Route Optimization in Mobile IP

David B. Johnson

Carnegie Mellon University

Charles Perkins

IBM Corporation

<draft-ietf-mobileip-optim-02.txt>

Protocol Extensions for Route Optimization

Problem with basic protocol:

All packets ***always*** go through home agent

Causes unnecessary network overhead

Causes unnecessary packet delivery latency

Route optimization allows a correspondent node to

- Learn current binding of mobile node,
- Cache this binding in a ***binding cache***, and
- Tunnel own packets directly there

Route Optimization Challenges

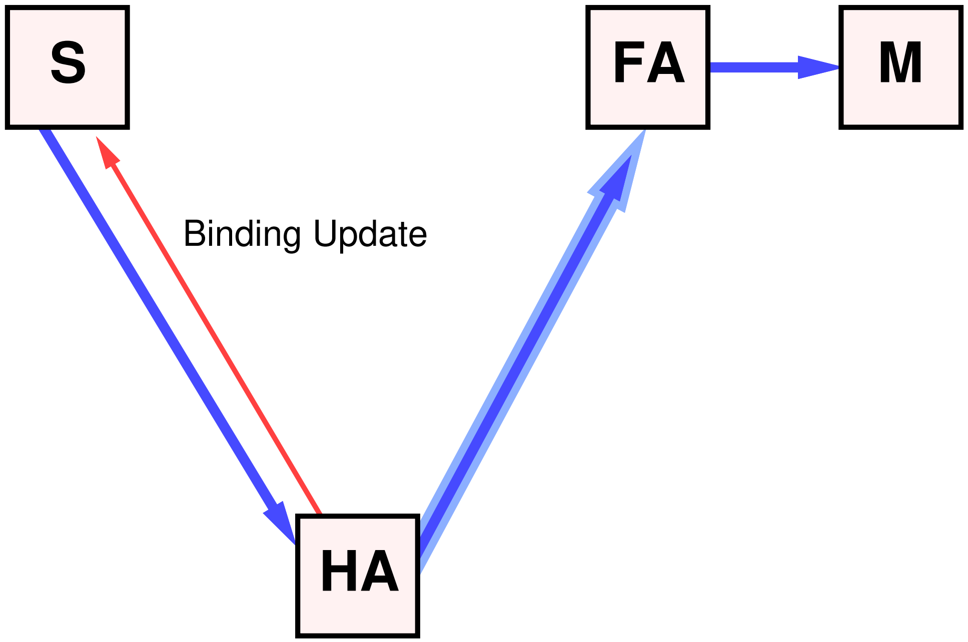
Cache is out-of-date after mobile node moves:

- Must solve ***cache consistency***
- Dynamically update cache when next used

Authentication is much harder than in basic protocol:

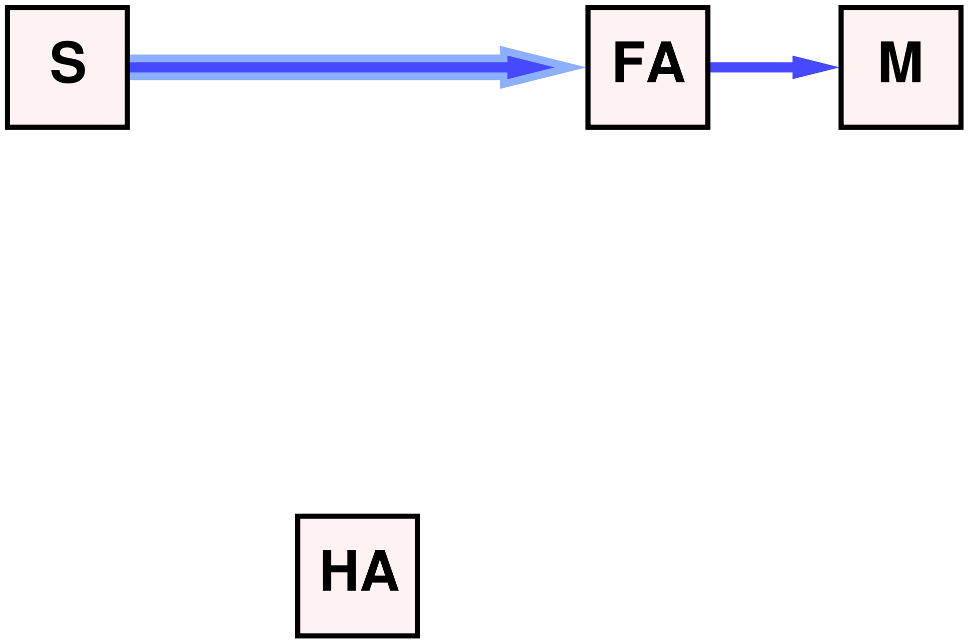
- Binding cache probably owned by different organization
- No general Internet authentication available
- Interim solution: require security association with home agent (not needed with each individual mobile node)

Sending the First Packet to a Mobile Node



Home agent returns authenticated ***binding update*** to sender

Once Sender Has a Binding Cache



Packets are tunneled directly to current foreign agent

(Minimal tunneling protocol adds only 8 bytes)

Foreign Agent Registration Keys

Optionally establish ***registration key*** during registration

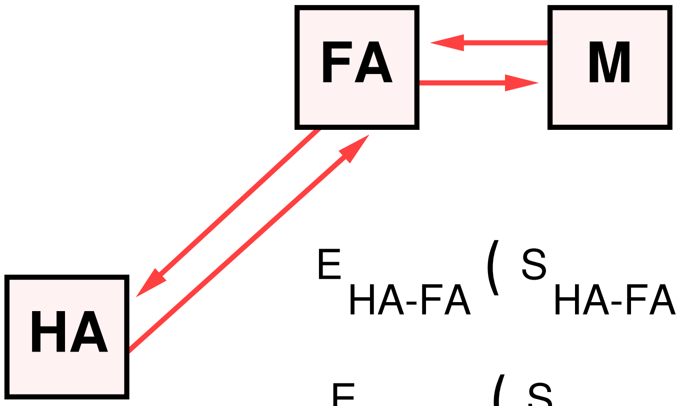
Secret shared between mobile node and current foreign agent:

- Use to authenticate notification to foreign agent of move to next care-of address
- Could also use to encrypt packets between mobile node and its current foreign agent

Two alternative methods for establishing:

- Using the home agent as a ***Key Distribution Center***
- Using ***Diffie-Hellman*** key exchange protocol

Home Agent as KDC



$$E_{HA\text{-}FA}\left(S_{HA\text{-}FA} \{ \text{ key } \} \right)$$

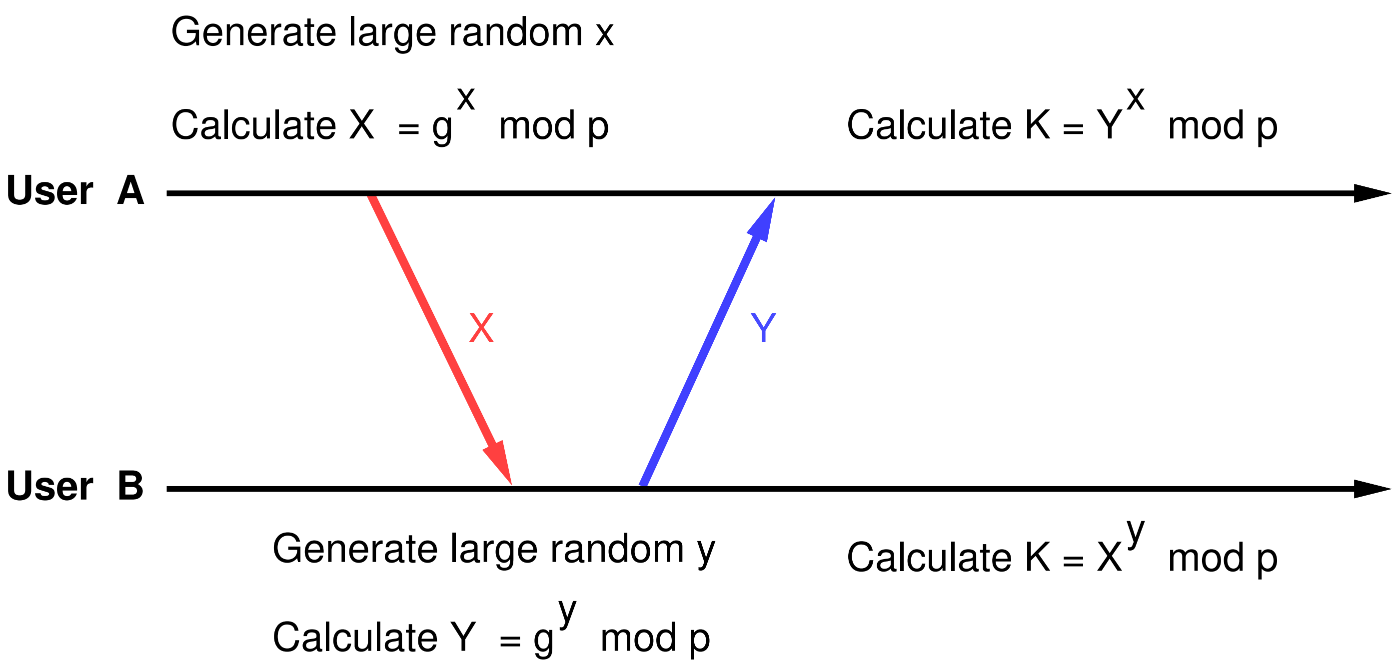
$$E_{HA\text{-}M}\left(S_{HA\text{-}M} \{ \text{ key } \} \right)$$

Foreign agent must have security association with home agent

Mobile node registers new binding with home agent

Home agent returns new registration key to both

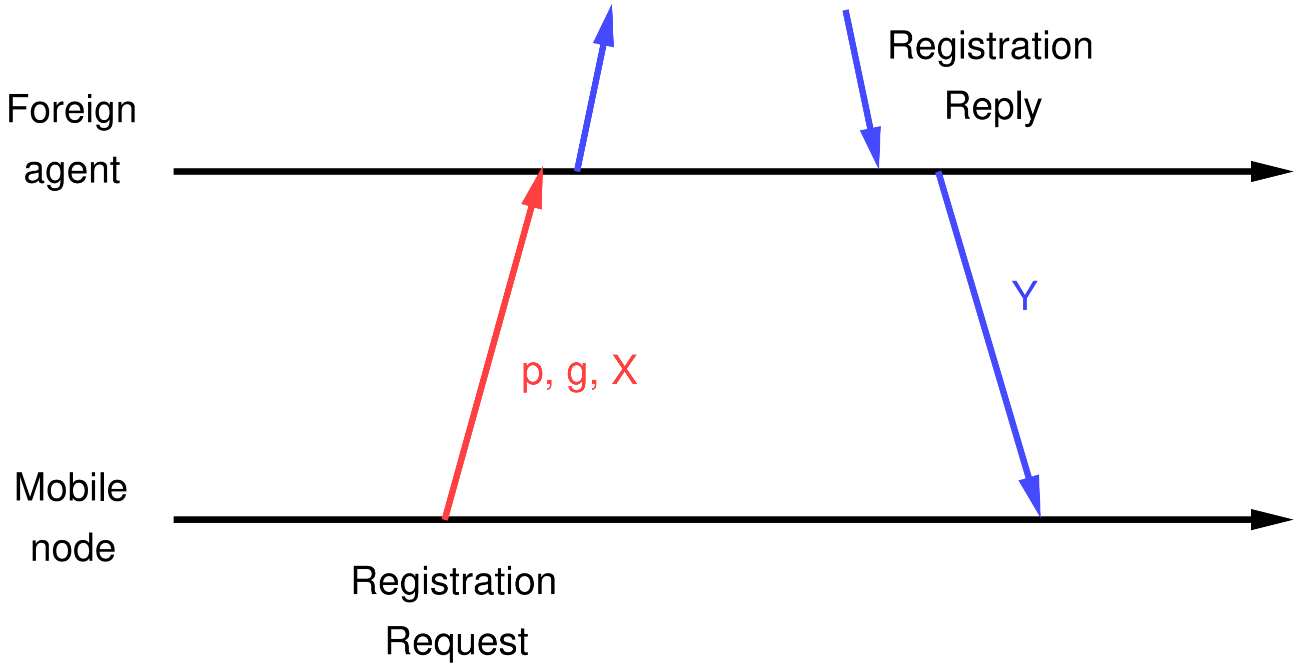
Diffie-Hellman Key Exchange



Public values: p is large prime number, g < p is base

K is resulting shared secret key

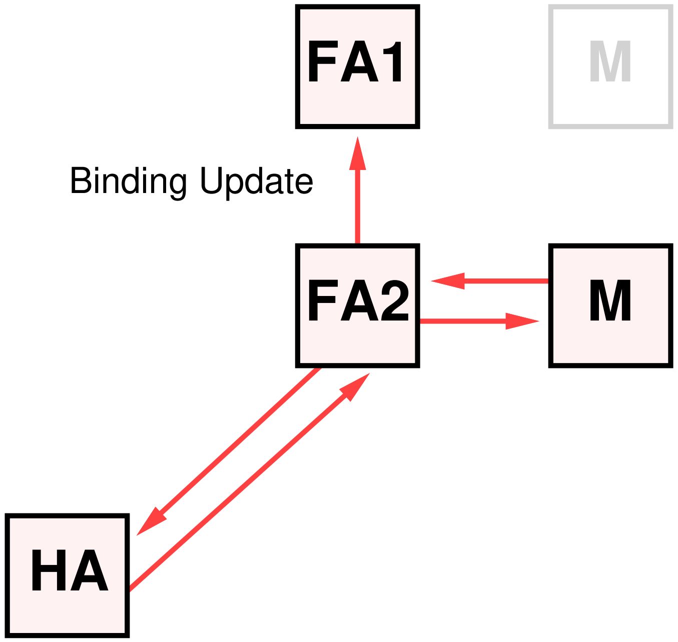
Diffie-Hellman with Foreign Agent



Mobile node sends p, g, and X in Registration Request

Foreign agent replies with Y in Registration Reply

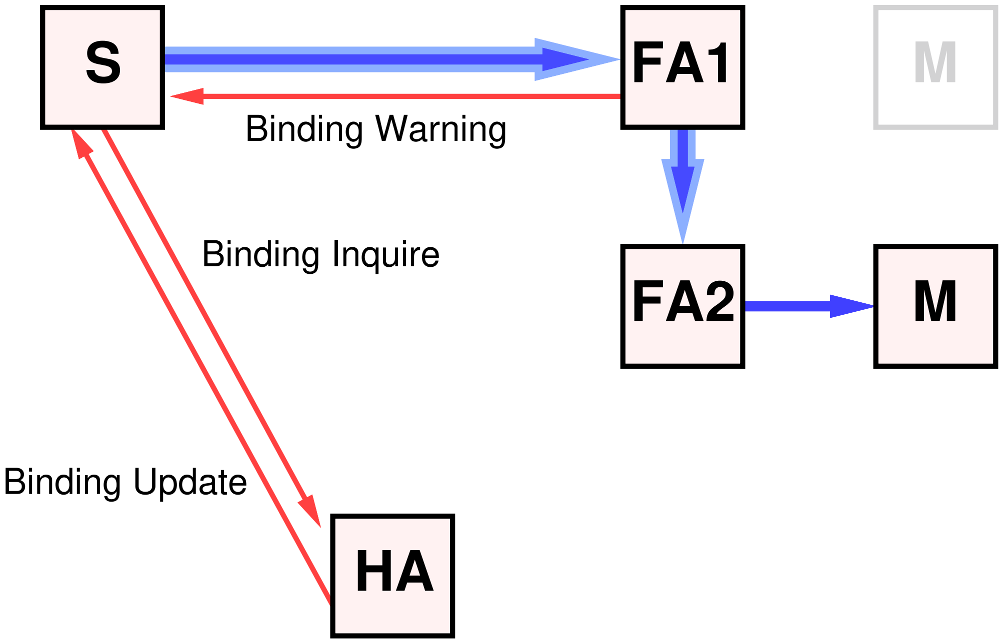
Notifying Previous Foreign Agent



Include authenticated notification in new Registration Request

New foreign agent just forwards to previous foreign agent

Sending First Packet After Movement



Previous foreign agent cache acts is forwarding pointer

(If FA1 has no cache entry, FA1 tunnels packet to home agent)