

IPv6 Forum Korea

Mobile IPv6 Security

2002. 3. 6

Mun@computing.ssu.ac.kr

List of Topics

 Securities Problems in MIPv6

 Detailed threat scenarios

 Schemes

 PBK

 BU3WAY

 SAP

 BAKE/2

 CAM-DH




 Shared Key


 BAKE

 Conclusions

Security Problems in MIPv6

 Is IPSEC adequate ?

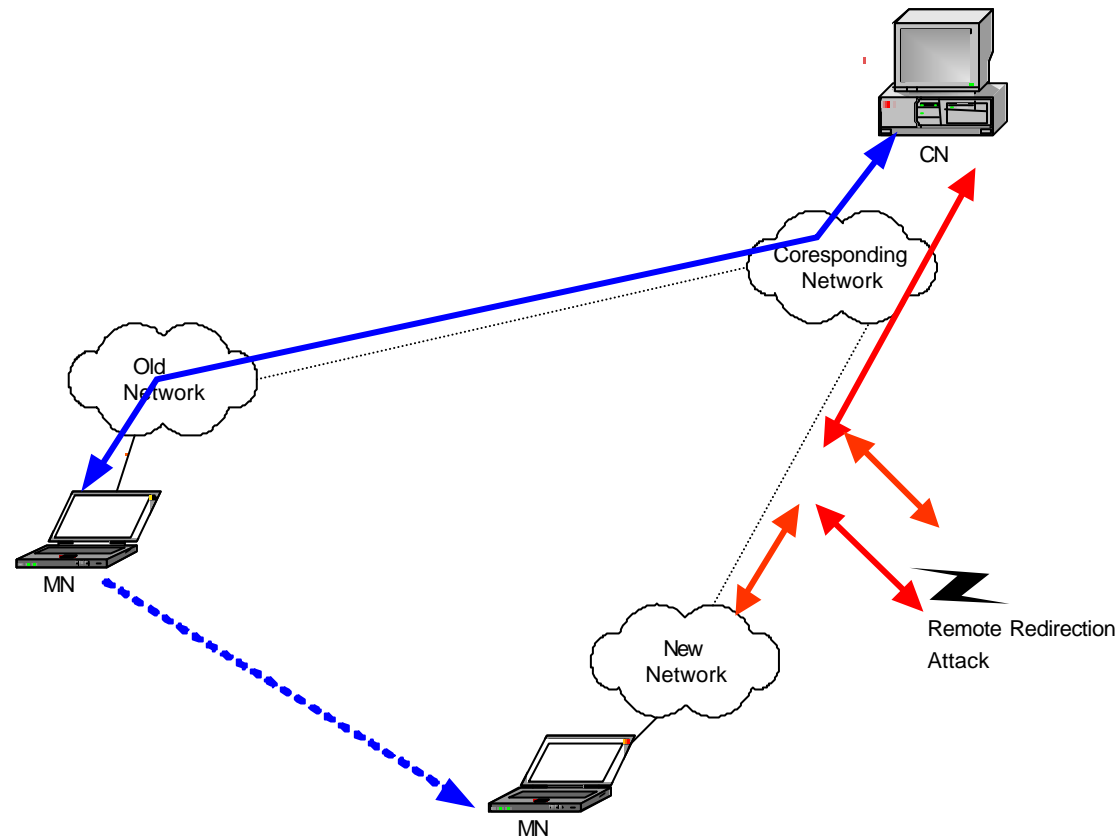
-  Global key distribution mechanism ?
-  Burden on the terminal of limited capability ?
-  Other possibility ?

 IPv6 problem ? vs. MIPv6 inherent problem ? vs. Problems aggravated due to wireless environment ?

Security Problems in MIPv6

 Redirect attack may be remote

- ✂ Attacker do not have to be on the same link as the communicating peers



Security Problems in MIPv6

 Home address ownership problem

 Tampering with the Binding Cache Entry

at HA / CN /at temporal HA



 Dos Attack

- Divert
- Make an entity busy, not doing any useful job

 Masquarading AP in wireless environment is disastrous

Attack

Passive attacks

-  Read packets (ex. Address, Password sniffing attack)

Active Attack: Modify or write packets

-  MITM Attack
-  DoS Attack
-  Masquarading Attack: MN(CN), HA, AP

Threat Models introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6

-  <draft-ietf-mobileip-mipv6-scrty-reqts-02.txt> by Allison Mankin

Detailed Threat Scenarios

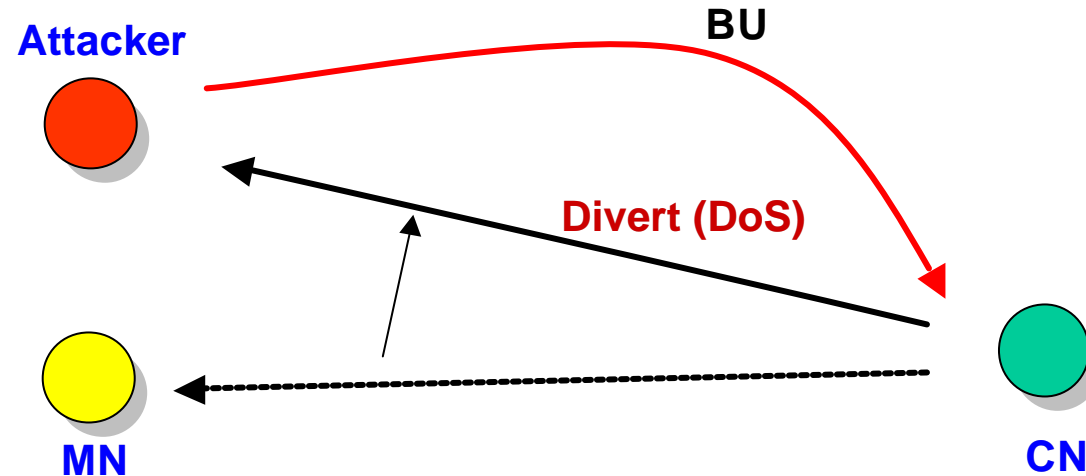
Attack	Attacker Location	Effect	Remarks
A1	Anywhere	MITM/DoS	Needs to know Home Address
A2	Anywhere	MITM/DoS	Needs to know Home Address
A3	Anywhere	DoS	No Prior knowledge needed
B1	MN's link	MITM/DoS	Using only BUs
B2	MN's link	MITM/DoS	Using Non-MIPv6 Mechanism
B3	Close to MN	MITM/DoS	Tamper with Radio Interface
B4	MN's (future) link	MITM/DoS	Tampering Binding Acks
C1	CN's link	MITM/DoS	Using Non-MIPv6 Mechanism
D1	HA's link	MITM/DoS	
D2	HA's link	Multiple	Acting as an HA
E1	CN $\not\leftrightarrow$ HA link	Masq/DoS	Attack without BUs
E2	CN $\not\leftrightarrow$ HA link	MITM/DoS	Defeat Home Address check
F1	MN $\not\leftrightarrow$ CN link	DoS	Attack without BUs
F2	MN $\not\leftrightarrow$ CN link	MITM/DoS	Immune to ingress filtering
G1	MN's (past) link	MITM/DoS	Fool temporary HA
H1	Anywhere	Disclosure	Topology information exposed
H2	Anywhere	DoS	Use HA as a reflector
H3	Anywhere	DoS	Use HA as a reflector

Attacker located anywhere

Threat A.1

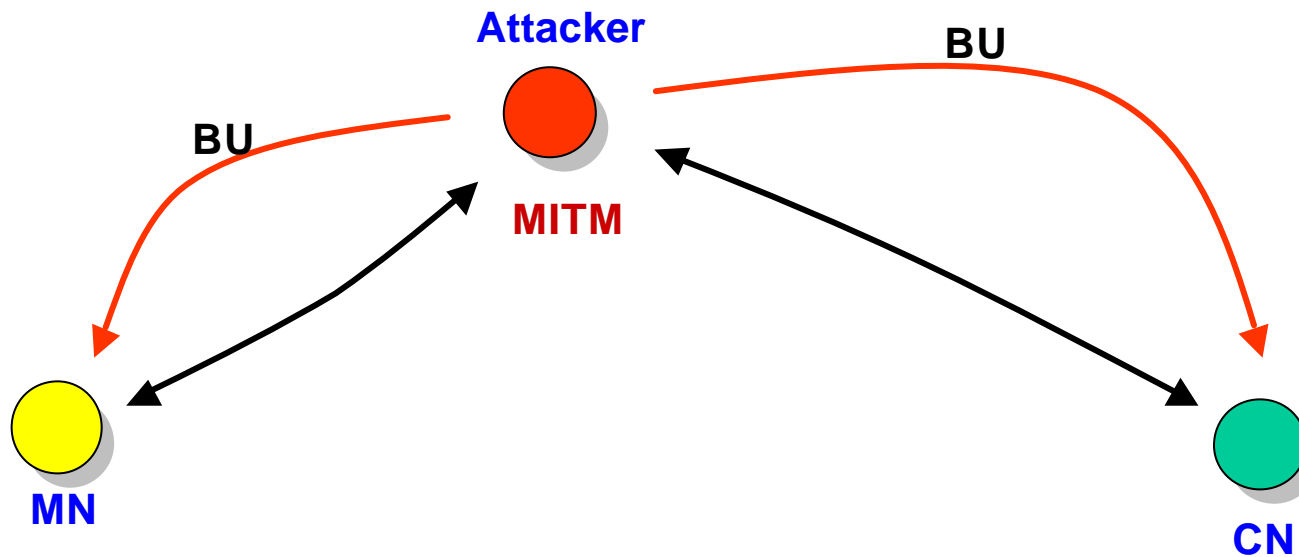
-  Attacker knows MN's Home Address (& CN's address)
-  Attacker sends BU to CN

Effect: DoS Attack



Attacker located anywhere

 Effect: MITM Attack



 Requirement

 BU node가 Home Address binding update

Attacker located anywhere

Threat A.2

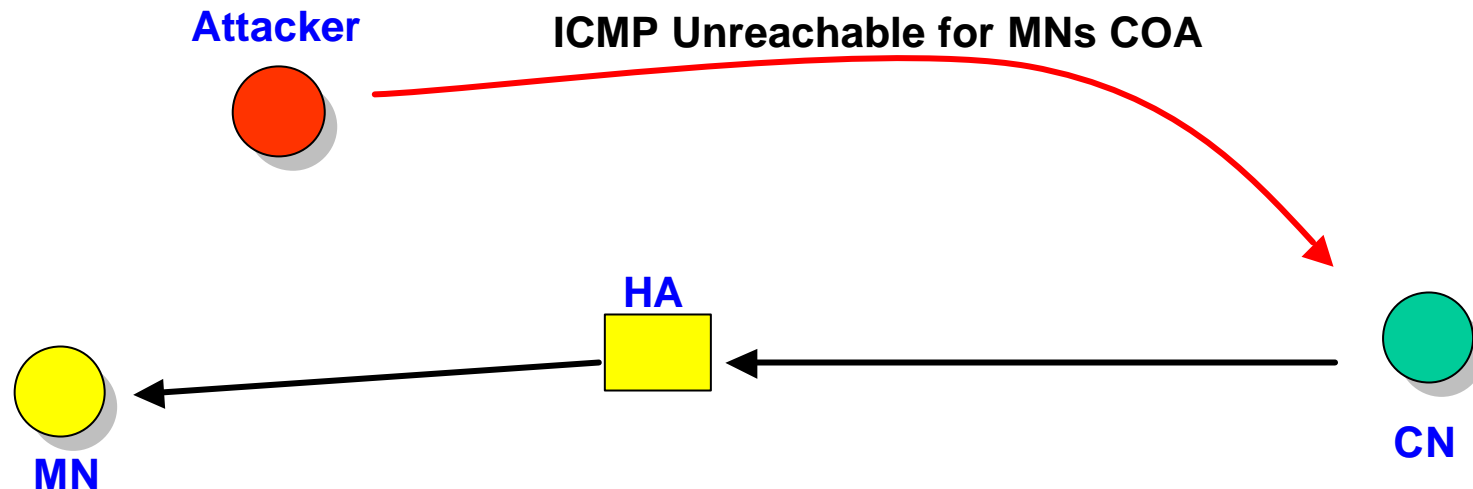
- ✂ Attacker sends ICMP unreachable for MNs COA

Effect

- ✂ Packet from CN will go through HA

Requirement

- ✂ Not specific to MIPv6





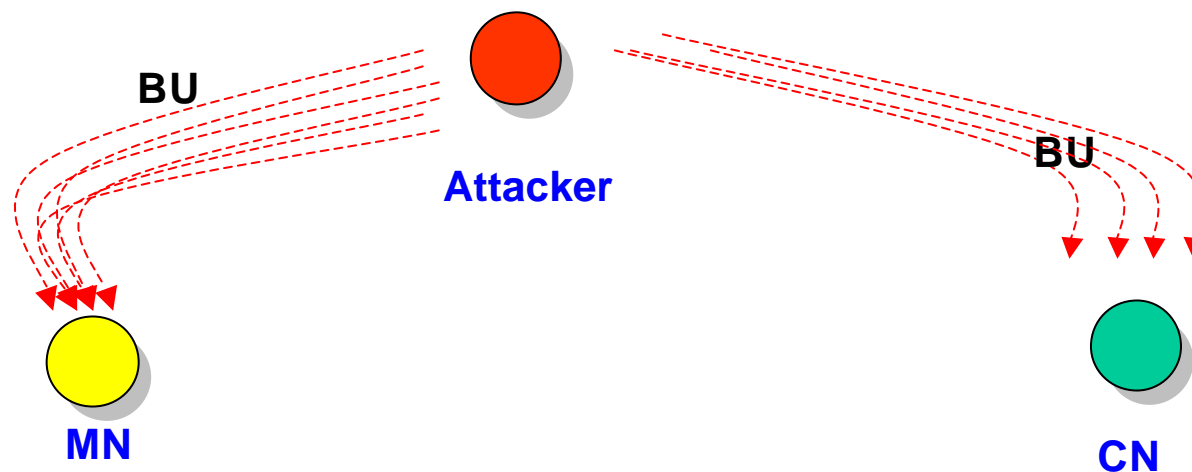
Attacker located anywhere

Scenario A.4 (BU Flooding)

-  Attacker sends MIPv6 nodes BU rapidly
-  Exhausts Binding Cache of MIPv6 nodes

Requirement

-  MIPv6 node SHOULD verify the authenticity of BU
-  MIPv6 node SHOULD have the capability of rejecting BU

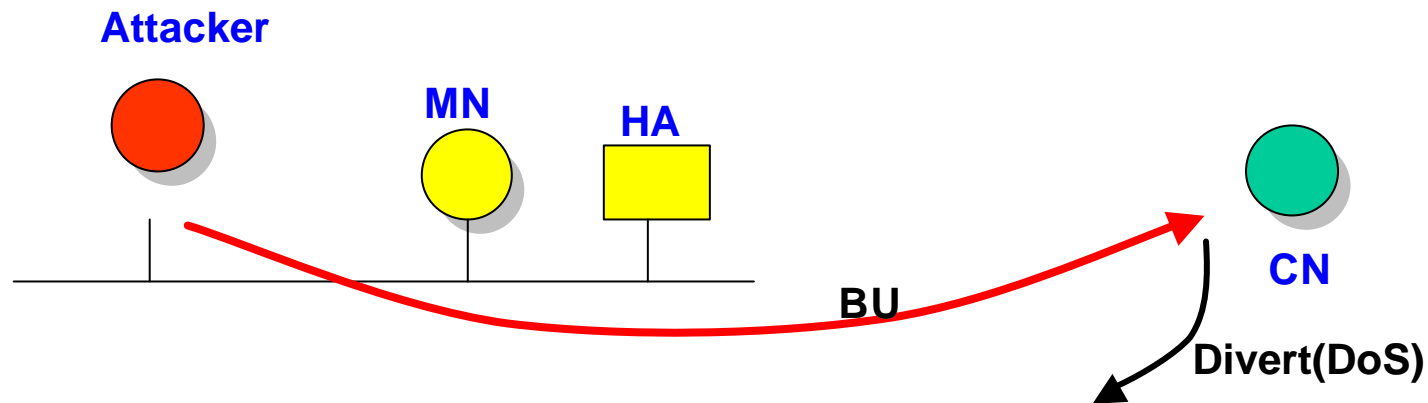


Attacker on Home Subnet

Threat D.1 (Fake BU to CN)

-  MN is on Home network  Attacker easily aware CN since it is on same subnet as MN
-  Attacker sends fake BU to CN

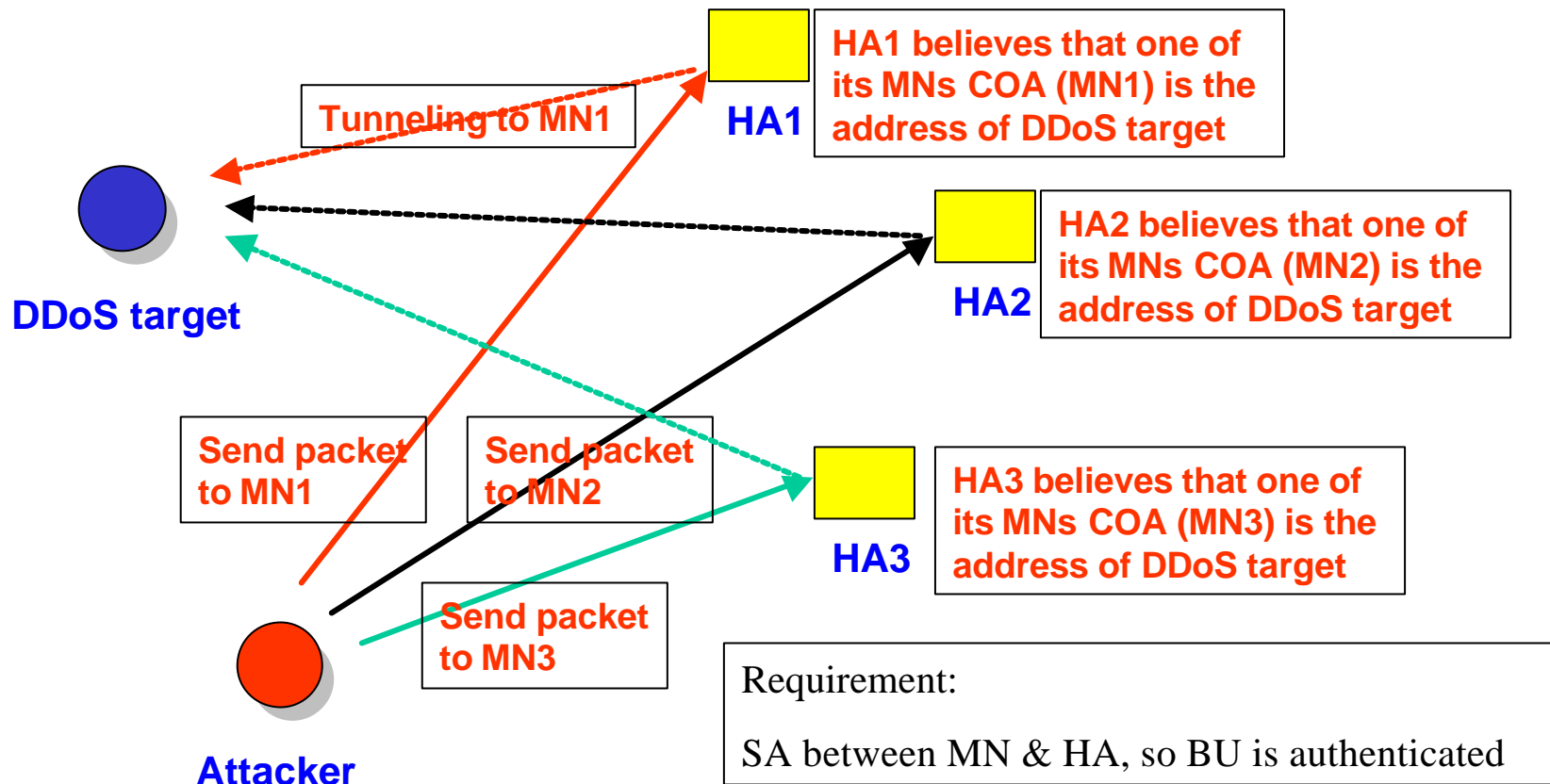
Effect: DoS Attack



Packet Reflecting Threats

Threat H.2 (HA as packet reflector)

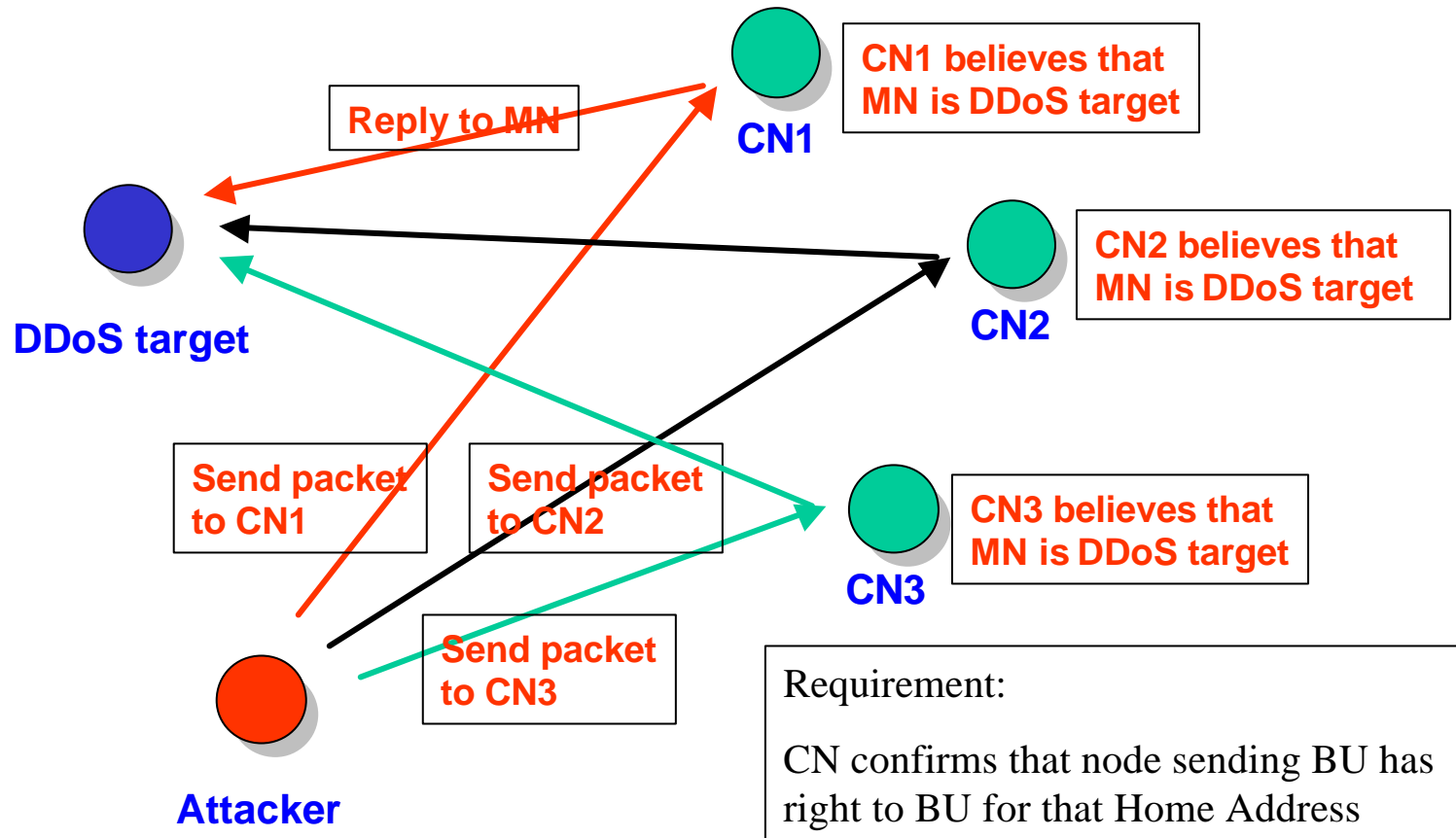
DDoS Attacker is easy to hide



Packet Reflecting Threats

Threat H.3 (CN as packet reflector)

DDoS Attacker is easy to hide





PBK

 A Framework for Purpose Built Keys (PBK)

 <draft-bradner-pbk-frame-00.txt>

 S. Bradner (Harvard), A. Mankin(USC), J.I. Schiller (MIT)

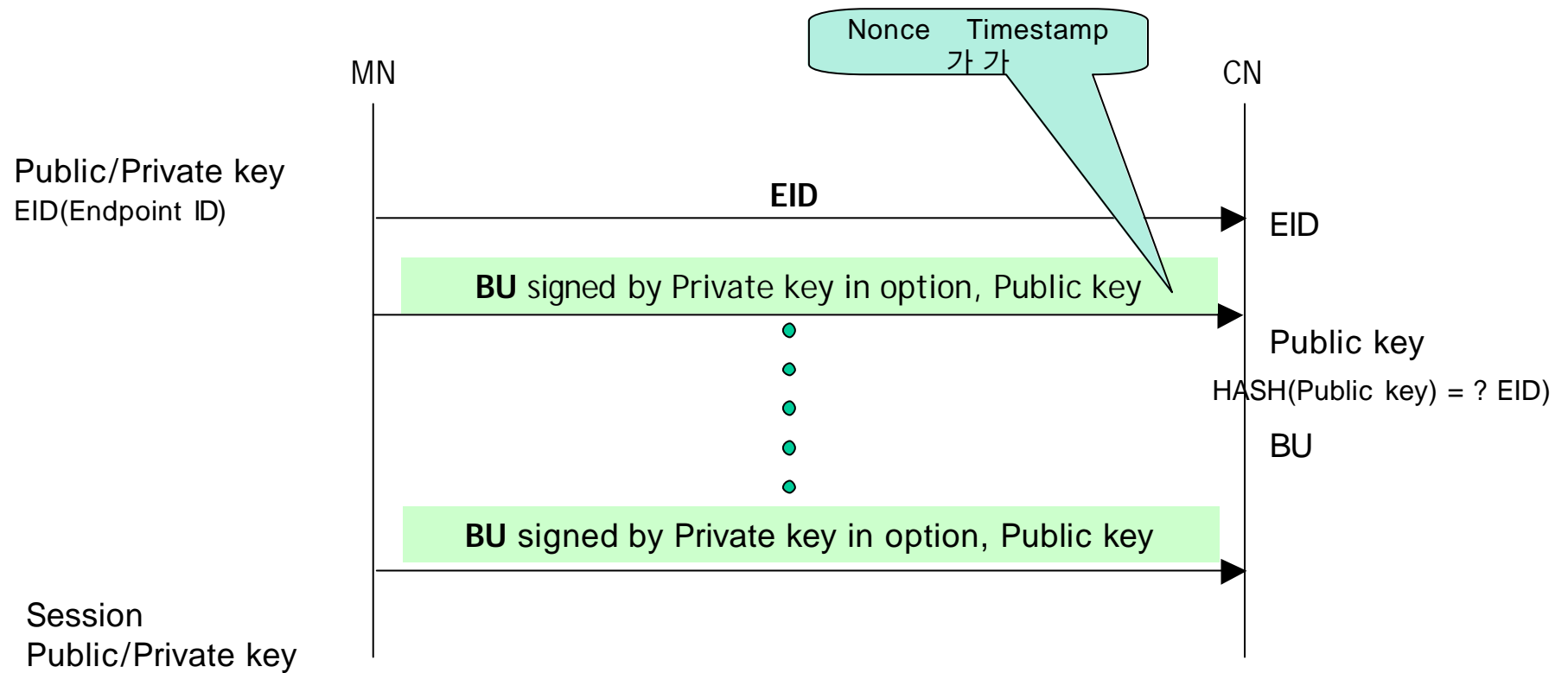
 Not intended to be used as the proof of the home address ownership

 Session BU (rebinding), BU
가 MN 가

 Session BU HoA ownership

 PBK: MN Public/Private key pairs

PBK-



BU3WAY

 Securing MIPv6 BUs using **return routability**

 <draft-nordmark-mobileip-bu3way-00.txt>

 Erik Nordmark (Sun)

 Assumption

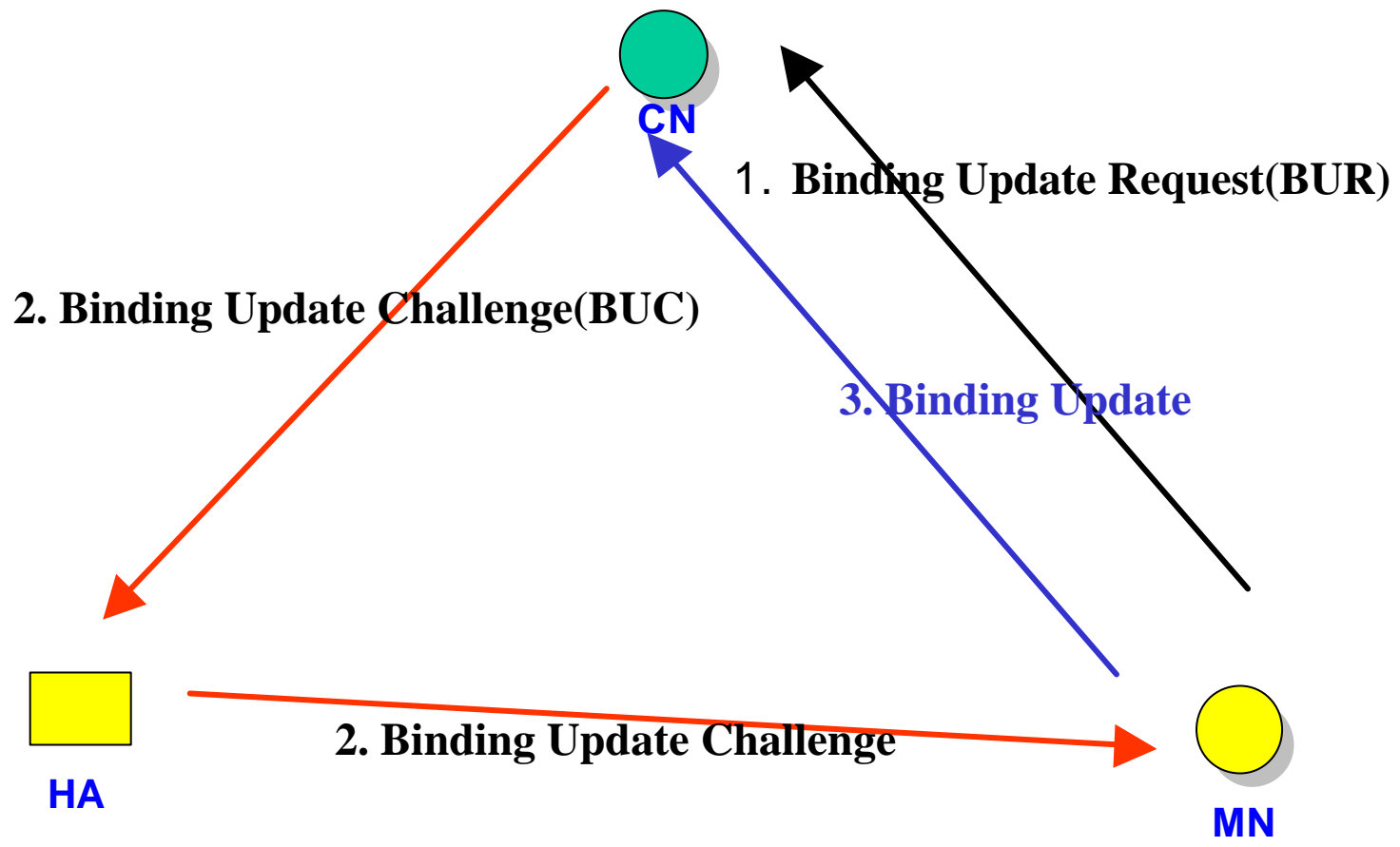
 MN & HA has SA (in both directions)

 Purpose




 Cookie가 가 ?

BU3WAY -



SAP

 Dynamic security association establishment protocol for IPv6

 <Draft-mkhail-mobileip-ipv6-sap-02.txt>

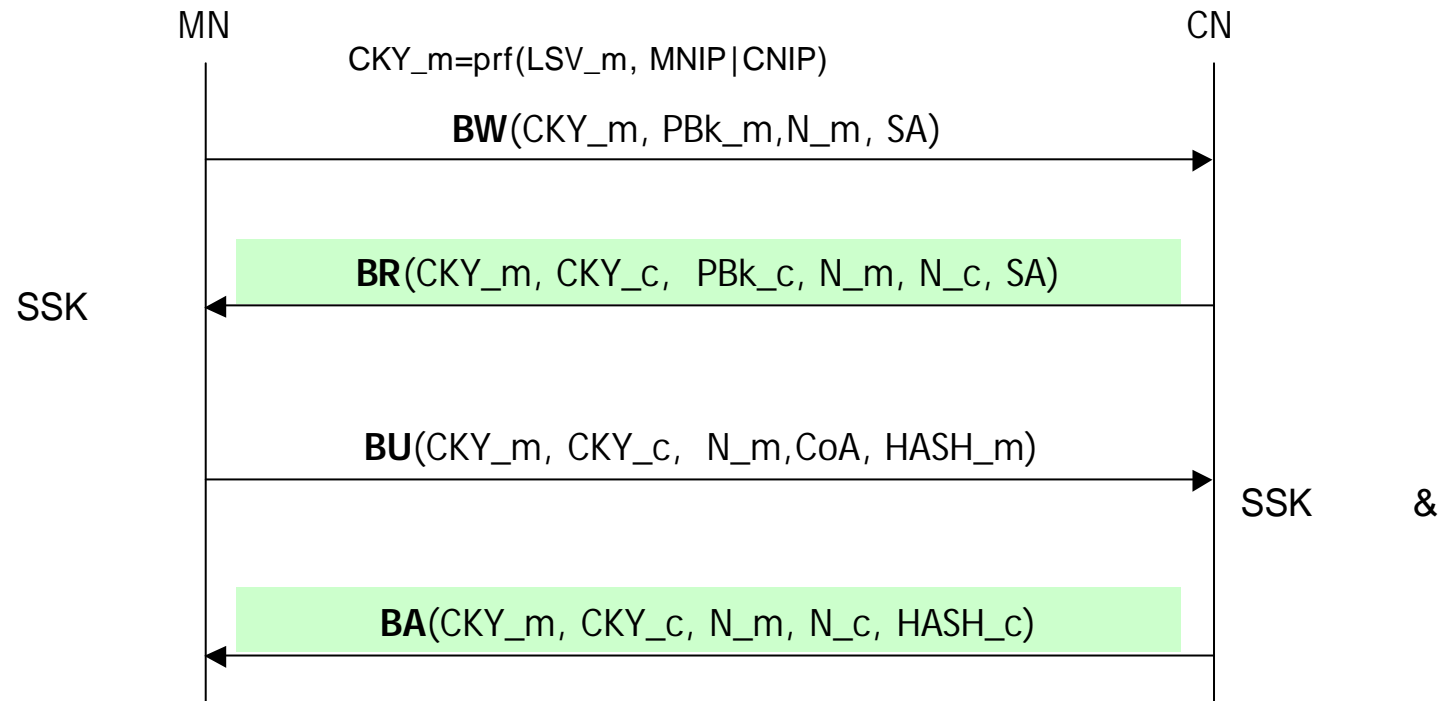
 M. Khalil, H. Akhtar, E. Qaddoura (Nortel)

 DH

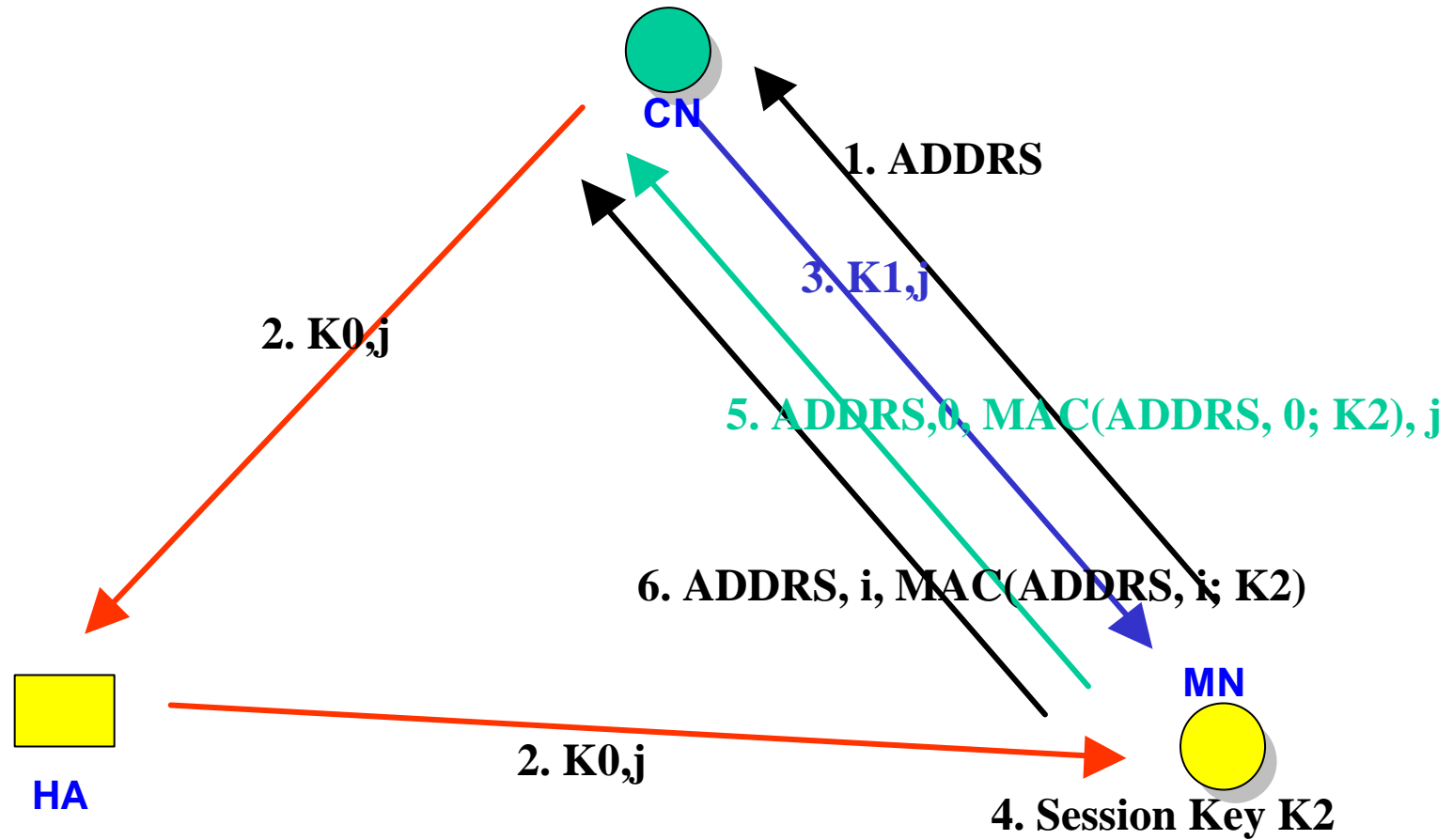


BU

SAP -



BAKE/2-

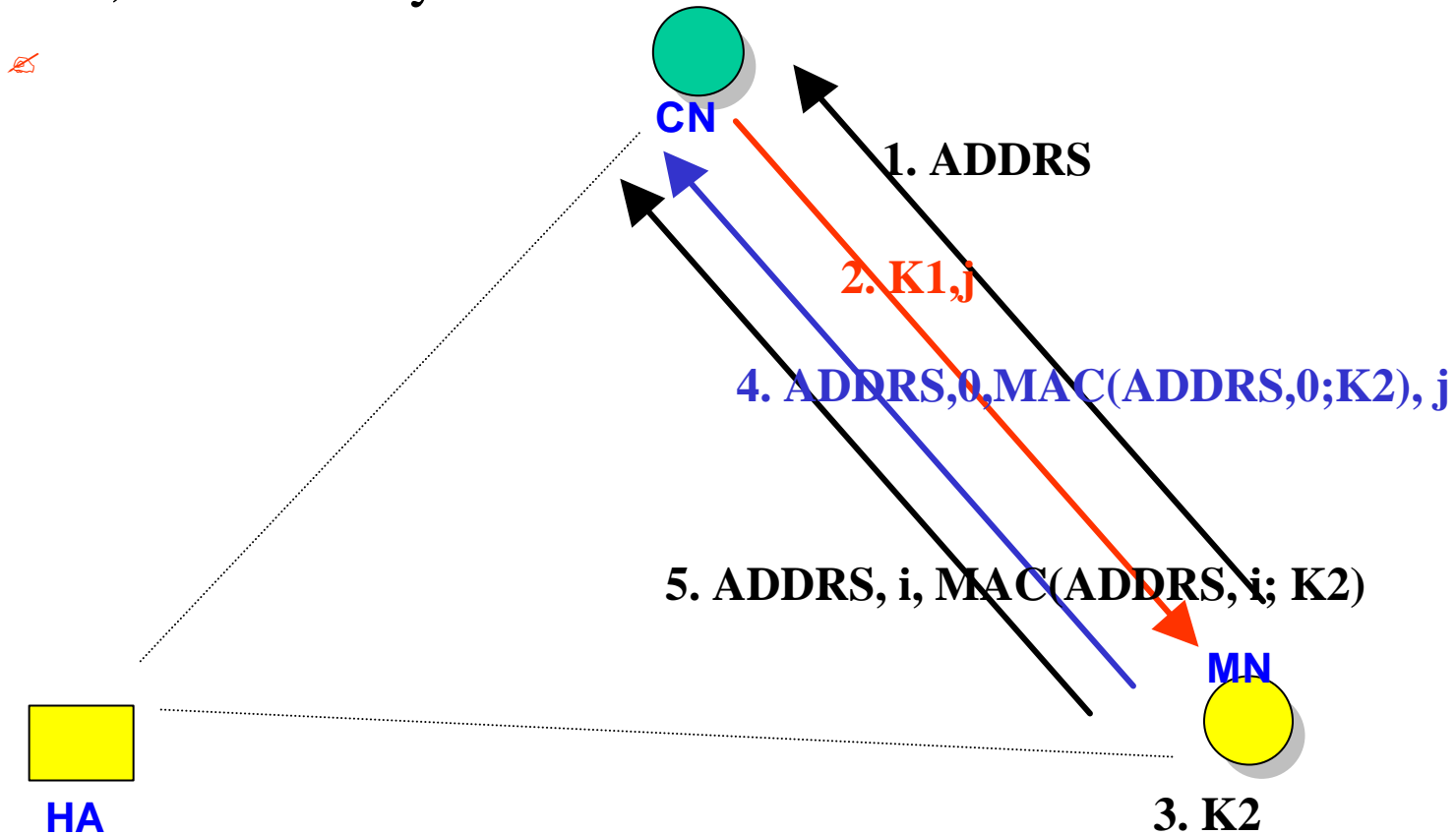


CAM - DH

- ✍ CAM-DH combines BAKE/2 with digitally signed Diffie-Hellman key exchange
- ✍ Each MN's HoA is algorithmically related to its public signature key

Shared Key


 MN CN
, Session key



BAKE

 Binding Authentication Key Establishment Protocol for Mobile IPv6

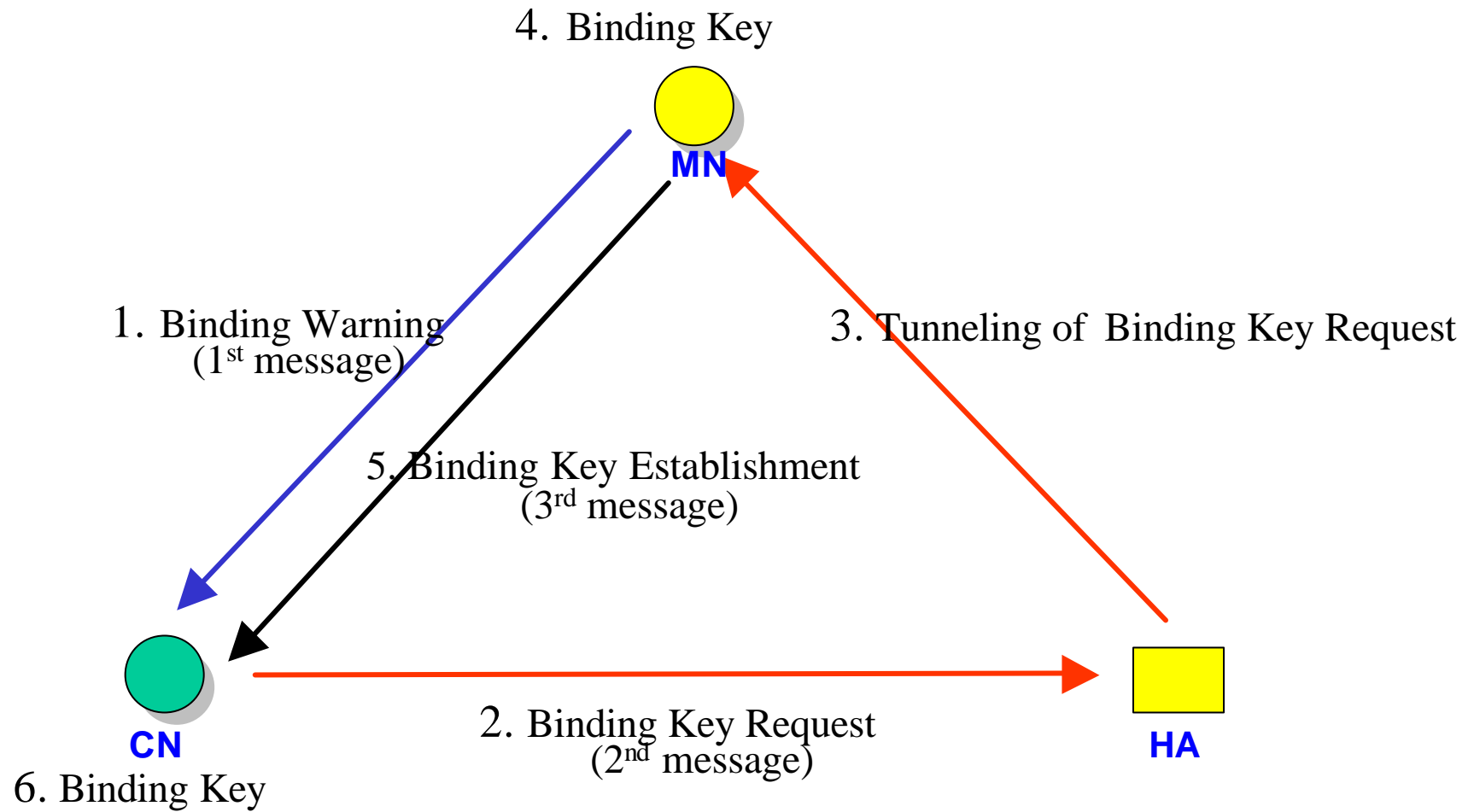
 <draft-perkins-bake-01.txt>

 Pekka Nikander (Ericsson) & Charles Perkins (Nokia)






 Tunnel between MN & HA is assumed

 Not necessarily protected by ESP

BAKE -



MIPv6

-   Not to be relied on global mechanism
-  IPSEC
 - Draft 15: Not mentioned
-  Expected not to be easily agreed
 - Effectiveness vs. Burden
-  Just one or more than one ?

IPv6

?