Mobile Network Security

Refik MOLVA
Institut Eurécom
B.P. 193
06904 Sophia Antipolis Cedex - France
Refik.Molva@eurecom.fr

Outline

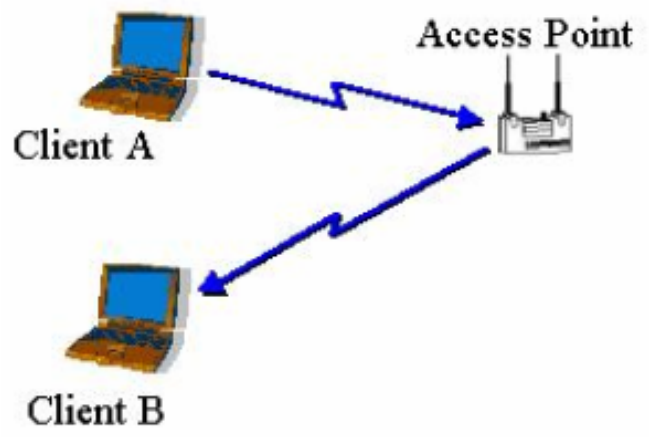
- Wireless LAN
  - 802.11 (WiFi)

- Mobile Telecommunications Security
  - GSM Security Features
  - 3GPP Security Architecture
  - CDPD Key agreement and authentication
  - Fraud management

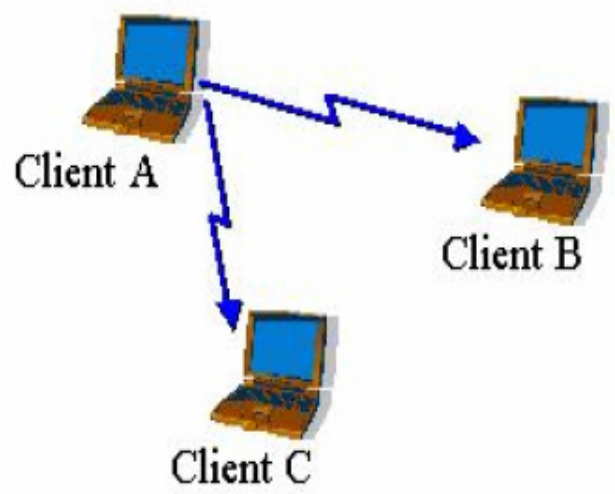
- Mobile IP
  - IPsec-based solution
  - Firewalls vs. Mobile IP vs. Packet Filtering

802.11 Wireless Networks

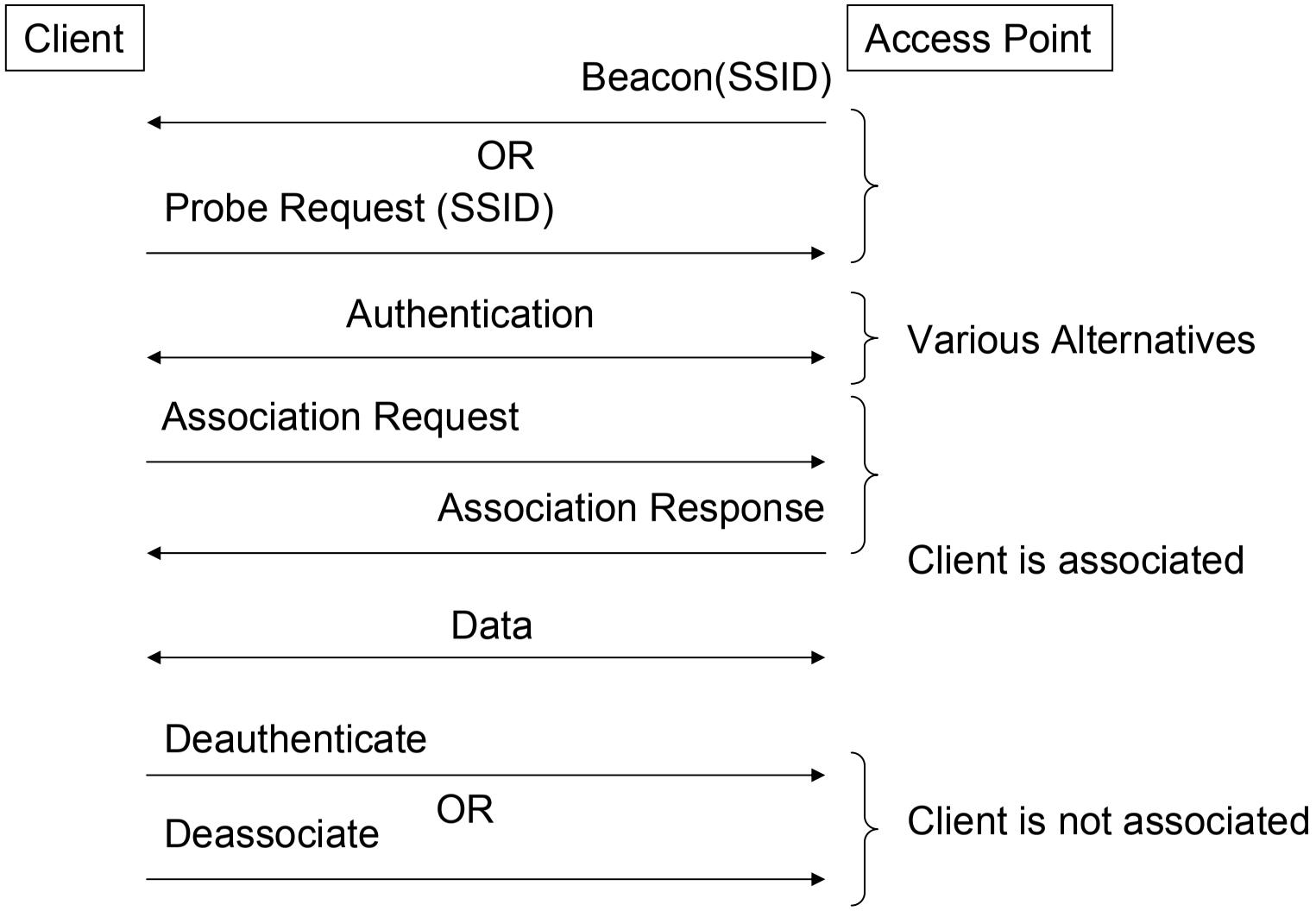
Infrastructure Mode



Ad Hoc Mode



Association Establishment in Infrastructure Mode



Specific Vulnerabilities and Threats

- lack of physical protection

- eavesdropping and spoofing are easier than with wired networks

- denial of (data link layer) communication service is feasible

Main attacks:
- eavesdropping
- man in the middle
- denial of service

Eavesdropping

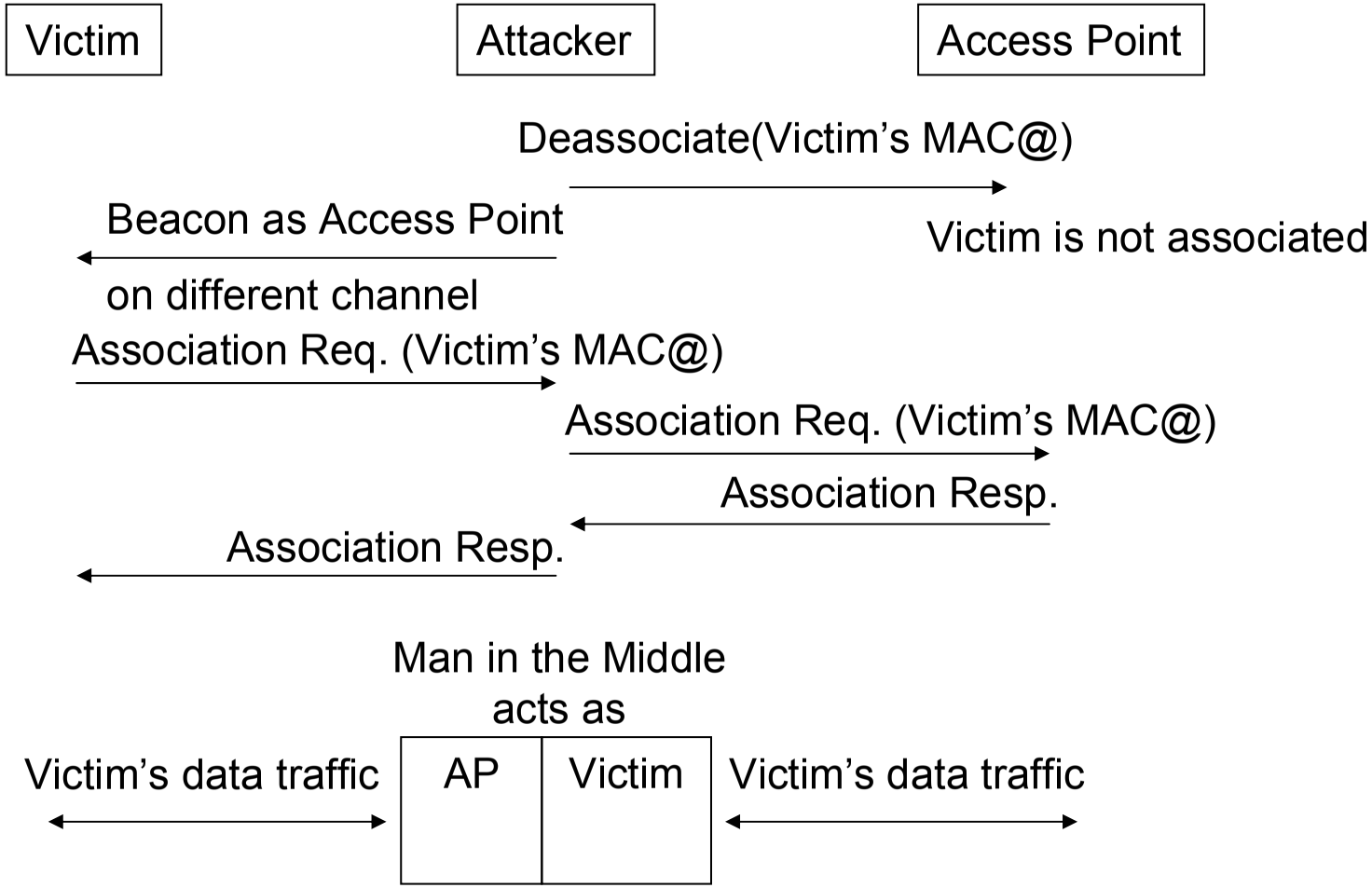
- 802.11is viewed as a standard Ethernet

but

  - media is shared as opposed to switched
  - each node can receive all frames

- traffic can be eavesdropped from few kilometers away using appropriate equipment

Man in the Middle Attack



Main reason why this attack works: Management frames (associate, deassociate) are not authenticated except in 802.11i.

Denial of Service

- Jamming
- Virtual carrier-sense attack
- Spoofing of deauthentication/deassociation messages
- De-synchronization attacks

Security Requirements

- no identification based on the physical access

  → Peer Entity Authentication
  → Data Origin Authentication

- ease of disclosure and tampering with data

  → Data Confidentiality and Integrity
  → Privacy (Anonymity)

- ease of access to communication media

  → Access Control (data link layer)

  → DoS prevention (?)

802.11 Network Access Control

- Network Identification based on SSID (Service Set Identifier)
  - “secret” SSID shared by too many
  - Exchanged in cleartext
  - Ease of replay
- Access Control: MAC-address based authorization to Access Point
  - MAC-addresses are not authenticated
  - MAC-addresses are easy to set on most cards
- 802.1x
  - Clients authenticated and screened by Radius Server
  - AP serves as proxy
  - Extensible Authentication Protocol (EAP)

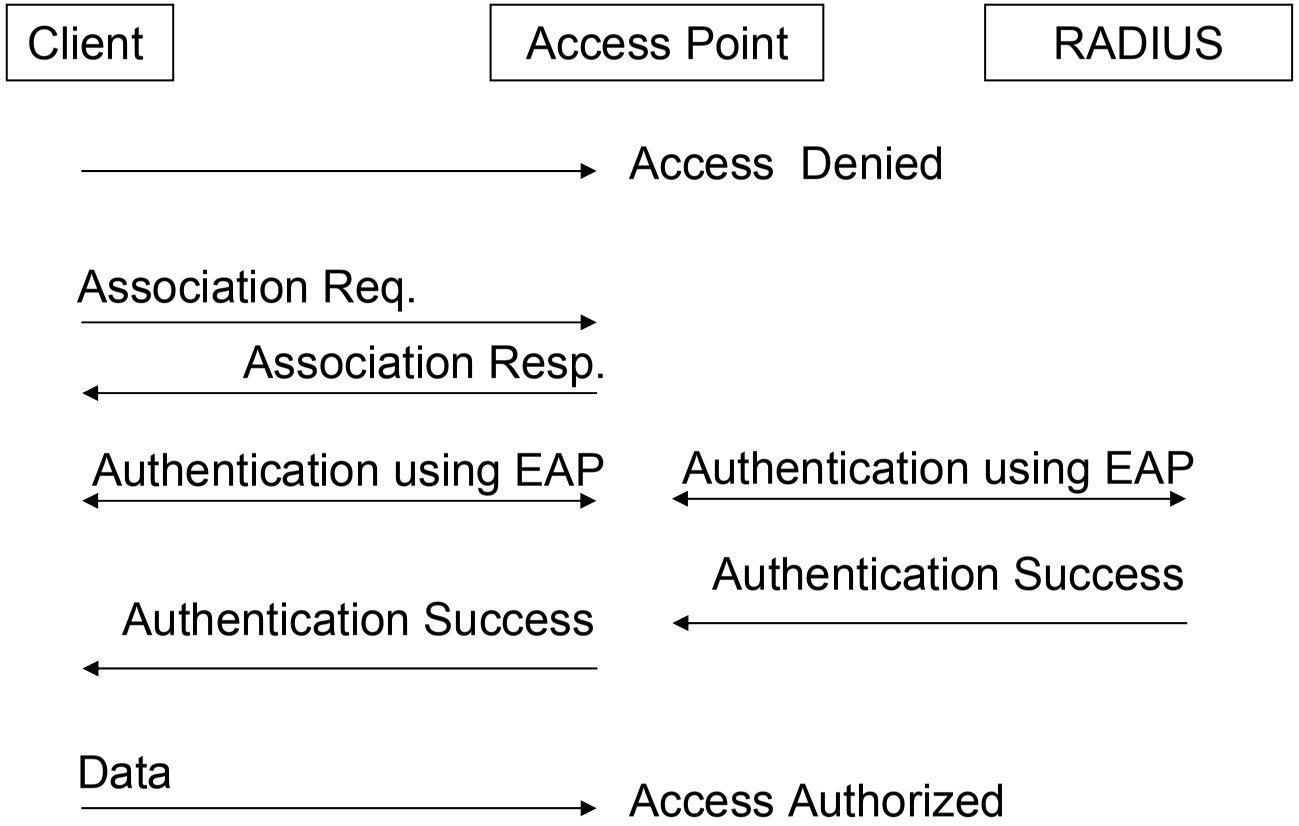
802.11 Client and Data Security

- Wireless Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- 802.11i (WPA2)

802.1x

- General purpose network access control mechanism
- 802.1x support in Access point
- No impact on clients' wireless interface
- Authentication and Authorization by RADIUS server
  - Extensible Authentication Protocol (EAP) RFC 2284
    - Alternative methods: password, smartcard, tokens, OTP
    - Alternative protocols: simple challenge response, EAP-TLS.
  - RADIUS server determines whether access to controlled ports of the AP should be allowed

802.1x Operational Flows



WEP Services

- Data Confidentiality
- Data Integrity
- Data Origin Authentication
- Access control through client authentication by the AP

WEP

- RC4 stream cipher
- 40bit and 104bit keys
- WEP key shared by all
- No key distribution

WEP operation

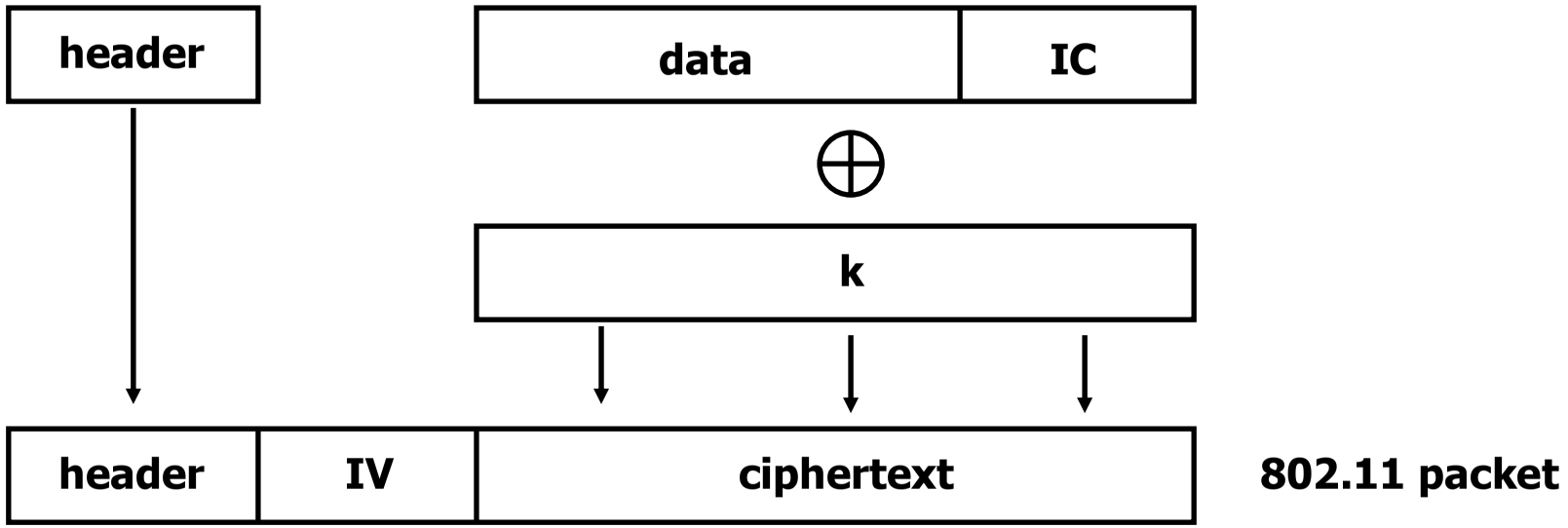
- K : shared key (40 or 104 bits)
- integrity check: IC = h(header|data)
- random initialization vector: IV (24 bits)
- Keystream generation:

$$k = RC4(K, IV)$$

- Encryption of data fragment m:

$$E_K(m) = m \oplus k$$

WEP packet



WEP Encryption flaws

If $C_1 = P_1 \oplus RC4(v,k)$ and $C_2 = P_2 \oplus RC4(v,k)$

$$C_1 \oplus C_2 = (P_1 \oplus RC4(v,k)) \oplus (P_2 \oplus RC4(v,k))$$

$$= P_1 \oplus P_2$$

- secret parts of P_1 can be retrieved based on known parts of P_2.
- keystream can be retrieved similarly.
- once keystreams are identified, new ciphertext can be decrypted based on (cleartext) IV used as index to an array of known keystreams if keystreams are reused.
- reuse of the same keystream:
  - standards recommend, but do not require, a per-stream IV to combat this
  - Some PCMCIA cards reset IV to 0 each time they're re-initialized and increment by 1, so expect reuse of low-value IVs
  - WEP only uses 24-bit IVs ➔ "birthday paradox"

WEP Message Authentication Flaws

- Hash function h, based on CRC-32, is a linear function of the message: $h(X) \oplus h(Y) = h(X \oplus Y)$

Modification attack: New (valid) ciphertext can be computed from existing ciphertext without the knowledge of the keystream:

- Existing ciphertext $C = RC4(k,v) \oplus (M \mid h(M))$
- New ciphertext resulting from a desired modification(D) on C:

$$C' = C \oplus (D \mid h(D)) = RC4(k,v) \oplus (M \mid h(M)) \oplus (D \mid h(D))$$

$$= RC4(k,v) \oplus (M \oplus D \mid h(M) \oplus h(D))$$

$$= RC4(k,v) \oplus (M \oplus D \mid h(M \oplus D))$$

WEP flaws continued

- Using flaws in encryption and message authentication, further attacks such as spoofing, dictionary attacks, traffic injection, route subversion can be mounted. Tools are available.

- Management messages (deassociate, deauthenticate) are not authenticated: DoS and MITM attacks still work.

- Advanced attack:

  Retrieve WEP keys using the attack described in "Weaknesses in the Key Scheduling Algorithm of RC4“ by Fluhrer, Mantin, and Shamir

  – Airsnort

  http://airsnort.shmoo.com

  – WEPCrack

  http://wepcrack.sourceforge.net/

Wi-Fi Protected Access (WPA)

- subset of the forthcoming IEEE 802.11i security standard (also known as WPA2)
- designed to overcome the weaknesses of WEP
- Compatible with existing 802.11 hardware using firmware upgrades
- **Features of WPA**
- Enhanced encryption scheme: Temporal Key Integrity Protocol (TKIP)
  - RC4, dynamic session keys
  - 48 bit IV

- Non-linear Message Integrity Checks (MIC) based on Michael
- Strong User Authentication using one of the standard Extensible Authentication Protocol (EAP) types available

WPA2 - 802.11i

Ultimate improvements over WPA

802.11i Features

- New encryption algorithm: Advanced Encryption Standard (AES)

  $\rightarrow$ impact on hardware

- Dynamic keys both for encryption and authentication

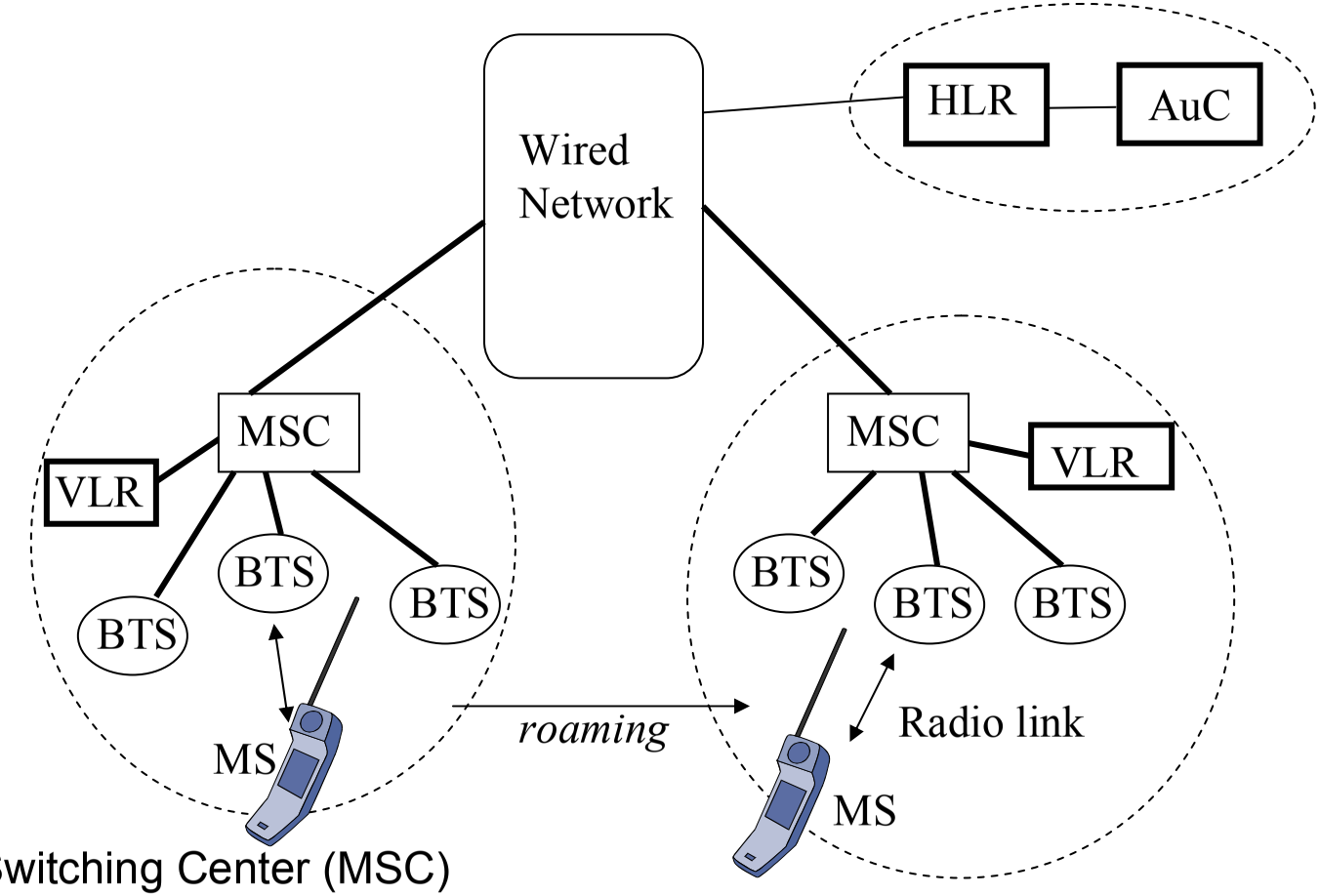
Outline

- Wireless LAN
  - 802.11 (WiFi)

- Mobile Telecommunications Security
  - GSM Security Features
  - 3GPP Security Architecture
  - CDPD Key agreement and authentication
  - Fraud management

- Mobile IP
  - IPsec-based solution
  - Firewalls vs. Mobile IP vs. Packet Filtering

GSM



Mobile Switching Center (MSC)
Base Station (BS)
Mobile Subscriber (MS) = Mobile Equipment (ME) + Subscriber Identity Module (SIM)
Home Location Registry (HLR)
Authentication Center (AuC)
Visiting Location Registry (VLR)

Security Requirements

- Security Threats
  - Eavesdropping on the Radio interface
    - data confidentiality
    - User anonymity
  - MS Impersonation (masquerade)

- Security Services
  - Subscriber identity protection
  - Subscriber authentication
  - Data confidentiality

Goal:

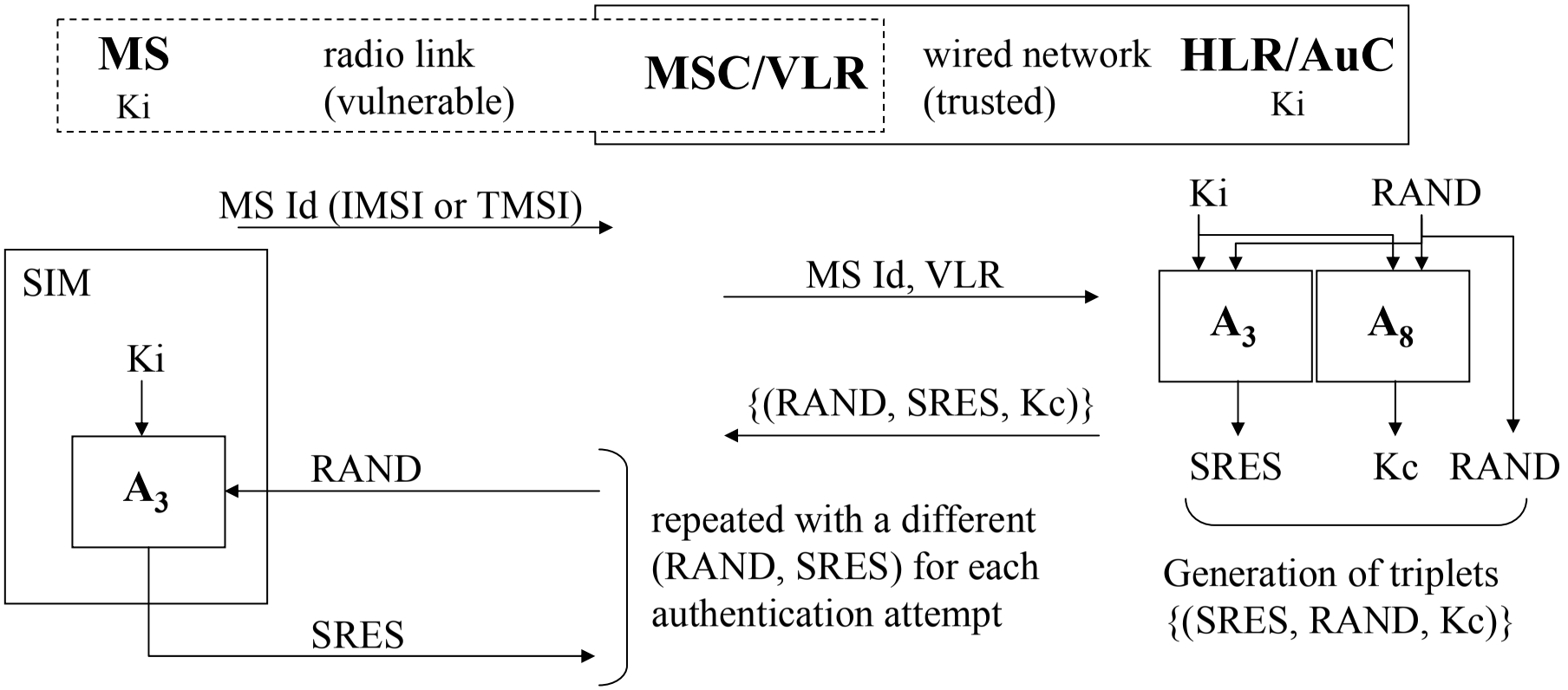
Wireless security equivalent to wired Network

Subscriber Identity Protection in GSM

- IMSI: universal identity (15 digits - 9 octets)
- replaced by TMSI (temporary mobile subscriber identity) (4 octets)

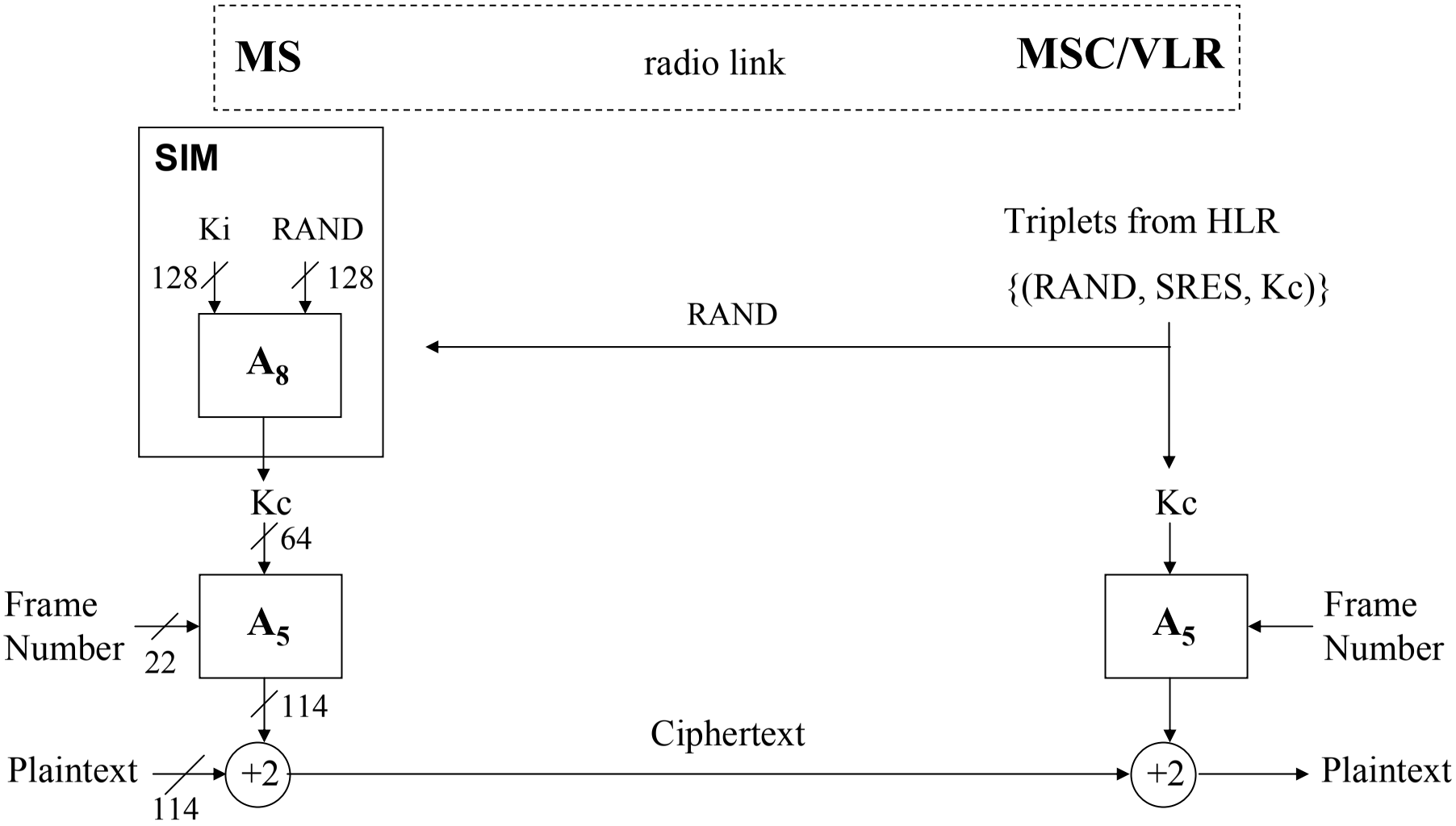
- First registration or after failure in VLR IMSI is sent in clear.
- TMSI allocated by the VLR where the MS is registered.
- TMSI protected by Data Confidentiality Service transmitted to MS.
- Subsequent identification of MS by VLR is based on TMSI.

Authentication in GSM



• bandwidth optimization: several verifications by the VLR can take place locally without communicating with the remote HLR.
• security: Ki is not disclosed to the VLR's of the visited areas.

Data confidentiality in GSM



GSM Algorithms

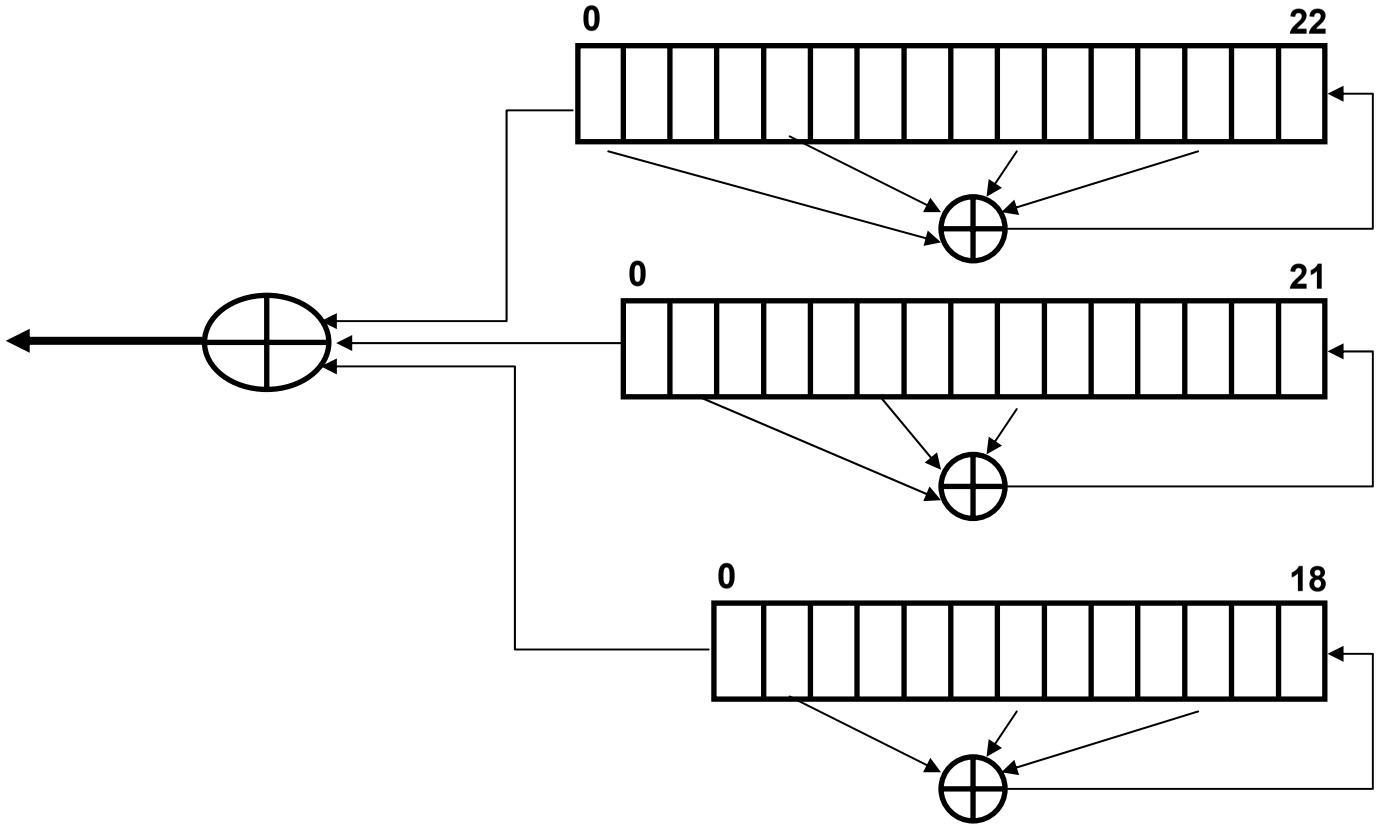
- A3 and A8
  - Defined by the network operator
  - Software implementation in the SIM
- A5 stream cipher
  - Hardware implementation in the ME
  - defined by the standard (interoperability)
  - Several versions: A5/1, A5/2, A5/3

A3 and A8

- Algorithm left at the discretion of the operator
- COMP128 - ill-advised by GSM standards
  - 128-bit hash function
  - first 32 bits producing the A3 output
  - last 64 bits producing the A8 output
  - major weaknesses
    - A collision just requires 2^{14} attempts

A5/1

- Based on a combination of LFSRs



clocking based on majority rule

Security of A5/1 and A5/2

- A5/1
  - Exhaustive search, complexity=2^{64}
  - Attacks based on time-memory trade-off
  - Attack
    - 2 disks (73 GB)
    - 2 seconds of plaintext
    - Key retrieved in a minute
- A5/2
  - Similar design, deliberately weak

A5/3

- Based on Block cipher
- Output Feedback Mode with BLCKCNT to prevent short cycles
- No security by obscurity
- Design by ETSI SAGE
  - Based on Kasumi, derived from MISTY1 (Mitsubishi)
- As part of 3GPP

GSM Security - Summary

Pros

- Effective solution to cloning
- Higher confidentiality compared with analogue systems

Cons

- Security limited to access network
- Lack of network authentication
  - Risk of bogus base stations
- Security by obscurity
- Ill advised use of weak algorithms
- Lack of control over activation of security for user and home network
- Lack of lawful interception

Outline

- Wireless LAN
  - 802.11 (WiFi)

- Mobile Telecommunications Security
  - GSM Security Features
  - 3GPP Security Architecture
  - CDPD Key agreement and authentication
  - Fraud management

- Mobile IP
  - IPsec-based solution
  - Firewalls vs. Mobile IP vs. Packet Filtering

Objectives of 3GPP Security

- Build on the security of GSM
  - adopt security features that have proved to be needed and that are robust
  - ensure compatibility with GSM to ease inter-working and handover
- Fix the security flaws of GSM
- Enhance with new security features to suit
  - new services
  - changes in network architecture
- Keep minimal trust in intermediate components

Lessons from GSM

- Mutual authentication between user and base station
- No security by obscurity
  - Make sure chosen algorithms have been tested by the scientific community
- Flexibility in standards
- Change in law enforcement for cryptography: longer keys (≥128 bits)

3GPP Security Services

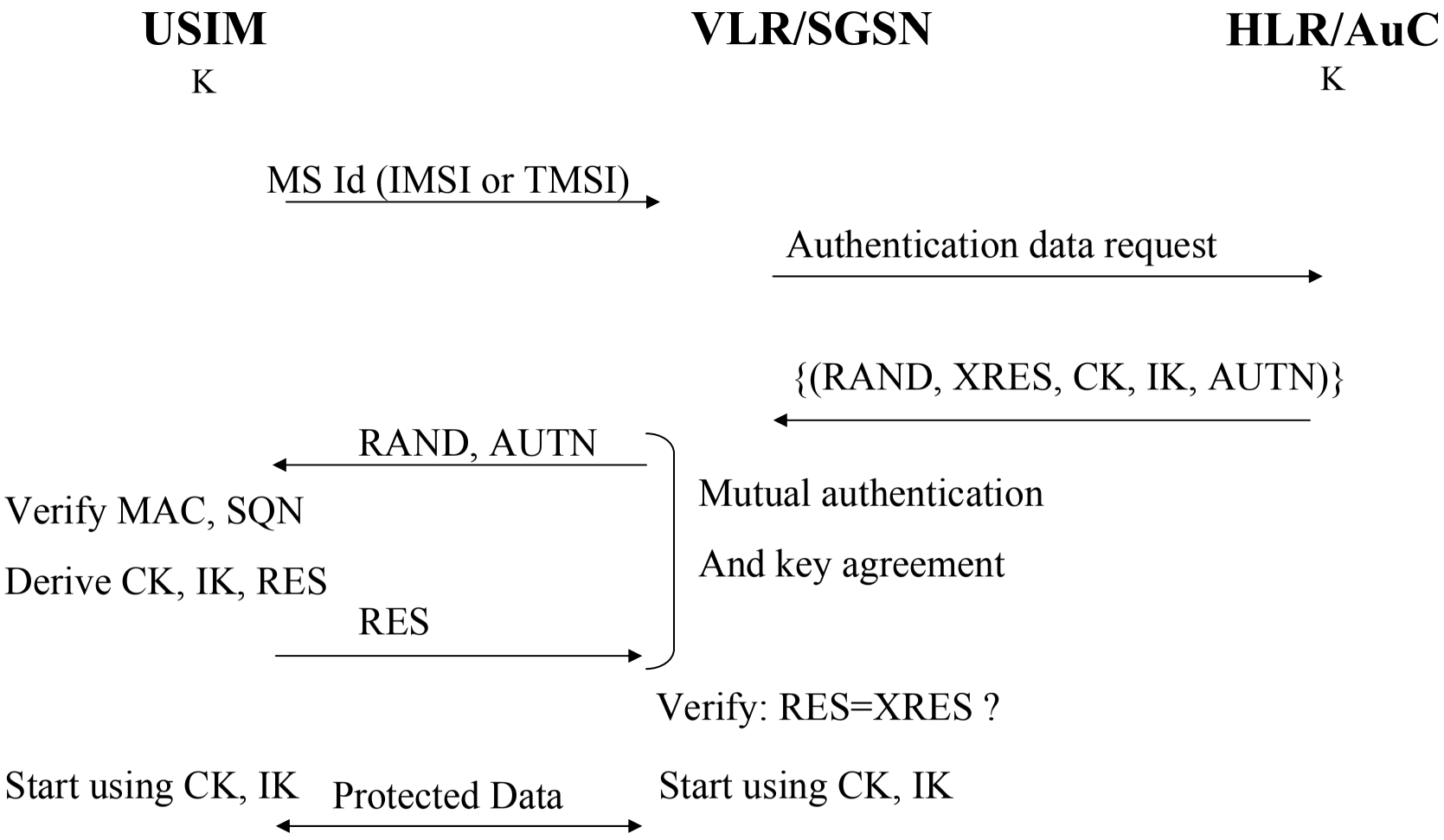
- Mutual Authentication between User and Network
- Data Confidentiality (user traffic and signalling data) (like GSM)
- User identity protection (like GSM)
- Data Integrity (over the air interface)

Authentication & Key Agreement (AKA)

Objectives

- Mutually authenticate user to network
- Establish shared keys between user and network
  - CK: 128-bit encryption key
  - IK: 128-bit integrity key
- Assure freshness of CK/IK
- Authenticated management field HLR → USIM
  - Authentication key and algorithm identifiers
  - Limit CK/IK usage for each AKA execution

AKA Message Flows



Data Encryption

- Applied on User & Signaling Data
- Over the air interface

- Stream Cipher
- Provision for different Algorithms
- Including Kasumi (A5/3 of GSM)

Outline

- Wireless LAN
  - 802.11 (WiFi)

- Mobile Telecommunications Security
  - GSM Security Features
  - 3GPP Security Architecture
  - CDPD Key agreement and authentication
  - Fraud management

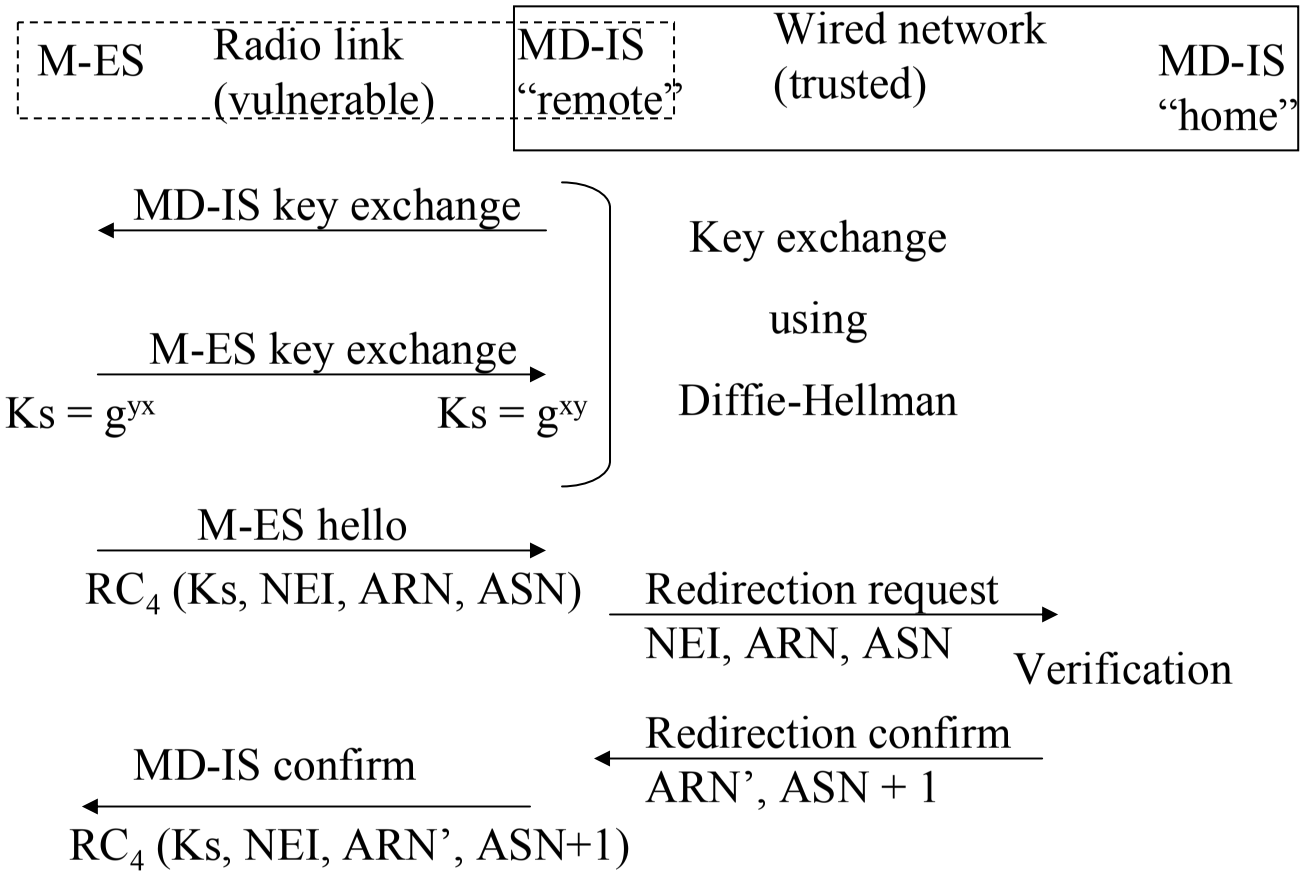
- Mobile IP
  - IPsec-based solution
  - Firewalls vs. Mobile IP vs. Packet Filtering

Cellular Digital Packet Data (CDPD)

- Data communication over the analog AMPS network
- Full-fledge network architecture including several layers

- Security services:
  - mobile unit authentication
  - data confidentiality over the wireless link
  - key exchange

CDPD - Mobile Unit Authentication



NEI : mobile unit id
ARN : nonce
ASN : sequence number

Fraud Management in Mobile Networks

Threats:
- Access fraud
- Subscription fraud

Security mechanisms like authentication and confidentiality prevent access fraud but they cannot help with subscription fraud.

Solution: real-time fraud detection

Principle:
- monitor subscriber behavior in real-time
- based on connection tickets
- detect deviations with respect to user/class profile
- prompt suspected users with explicit authentication challenge
- adapt user/class profile based on the monitoring

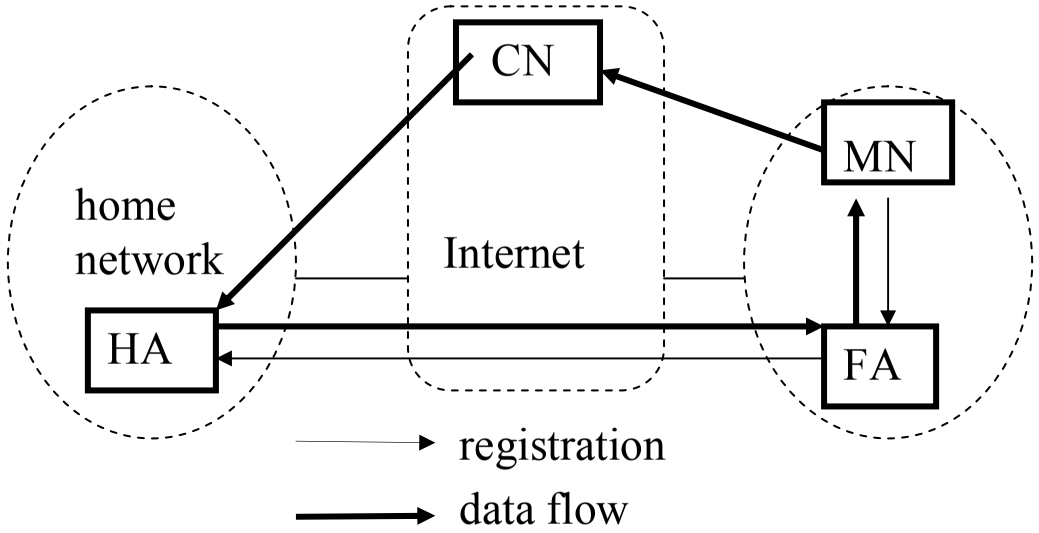
Outline

- Wireless LAN
  - 802.11 (WiFi)

- Mobile Telecommunications Security
  - GSM Security Features
  - 3GPP Security Architecture
  - CDPD Key agreement and authentication
  - Fraud management

- Mobile IP
  - IPsec-based solution
  - Firewalls vs. Mobile IP vs. Packet Filtering

Mobile IP



Mobile Node (MN) - Correspondent Node (CN)
Home Agent (HA) - Foreign Agent (FA)

CN → MN :
IP within IP tunneling between HA and FA:
• outer IP: dst@: care of address(COA), src @: HA@
• inner IP: dst@: MN@, src@: CN@

MN → CN :
regular IP

Mobile IP Security Requirements

MN registration

- impersonation of MN by intruders or malicious FA
- replay
- subversion of traffic destined to MN

Solution: authentication of MN by HA

- Mobile IPv4
  - Authentication based on keyed MD5 or HMAC using timestamps or nonces

- Mobile IPv6
  - default IP AH support
  - security association between MN and HA
  - key management might be a problem.

Mobile IP Security Requirements

CN → HA → MN

Difference / wired networks: MN possibly located in an untrusted remote network

Solution:
IPsec
-IP Authentication Header
-IP Encapsulating Security Payload
-Key Management

Mandatory requirement: Security Association between HA and MN.
End-to-end security: SA between CN and MN

MN → CN

Exposure is similar
Solution: IPsec with an SA between MN and CN

Mobile IP vs. Firewalls

• Firewall traversal for Mobile IP

Firewall policy (usually) does not allow inbound connections from external networks.
How can a remote MN connect to the home network under such policy.

• ingress filtering

Even if there is no firewall, simple packet filtering exists in most networks.
Mobile IP traffic can be blocked by such filtering.

• CN's inside home network may use **private** IP addresses together with NAT
MN $\rightarrow$ CN packets may simply not get routed in Internet.

Solution for all:

IPsec tunneling through the firewall

Mobile IP vs. Packet Filtering

MN@ does not belong to remote network.

If packet filtering is implemented problems may arise:

• MN → CN packets gets rejected by remote network filtering because they have an illegal source address (outbound packet with an external source address).

• MN → home network packets get rejected by the filtering at the home network because they have an illegal source address (inbound packet with an internal source address).

Such packet filtering is due to countermeasures called anti-spoofing.

Anti-spoofing

IP Spoofing Attacks based on IP packets with bogus source address:

- Land attacks: src@=dst@, destination host hangs.
- smurf: ping with directed broadcast address may use a bogus source address in the same network as the destination; the host at the source address gets flooded by the replies to the broadcast.
- SYN attacks: TCP SYN packet causes allocation of kernel memory, may use bogus source address belonging to the destination network.

Anti-spoofing measures

Drop packets with obvious inconsistency:

- outbound packet with an external source address
- inbound packet with an internal source address
- inbound packets with private IP source address

Cisco IOS anti-spoofing rules for network 192.65.32.0/24

- on the external router interface (inbound packets):

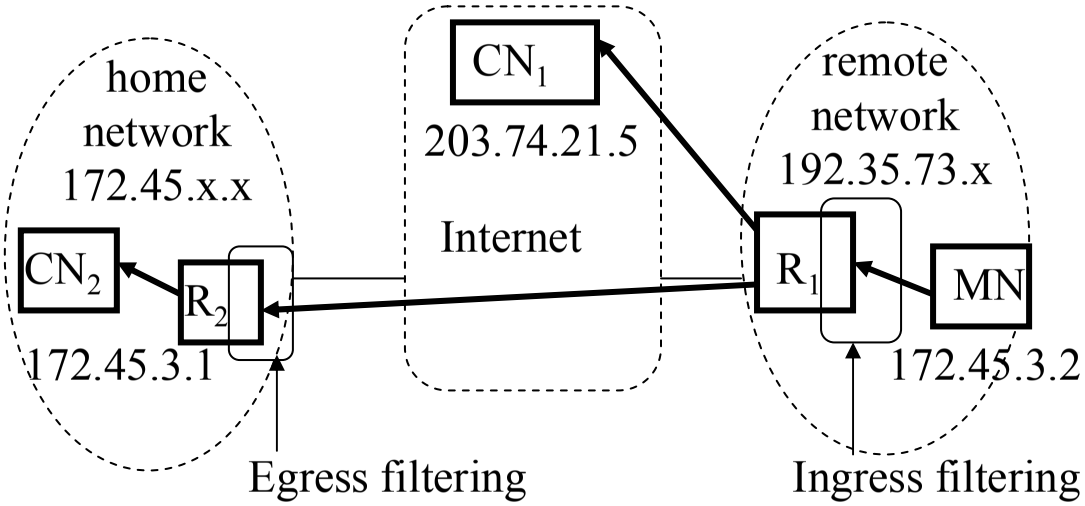
```
access-list 101 deny ip 192.65.32.0 0.0.0.255 any
```

- on the internal router interface (outbound packets):

```
access-list 101 permit ip 192.65.32.0 0.0.0.255 any
access-list 101 deny ip any any log
```

Anti-spoofing vs. Mobile IP

Why MIP packets get blocked by anti-spoofing ?

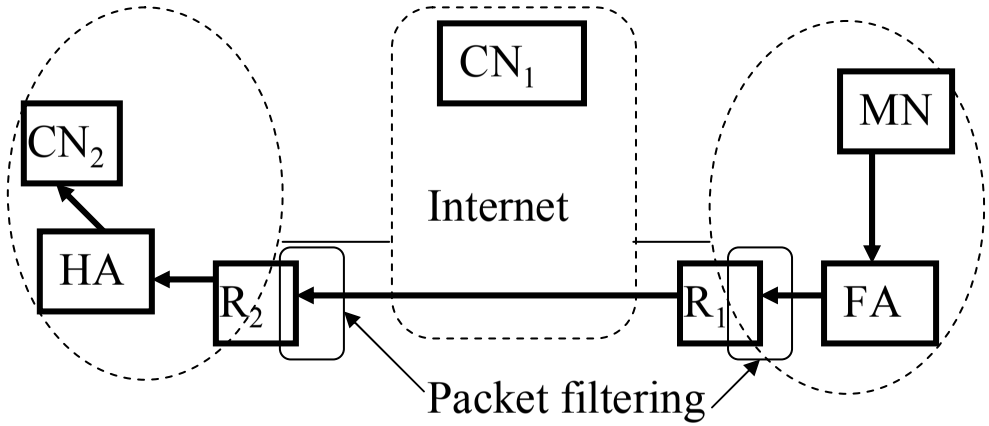


MN → CN_1 packets blocked by the ingress anti-spoofing in router R_1:
access-list 101 permit ip 192.35.73.0 0.0.0.255 any
access-list 101 deny ip any any log

MN → CN_2 packets blocked by egress anti-spoofing in router R_2:
access-list 101 deny ip 172.45.0.0 0.0.255.255 any

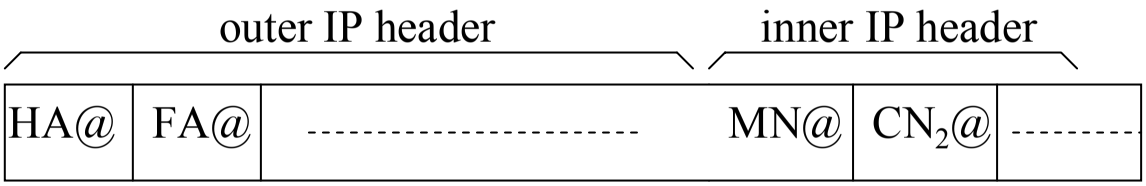
How can MIP pass through anti-spoofing

Reverse tunneling to by-pass anti-spoofing



Packets originated at MN

- take the path MN → FA → HA → CN_2
- IPwithinIP encapsulation between FA and HA:



No illegal addresses any more.

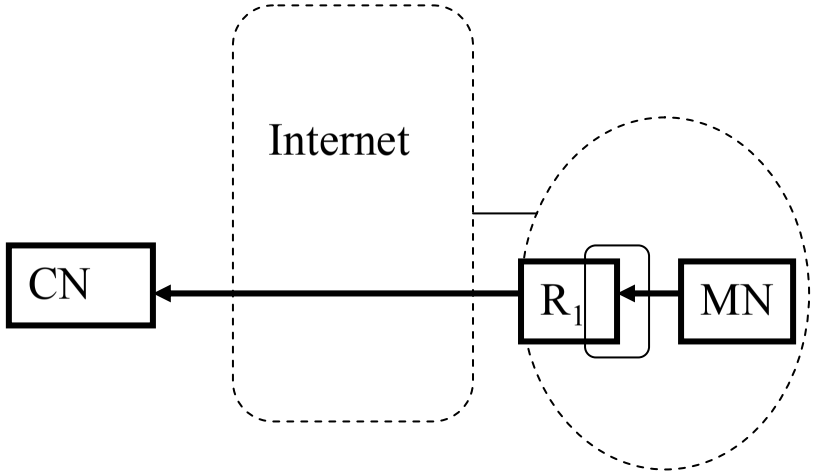
New problem with Reverse Tunnelling

Intruders can perpetrate spoofing attacks by sending encapsulated (IPIP) packets with bogus addresses in the inner header.

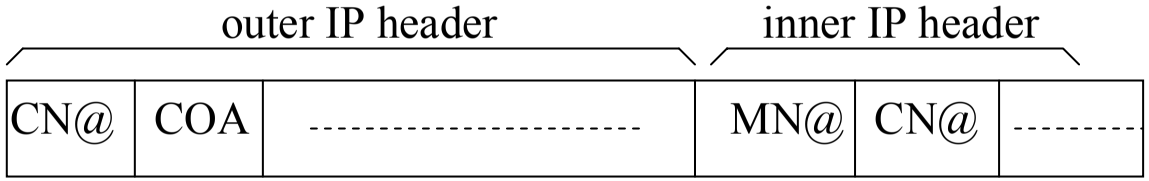
$\Rightarrow$ No spoofing defense any more

How can MIP pass through anti-spoofing

Direct tunnelling of data traffic by MN:



IPwithinIP encapsulation between MN and CN:



COA: Care of address

Problem: CN must be able do de-encapsulate IPIP packets.

Solution: Firewall compatible with Mobile IP

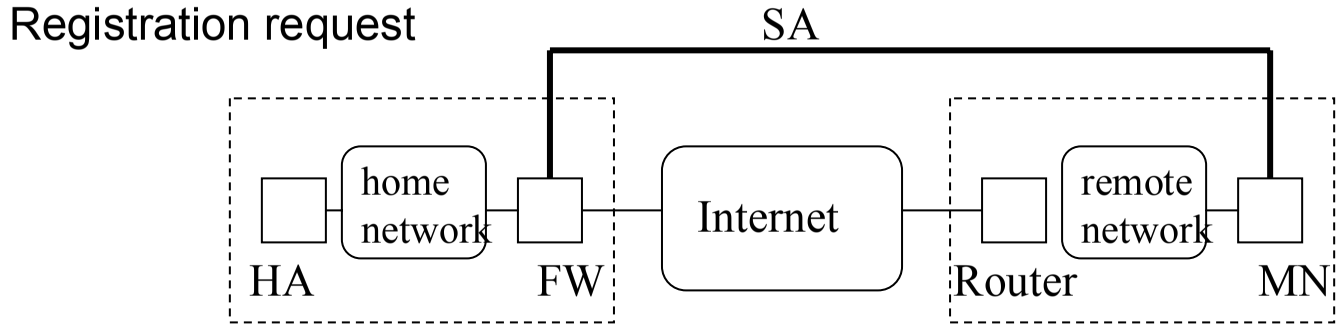
Idea:MN should enjoy the same level of connectivity and security as if it were in the secure home network.

Principle: all traffic between MN and home network goes through a firewall.
Problems due to filtering and addressing discrepancies are also solved.

Possible approaches:

- Application gateway or circuit gateway:
  - strong authentication
  - complex interactions
  - no data confidentiality and integrity
- IPsec tunnelling
  - most suitable to create a virtual home network abroad
  - external links can be viewed as secure as internal ones
  - data confidentiality and integrity in addition to authentication

IPsec tunnelling Firewall



IP Datagram between MN and FW

Tunnel Mode SA

IP2	AH	IP1	registration request

IP2	ESP	IP1	registration request

IP Datagram between FW and HA

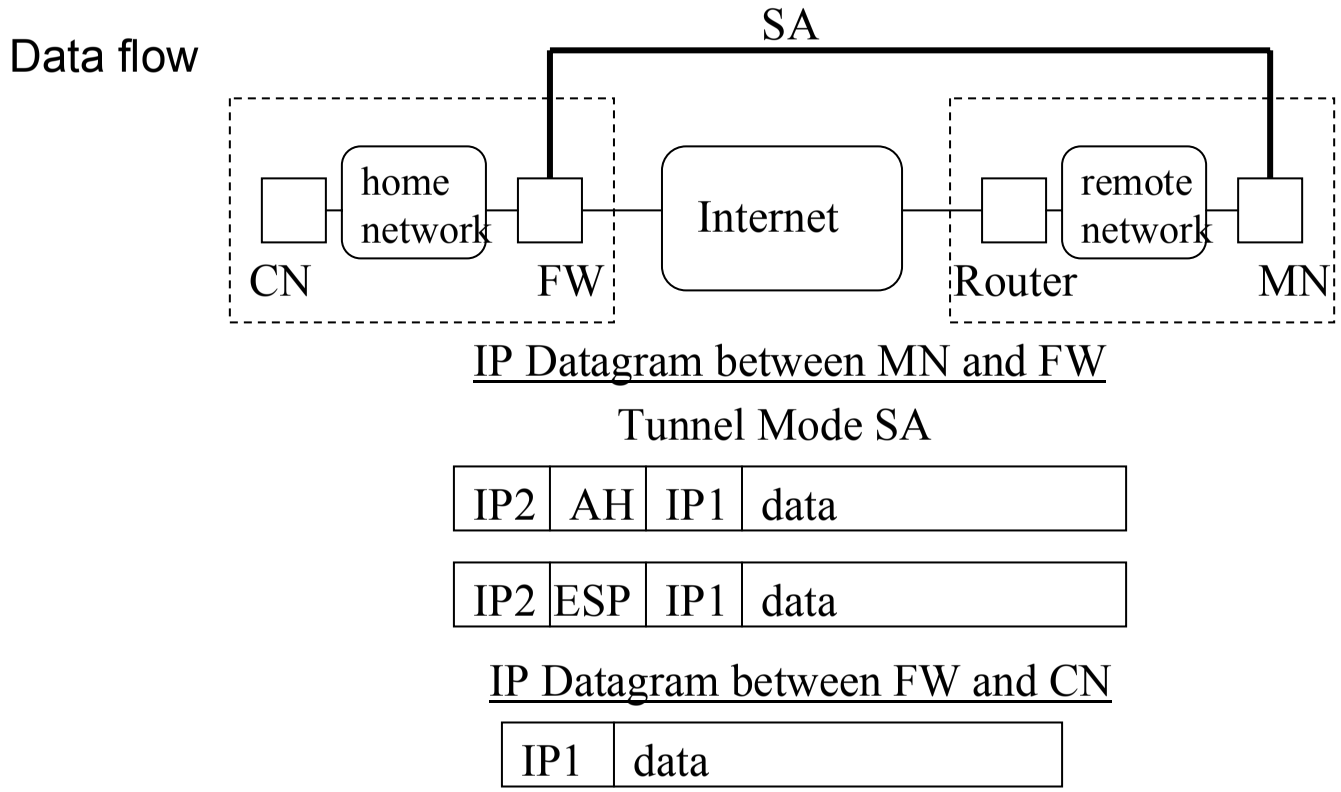
IP1	registration request

IP1 : src@=COA; dst@=HA@
IP2 : src@=COA; dst@=FW@

COA : care of address obtained from DHCP
COA ∈ remote network

- Optional tunnel SA between FW and HA
- SA's must be established manually or using key management (IKE, ISAKMP)
- FW retrieves security parameters of the SA using the SPI in the IPsec (AH or ESP) header.

IPsec tunnelling Firewall



IP1 : src@=MN@; dst@=CN@
IP2 : src@=COA; dst@=FW@

COA ∈ remote network
MN @ ∈ home network

- Optional FW-CN tunnel SA or MN-CN transport/tunnel SA
- SA's must be established manually or using key management (IKE, ISAKMP)
- FW retrieves security parameters of the SA using the SPI in the IPsec (AH or ESP) header.

IPsec tunnelling Firewall - Conclusion

• Secure extension of protected home network to mobile nodes abroad

• By-product: packet filtering problems are avoided

• communications between MN at home and external CN: regular (non-mobile) security controls apply in this case.

• communications between MN on public network and external CN: use bi-directional IPsec tunnels.