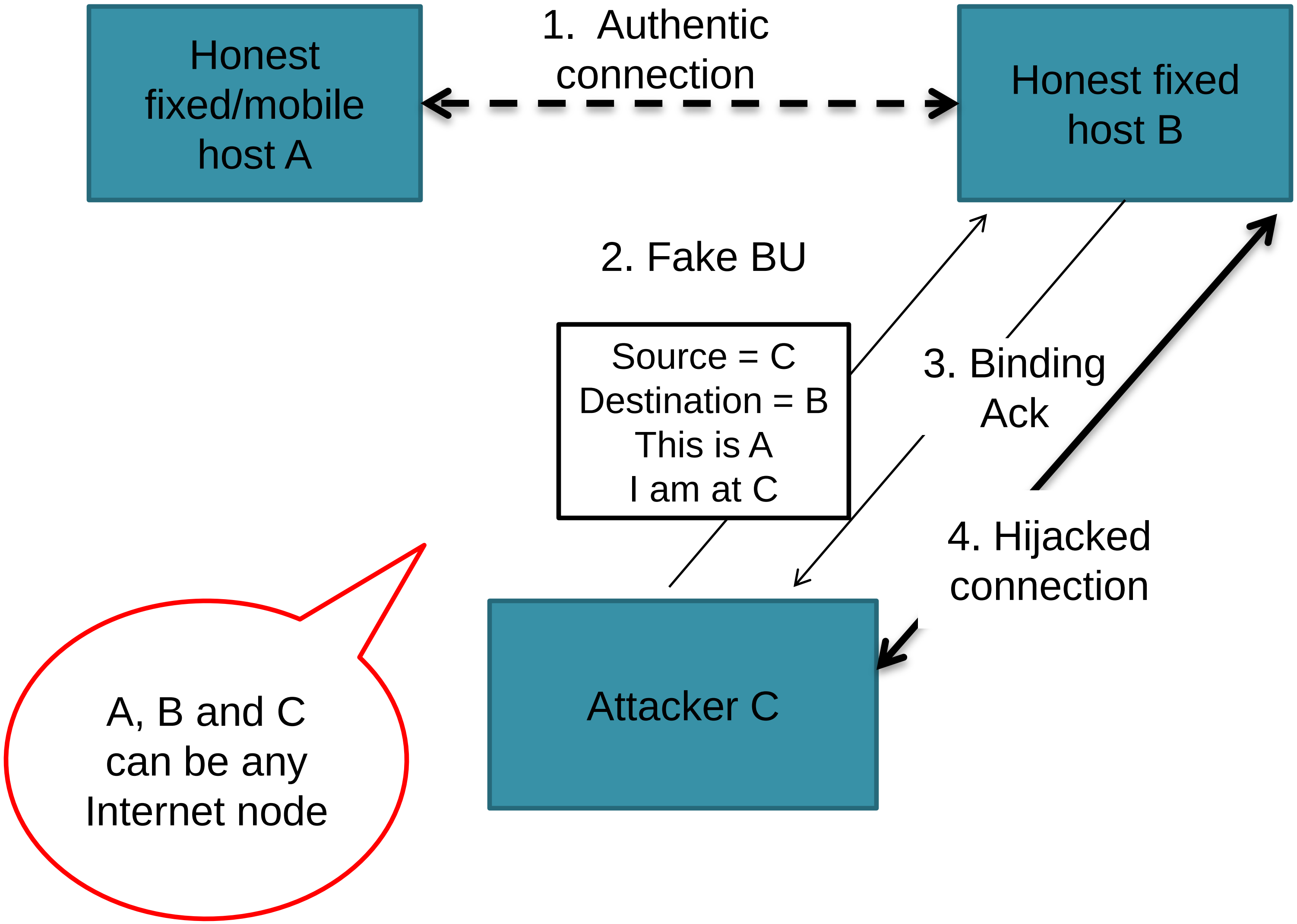
HAO and RH

- home-address destination option (HAO): contained in direct packets from mobile to correspondent, it's a IPv6 Destination Option extension header
- Routing header (RH): contained in packets from correspondent to mobile
- Both of two headers contain home address of mobile
- Benefit of this design: avoid redundant header fields resulted from full IP encapsulation

What will mobile and correspondent do with RH and HAO

- Mobile: upon receiving a packet, copies home address from RH into destination address field, in order to re-produce original IP packet
- Correspondent: after receiving a packet, overwrites source address field with home address in the HAO, thus also re-produce original packet
- In this way, mobility is transparent to upper layers (IPsec, transport layer)

Vulnerability: BU spoofing



Honest fixed/mobile host A

1. Authentic connection

Honest fixed host B

2. Fake BU

Source = C
Destination = B
This is A
I am at C

3. Binding Ack

4. Hijacked connection

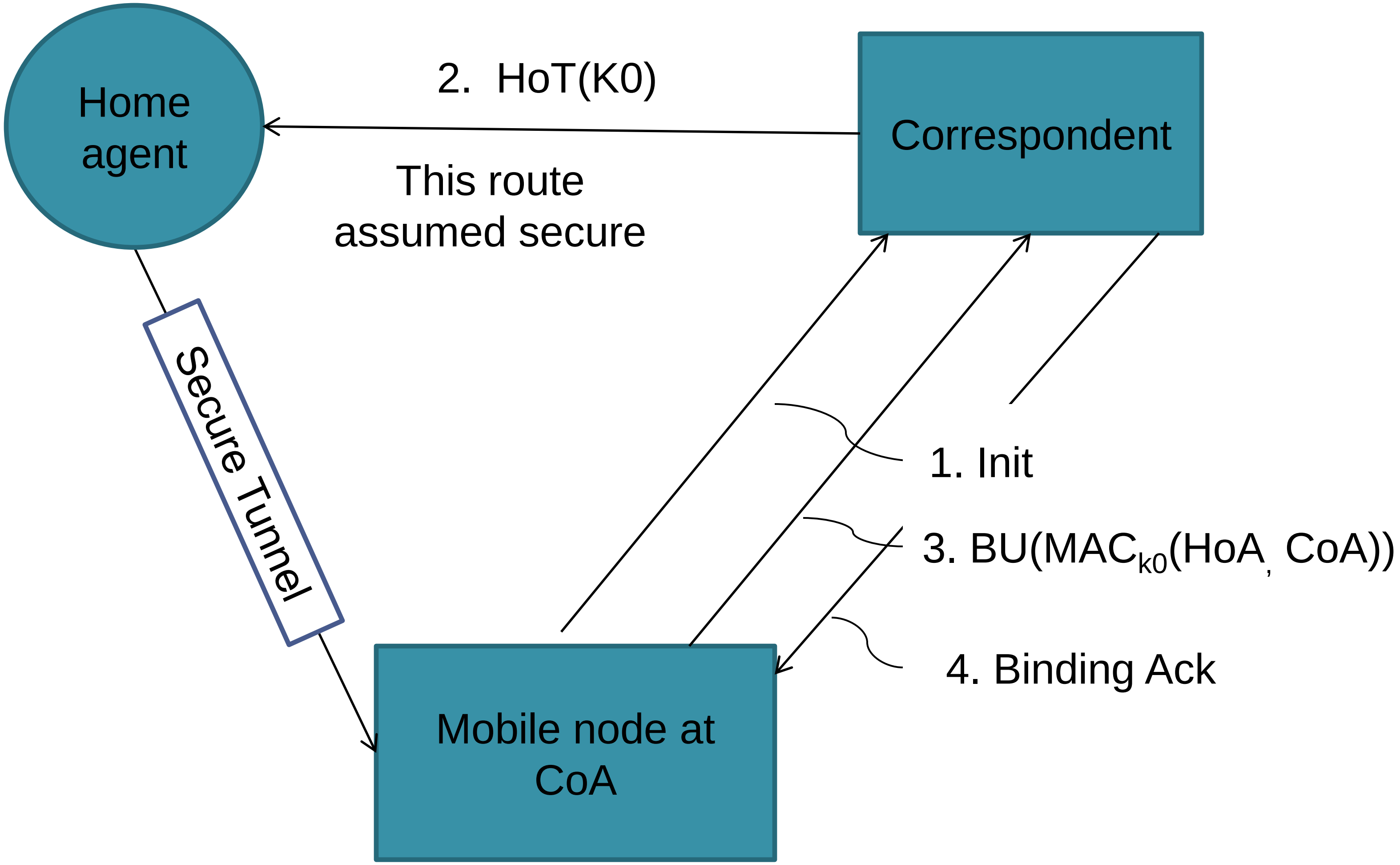
Attacker C

A, B and C can be any Internet node

Solution: infrastructureless authentication

- Goal: as secure as current non-mobile IPv4 Internet
- Not practical to set up infrastructure for all IPv6 nodes
- Consider somehow unconventional and “weak” authentication method
- Ambition of designer: Mobile IPv6 does not bring new vulnerability to Internet

Return routability test

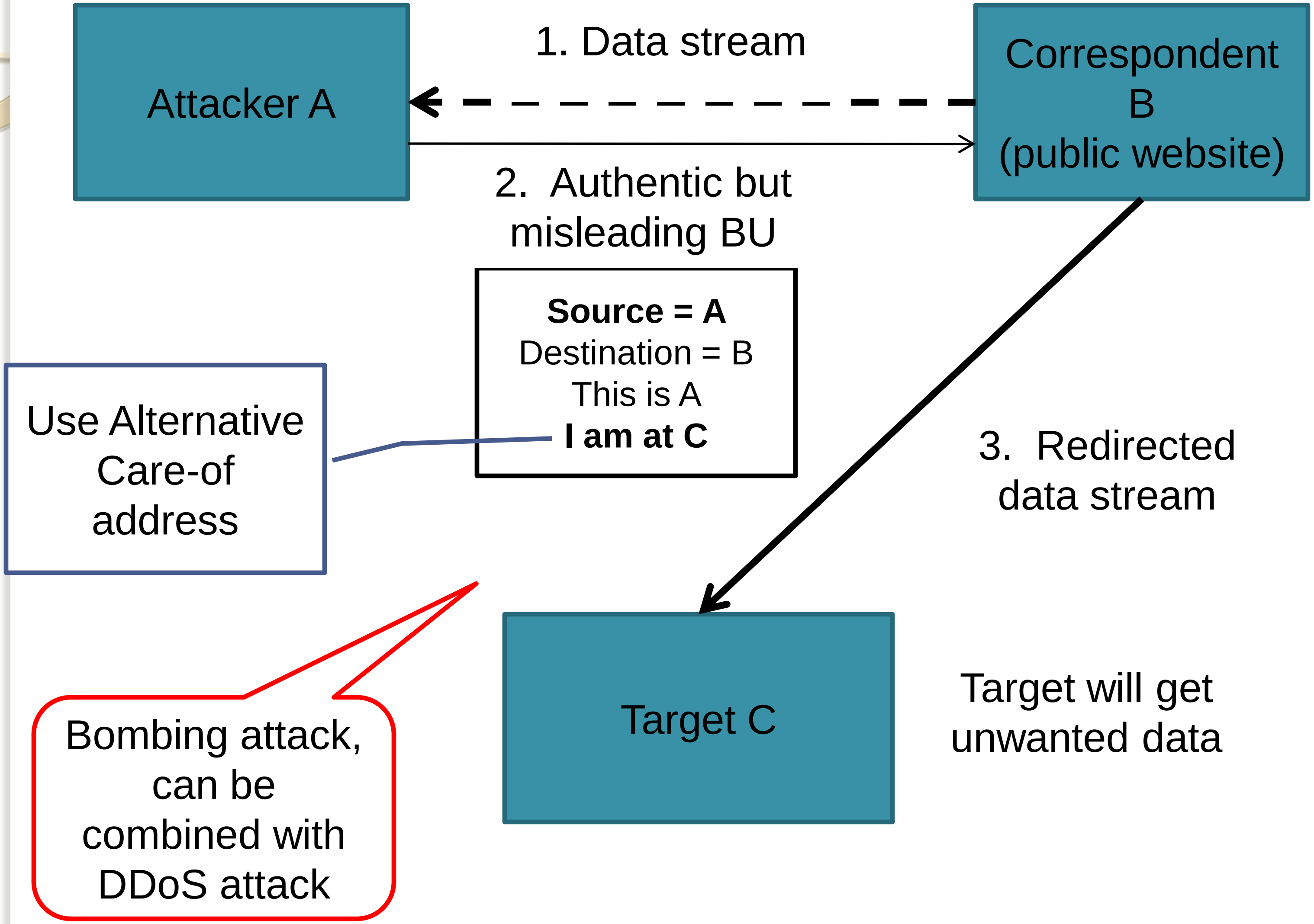


Analysis of RR for HoA

- Based on the fact: it's hard for an attacker to change the route of packets if she is not on the route
- Not secure against standard network-security attacker model
- But two strong arguments support the design:

1. Number of potential attackers is dramatically reduced
2. Achieved the original design goal

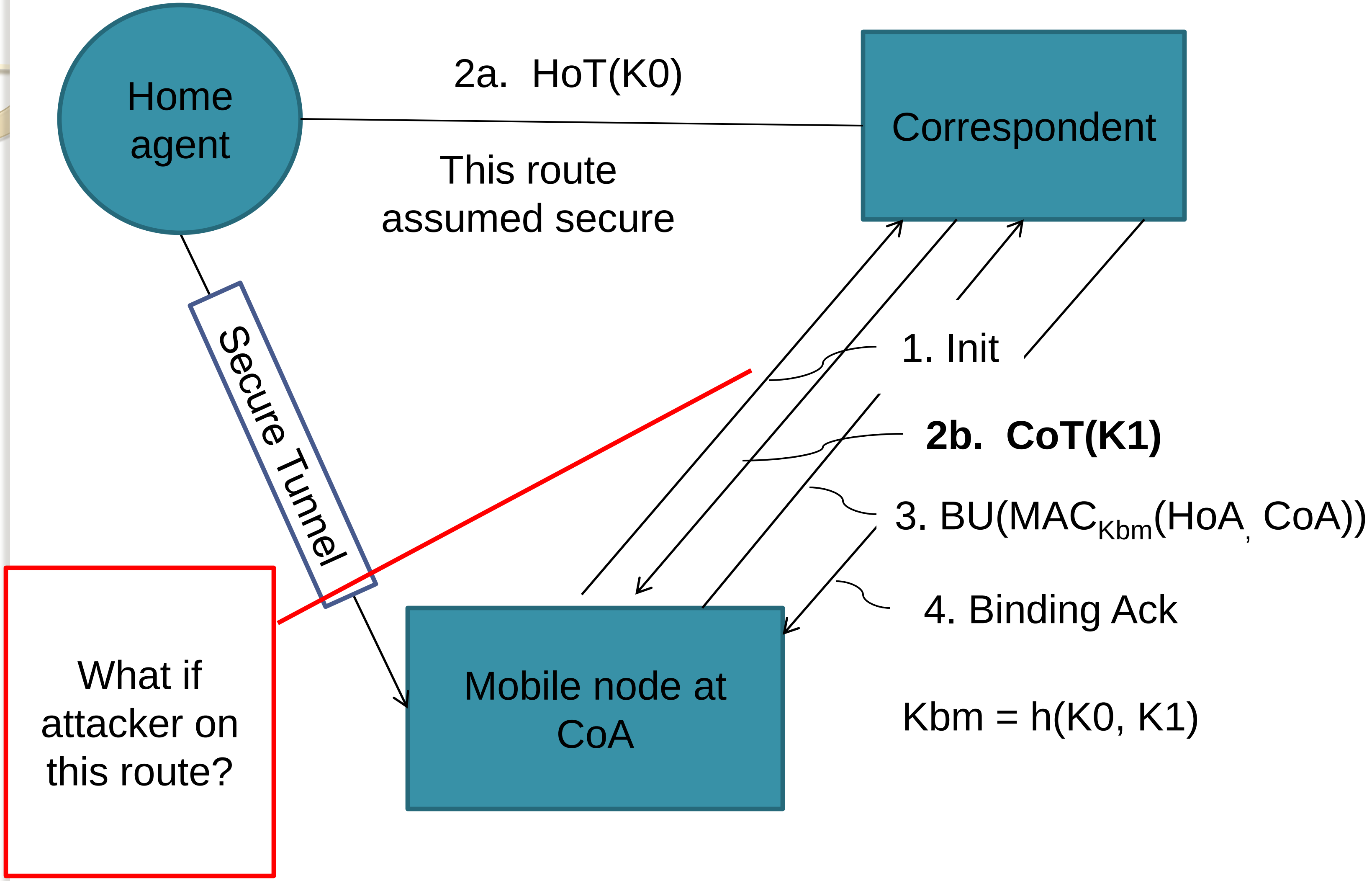
Vulnerability: current address


Attacker A
1. Data stream
Correspondent B (public website)
2. Authentic but misleading BU
Source = A
Destination = B
This is A
I am at C
Use Alternative Care-of address
3. Redirected data stream
Bombing attack, can be combined with DDoS attack
Target C
Target will get unwanted data

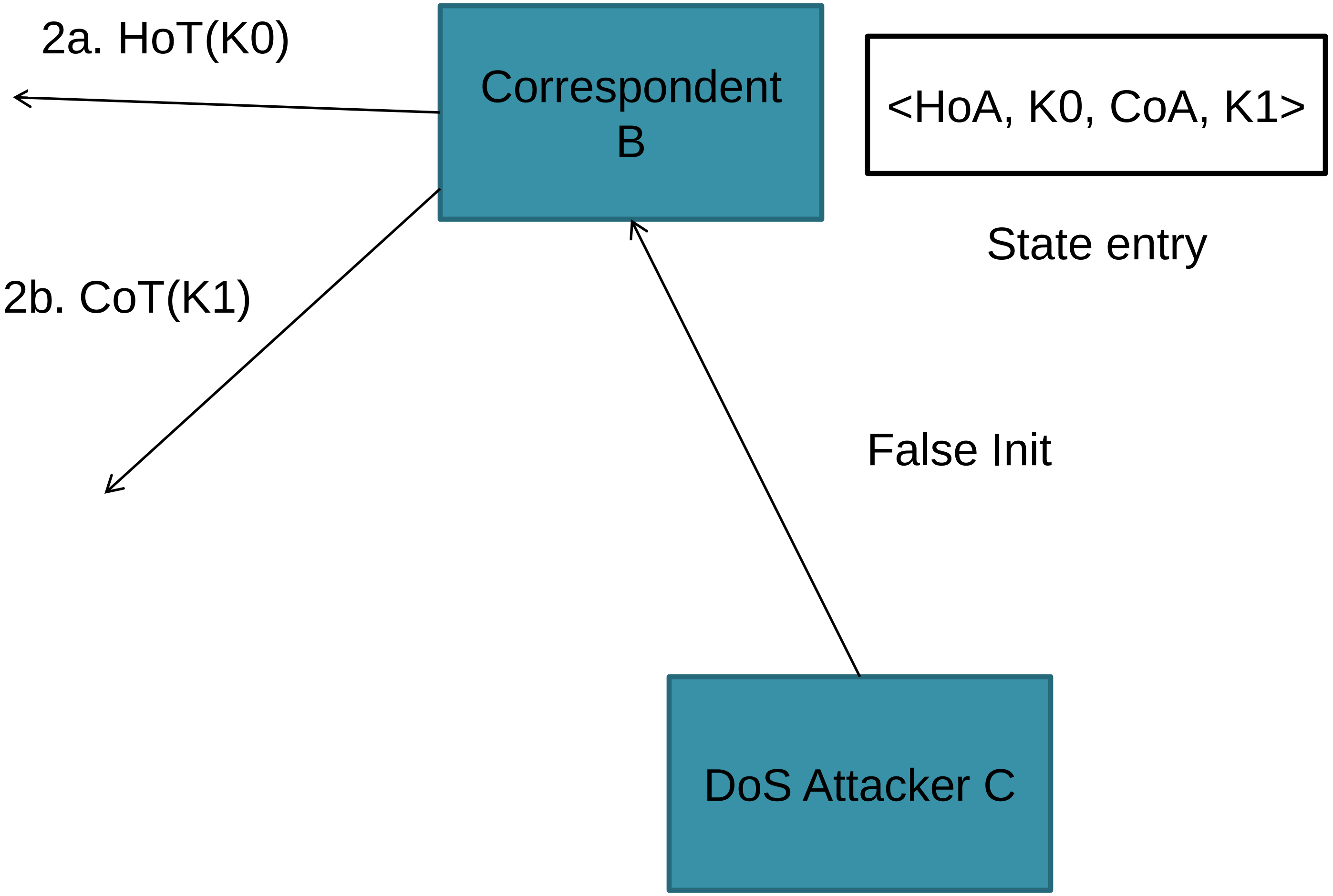
What can target do?

- Target will not acknowledge those unsolicited packets, but attacker will
- TCP Rest: will never be sent, because of routing header

Solution: return routability test for care-of address



Attack: state-storage exhaustion



2a. HoT(K0)

Correspondent B

<HoA, K0, CoA, K1>

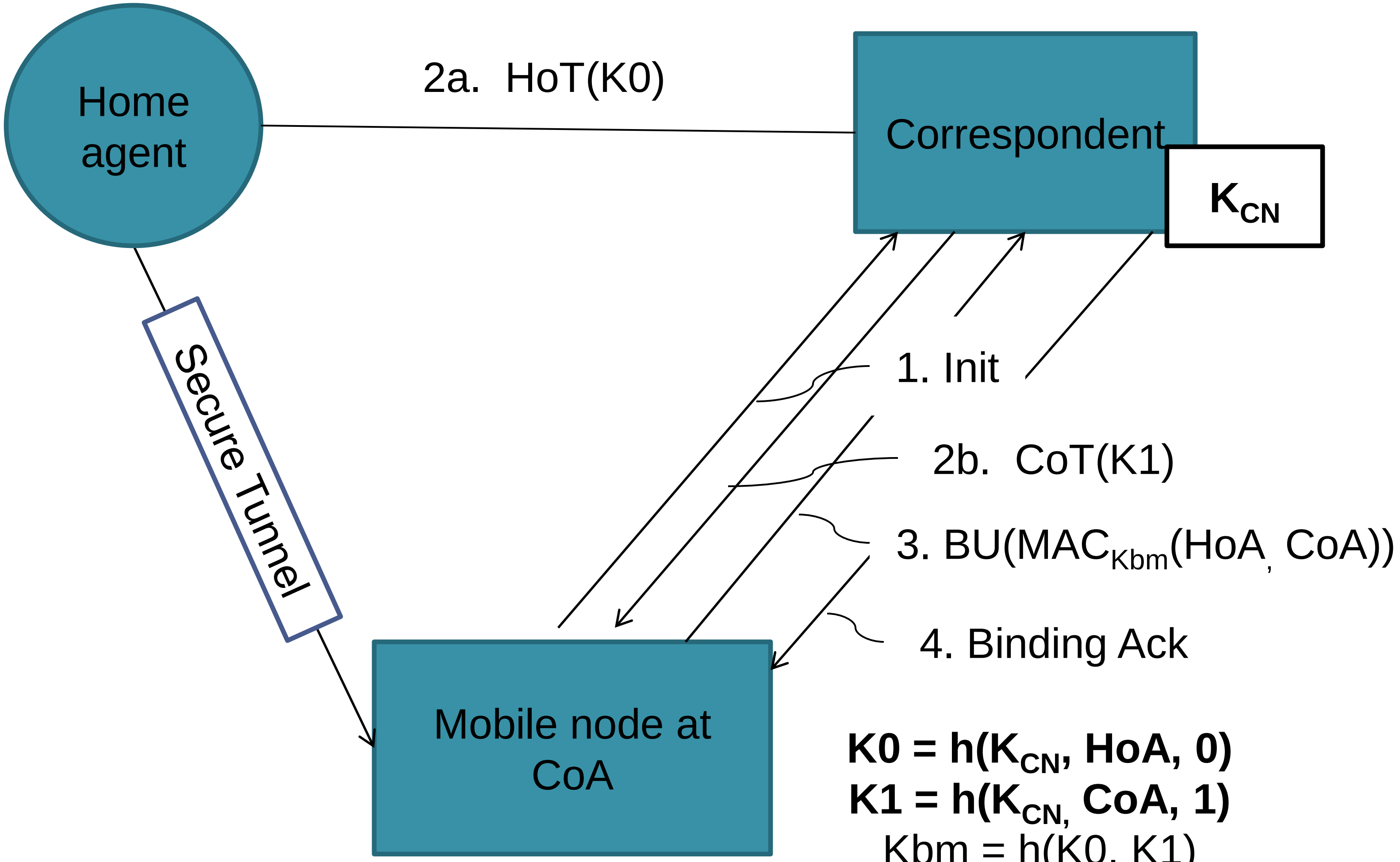
State entry

2b. CoT(K1)

False Init

DoS Attacker C

Solution: Stateless correspondent



Home agent

2a. HoT(K0)

Correspondent

K_{CN}

Secure Tunnel

1. Init

2b. CoT(K1)

3. BU(MAC_{Kbm}(HoA, CoA))

4. Binding Ack

Mobile node at CoA

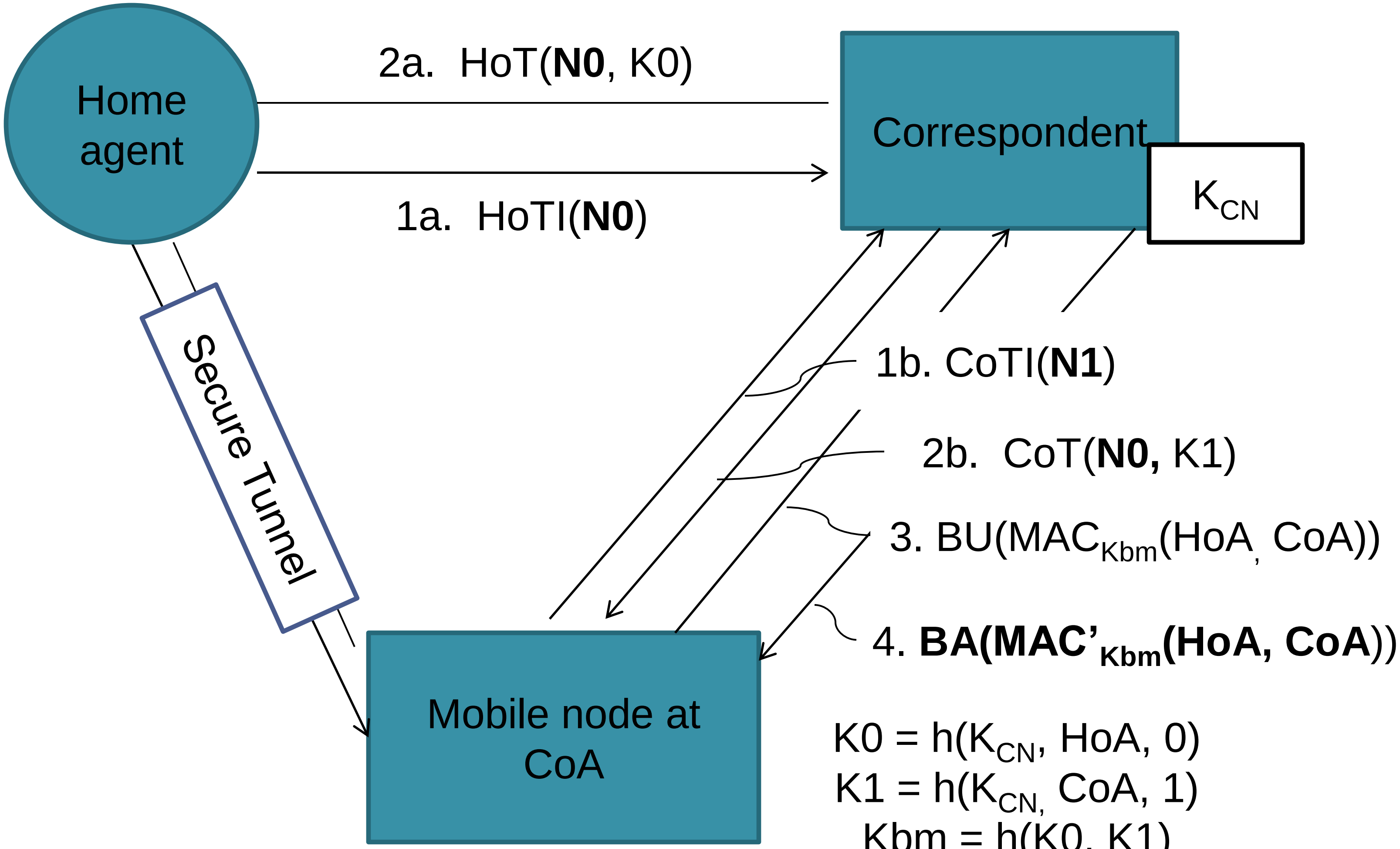
K0 = h(K_{CN}, HoA, 0)
K1 = h(K_{CN}, CoA, 1)
Kbm = h(K0, K1)

HoT, CoT and BA spoofing

- No authentication of HoT and CoT
- Solution: include nonces

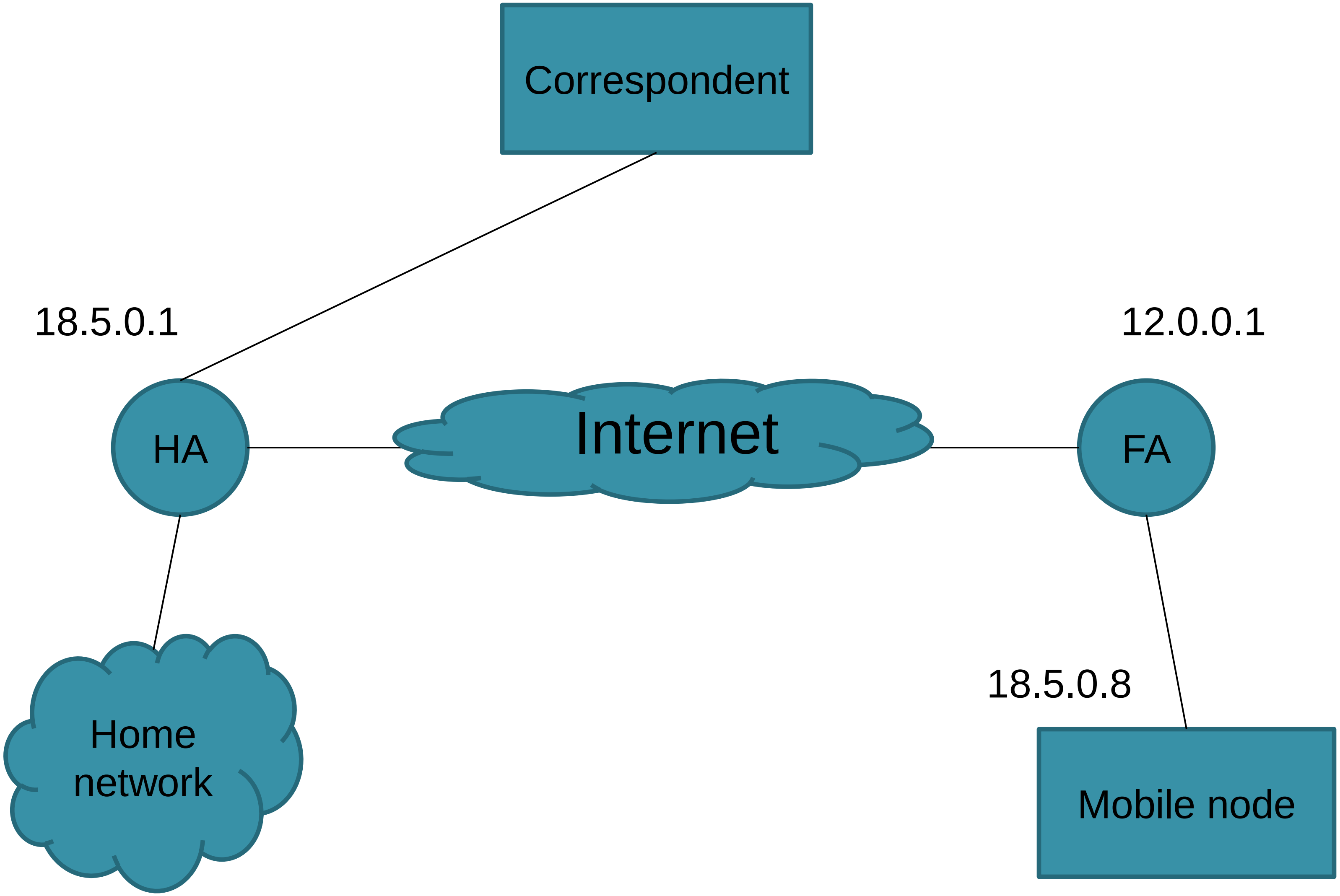
- No authentication of binding acknowledgement
- Solution: the same way as authenticate BU
- Tuomas thinks it's not necessary to authenticate BA

The complete BU protocol



$K0 = h(K_{CN}, HoA, 0)$
$K1 = h(K_{CN}, CoA, 1)$
$Kbm = h(K0, K1)$

Simple introduction of Mobile IPv4



Major differences of MIPv6 and MIPv4

- Mobile IPv6: no special router as "foreign agent"
- Mobile IPv6: route optimization is a fundamental part, while in Mobile IPv4 it's a nonstandard set of extensions
- Mobile IPv6 uses routing header, avoiding overhead resulted from IP encapsulation in Mobile IPv4

Conclusion

- Route optimization: resulted in many vulnerabilities during design
- Goal achieved: prevents new threats, rather than generic strong security protocol.

References

- Tuomas Aura, Mobile IPv6 security. In Proc. Security Protocols, 10th International Workshop, LNCS, Cambridge, UK, April 2002. Springer.
- Tuomas Aura, Michael Roe, Designing the Mobile IPv6 Security Protocol, April 2006 Technical Report MSR-TR-2006-42
- D. Johnson, C. Perkins, J. Arkko, Mobility Support in IPv6, RFC 3775, June 2004
- C. Perkins, IP Mobility Support for IPv4, RFC3344, August 2002
- S. Deering, R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December 1998