

GMD
German National
Research Center for
Information Technology



The Evolution of Mobile IP Towards Security

Matthias Hollick

Innovation
through
Research

www.ipsi.gmd.de

GMD IPSI MOBILE
Dolivostr. 15
D-64293 Darmstadt, Germany
Tel: 49.6151.869.847
Fax: 49.6151.869.6847
<http://www.ipsi.gmd.de/mobile>

Overview

Motivation

Introduction to Mobile IP

- Basic Operation of Mobile IP
- Security Problems of Mobile IP

Approaches to Apply Security to Mobile IP

- Mobile IP Integrated Security
- Mobile IP and IPSec
- Mobile IP and Firewall Systems
- Mobile IP and AAA – Authentication, Authorization, Accounting

Conclusion / Future Research Plans

Summary

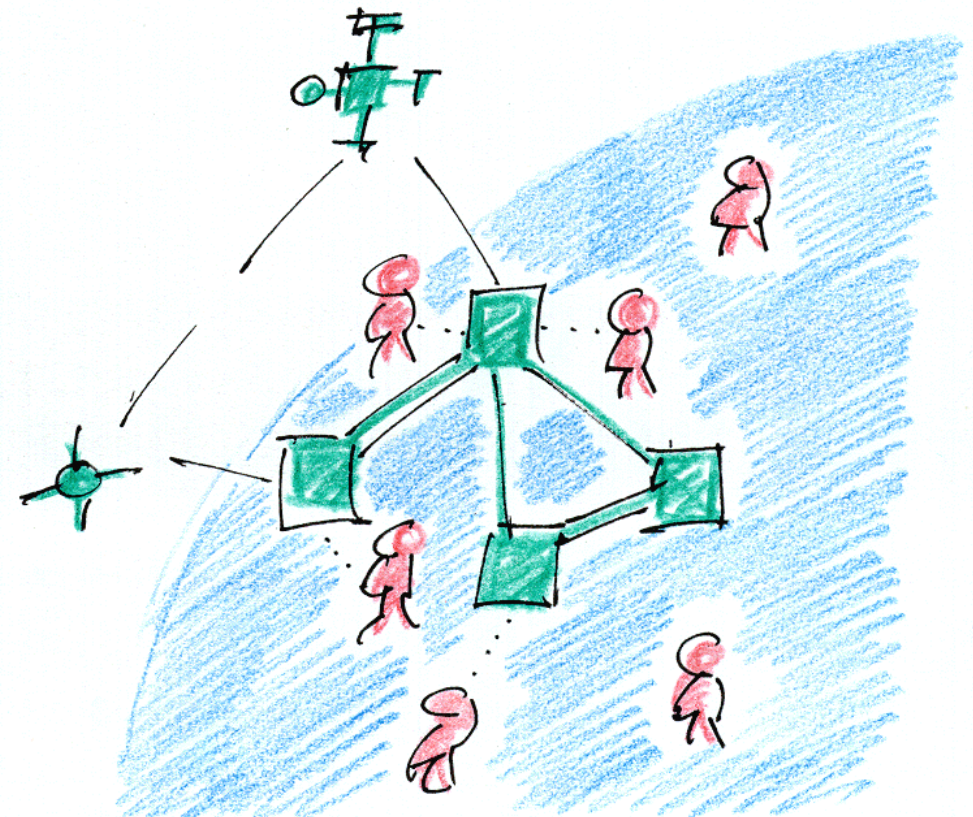
Motivation

Mobility

- Drives the evolution of the „information society“
- Will bring telecommunication- and Internet-technology together
- The UMTS-Forum predicts >>1.000.000.000 mobile users until 2010

IP-Mobility

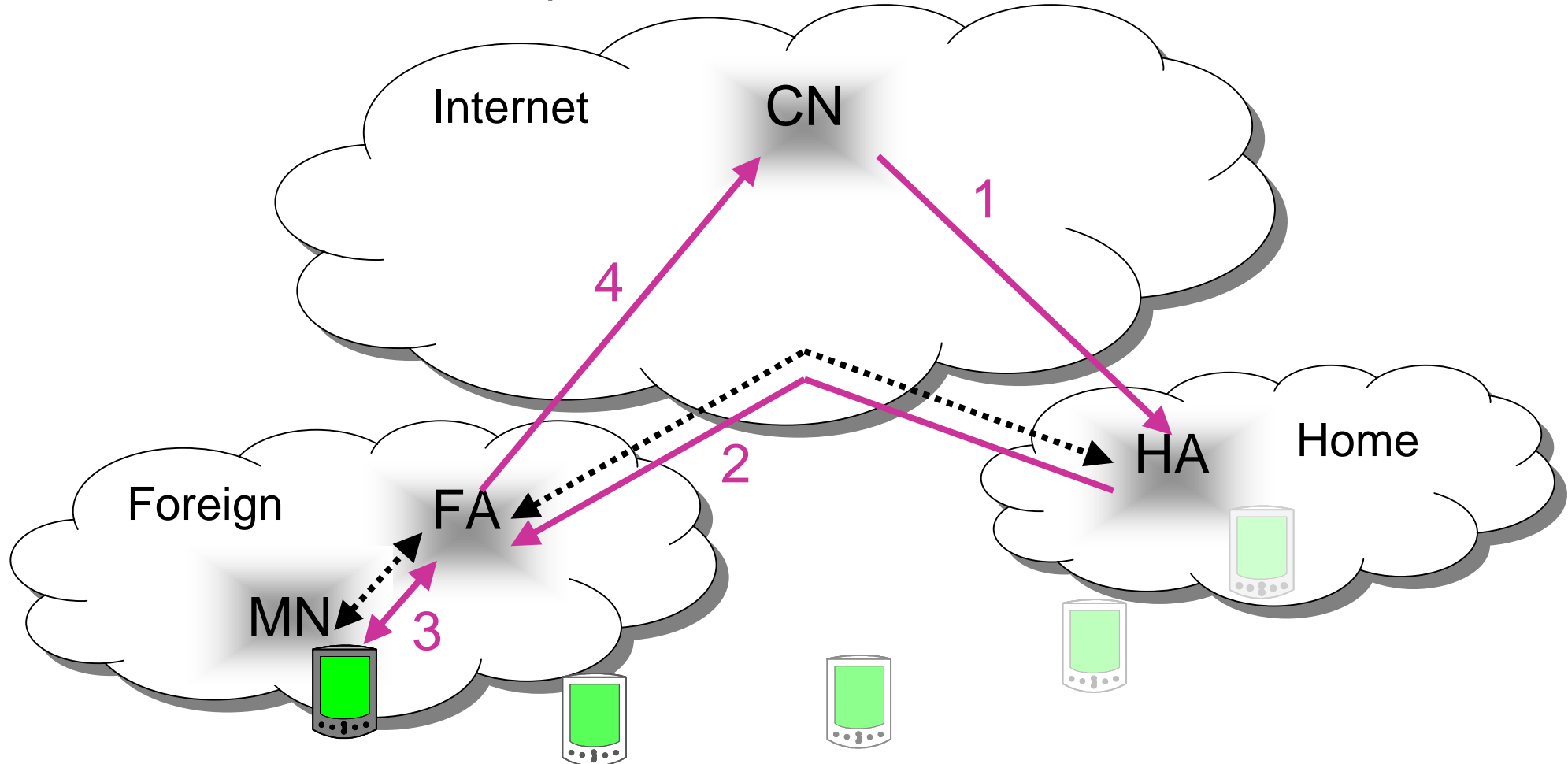
- Enables transparent host mobility within the Internet
- Is not in heavy use today related to security and performance issues
- Will most probably be the platform for UMTS mobility management (based on IPv6)



Basic Operation of Mobile IP

Mobile IP

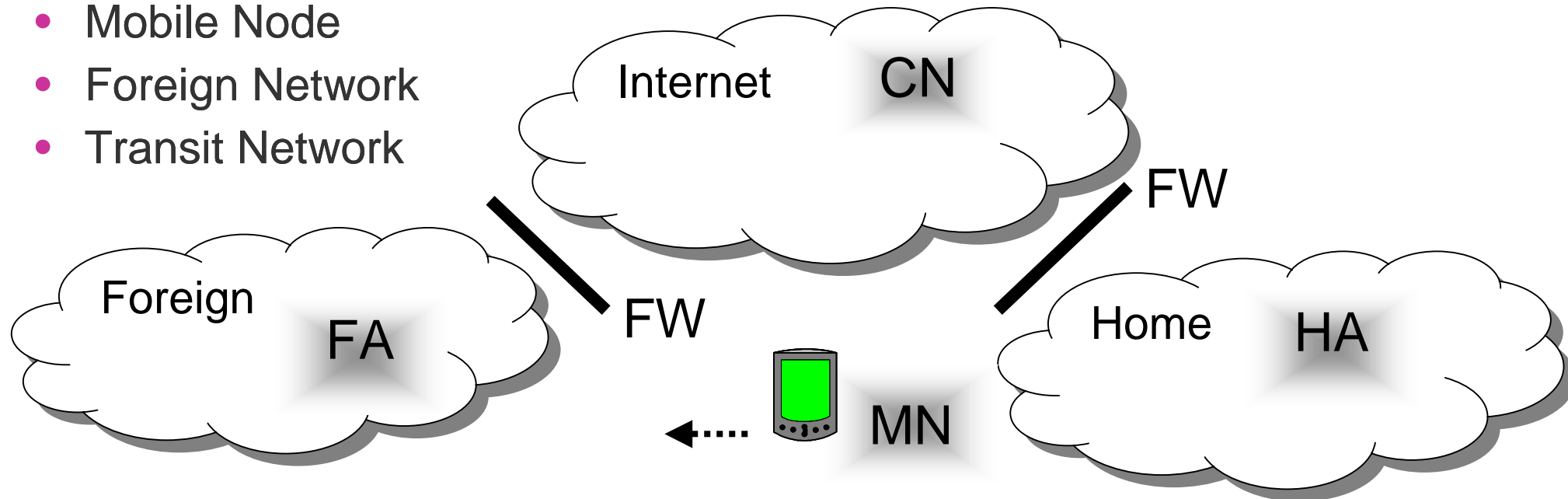
- „Control Plane“ to establish Bindings between Mobile Node, Home Agent and Foreign Agent
- „Data Plane“ to forward packets to the Mobile Node



Security Problems of Mobile IP

Areas of security to consider

- Home Network
- Mobile Node
- Foreign Network
- Transit Network



Principles of security to consider

- Authenticity
- Integrity
- Nonrepudiation
- Availability
- Confidentiality

Mobile IP Integrated Security

Mobile IP integrated security is limited to

- Security associations between MN and HA (optional between MN and FA, FA and HA) through pre-shared secrets and by means of a Security Parameter Index (SPI)
- Timestamps / Nonces (Replay Protection)

	Control Plane	Data Plane
Authenticity	Yes / Optional	No
Integrity	Yes / Optional	No
Nonrepudiation	No	No
Availability	No	No
Confidentiality	No	No

Mobile IP and IPSec

Internet Protocol Security

IPSec

- Authenticated Header Mode (AH)
- Encapsulated Security Payload Mode (ESP)
- Transport Mode vs. Tunnel Mode

Transport Mode

- From MN to CN if required (data)
- From MN to HA if required (control)

Tunnel Mode

- Tunnel endpoints FA to HA? Firewall? (control + data)
- Tunnels may get tunneled (e.g. VPN with L2TP)

Problems

- Firewall traversal of encrypted traffic
- Key Exchange (Security Associations)

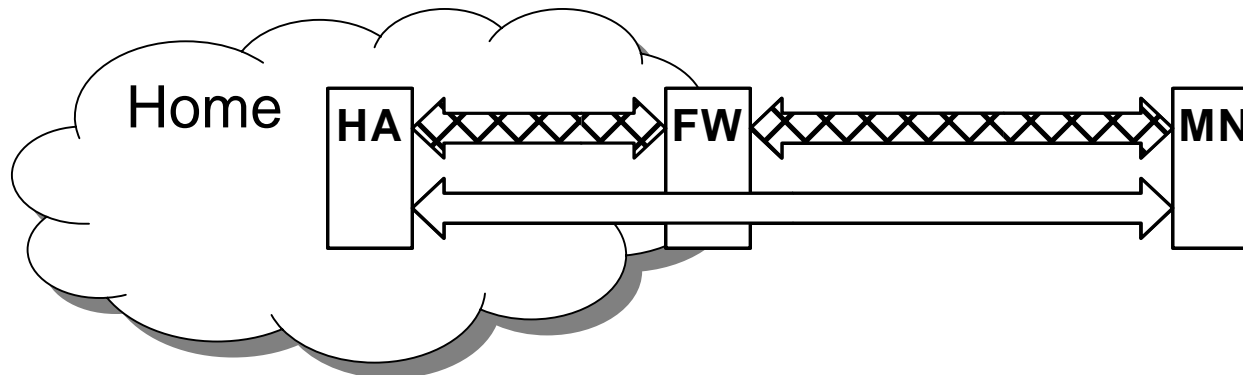
Mobile IP and Firewall Systems

Firewall Systems

- Often use ingress and egress filtering
- Often do not allow IP in IP encapsulated packets
- The Mobile Node uses topologically incorrect IP addresses to send packets to the Correspondent Node (triangular routing)
- Reverse tunnels allow for topological correct tunnels but decrease performance

IPSec solutions combined with Firewall Systems

- Firewall should not be tunneled
- Mobile IP Security deals with Mobility Agents located inside the Home and Foreign Network



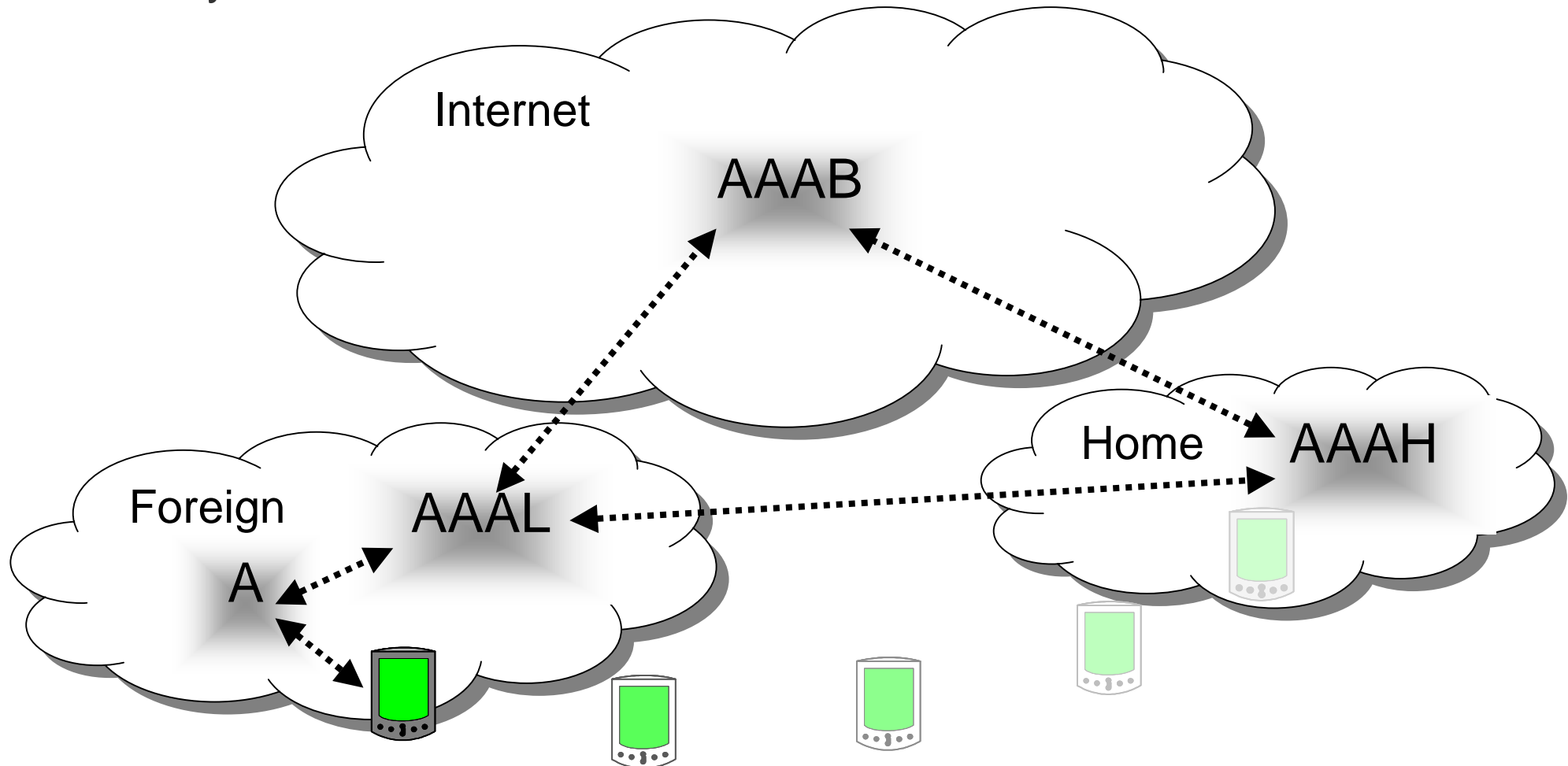
IPSec (AH + ESP) - data path
control path

The AAA Framework

Authentication, Authorization, Accounting

Next step towards security in Mobile IP

- Scalability and ease of use are essentials for Mobile IP security
- The AAA framework provides an infrastructure to deal with all necessary security associations



Conclusion / Future Plans

Conclusion

- Mobility vs. Security will always be a tradeoff
- IPSec can be used to secure the Control Plane and the Data Plane of Mobile IP

	Control Plane	Data Plane
Authenticity	Yes / Optional	Yes
Integrity	Yes / Optional	Yes
Nonrepudiation	No	No
Availability	Not really	Not really
Confidentiality	Yes	Yes

- Firewall Systems and security considerations (Home Network, Mobile Node, Foreign Network, Transit Network) establish the need for scalable and manageable security associations between each pair of all entities
- AAA will help to overcome these limitations

Summary / Index

Open Issues? Questions?

Motivation

Mobile IP

- Basic Operation of Mobile IP ([link](#))
- Security Problems of Mobile IP ([link](#))

Approaches to Apply Security to Mobile IP

- Mobile IP Integrated Security ([link](#))
- Mobile IP and IPSec ([link](#))
- Mobile IP and Firewall Systems ([link](#))
- Mobile IP and AAA – Authentication, Authorization, Accounting ([link](#))

Conclusion / Future Research Plans

