IP Transform Policy Distribution Using Mobile IP/DIAMETER

draft-mccann-transform-00.txt

Pete McCann & Tom Hiller

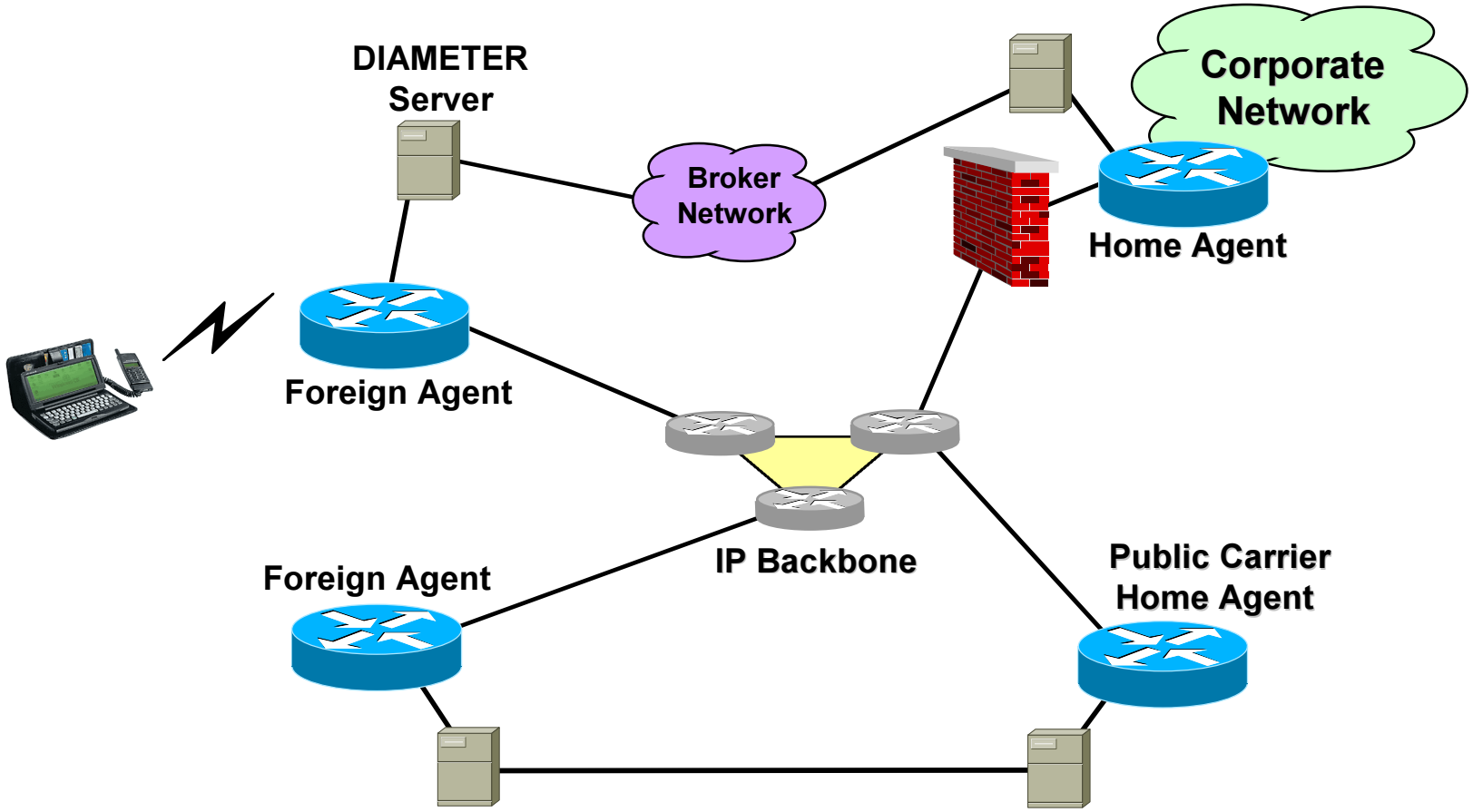
July 1999

Outline

- IP Security Scenarios
- Negotiating Security Associations
- Mobile IP/DIAMETER Extensions
- Alternative Solutions
- Why this is Better

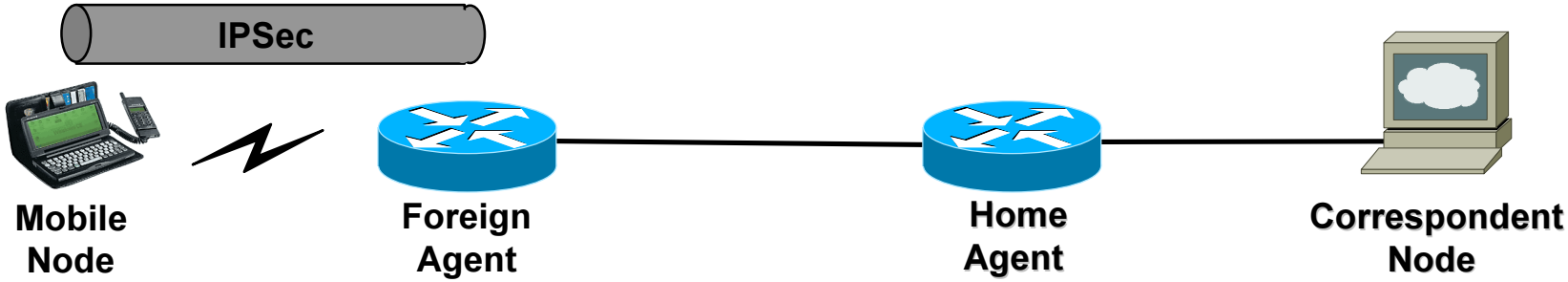
Security Scenarios

- MN may have private address
- "FA & HA will have public addresses (for now)" - TR45.6



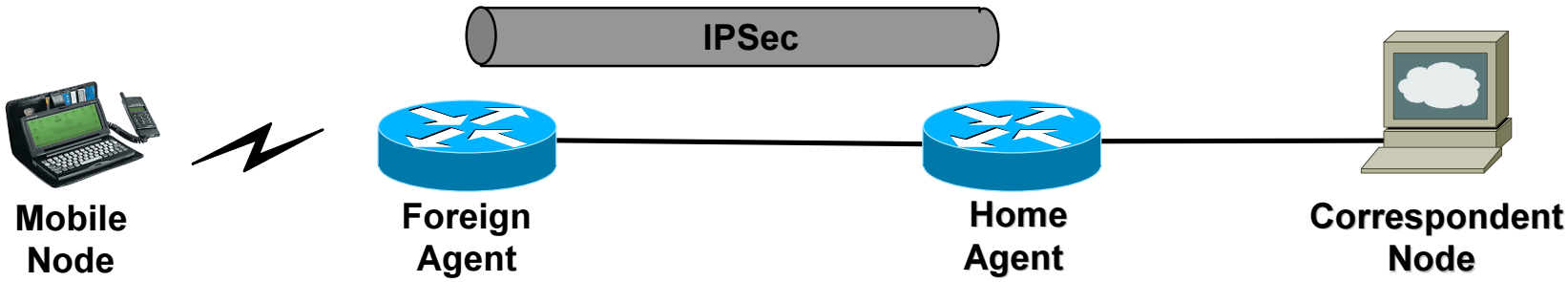
MN to FA Security

- Protects from eavesdropping on the wireless link
- Authenticates MN traffic



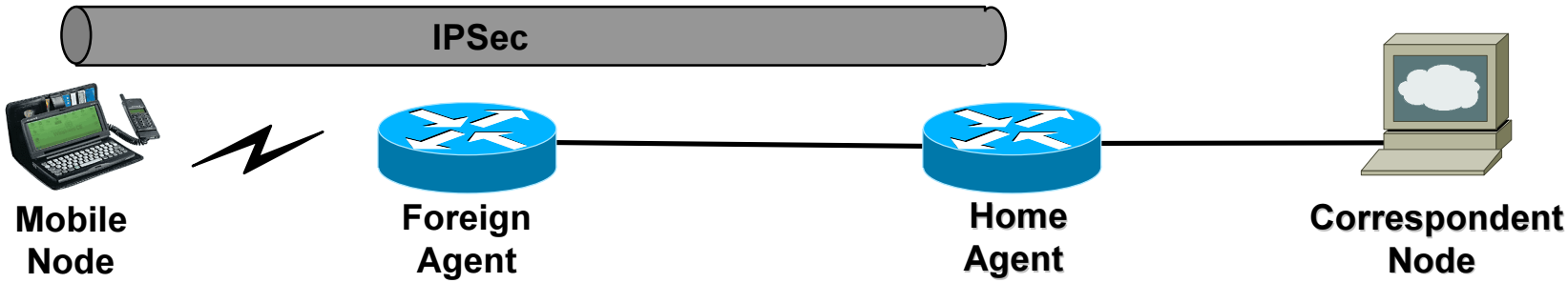
FA to HA Security

- Link-layer authentication and encryption may be good enough
- Low power MNs may not support IP Security
- Some wireless users may not wish to pay carriers for tunnel and IPsec overheads on wireless interface
- Similar security to a dial-up remote access



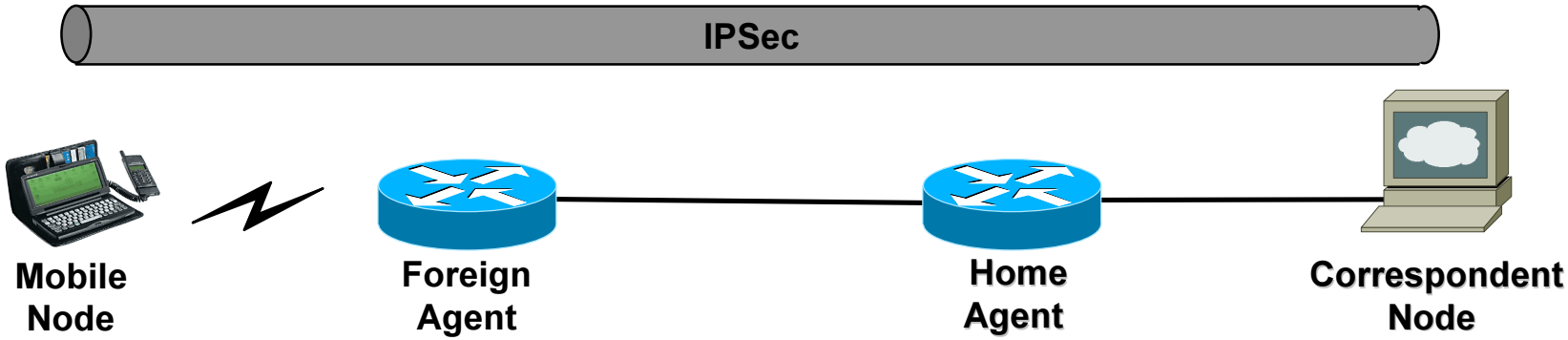
MN to HA Security

- **Sort of end-to-end**
  - (At least it's back to the home network)



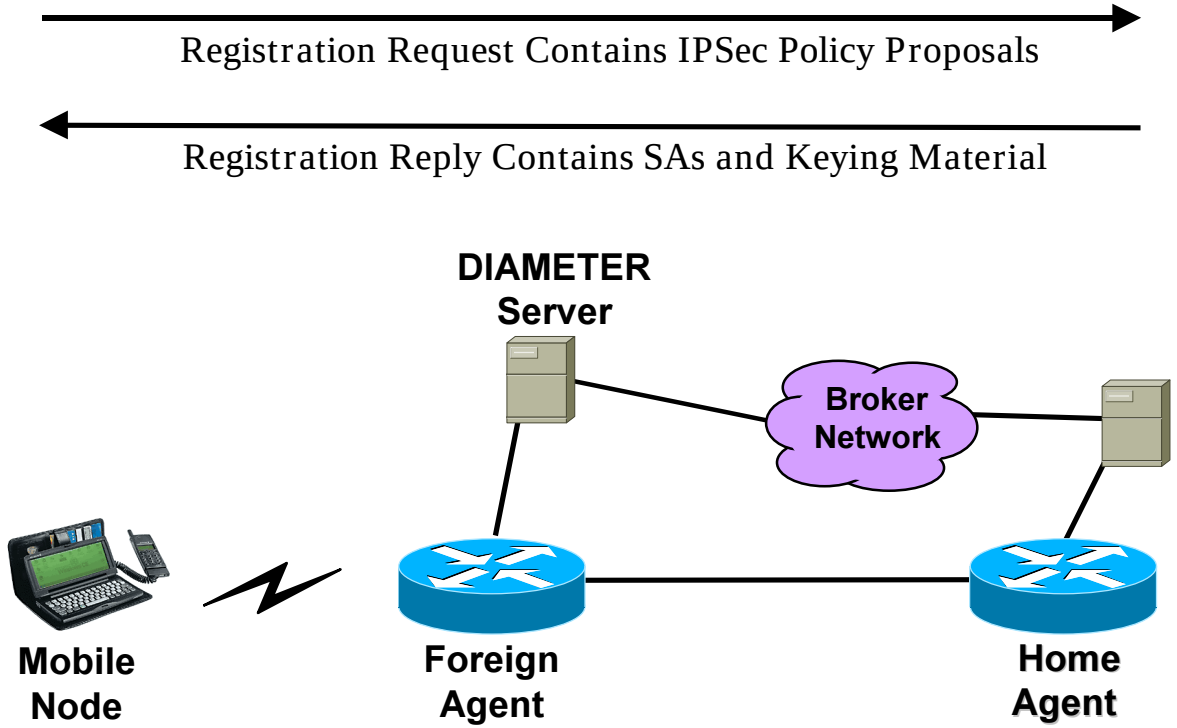
MN to CN Security

- Truly end-to-end
- Outside the scope for now



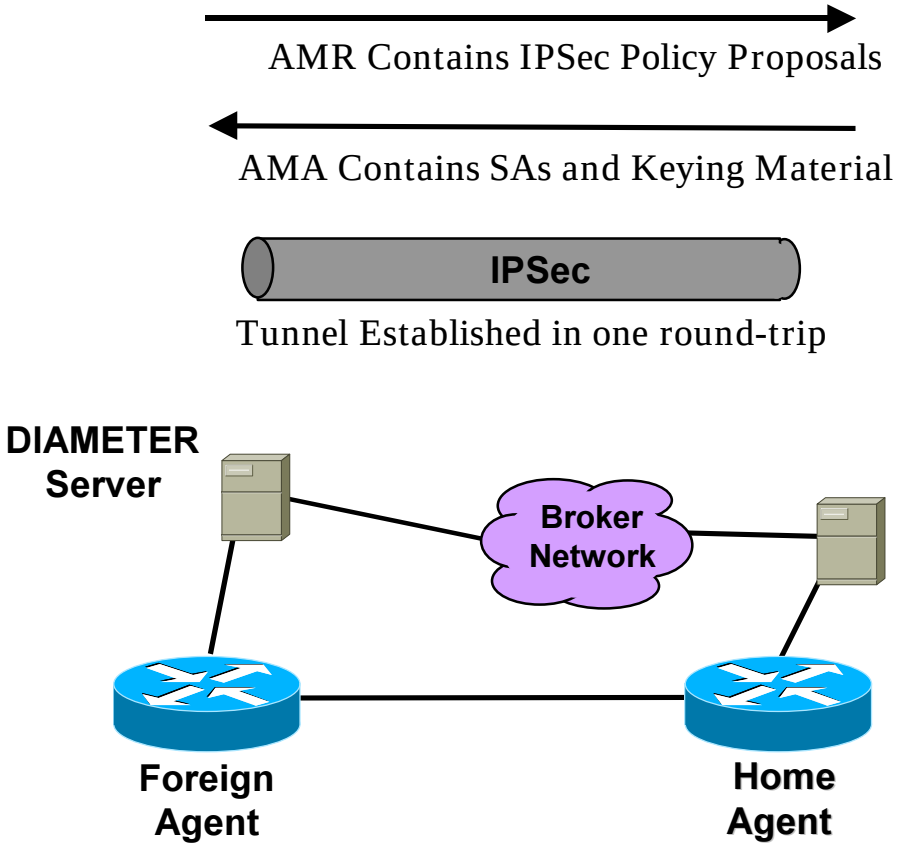
Distribution of Security Associations

- Use the DIAMETER infrastructure as a web-of-trust
- Protect MN keys end-to-end
- Protect FA keys hop-by-hop or end-to-end



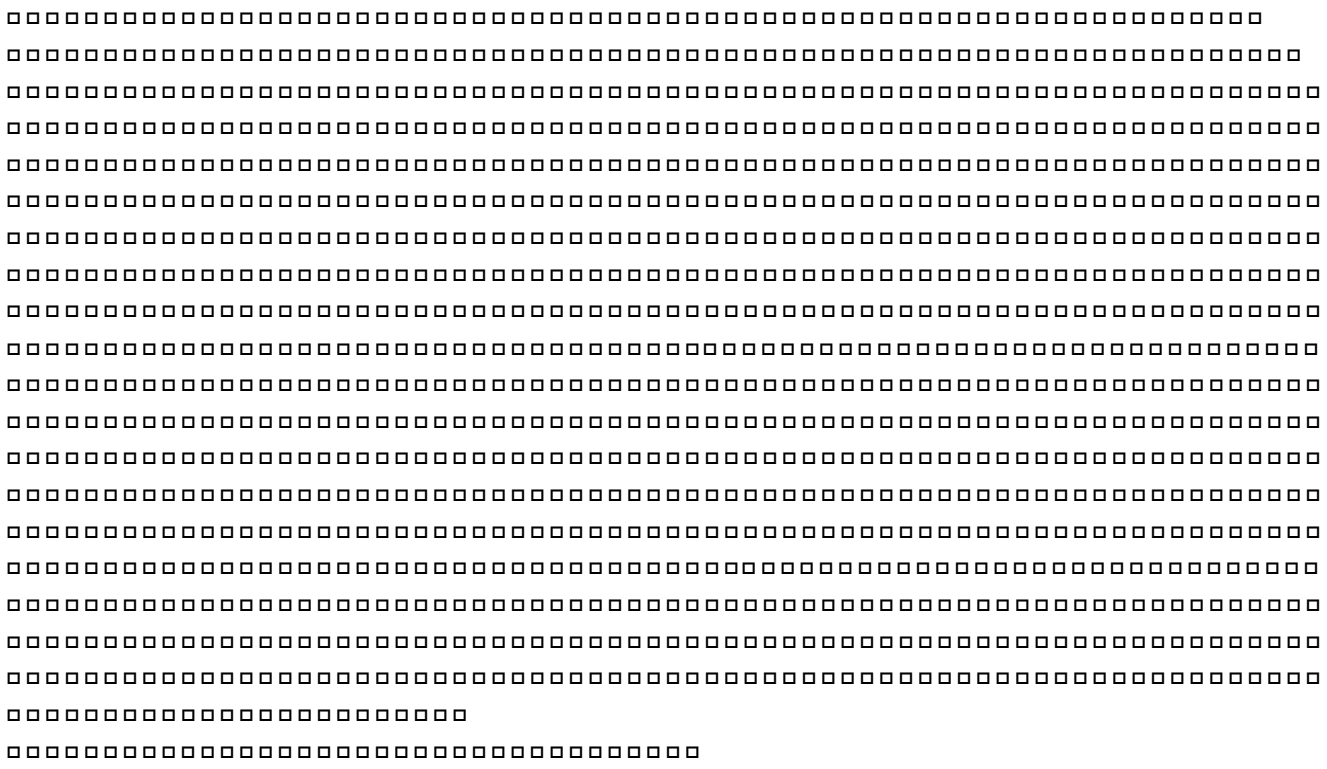
Example: FA-HA

- Requires no participation by MN
- Requested feature by CDMA wireless data standards



IPSec Policy AVP

- Proposal consists of one or more Transform AVPs
- Tunnel Spec tells where it applies (MN-FA, FA-HA, MN-HA...)

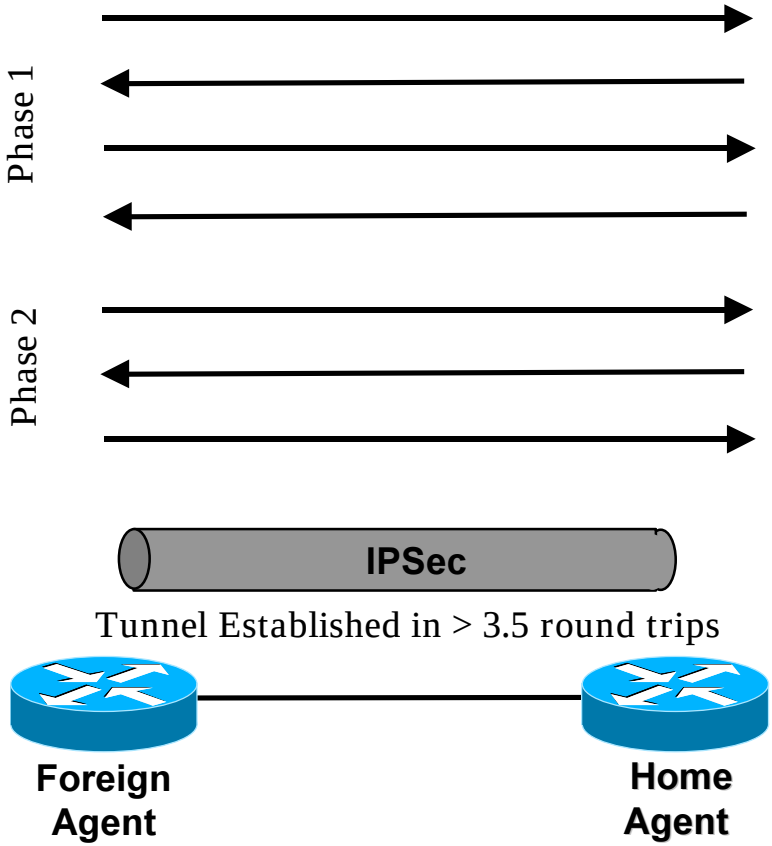


IPSec Policy MIP Extension

- Same fields as DIAMETER AVP
- Protected by MN-home AAA shared secret

Alternative: IKE

- **Run IKE at each new FA**
  - Requires use of certificates, or
  - Pre-shared secrets



Problems with IKE

- **More overhead - up to 9 messages**
  - Distribution with MIP Reply is single round-trip
- **How do we associate policies with MNs/Users?**
  - Use of NAI in MIP Request enables this
- **Do we need a PKI?**
  - No:
    - » DIAMETER web-of-trust is used to directly encrypt keys
    - » If intermediate nodes must not see keys, then use

Details

- **Reverse Tunnel Policy**
  - Optional, Required
  - Direct access to public Internet from FA is still possible with NAT
- **Tunnel Formats and Applicability**
  - Private addresses should be handled properly by FAs & HAs
  - Indexing the SA is tricky when using MN-FA tunnel and private addresses