



Location Privacy in MobileIPv6

“Tracking the binding updates”

Alberto Escudero <alberto@it.kth.se>

*Institute for Microelectronics and Information Technology
Royal Institute of Technology KTH-IMIT. Kista - Sweden*

MobileIPv6 Tutorial as part of IDMS2001*

**8th International Workshop on Interactive Distributed
Multimedia Systems. 4-7 Sep 2001. Lancaster. UK.*

▷ *Agenda*

▷ *About secure communications*

▷ *MobileIP Route optimization*

▷ *Stateless Address Autoconfiguration vs Privacy*

▷ *The problem(s)*

▷ *The goal*

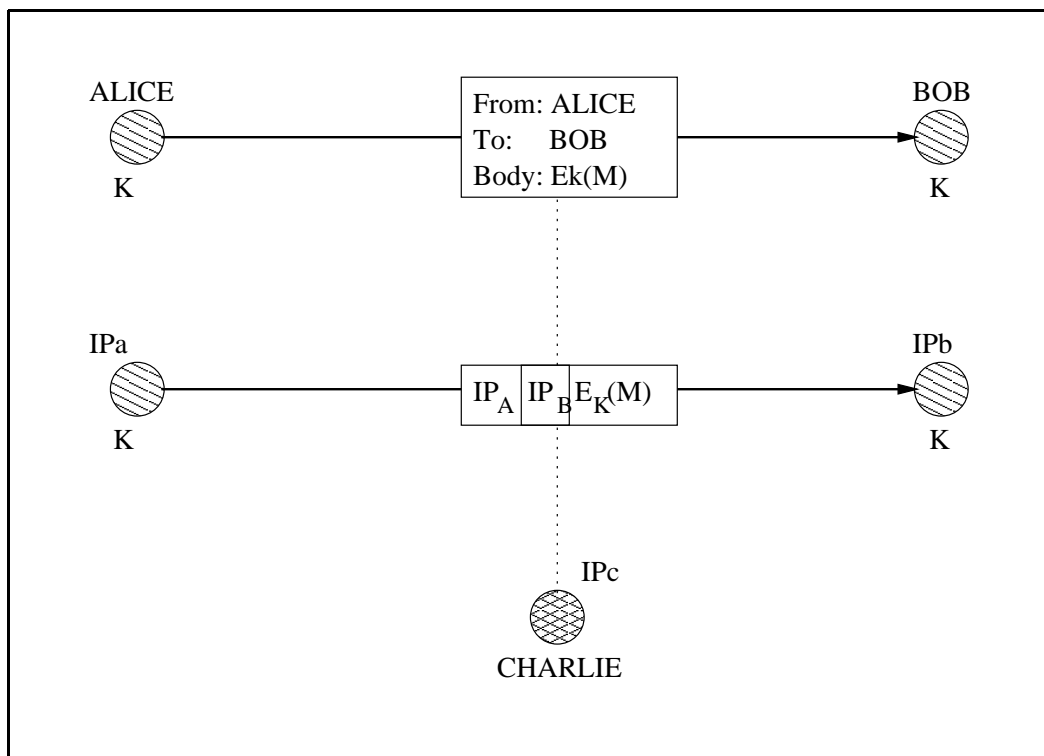
▷ *Some solutions: RFC3041, TMI, HMIPv6, Cloaking, Freedom AIP*

▷ *Conclusions*

▷ *Secure communications*

Alice sends a *Message* to Bob

- **Integrity:** No alteration of *Message*
- **Authentication:** Alice *is* Alice, Bob *is* Bob.
- **Confidentiality:** Charlie can not read *Message*



▷ *Secure communications*

Alice $\xrightarrow{E_k(M)}$ *Bob*

00 00 0c 07 ac 14 00 60 1d f1 64 d4 08 00 45 00	$MAC_R - MAC_B$
00 54 4a 26 00 00 40 01 f5 92 82 ed 14 e3 82 ed	IP_A
20 33 08 00 62 e1 1c 05 02 00 57 2d 1a 3b 19 ae	IP_B
01 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15	$E_k(M)$
16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25	$E_k(M)$
26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35	$E_k(M)$

Charlie doesn't know about M but knows:

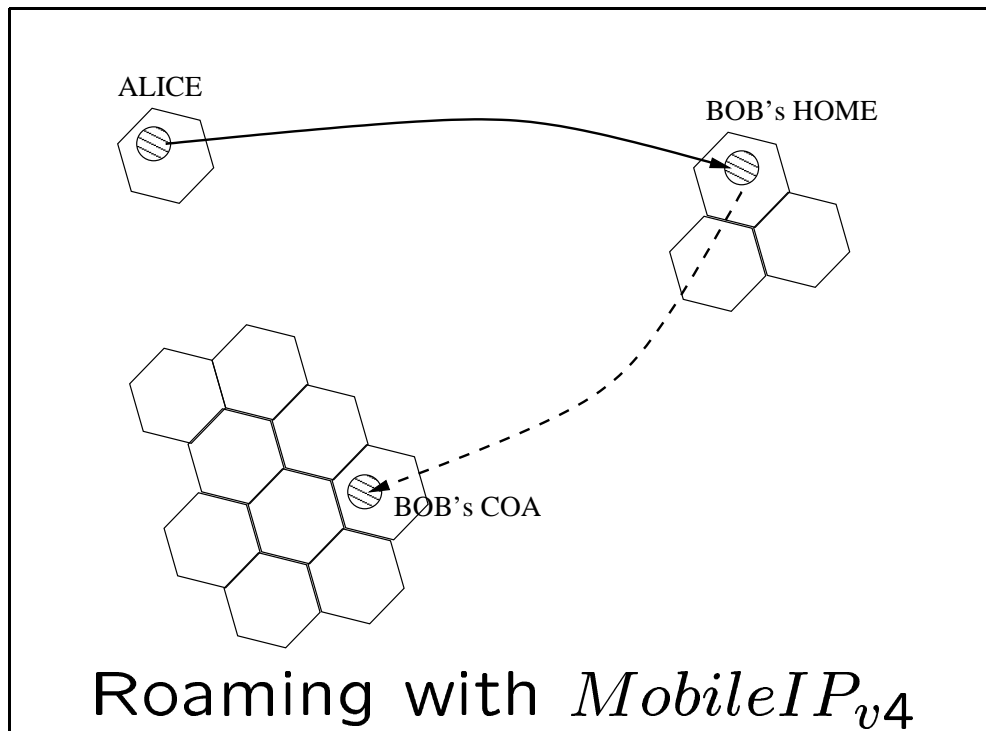
- That *Alice* is sending $E_k(M)$ to *Bob*
- $MAC_{\{A,B\}}$ if present in $Link_{\{A,B\}}$

▷ MobileIPv4

Alice sends a Message to Bob

Bob is away from $Home_{Bob}$

$Home_{Bob}$ delivers the Message to Bob's care – of – address



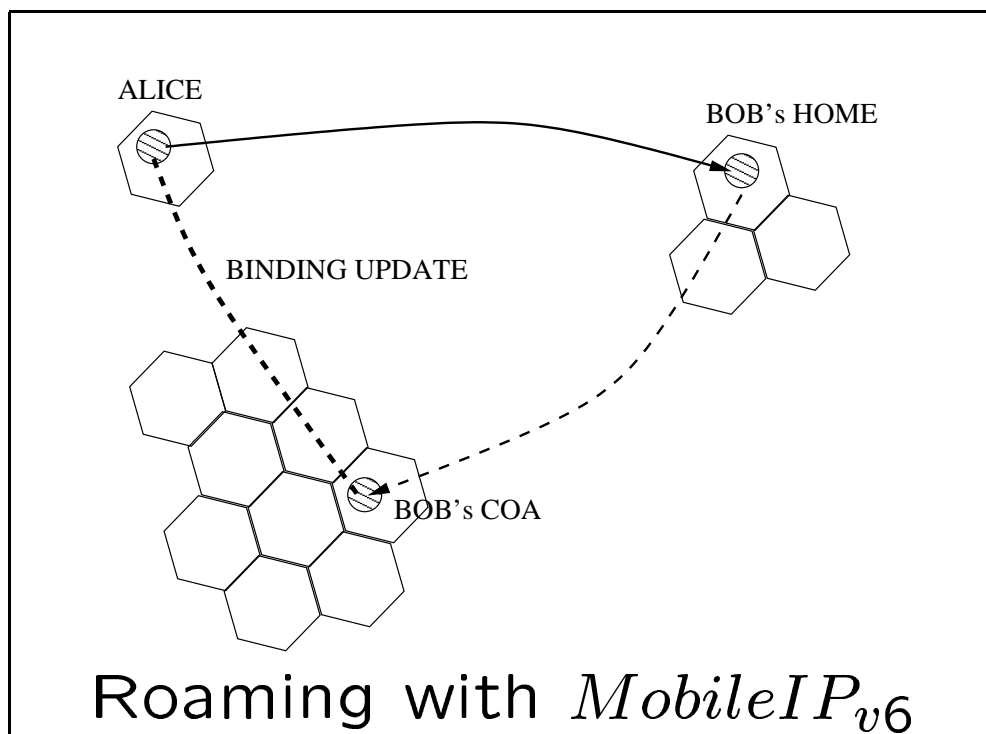
- Bidirectional tunneling conceals COA_{Bob} from Alice but not from $Home_{Bob}$ or Charlie.

- IP_{v4} Route optimization is not possible with a random correspondent node.

▷ *MobileIPv6*

$\approx \text{MobileIPv4} + \text{Routing Optimization}$

Bob can send a Binding Update to Alice
Alice can send a Binding Request to Bob



▷ MobileIPv4

$Alice \xrightarrow{E_k(M)} Bob_{HA} \xrightarrow{E_k(M)} Bob_{COA} \xrightarrow{E_k(M)} Bob$

At home: $CN \Rightarrow MN$

Roaming: $CN \Rightarrow (HA \Rightarrow COA) \Rightarrow MN$

00 60 1d f1 64 d4 00 02 4b de ea d8 08 00 45 00	$MAC_B - MAC_r$
00 68 b7 ee 40 00 3e 04 94 e2 82 ed d5 03 82 ed	$IP_{HA} \Rightarrow IP_{COA}$
14 e3 45 c0 00 54 7d 70 00 00 f9 01 47 79 82 ed	
20 34 82 ed d5 f0 00 00 06 25 4b 07 22 00 e2 39	$IP_{CN} \Rightarrow IP_{MN}$
1a 3b a2 5b 03 00 08 09 0a 0b 0c 0d 0e 0f 10 11	$E_k(M)$
16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25	$E_k(M)$
12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21	$E_k(M)$
22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31	$E_k(M)$

Charlie doesn't know about M but knows that:

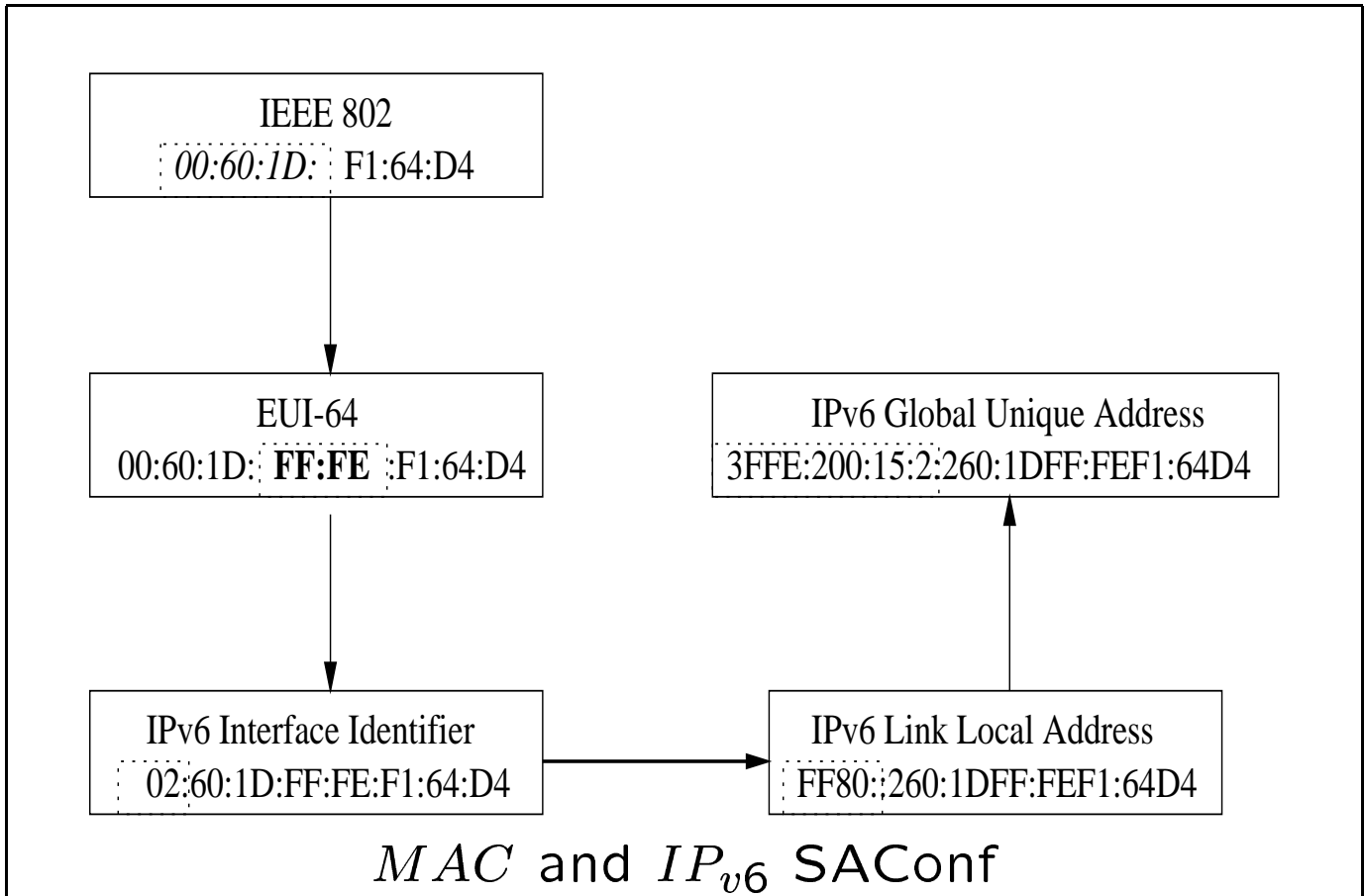
- *Alice* is sending $E_k(M)$ to *Bob's* home network
- *Bob* is not at home
- *Bob* is roaming using his *care-of-address*

In *MobileIPv6*:

- *Alice* \approx *Charlie*

▷ IPv6

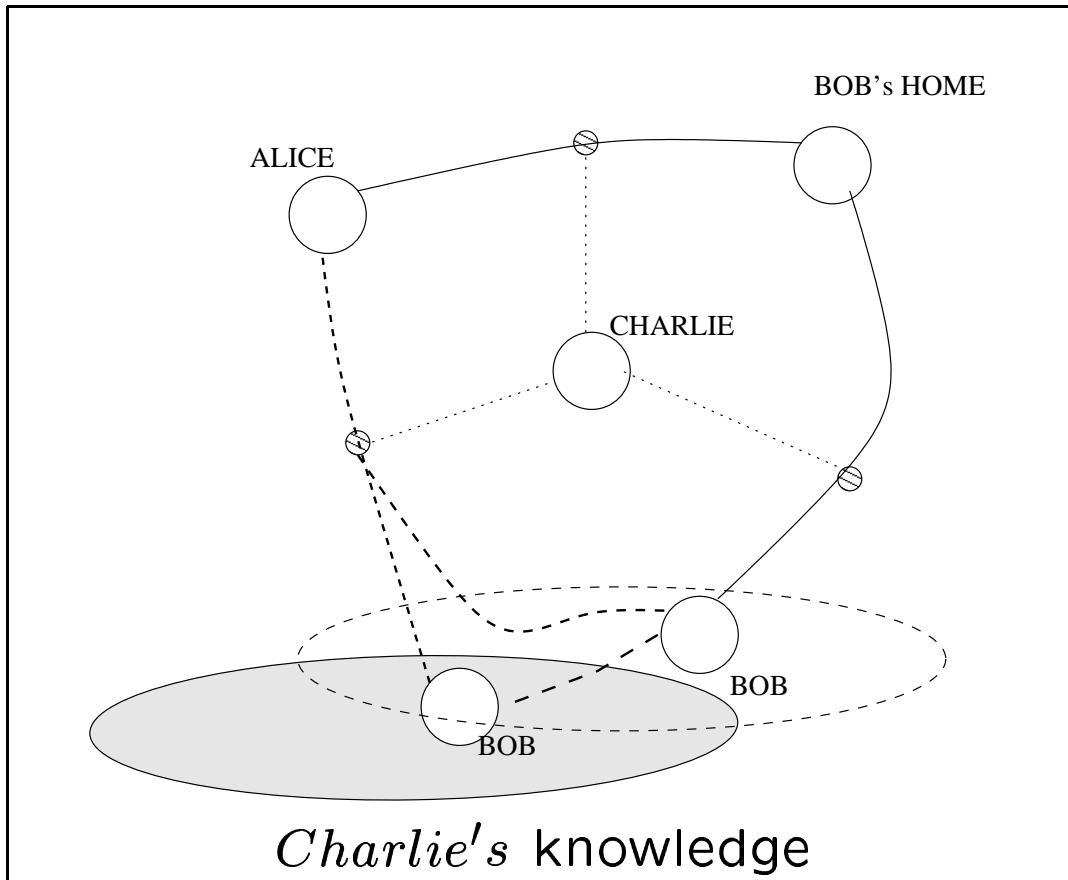
Stateless Address Configuration



The IPv6 address generated via Stateless Autoconfiguration contains:

The **same interface identifier** regardless of the **location** the mobile node is attached to the Inet.

▷ *The problem*



- *Charlie* can obtain consecutive $COA_{Bob}(t)$
- *Bob's movements* can be easily tracked
- *Bob's IP* activities are linked with his location

▷ The “goal”

Allow a mobile node to **seamlessly “roam”** among IP subnetworks and media types whilst being **untraceable**

- Untraceable:

The capability of the mobile node to conceal the relation between its personal identifiable information and geographical location from third parties

<p><i>Home_{Bob}</i> doesn't know <i>Foreign_{Bob}</i> <i>Foreign_{Bob}</i> doesn't know <i>Home_{Bob}</i> <i>Charlie</i> doesn't know <i>Home_{Bob}</i> and <i>Foreign_{Bob}</i> <i>Charlie</i> doesn't know <i>Bob</i> is talking with <i>Alice</i></p>

▷ *IPv6 Privacy Extensions*

RFC & Internet Drafts

- RFC3041

T. Narten (IBM)- R. Draves (Microsoft)
"Privacy extensions for IPv6 Stateless Address Autoconfiguration".

- Internet Draft - MobileIP privacy

C. Castelluccia (INRIA) - F. Dupong (ENST).
"A Simple Privacy Extension for Mobile IPv6".

- Internet Draft - Hierarchical MobileIPv6

H. Soliman (Ericsson), C. Castelluccia (INRIA)
K. El-Malki (Ericsson) - L. Bellier (INRIA).
"Location privacy with HMIPv6 basic mode".

Papers

- Cloaking: Location Hiding in IPv6

J. Wells and C. Castelluccia (INRIA).

- Anonymous Internet Proxies and Location Hiding

A. Escudero , M. Hedenfalk, P. Heselius. (KTH)
"Location Privacy in Mobile Internet - An extension to Freedom Network". INET2001.

RFC3041

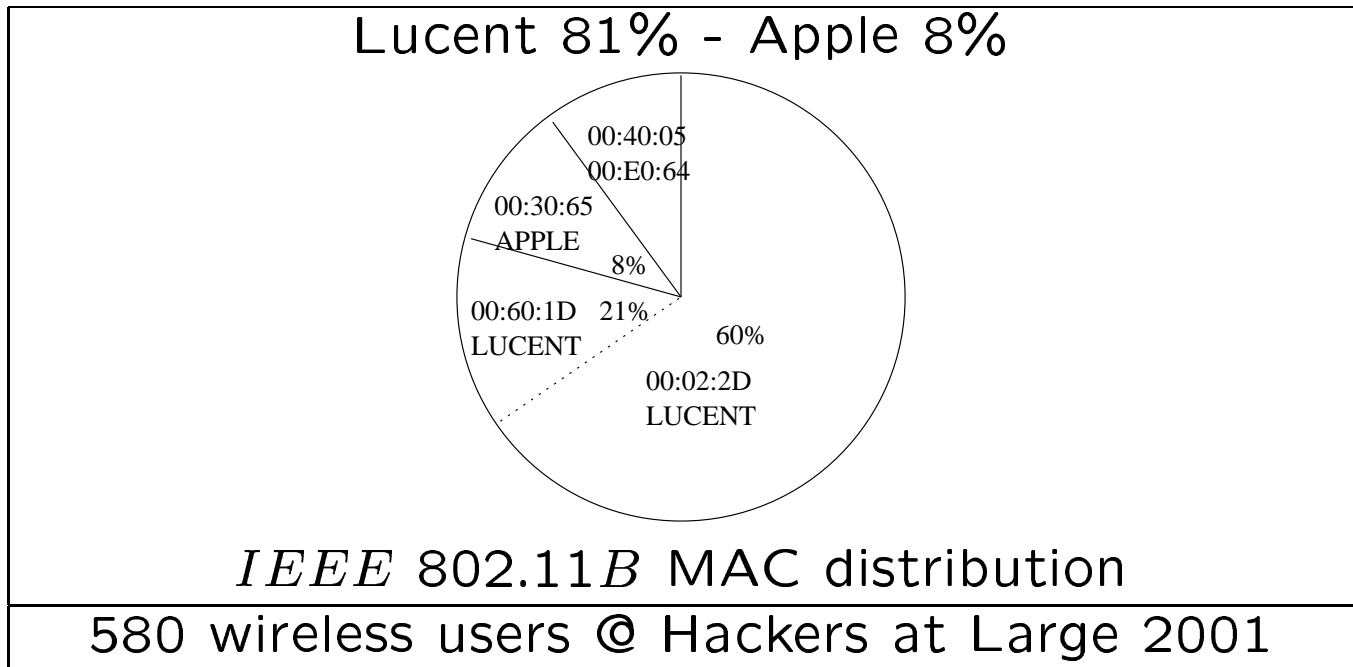
“Privacy ext. for *IPv6* Stateless Address Autoconfiguration”

Main idea

- Interface Identifier is generated randomly (history scheme)

Better solution

- Unobservable pseudo random interface identifier.



12:34:DE:AD:DE:AD ⇒ Private IEEE 80211

<p style="text-align: center;">Internet Draft-castellucia Simple MobileIP Privacy extension</p>

The Home address of a MN is present in

- Home address destination option.
- Corresponding node routing header.

MobileIP Privacy Extension main idea is

When MN initiates the communication then:

- The MN sends the TMI instead of Home Address in the destination option.
- The CN sends the TMI in the routing header.

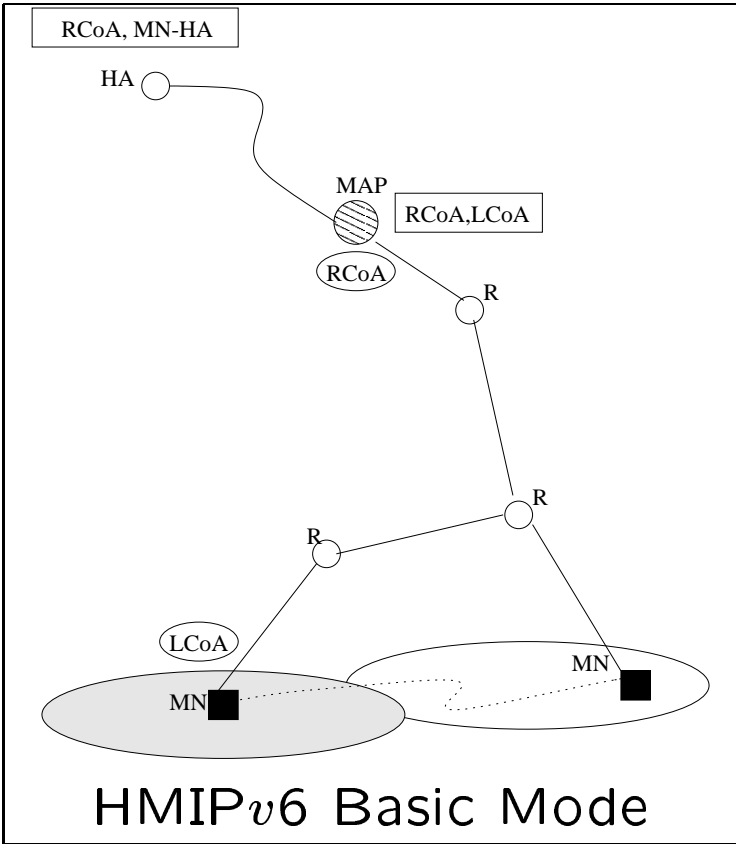
Requirements

- A dedicated TLA identifier (16 bits) should used (112 bits for TMI).

Drawbacks

- The first 16 bits are fixed
- A “privacy enable” TMI is very easy to recognize.
- Private TLA is unroutable.

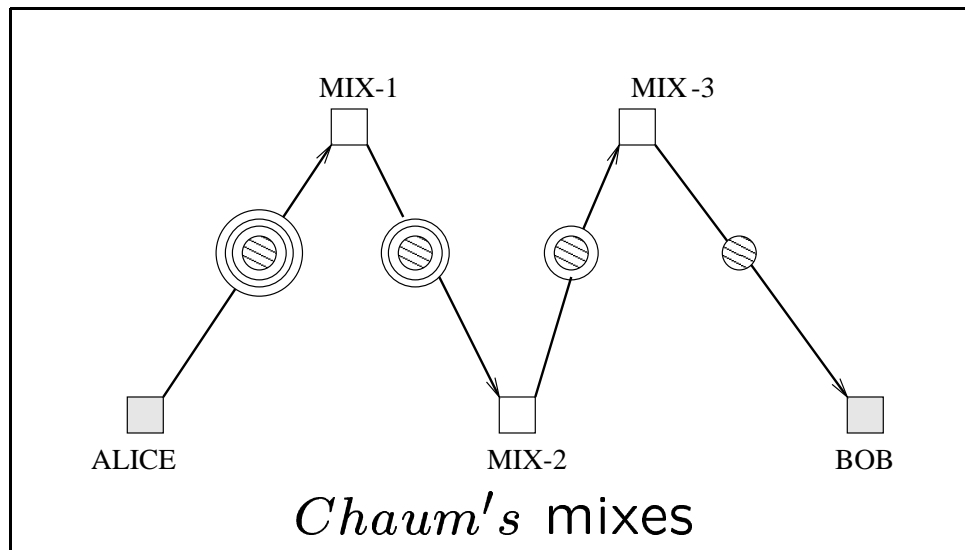
Internet Draft-Soliman
Privacy extension in HMIPv6 basic mode



The HMIPv6 Basic mode:

- Use MAP (Mobility Anchor Point) as HA
- The MN obtains a RCoA and registers LCoA - RCoA in the MAP.
- The MN registers the RCoA with its HA.
- The MAP will receive packets addressed to the MN's RCoA (from the HA or CNs).
- The MAP tunnels from the MAP to the MN's LCoA.

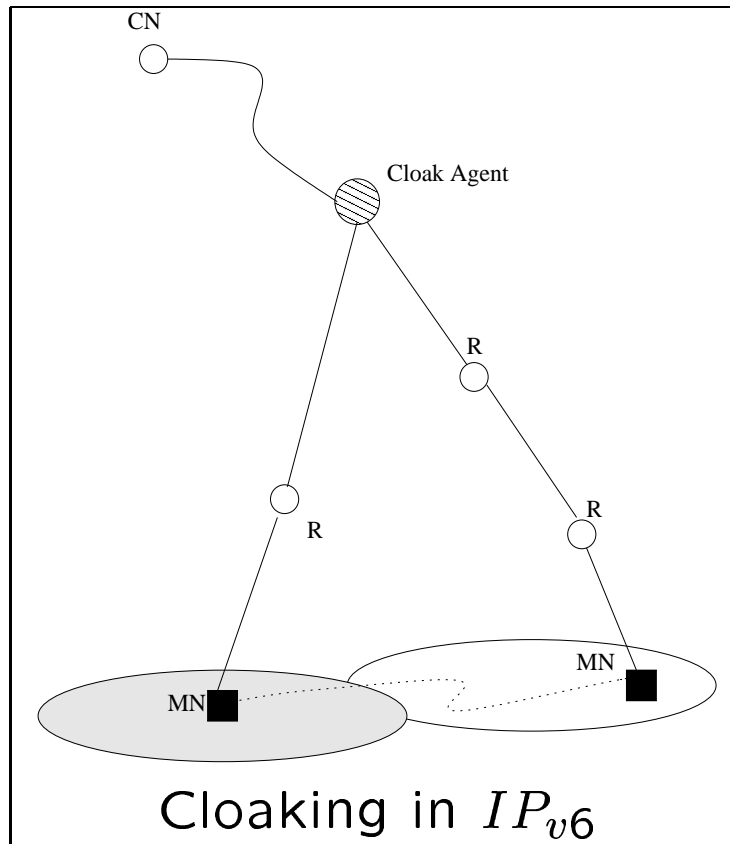
▷ *The core technology*



- **Mixes**
(D. Chaum -1981)
- **Onion Routing**
(M. Reed, P.Syverson and D.Goldschlag - 1996)
- **Non Disclosure Method (NDM)**
(A.Fasbender, D. Kesdogan and O. Kubitz - 1996)
- **Pseudonymous IP Network (PIP)**
(I. Golberg - 2000)
- **Freedom System**
(Zero Knowledge Systems Inc.)

Cloaking IPv6

Location hiding in IPv6



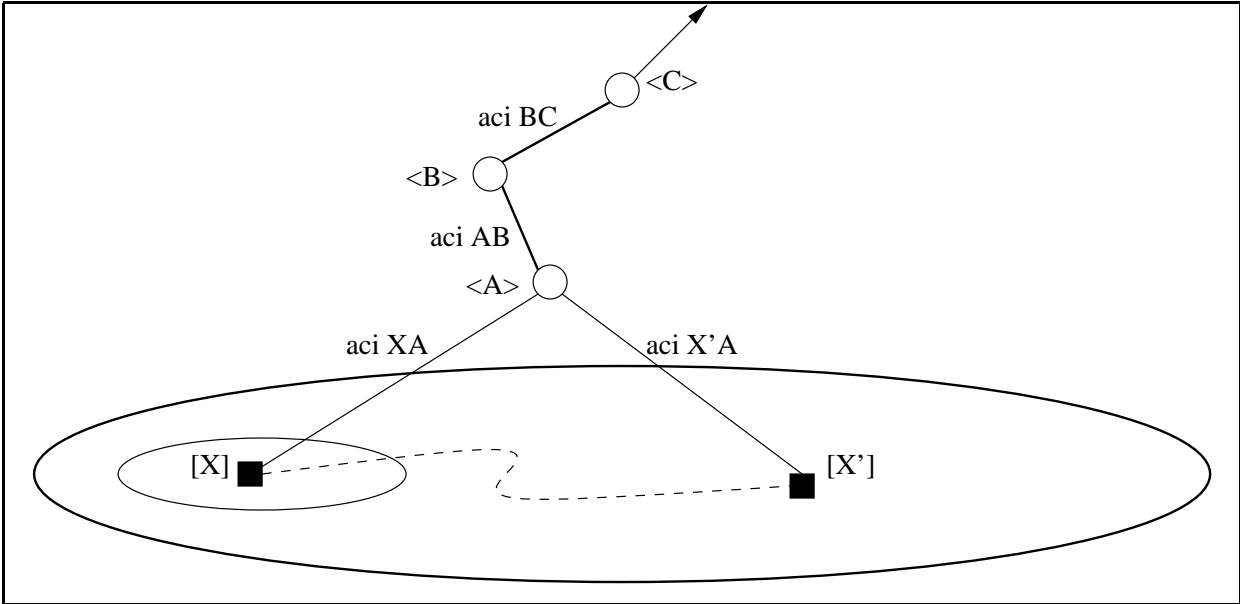
- Similar to HMIPv6 Basic Mode

but:

- Uses bi-directional tunnel.

- Cloaking agents (\approx MAPs) are not announced.

ZKS's Freedom Network
Mobility Extensions to Freedom Network



Freedom PIP Network:

- Provides privacy protection
- The Anonymous Internet Proxies AIP_i are the core privacy daemons
- The Freedom Client creates a “virtual circuit” inside of the freedom network
- Multilayer nested encryption (Telescope encryption)
- Route to next hop by use on Anonymous Circuit Identifier ACI
- The AIP_{exit} or freedom wormhole acts as a NAT

The Freedom Mobility extensions allow:

- Rebuilding parts of the virtual link without notifying to the exit point.

▷ *Conclusions*

- * Encryption does not solve all security/privacy problems.
- * Users interested in privacy protection are highly observable.
- * Route optimization vs Privacy.
- * MobileIP and HMIPv6 features can be used.
- * “Mixing” technologies will be again applied.
- * Maybe in IPv7 ?