IETF 81 - Quebec City, Canada
July 24 - 29, 2011

HIP based Femtocell Networks :

(Securing the Backhaul for Mobile and Multi-homed Femtocells)

Suneth Namal, Andrei Gurtov
Centre for Wireless Communications
University of Oulu, P.O. Box 4500, FI-90014 Oulu, Finland

Motivation Towards Femtocell Technology

Motivation:

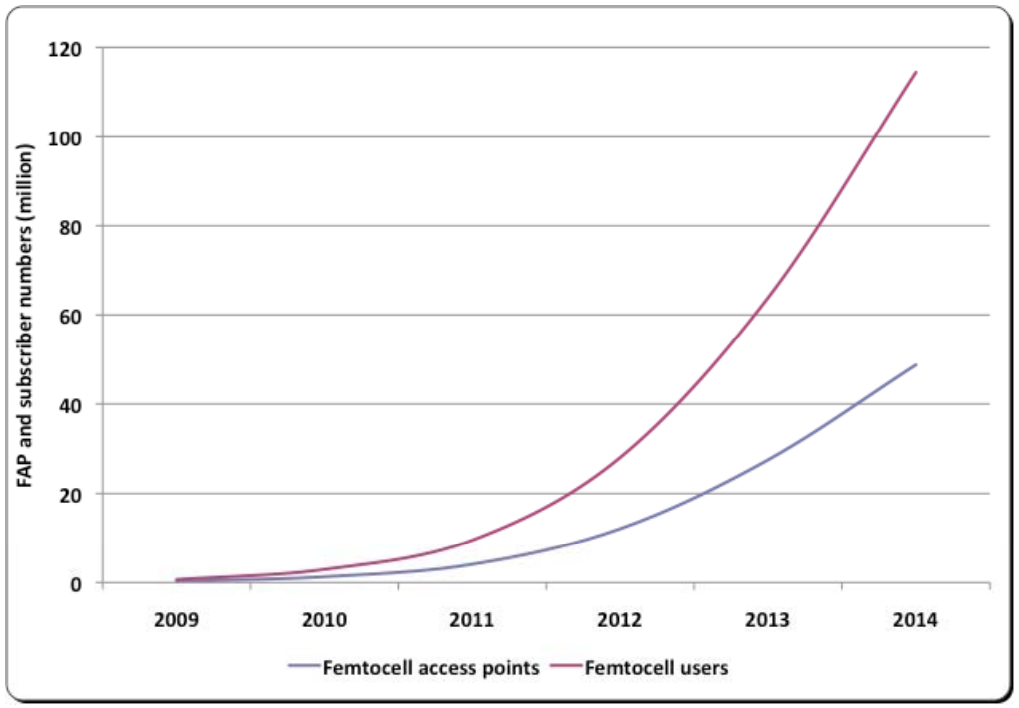
- The evolution of femtocells in residential networks expect to accelerate dramatically in next few years. Wide variety of services, attractive features such as,
  - improved indoor coverage
  - reduction of in home call charges
  - backhaul traffic, ease of use
  - privacy bring more interest in femtocell deployment.

Proposed Solution:
Host Identity Protocol Based Secure Backhaul for Femtocell Networks

- HIP is used as a transport protocol in the proposed architecture meantime it is used as an authentication protocol.
- Protocol level modifications are proposed to fit it to the mobile communication.

Secure Backhaul for Femtocell Networks

- **Femtocell Security*:*** The femtocell security is divided into two sections such as FAP **authentication** and **message encryption** across the unreliable public network among HeNB and SeGW.



Expected femtocell usage

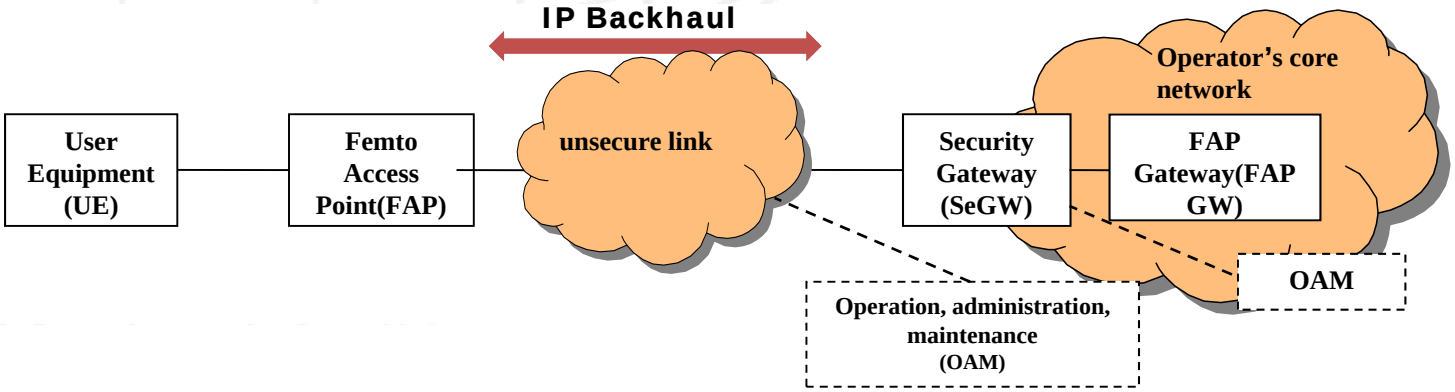
The IP address depicts both location and the identity of a mobile device.

– The PMIPv6 assigns a CoA to the mobile device that allows home agent to forward the packets to the mobile.

– IP address is the temporary identity assigned to the mobile node.

– HIP based host identifier is unique unlike an IP address. In HIP, IP is no longer an identifier, but a locator which signifies the geographical location of the mobile device.

Femtocell Backhaul

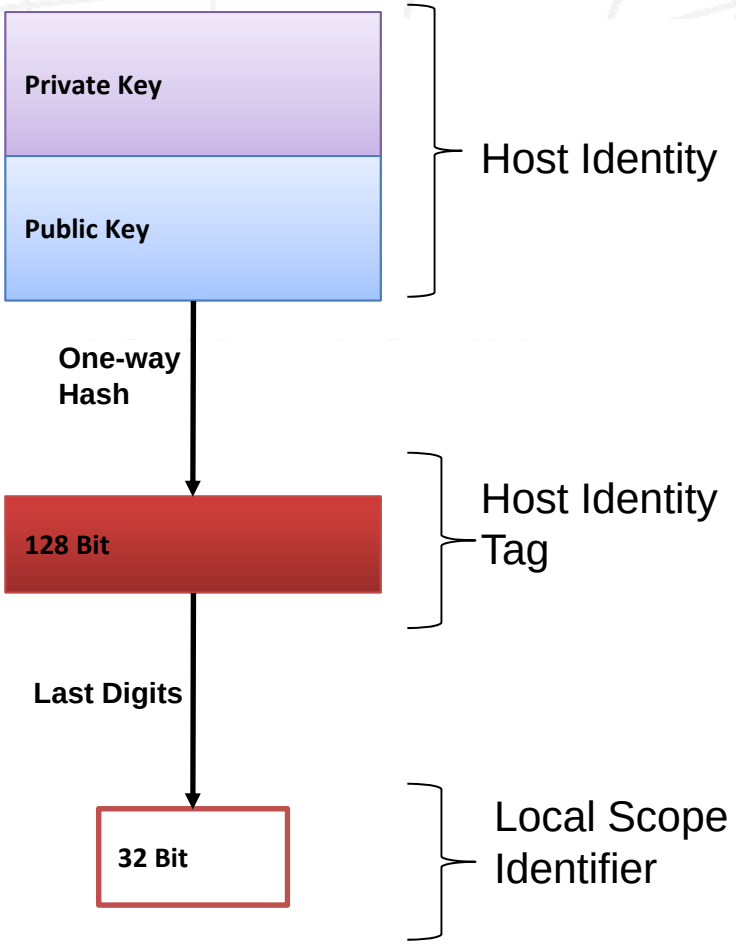


- Setting up a secure backhaul connection between FAP and the operator network requires mutual authentication between FAP and the core network.

- FAP should set up at least one IPsec tunnel, i.e., a pair of unidirectional Secure Associations (SAs) between FAP and SeGW. The FAP should initiate the creation of the SA, i.e., it should act as initiator in the Traffic Selector negotiation. Upon successful authentication, the SeGW allocates IP address to the FAP.

- The FAP and SeGW use the IKEv2 mechanisms for
  - detection of NAT
  - UDP encapsulation for NAT Traversal
  - FAP initiated NAT keep-alive
  - IKE and IPsec SA rekeying
  - Dead Peer Detection (DPD).

Host Identity Protocol (HIP)



- Host Identity Protocol (HIP) architecture proposes an alternative to the dual use of IP addresses as
  1. Locators (routing labels)
  2. Identifiers (endpoint, or host, identifiers).

- Host Identity Protocol (HIP) Introduce a separate cryptographic identifier which is globally unique.

- There are two main representations of the Host Identity,
  1. Full Host Identifier (HI) : The HI is a public key and directly represents the Identity.
  2. Host Identity Tag (HIT).

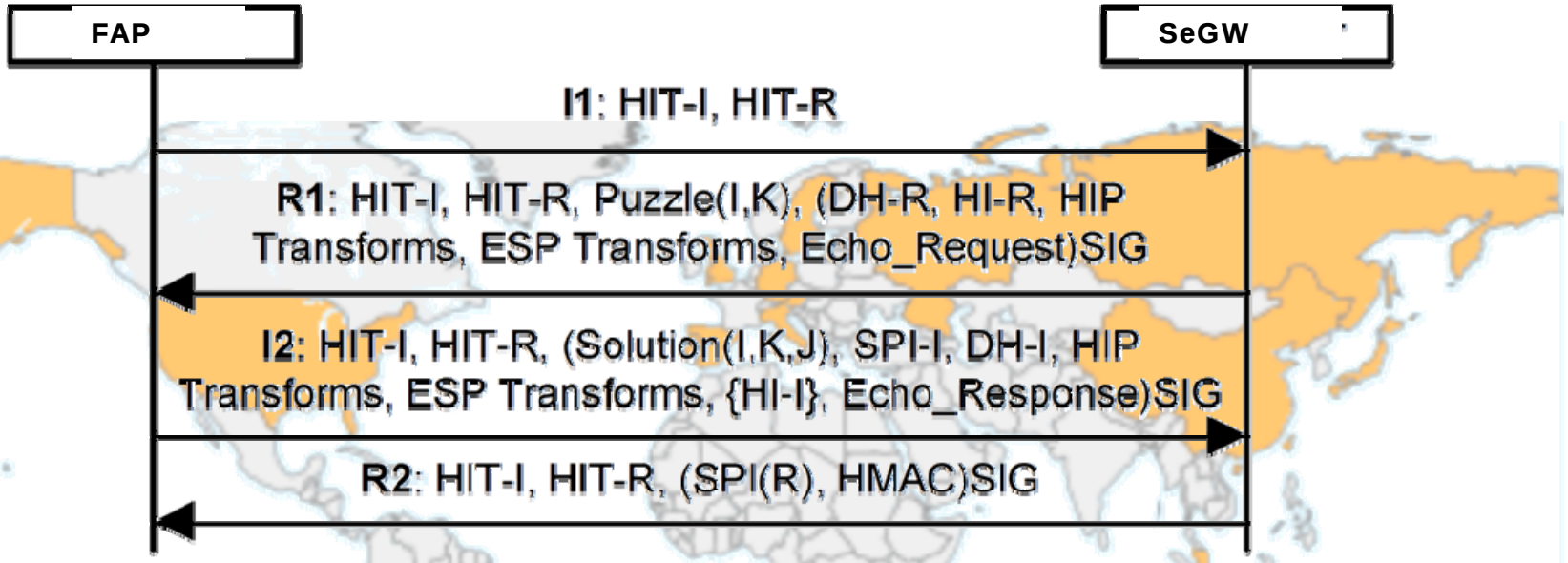
- HI is not good for use as a packet identifier. Thus, a hash of the HI, the Host Identity Tag (HIT), becomes the operational representation.

Host Identity Protocol (HIP)

- Mobile node is identified with a cryptographic identity
  - Implements an ID/locator split scheme
  - Public/private key pair as identifier
  - Host Identity Tag (HIT) used by apps
- Authentication over Internet protocols
  - Mutual authentication via public keys
  - Opportunistic negotiation of SA pairs
  - Data protected over ESP (SPI as ID)
- Support for host mobility and multihoming
  - Mobility events handled via HIP UPDATE messages (part of IP stack)
  - ID/locator separation to HIT and IP address enables simultaneous multihoming between the IPv4 and IPv6 protocols and interfaces assigned to a host

HIP based FAP Authentication

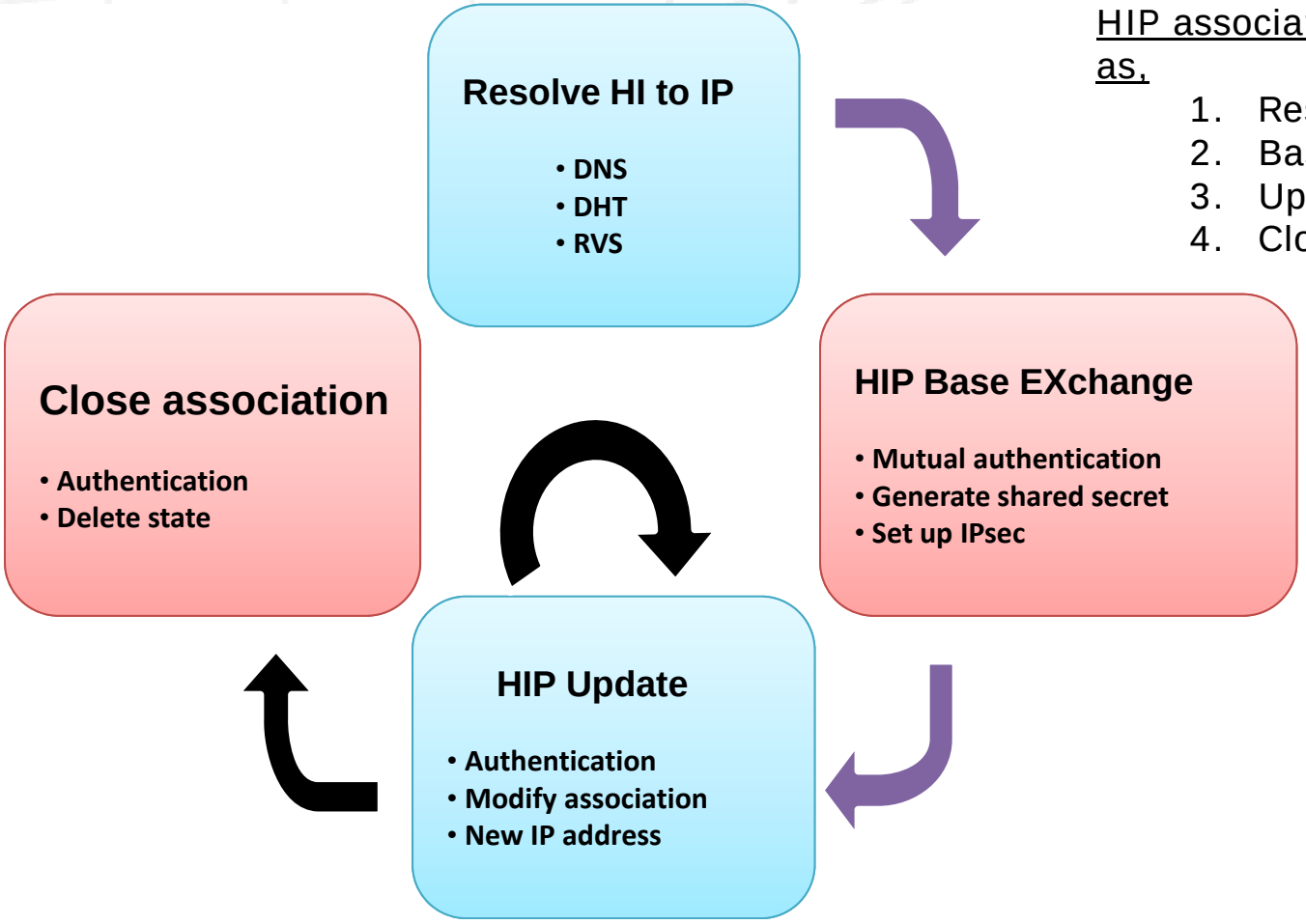
HIP peers follow a procedure called Base-Exchange which is a four-way handshake between the mobile node and the core network.



No certificates are required for the authentication because the HITs are self-certifying.

The base exchange is built around a classic authenticated Diffie-Hellman key exchange though there are some unusual features for DoS-protection.

Life Cycle of a HIP Association



HIP association has four stages such as,

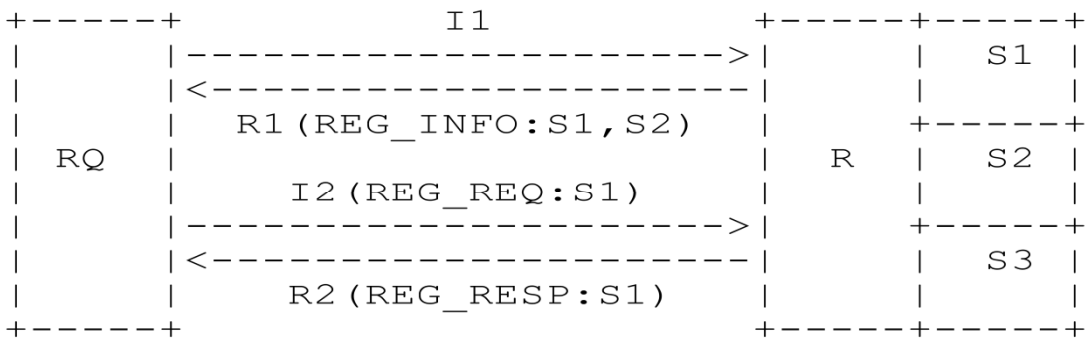
1. Resolving HI
2. Base-Exchange
3. Update Exchange
4. Closing association.

Registration Extension for HIP

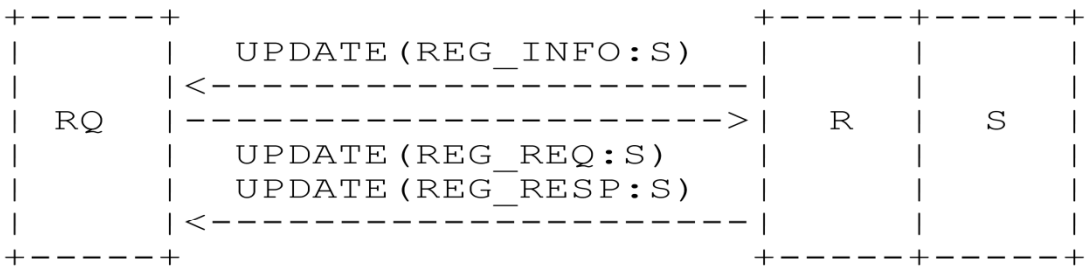
•To request registration with a service (S): A requester (RQ) constructs REG_REQUEST parameter and includes into I2 or UPDATE packet which is then sent to the registrar (R).

•If the requester has no HIP association established with the registrar: Requester *SHOULD* already send the REG_REQUEST in the I2 packet. A registrar *MAY* end a HIP association that does not carry a REG_REQUEST by including a NOTIFY with the type REG_REQUIRED in the R2.

Registration Extension with Base Exchange



Registration Extension with Update Exchange



Source: draft-ietf-hip-registration-02

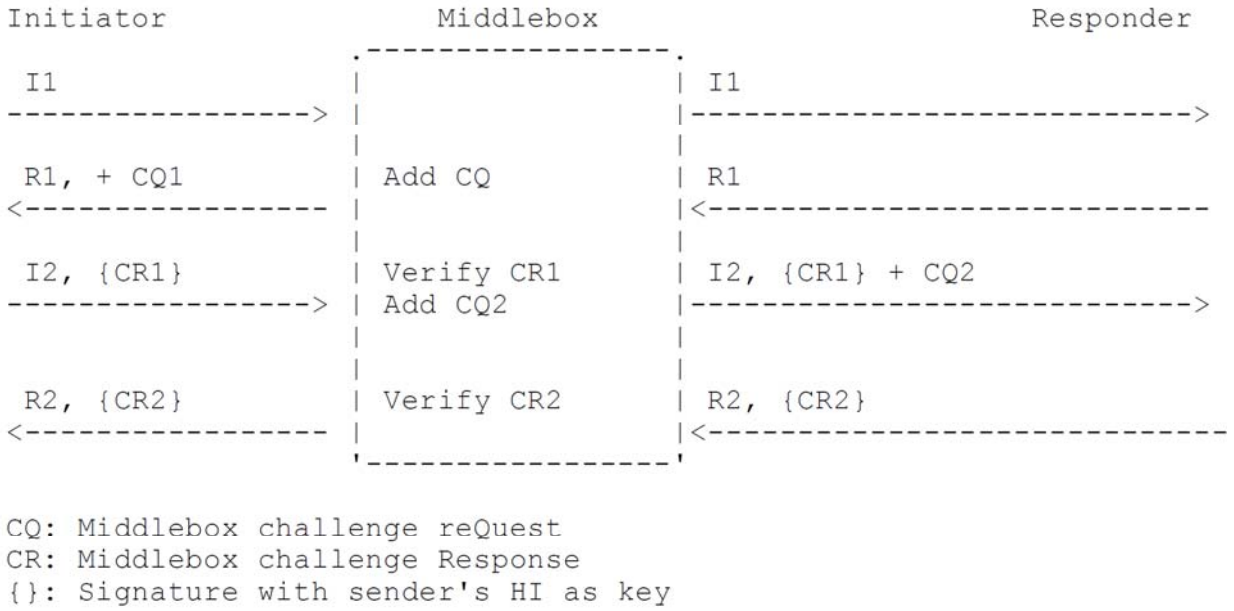
Identity Verification with HIP

- Middleboxes add CHALLENGE_REQUEST (CQ)parameters to the R1, I2, and to any UPDATE packet.

- CQ parameter contains an opaque data block of variable size which middlebox uses to carry arbitrary data (e.g., a nonce).

- The HIP packets that carry middlebox challenges may contain multiple CHALLENGE_REQUEST parameters, since all middleboxes on the path may add these parameters (CQ).

Base Exchange oriented identity verification



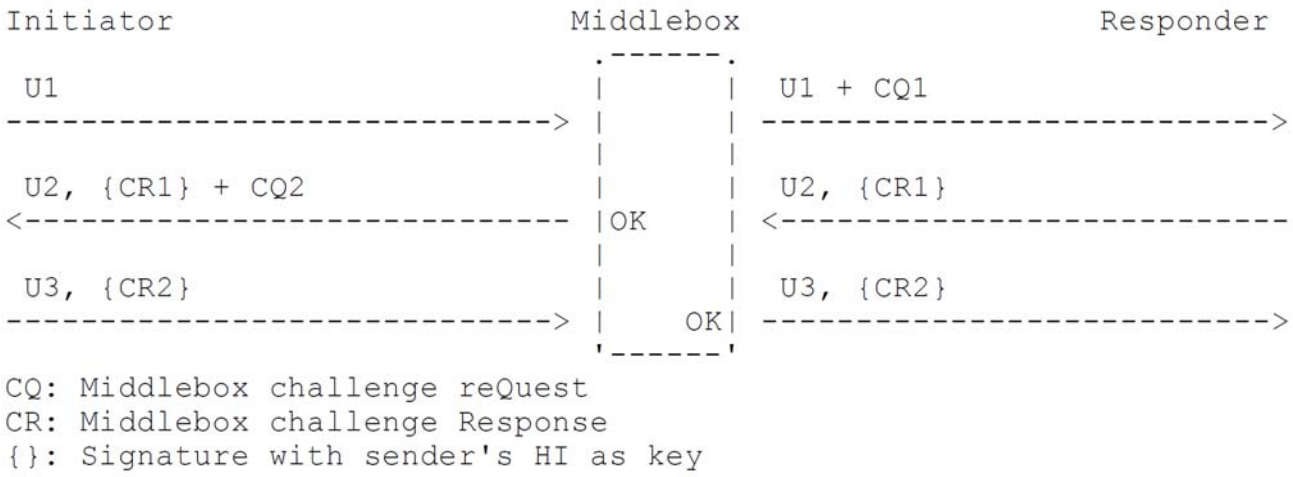
Source: draft-heer-hip-middle-auth-02 - End-Host Authentication for HIP Midd...

Identity Verification with HIP Contd...

- A HIP host, receiving a CHALLENGE_REQUEST MUST reply with a CHALLENGE_RESPONSE in its next I2 or UPDATE packet.

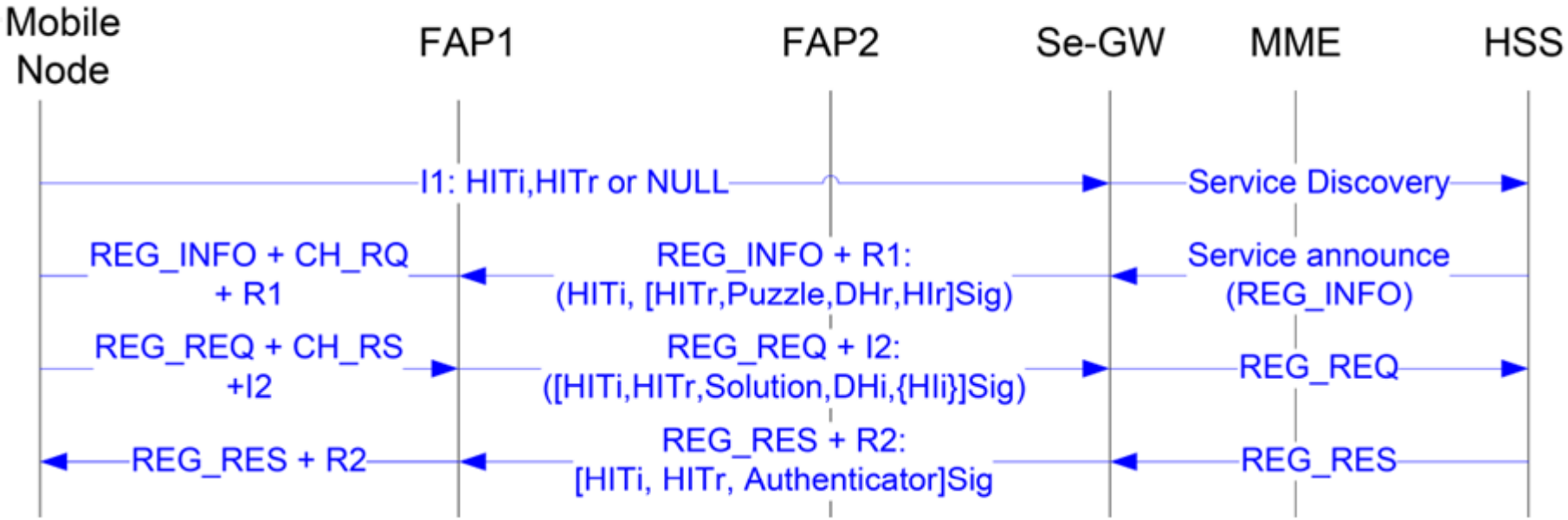
- At the time being, identity verification during the closing of a HIP association is not supported. Hence, the middlebox *MUST* preserve the state until it expires according to local policies.

Update Exchange oriented identity verification



UPDATE process consists of three packets (U1, U2, U3) which all traverse through the same middlebox. The middlebox can verify the Initiator's identity by verifying its signature and the CHALLENGE_RESPONSE in the U3 packet.

Service Registration and Identity Verification Embedded in to HIP Base-Exchange

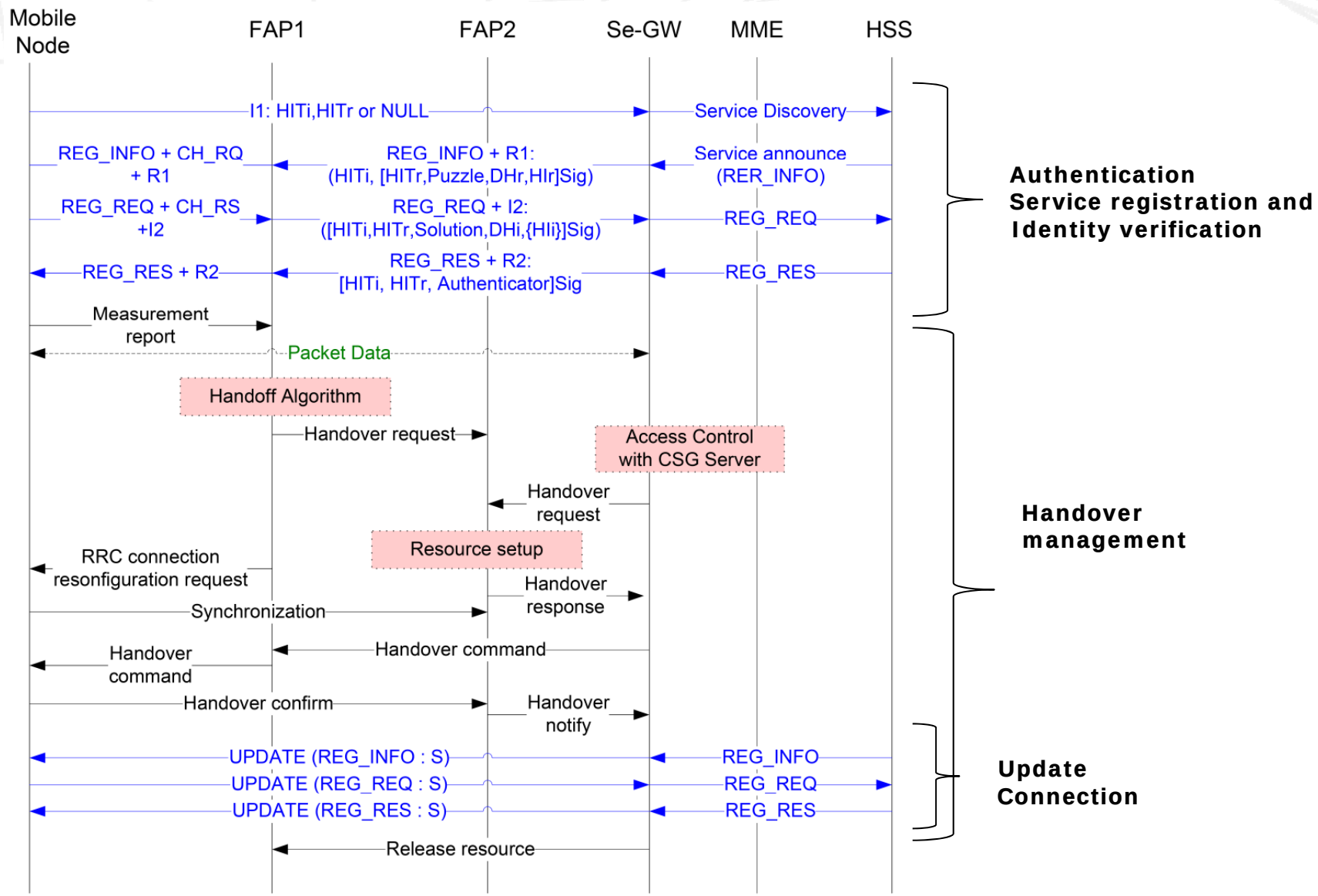


- Assuming the core network elements are trustworthy, identity verification is implemented at the Femto Access Point (FAP1).

- Meantime, mobile node is notified available services with REG_INFO parameter concatenated into R1.

- The REG_REQ parameter inform the prefered services to the registar (HSS) to which the mobile node would like to subscribe. Finally, with the response (REG_RES) message mobile node is comformed the registration.

FAP and SeGW Coordinated Handover

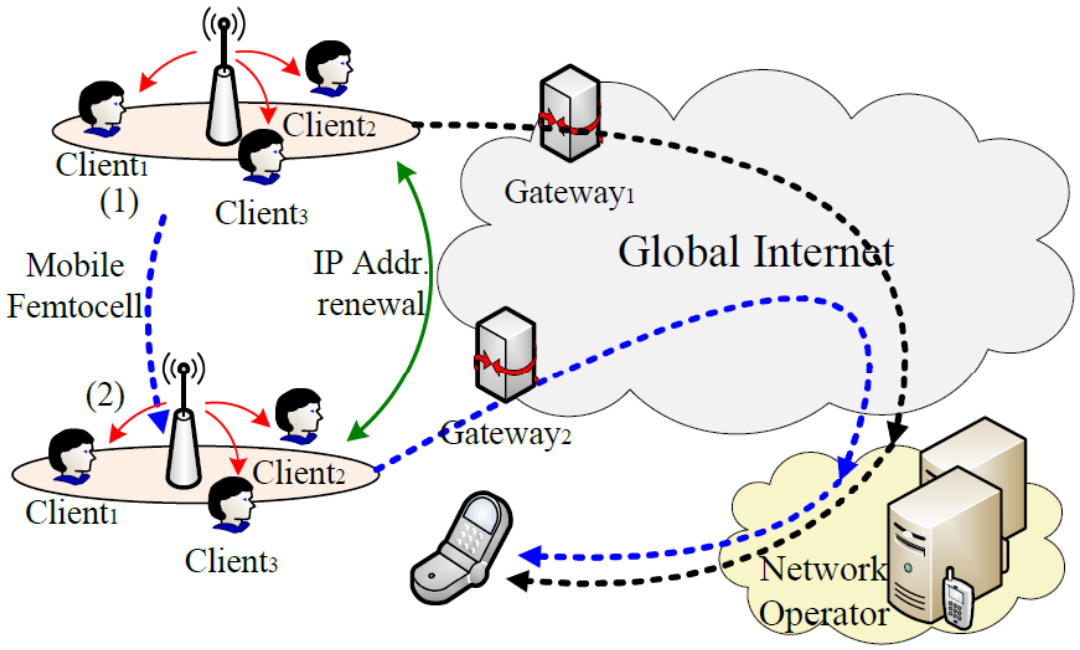


ESP IPSec message protection

Ipsec provides origin authenticity, integrity, and confidentiality for IP packets.

- ESP supports encryption-only and authentication-only configurations, but using encryption without authentication is strongly discouraged since it is insecure.
- Unlike Authentication Header (AH), ESP does not protect the IP packet header.
- However, in Tunnel Mode, where the entire original IP packet is encapsulated with a new packet header added, ESP protection is afforded to the whole inner IP packet (including the inner header) while the outer header remains unprotected.
- ESP operates directly on top of IP, using IP protocol number 50

HIP Based Network Mobility Scenario



- Sometimes, mobile nodes do not move alone, but, as a part of a small network (Ex: access point inside a Bus or a Train).

- Entering to a new domain, FAP configures a new IP address for the new association without renewing the assiciations with connected mobile nodes.

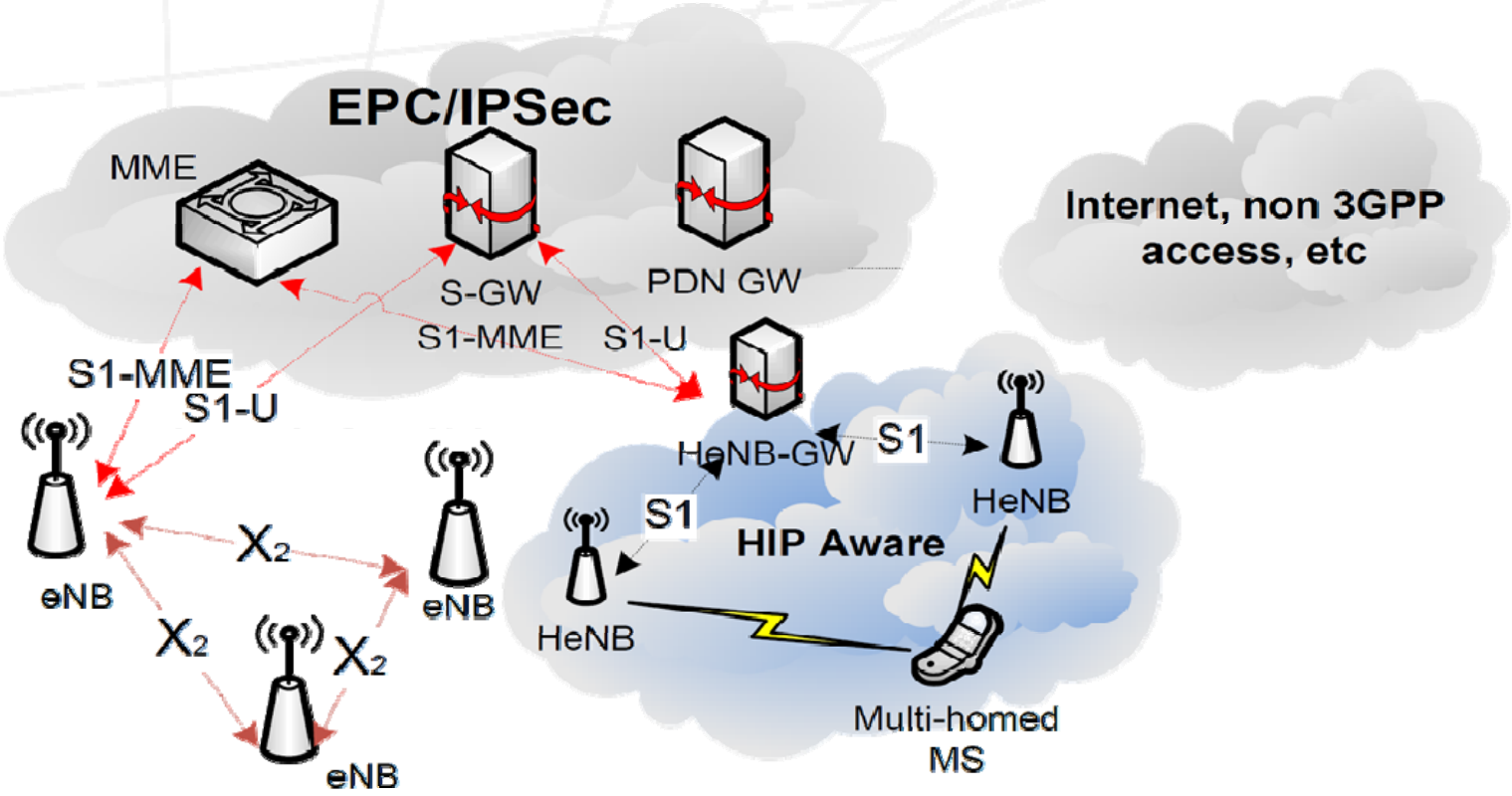
- New association is updated to the associated LRVS, SeGW and the DNS using UPDATE_PROXY message. In processing perspective, the UPDATE_PROXY exchange is handled similar to the UPDATE exchange.

- It is impractical, the mobile nodes change their IP configuration each time the FAP update the location. Thus, prefixes are rewritten in the packet headers when they pass by the FAP.

Advantages Over Proposed Scheme

- Nodes can drop the HITs and forward the packets using the SPI value in the packet header reducing the packet overhead.
- ESP provides confidentiality and integrity by encrypting data and placing them in the data field of the IP ESP packet with guaranteed data origin authentication, connectionless integrity, anti-replay service and limited traffic flow confidentiality.
- Base Exchange let the nodes to concatenate or append several parameters into the message exchange enabling several tasks to be performed simultaneously.
- Identity verification make sure the communication happens only with the authorized party.
- HIP supports for interoperability between IPv4/IPv6 while NAT traversal ensures the backward compatibility.
- Locator/Identity separation and the assignment of unique global identity simplifies complex problems related to mobility and scalability.
- HIP support for multihoming can ensure the minimum delay during handover.
- Reducing authentication to 2 RTTs whereas EAP-AKA takes 4 RTTs.

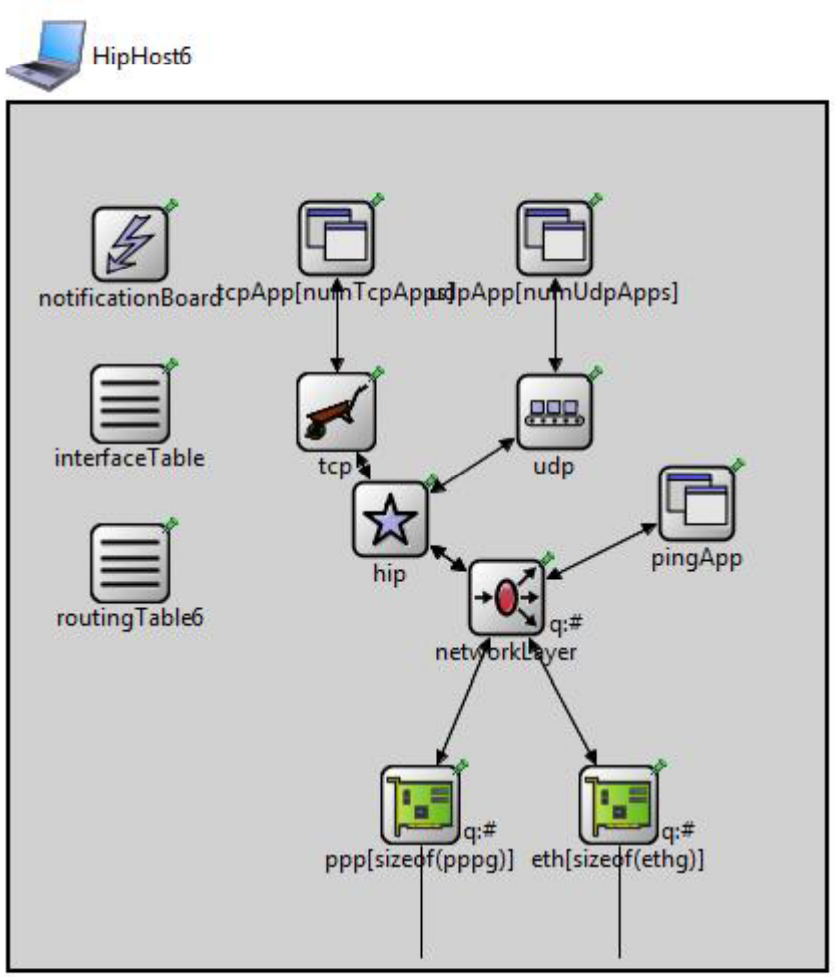
Evaluation

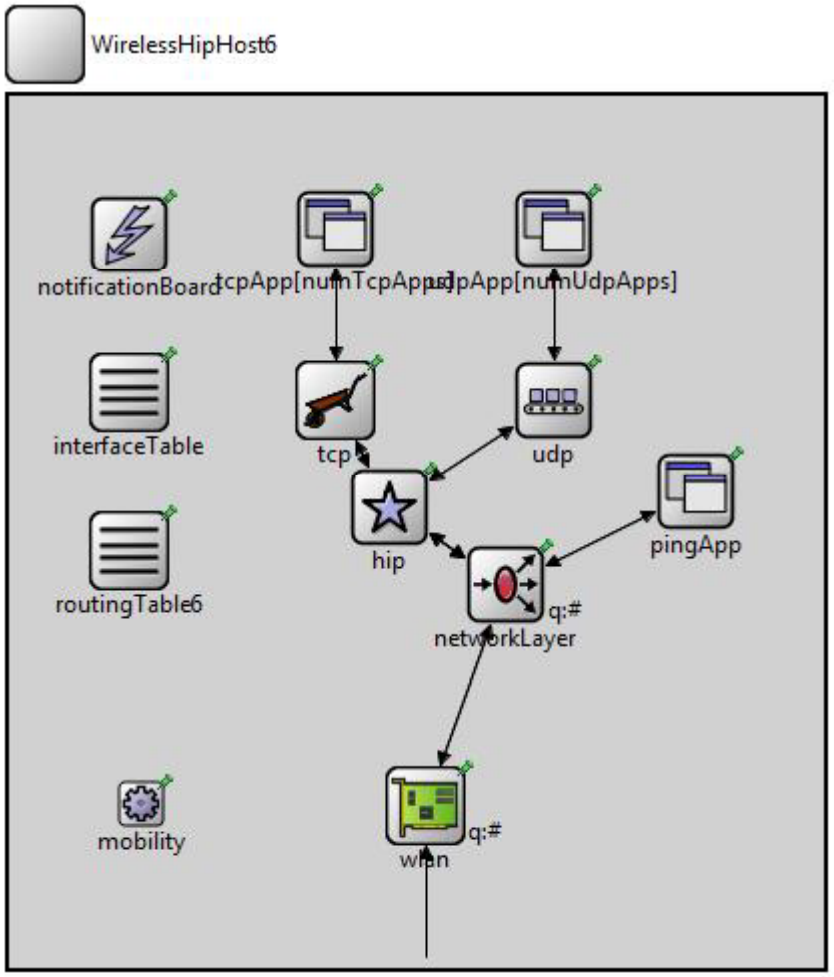


- Evaluation based on simulation (OMNet++ Simulation environment)
  - Mobile Network Scenario (measure handover delay, packet loss, authentication overhead and throughput)
  - Fixed Network Scenario (measure handover delay, packet loss, authentication overhead and throughput)

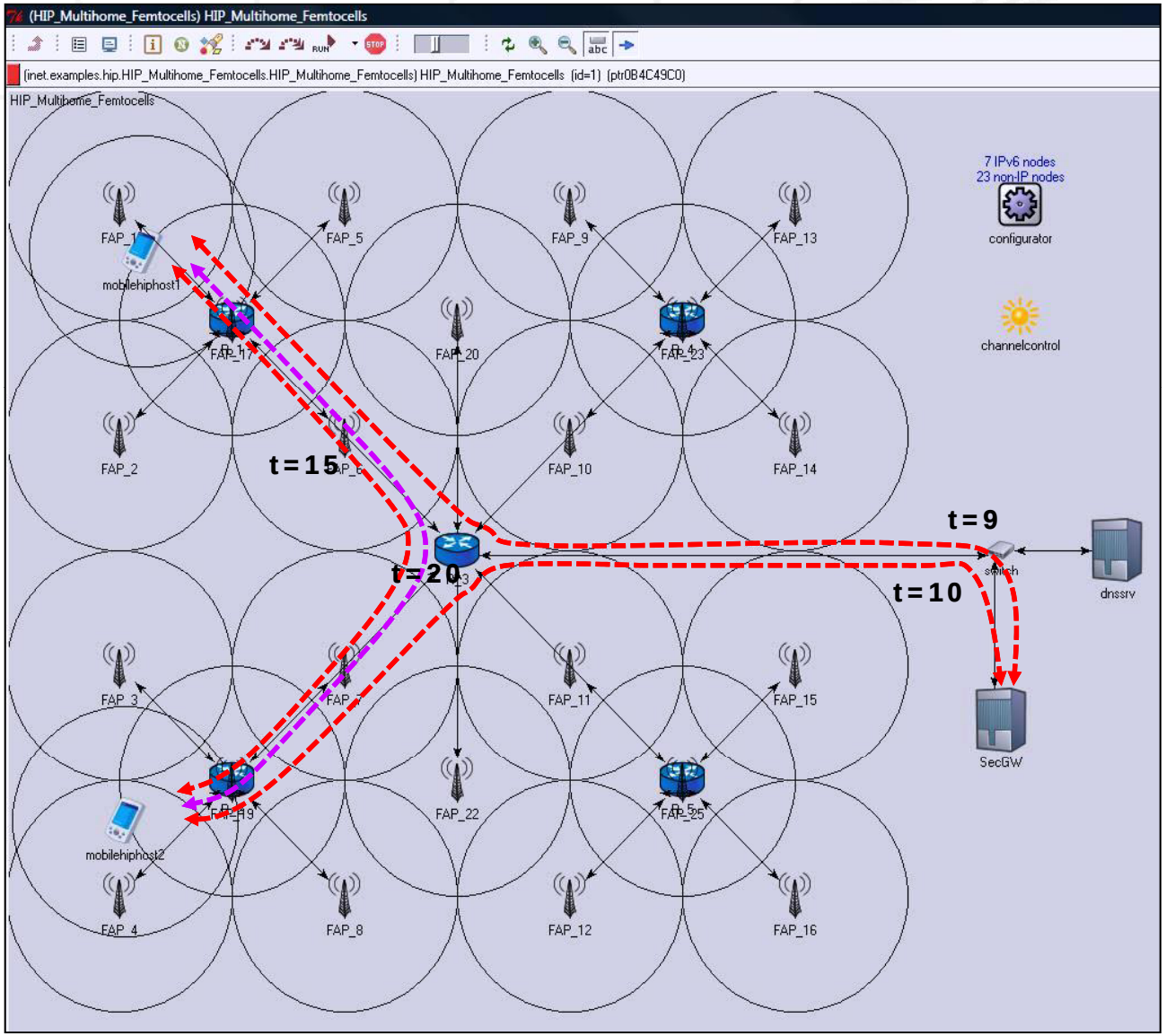
OMNet++ based HIP modules

- HipHost6 – Fixed HIP node with TCP, UDP and Ping application
- WirelessHipHost6 – Mobile HIP node with TCP, UDP and Ping application





HIP based femtocell networks.



WirelessMultihomeHipHost6: Multihomed mobile nodes maintain an array of TCP and UDP applications that allow simultanous communication with multiple FAPs.

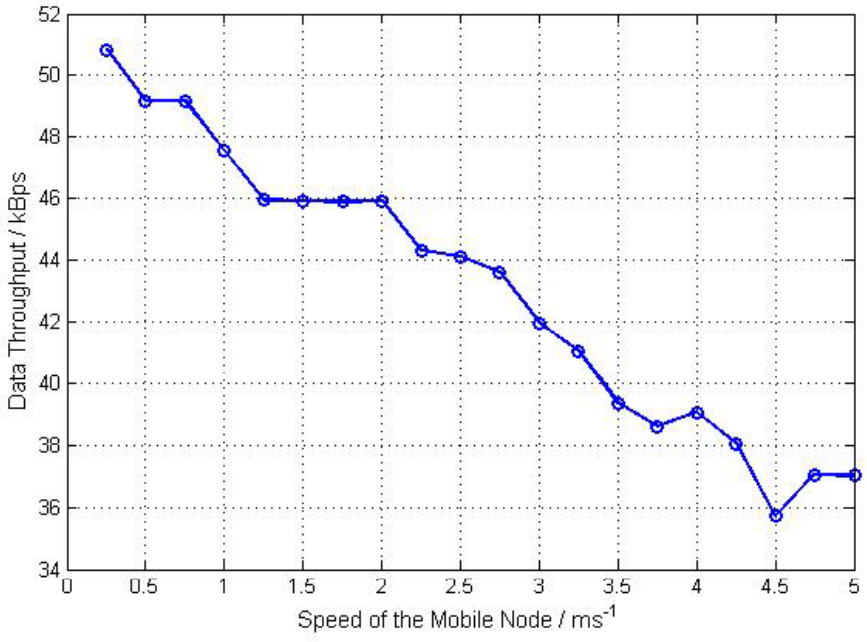
Nodes are having a defined mobility pattern - **RectangleMobility**

Time **"t"** define the time nodes start,

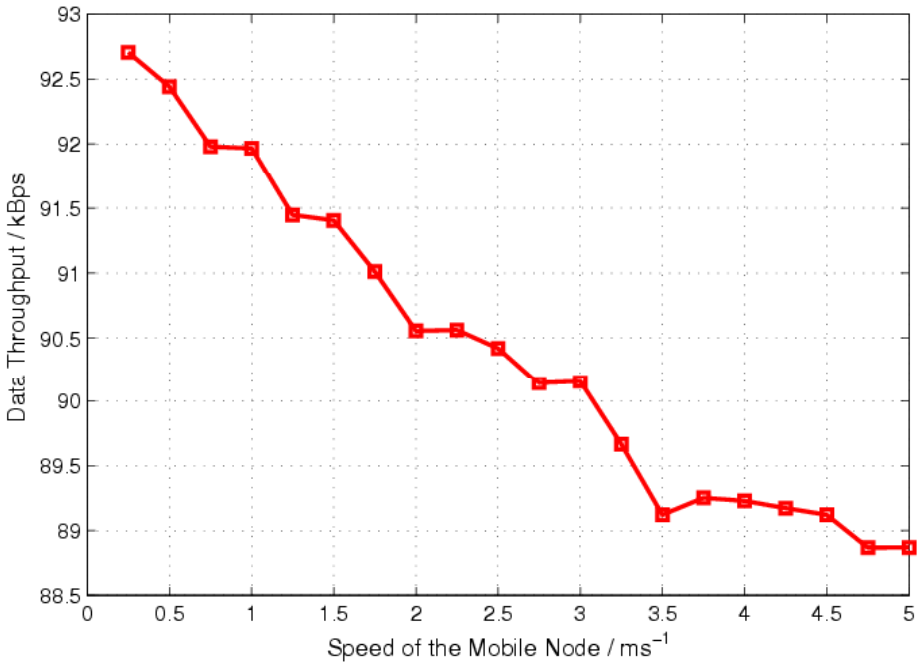
registration(**Red Line**) and
ESP transport (**Violet Line**).

At the moment ESP data throughput measurements are presented in the next slide

Throughput measurement for HIP based Femtocell



Throughput of a Wirelss HIP mobile node



Throughput of a Multihomed Wirelss HIP mobile node

Data throughput over WirelessHipHost6 and MultihomedWirelessHipHost6 under following measurements:

Ethernet data rate = 100Mbps
minIntervalBetweenRAs = 1 s
sensitivity = -82 mW
pathLoss Alpha = 2

Wireless data rate = 2 Mbps
maxIntervalBetweenRAs = 3 s
Thermal Noise = -110 dBm
SNIR Threshold = 4 dB

Expected Results Based on the Model

Handover delay:

L3 handover delay (Time duration from UPDATE1_SENT to UPDATE2_RECEIVED)

UDP packet loss:

DATA

- Using UDPBasicApp

VIDEO Traffic

- Using UDPVideoStream

TCP throughput under spoofing:

Using TCPSpoof application

Thank you!!