CWC Oulu CENTRE FOR WIRELESS COMMUNICATIONS
University of Oulu

Mobil Innovációs Központ
Mobile Innovation Centre
Budapest University of Technology and Economics

HIP in 3GPP EPC

IETF 82, HIPRG session, November 17, 2011, Taipei

Zoltán Faigl zfaigl@mik.bme.hu, BME-MIK
Jani Pellikka jpellikk@ee.oulu.fi, CWC
László Bokor bokorl@hit.bme.hu, BME-MIK

Sándor Imre imre@hit.bme.hu, BME-MIK
Andrei Gurtov gurtov@ee.oulu.fi, CWC

Outline

- The MEVICO project
- HIP roles in EPC and research questions
- HIP DEX AKA user access authorization in EPC
- HIP signaling delegation services
- HIP delegation based inter-GW mobility

Project description

MEVICO –

Mobile Networks Evolution for Individual Communications Experience

„MEVICO will research the **network aspects of the 3GPP LTE-mobile broadband network** for its evolution **in the mid-term in 2011-2014**. The goal is to contribute to the technical drive and leadership of the **EPC network (3GPP)**, and thus support the European industry to maintain and extend its strong technical and market position in the mobile networks market. The results can be used as contributions for further **development of the 3GPP standard on EPC in Rel11-Rel13**." [http://www.celtic-initiative.org/]

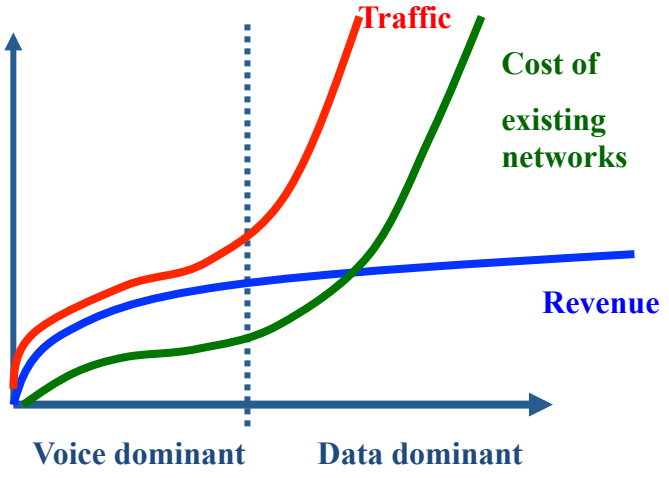
Project description

- Nokia Siemens Networks Oy
- University of Vienna
- AALTO University/ School of Science andTechnology (AALTO)
- EXFO NetHawk
- University of Oulu, Centre for Wireless Communications
- VTT Technical Research Centre Of Finland
- Alcatel-Lucent Bell Labs France
- CEA Centre
- France Telecom
- Montimage
- Artelys
- Technische Universität Berlin
- Nokia Siemens Networks GmbH
- O2 Germany
- Deutsche Telecom
- Chemnitz University of Technology
- Budapest University of Technology, Mobile Innovation Centre
- Nokia Siemens Networks Hungary
- RAD Data Communications
- Ericsson
- Ericsson Turkey
- Turk Telecom
- Avea

Scalability Problems in Future 3GPP Networks for IP-based Services

- In centralized architecture, an equipment is in charge of allocating an IP address to the terminal and managing the context
  - Traffic is anchored in this router
  - Tunnels (GTP, MIP, P-MIP) are set up between terminals and centralized routers to transport IP traffic
  - Intermediary equipments could also be used to aggregate traffic
- Scalability issue concerns the user plane of these centralized equipments when the number of connected users and the bandwidth per user increase
  - One context per connected user → mapping between customer profile, IP @, tunnel id, IP-CAN context => required memory and CPU resources
  - For each packet, IP routing is made according to user's context and not only on IP header

- Depending on the speed of the data bandwidth increase, constraints for centralized equipments are
  - CAPEX/OPEX proportional to traffic volume at busy hour
  - Operational constraints to roll out and to upgrade
- User traffic anchors in 3GPP: GGSN, PDN GW, HA
- Control traffic anchors: P-CSCF, MME



Main objectives

- Ensure user plane and control plane scalability for high bitrate data services in 3GPP
  - filter out unwanted traffic
  - offload traffic to broadband access networks
  - increase bachaul and core transport network capacity
  - better and adaptive load distribution on transport and service level (distribution of core network functions, multipath communication)
  - access technology agnostic
  - reduce signaling overhead (attachment, session establishment, handover)
  - better QoS support for applications, smart traffic management (application-level traffic identification, E2E QoS for application classes, improved resource selection and caching, multiaccess, access GW selection)
  - reduce OPEX of network management (self-organizing network functions)

Possible roles of HIP in EPC

- HIP roles :
  - user access authorization.
  - IP mobility management for any legacy application.
  - network security (e.g, from femtocells to security gateways)
  - enforcement of security policies (filters out unwanted traffic)
  - load distribution (HIP provides opportunities for smart traffic steering in the HIP peers)
  - access technology agnostic, IPv4 and IPv6 coverage
- Research questions:
  - Support resource-constrained devices / high re-authentication rate
  - Support frequent inter-GW mobility without requiring frequent HIP BEXs when HIP is used between the UE and the GW
  - Bind HIP transport protocol (e.g IPsec ESP beet mode) with EPC bearers to provide appropriate QoS for different application classes.
  - Issues with introducing HIP on 3GPP-access networks

Introducing HIP on 3GPP-access networks

- 3G AKA or 2G SIM based authentication and key agreement already provide user access authorization.
- The benefits of introducing HIP in this case are support for
  - multihoming,
  - IP-mobility,
  - IPv4 and IPv6 interoperability,
  - NAT,
  - DoS resistance
- The tradeoff between benefits and processing overhead should be considered
- In operator-based environment the cross-layer authorization concept could be used*:
  - HIP and IPsec keying material derived from L2 authentication and key agreement procedure
  - Binding of L2 and HIP level identity is needed

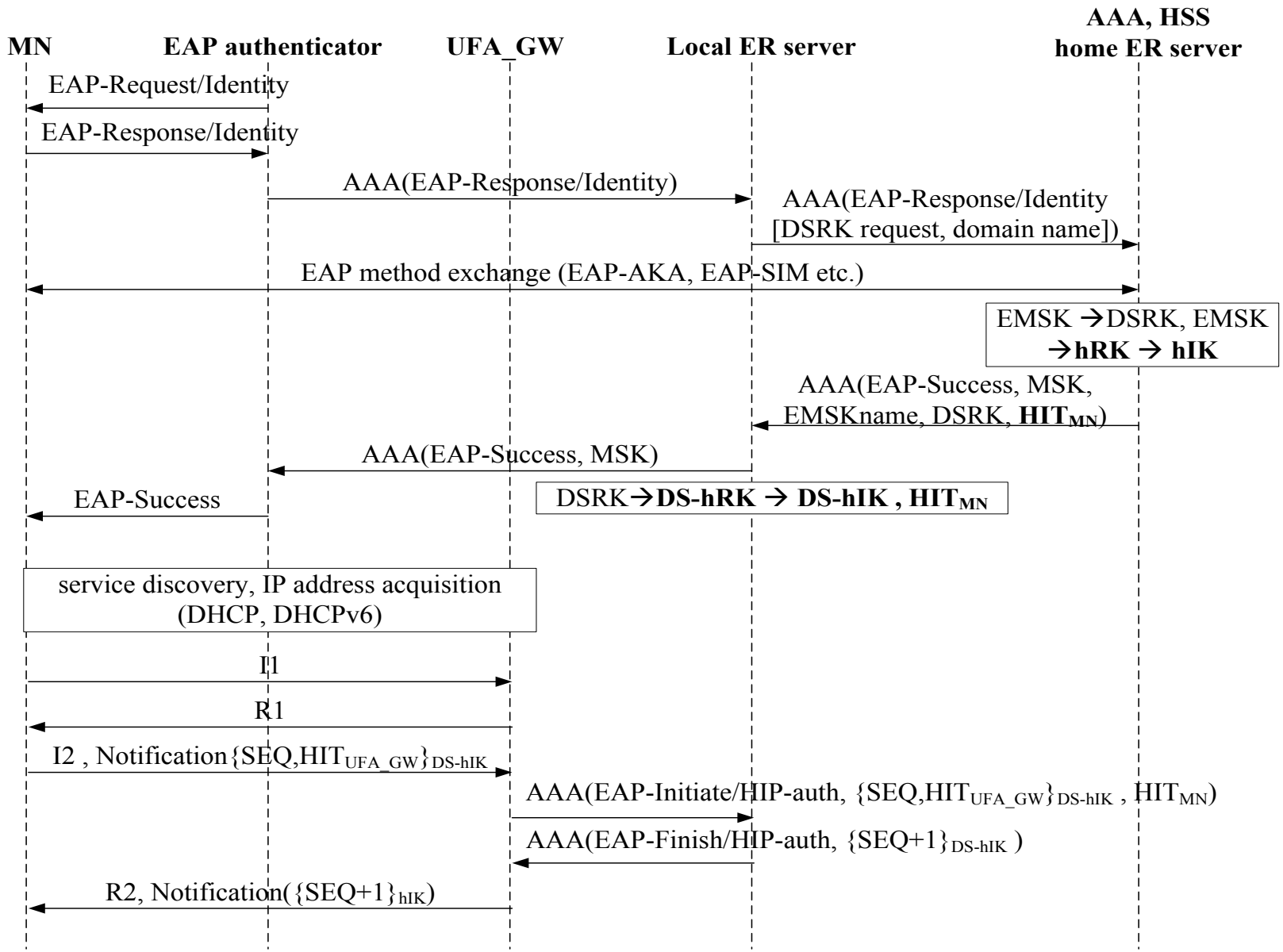
*[L. Bokor, Z. Faigl, S. Imre, A delegation-based HIP signaling scheme for the ultra flat architecture, in: Proceedings of the 2nd International Workshop on Security and Communication Networks (IWSCN'10), Karlstad, Sweden, 2010, pp. 9–16.]

L2 and HIP Level Access Authorization

- Problem:
  - HIP supports certificate-based peer authorization, or
  - The UFA_GWs should maintain ACLs for MN identities, and vice versa
- L2 access authorization (assumption):
  - EAP(-AKA) (RFC 3748, 5448)
  - ERP for fast L2 handoffs (RFC 5296, 5295)
- HIP-level:
  - Profit from the existing ERP architecture
  - We introduce a new HIP access authorization usage type for root keys
- New HIP key hierarchy: EMSK/DSRK->hRK->hIK
  - hIK mutually authenticates the MN and the local ER server on HIP level
  - Cryptographically separated from other root keys, derived keys (used for L2 EAP, ERP)
  - UFA_GW proves to be in trust relationship with the local ER server
  - Authorization state of the MN and UFA_GW is checked by the aid of the home or local ER server
- Independent fast re-authentication on L2 (rIK), and HIP level (hIK).
- Key lifetimes
  - EMSK ≥ DSRK ≥ DS-hRK = DS-hIK

[L. Bokor, Z. Faigl, S. Imre, A delegation-based HIP signaling scheme for the ultra flat architecture, in: Proceedings of the 2nd International Workshop on Security and Communication Networks (IWSCN'10), Karlstad, Sweden, 2010, pp. 9–16.]

L2 and HIP Level Access Authorization



Distribution of network functions

Main entities involved in distribution

- EPC: P-GW, S-GW, MME, PCC functions
- IMS: P-CSCF, I-CSCF

Several distribution levels are possible:

- Centralized:
  - EPC, IMS functions are mainly deployed in the national POP (Point of Presence)
- Distributed:
  - most of the core functions are deployed in regional POPs
- Flat:
  - most of the core functions are deployed in local POPs, access sites

Inter PGW mobility in EPC Release 10

- Phase 1 (attachment):
  - Authentication/registration to the network
  - Authentication/registration to IMS through the P-GW
  - UE is allocated with a new IP address
  - UE discovers P-CSCF and updates its SIP signaling route in the P-CSCF and the S-CSCF
- Phase 2 (session establishment):
  - the MN establishes a SIP dialog though P-GW towards P-CSCF.
  - establishing a context in the P-CSCF
  - informing the P-CSCF about the description of the service (SDP)
  - policy rules will be enforced from P-CSCF to the P-GW that will establish a bearer
- Phase 3 (inter-PGW handover):
  - mobility execution protocol: the UE' s new IP address will be updated in the network (DSMIP, Proxy MIP)
- Notes:
  - These phases occur each time the UE mobility induces a P-GW change, in a break before make manner.
  - It is very likely that distributed P-GWs offer the same type of a physical access (e.g. through the e-NB). UE should have broken the link with the source eNodeB and source P-GW.
  - As phases 1, 2, 3 take time, the handover performance will be impacted.

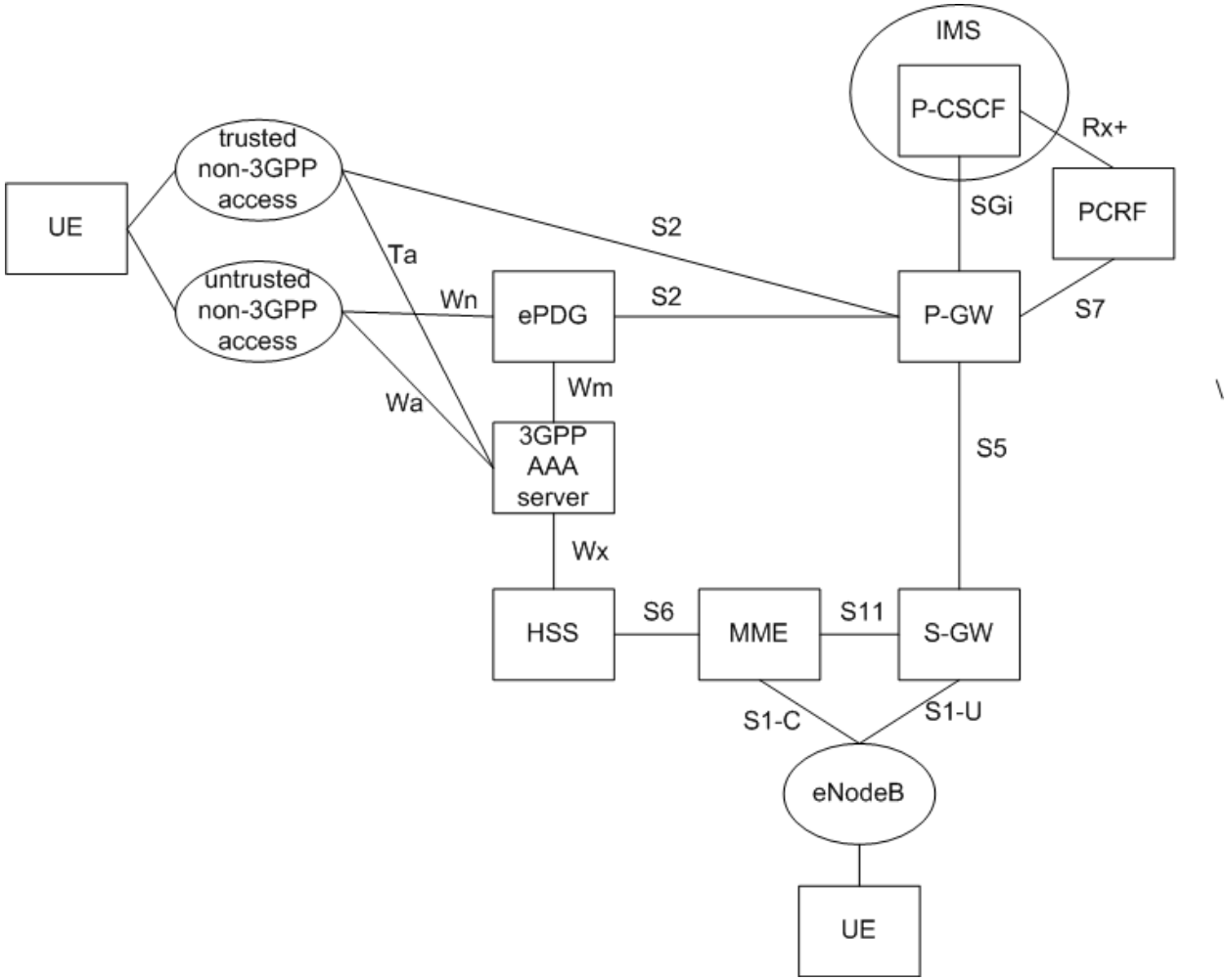
Ideas

- Simplify user access authorization
  - In phase 1 : two user access authorizations (access network and IMS)

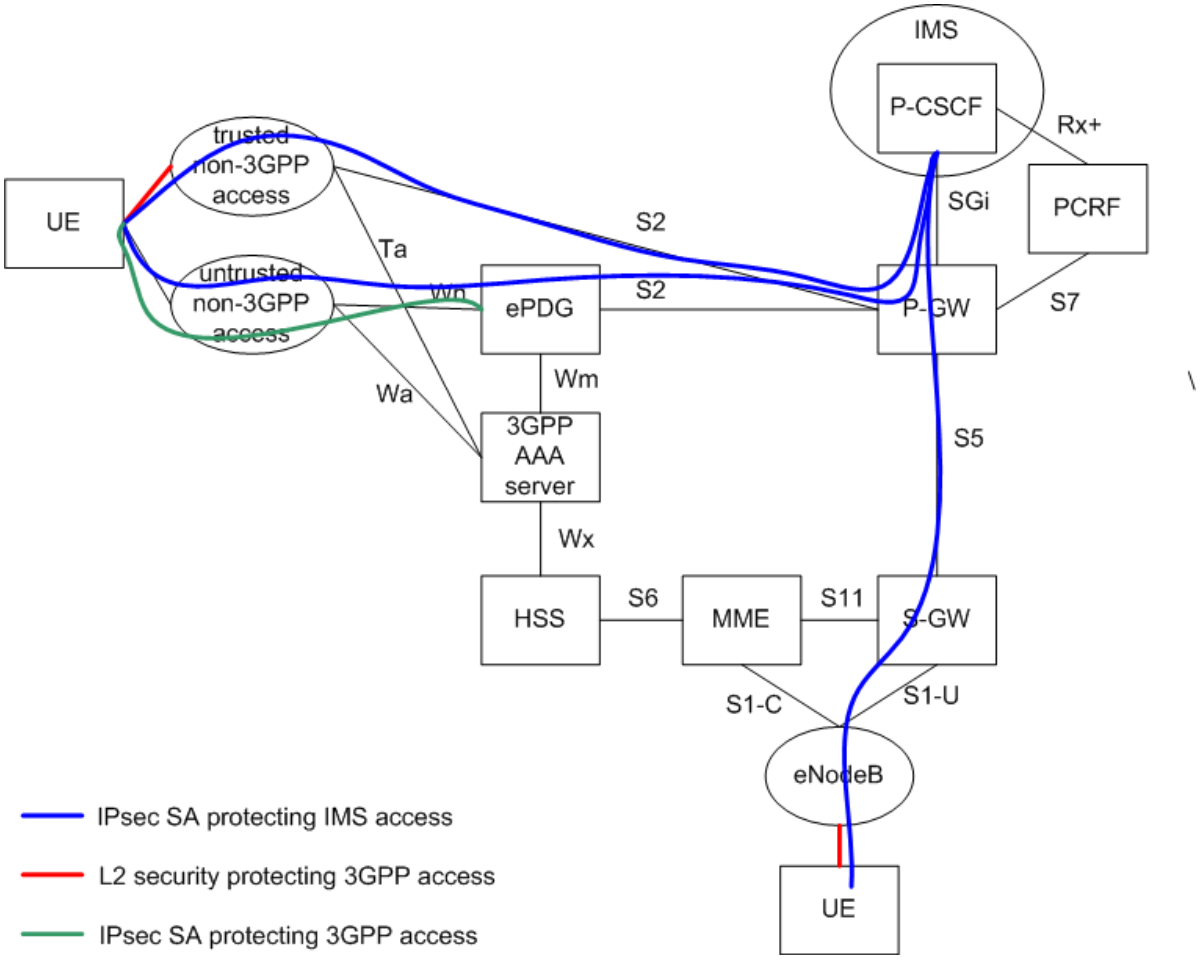
	authenticator	authentication server
LTE/EPC access	eNodeB (L2 security association endpoint)	MME (+HSS)
Trusted non-3GPP access	access point (L2 SA endpoint)	3GPP AAA (+HSS)
Untrusted non-3GPP access	ePDG (IPsec endpoint)	3GPP AAA (+HSS)
IMS access	P-CSCF (IPsec endpoint)	S-CSCF (+HSS)

  - Reduce to one HIP based user access authorization
    - What to do if L2 security is also important? See slide on cross-layer authorization

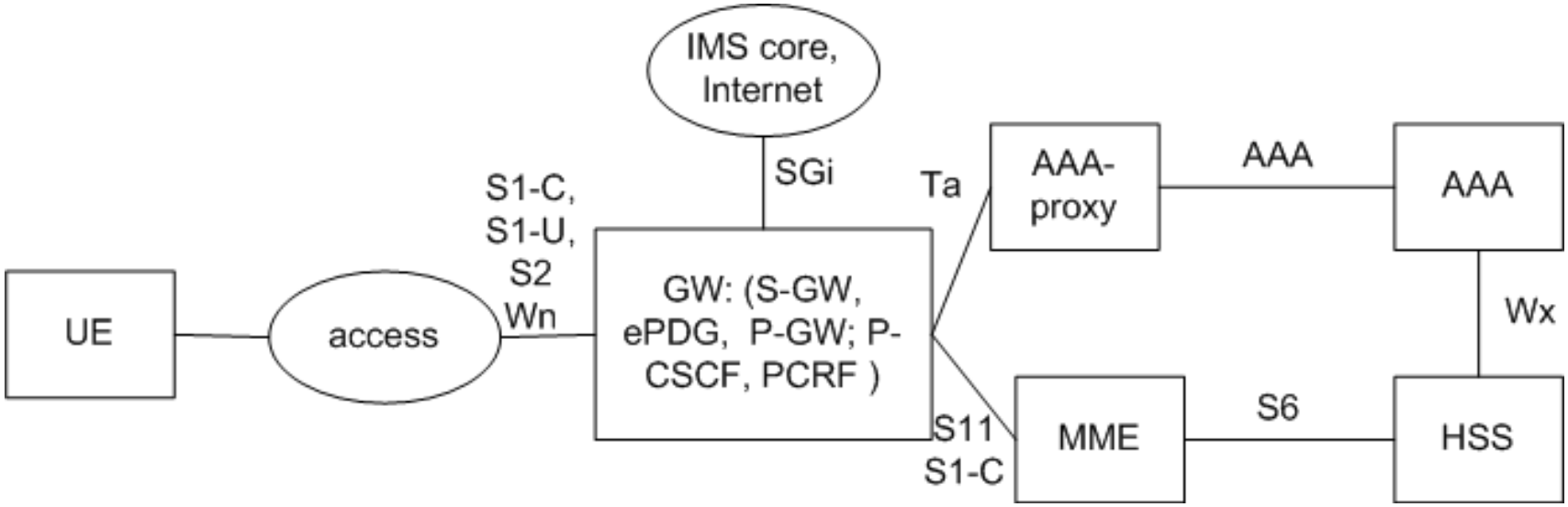
EPC Release 10



EPC Release 10



Distributed EPC (work in progress)



HIP-based user authentication in EPC

Jani Pelikka, CWC
Zoltán Faigl, László Bokor, BME-MIK

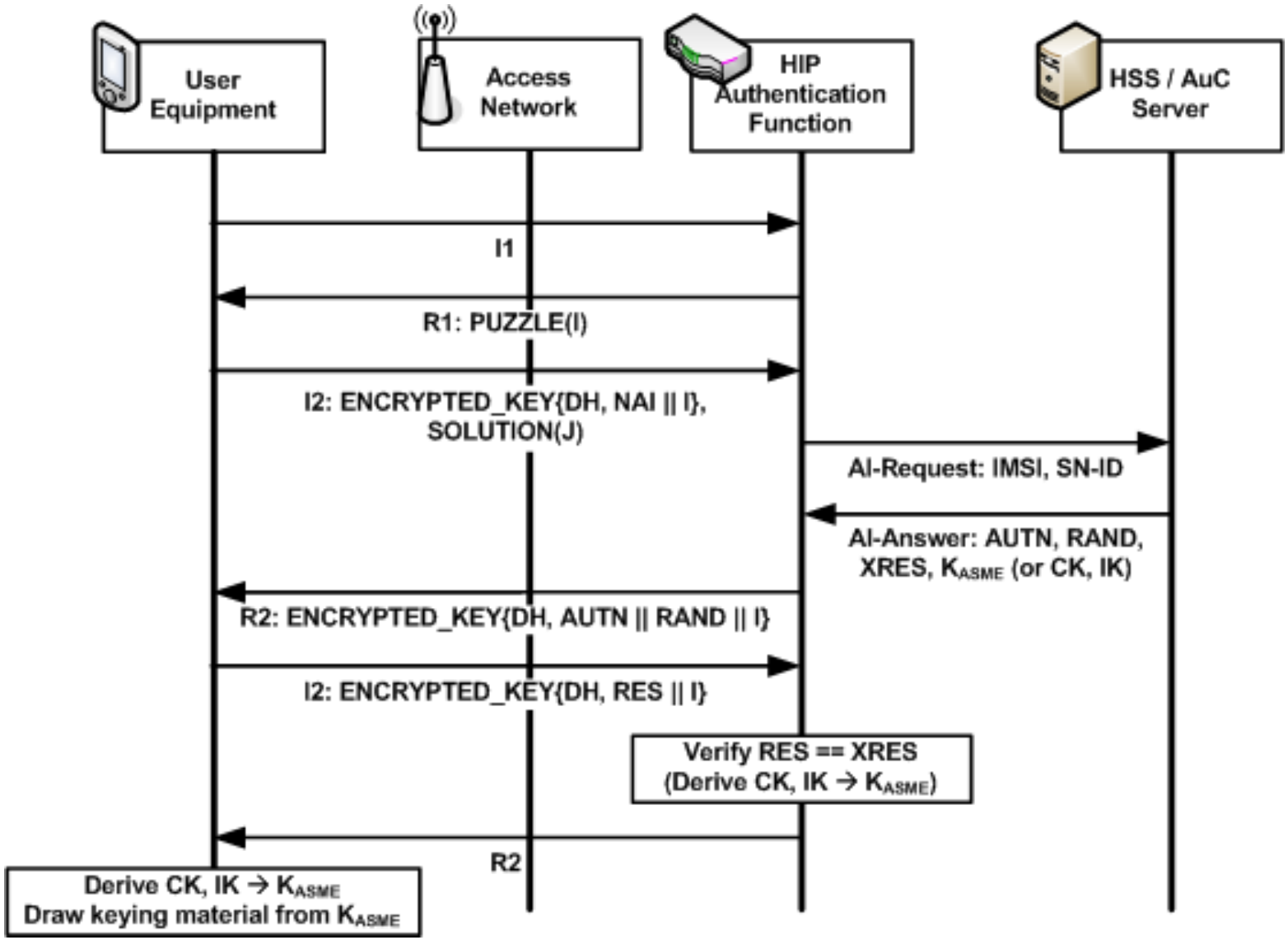
HIP-Based Re-Authentication

- HIP Diet Exchange with AKA authentication
- HIP DEX AKA provides similar functionality as the Internet Key Exchange protocol v2 (IKEv2) with EAP-AKA: it could control user access authentication and authorization of USIM based UEs in non-managed non-3GPP access networks.
- Both services provide mutual authentication and establish an IPsec security association pair to protect the path between the UE and the ePDG in the network layer.
- HIP DEX AKA is intended as a uniform L3 authentication service on the top of disparate access networks.

HIP-Based Re-Authentication

- Challenges with inter-PDN-GW and inter-ePDG mobility
  - Re-authentication in handovers involves multiple protocols (IKEv2 and EAP) of different layers (L3 and L2, respectfully) currently
  - The above mentioned protocols induce extensive amount of signaling
  - Distributed GWs mean more handovers and re-authentications; heavy frequent cryptographic operations in re-authentications can deplete UE's battery quickly
- Replace 3GPP L2/L3 authentication with HIP Diet Exchange (DEX)
  - Utilize the HIP protocol combined with 3GPP AKA method, as well as the corresponding keys in handovers; similar to Fast Initial Authentication (FIA)
  - Utilize a lightweight L3 HIP authentication scheme, HIP Diet Exchange
  - Removal of L2 authentication protocols (i.e. loose the EAP protocol)
  - Reduction of elements in the authentication (i.e. an AAA/EAP server)
- Anticipated benefits of the proposal include the following:
  - Faster handovers, as re-authentication process is improved due to disinvolvement of L2 protocols and elements other than HIP and a backend authenticator (e.g. HSS) and GW, respectively
  - Lower computing and signaling overhead on and between GW and UE

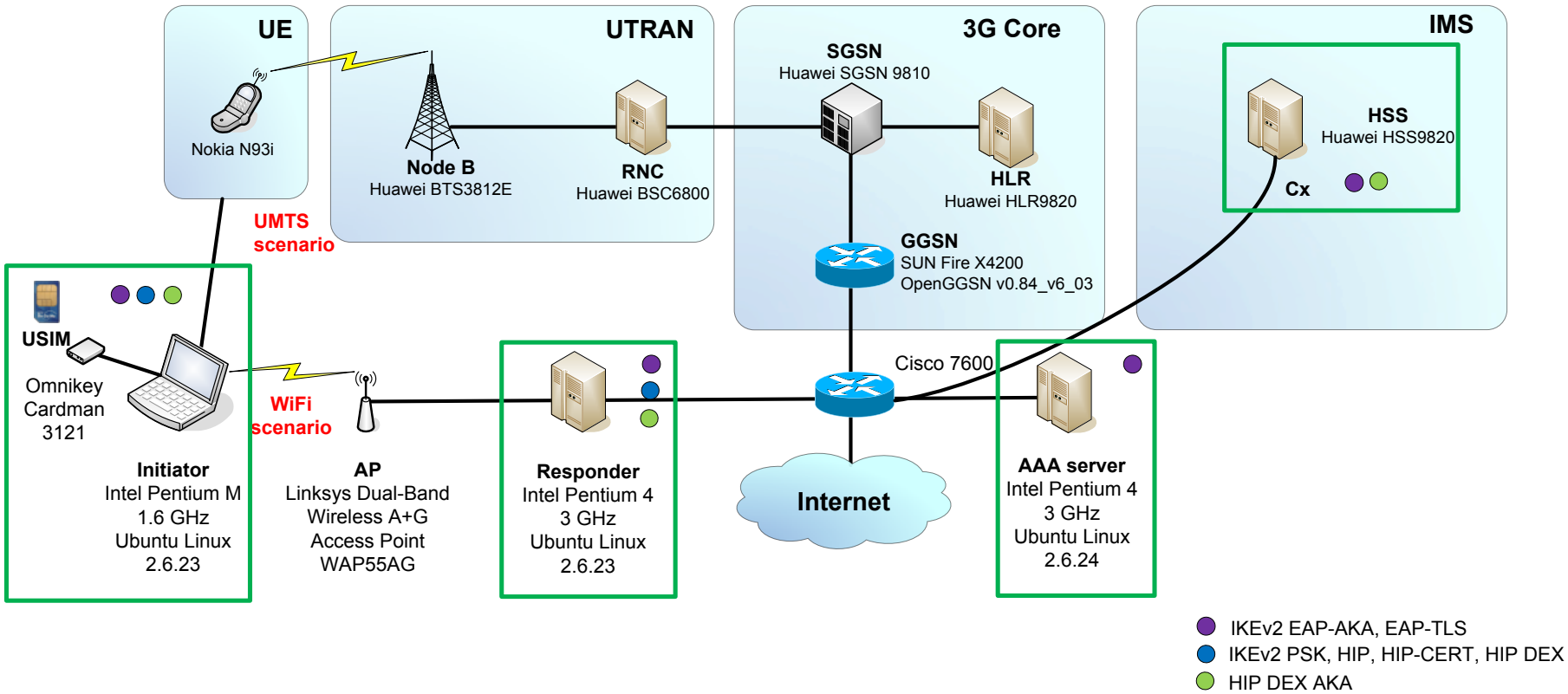
HIP-Based Re-Authentication



HIP-Based Re-Authentication

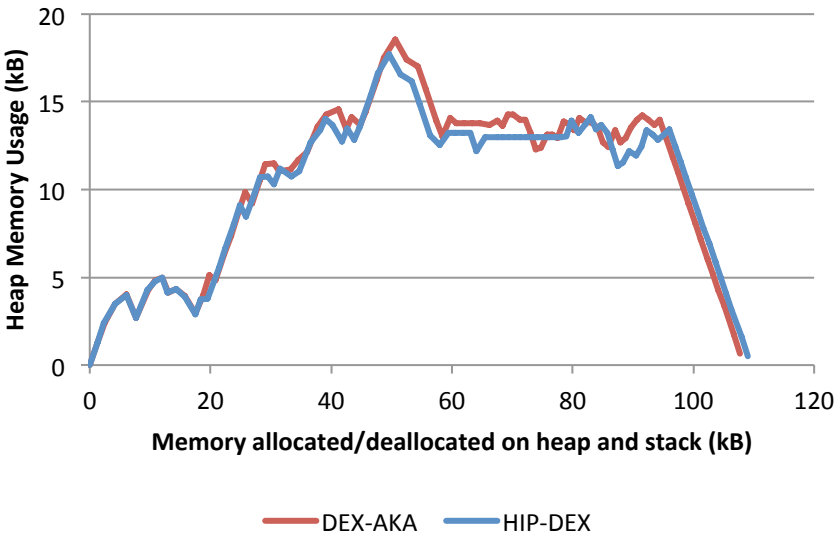
- Real-life implementation and testbed validation
- Validation status
  - HIP-DEX base protocol implemented in the C++ language for GNU/Linux
  - Two versions of HIP-AKA implemented in the C++ language for GNU/Linux
    - One is running in a testbed at CWC premises
    - And the other in a testbed at BME-MIK premises
- Validations will use both BME-MIK's testbed and CWC's testbed
  - In the beginning, validations are carried out using only the BME-MIK's more extensive testbed (Wi-Fi and UTRAN accesses supported); though some measurements and development work is done using the CWC's testbed
  - Testbed configurations emulate the flat (long-term) MEVICO LTE architecture
  - Later, bootstrapping and Femtocell (possibly DEX used on L2) studies will be performed in CWC's testbed
  - We also intend to run our protocol in resource constraint mobile devices such as Android smart phones

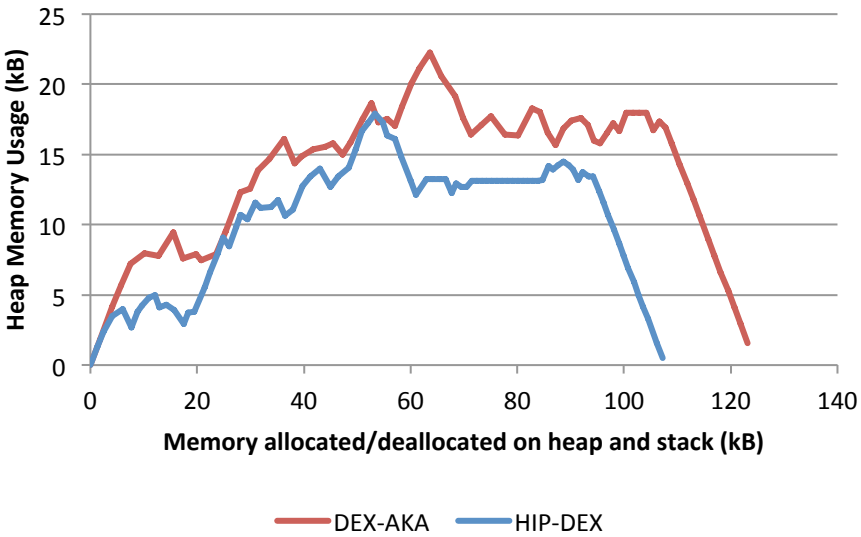
Validation environment (BME-MIK)



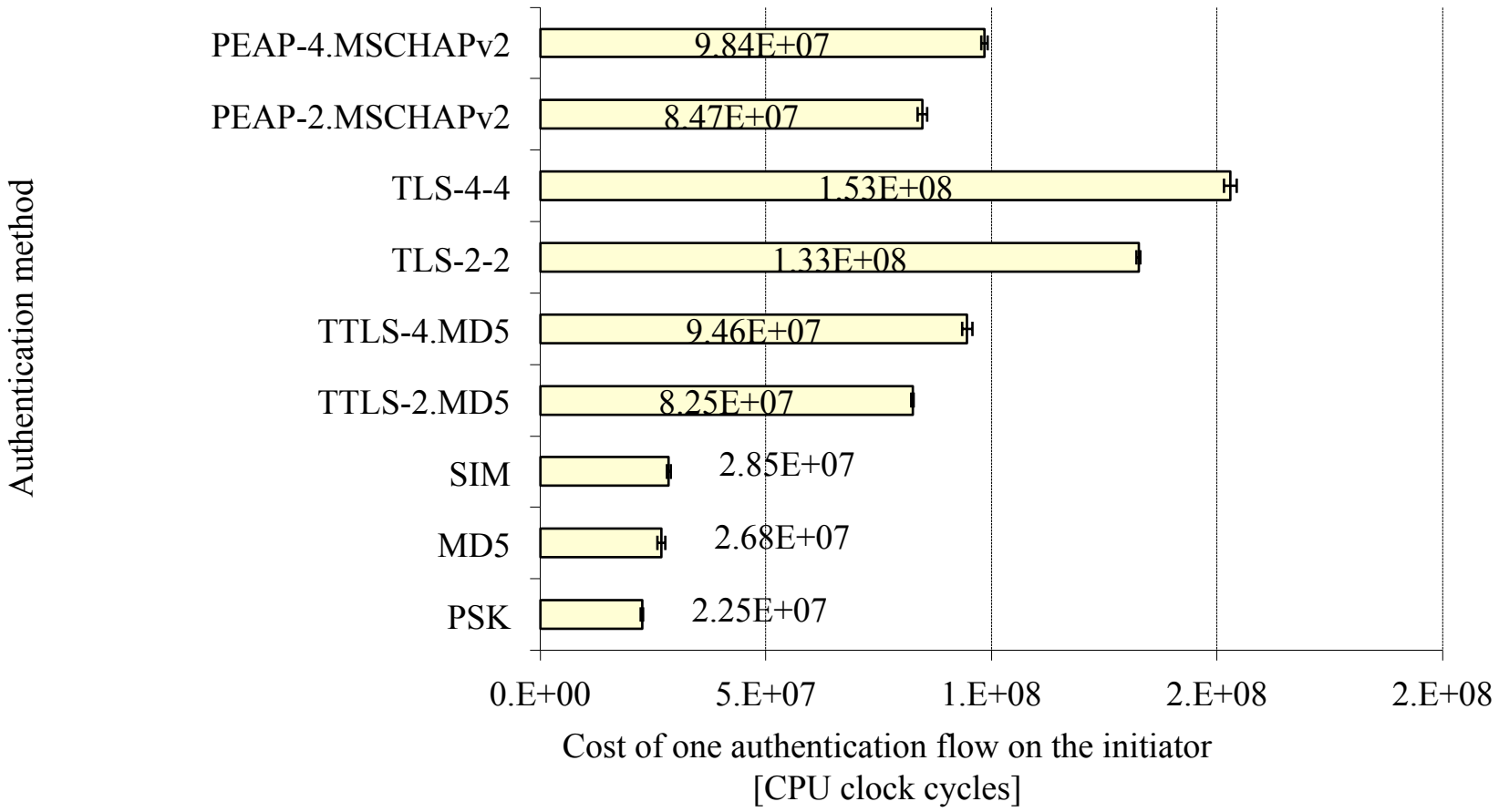
Preliminary results for CPU and memory measurements

Method	CPU load (UE) [clock cycles * 10^6]
HIP BEX (infraHIP)	64.2
HIP DEX AKA (CWC)	13.0
HIP DEX (CWC)	6.4
IKEv2 EAP-SIM (ikev2 project)	28.5





Results for IKEv2 (for comparison)



[Z. Faigl, S. Lindskog, and A. Brunstrom, "Performance evaluation of IKEv2 authentication methods in next generation wireless networks" Security and Communication Networks, 3: 83–98, 2010, doi: 10.1002/sec.114]

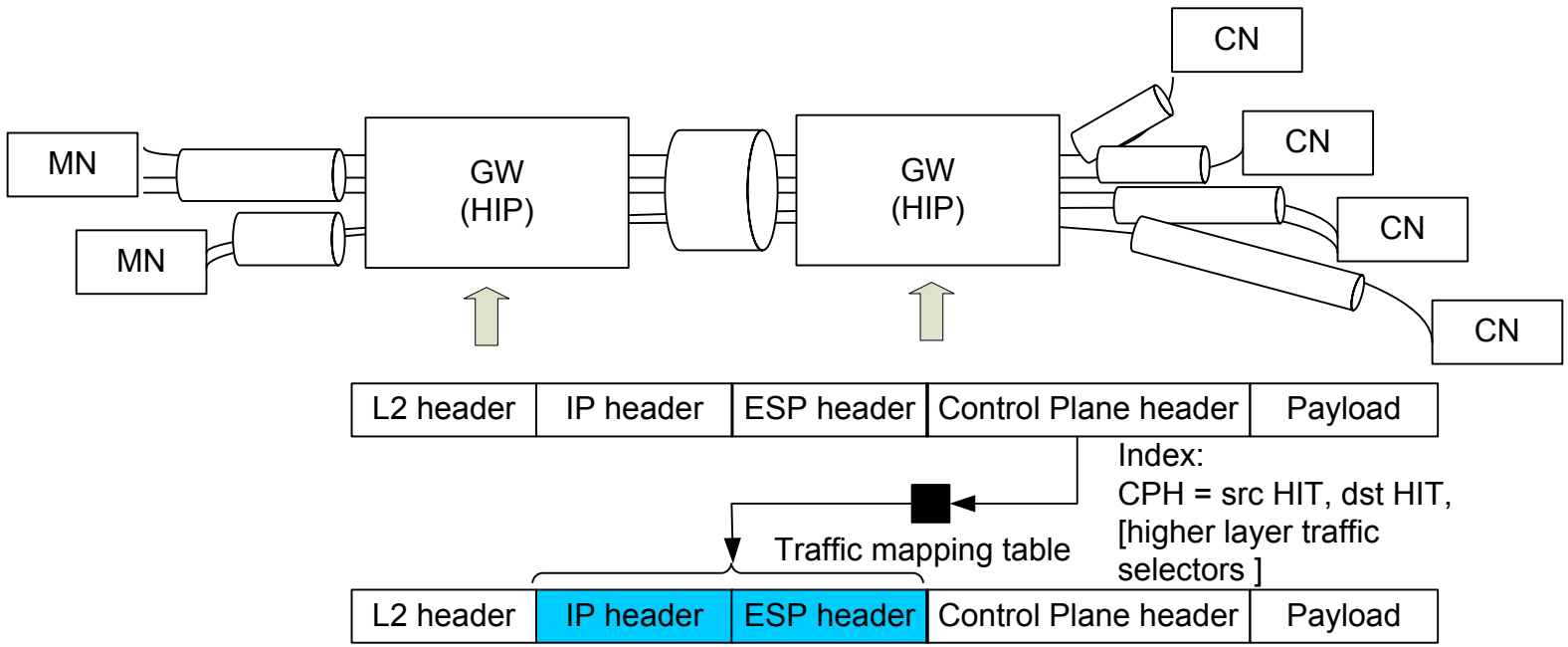
HIP signaling delegation services providing inter-GW mobility

Zoltán Faigl, László Bokor, BME-MIK

Delegation-based HIP mobility service in distributed/flat architectures

- Problem statement
  - Inter-GW mobility requires new mechanisms to avoid unnecessary HIP BEX
  - Reduce signaling overhead on the air interface
- General solution
  - Introduce signaling delegation service for HIP
    - Enables HIP host association and IPsec SA establishment by a delegate. Secure security context transfer is needed from delegate to delegator (CXTP over IPsec)
    - Enables HIP BEX, HIP updates by a delegate
  - Delegation introduces a new hop-by-hop traffic forwarding scheme providing flow mapping in the GWs based on fivetuples
    - This reduces significantly the number of E2E HIP host associations and IPsec SAs in the network,
    - Better for traffic management, legal interception
- Using these services, inter-GW mobility can be performed without complete reassociation (HIP BEX)

Traffic forwarding



Motivations for „hop-by-hop" traffic forwarding

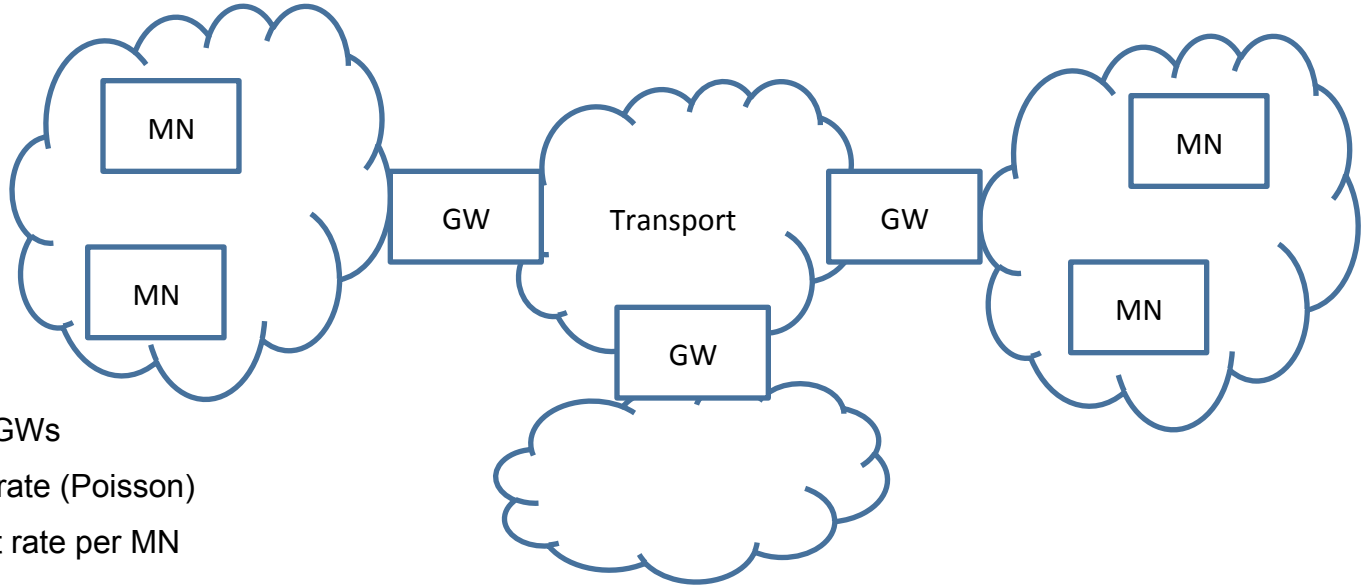
- E2E HIP concept does not fit 3GPP because several functions in the GW require information above the network layer.
  - Application classification, user clustering
  - Application class based QoS enforcement
  - Deep packet inspection for network monitoring and network management
  - Legal interception
  - etc.
- E2E concept requires much more HIP BEXs and updates in the network.
- This separation enables the introduction independent addressing and routing mechanisms in the access networks and the core network

Performance evaluation of Hop-by-hop vs. E2E HIP

Zoltán Faigl, BME-MIK

Macroscopic analysis

- Objective: average number of HIP BEXs per unit time due to attacment and session establishment



M – number of GWs

α – attachment rate (Poisson)

ω – detachment rate per MN

λ – session establishment rate per MN

μ - session ending rate per MN

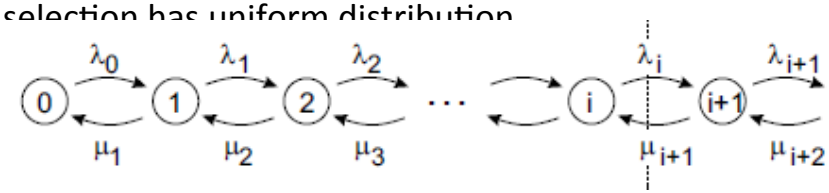
T – unused association lifetime

γ – average mobility rate per MN

Average number of HIP BEXs per unit time

- Attachment – detachment is modeled with a birth-death process
  - Poisson arrival α, exponential service times $n*\omega$, $n=0..\infty$ is the state number, i.e., number of attached users
  - Expected number of attached users is α/ω
- Session establishment and ending rate
  - Birth-death process
  - E2E case : states represent the number of existing application sessions between a given pair of MN
  - UFA case : states represent sessions between a given pair of GW
  - Death rate: $k*\mu$, session ending rate, k is number of sessions between the two entities
  - Birth rate: arrival rate of sessions,
    - Requires assumptions on the
      - topology (in UFA case),
      - call desination distributions (both cases)
    - Simple assumptions for macroscopic view:
      - users are uniformly distributed among GWs, and
      - destination selection has uniform distribution

Birth-death process:



$\lambda_i = \lambda$

$\mu_i = i\mu$

Average number of HIP BEXs per unit time

- unused HIP association is closed after a constant time (T)

- number of HIP BEXs per unit time between a pair =
  probability of zero sessions (state 0) between a pair ·
  probability that sojourn time in state 0 is greater than T ·
  transition rate from state 0 to 1

- cumulated number of HIP BEXs per unit time
  - E2E: (%·number of MN pairs
  - UFA: (%·number of GW pairs) + α

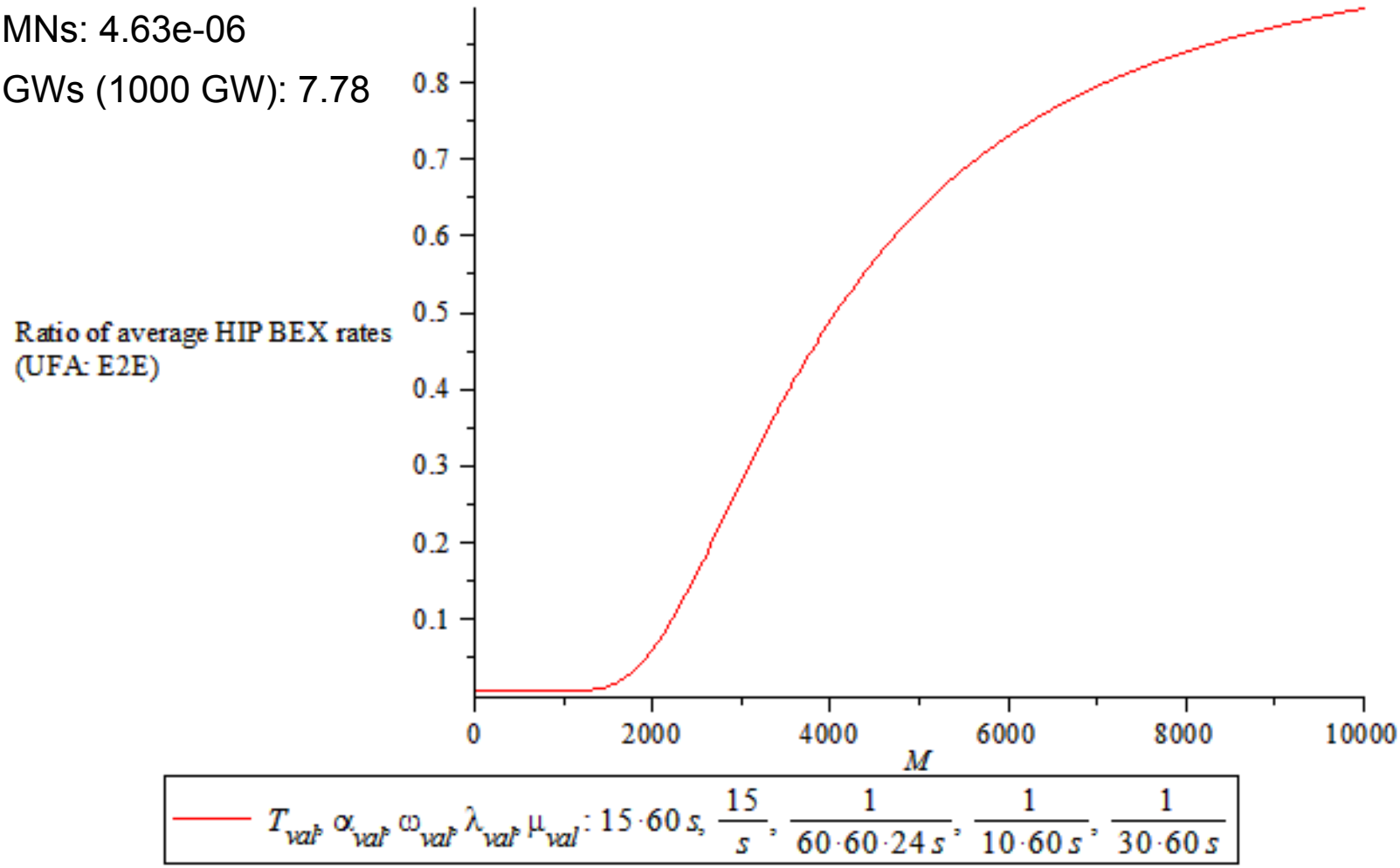
- Ratio of the average number of HIP BEXs per unit time is given in the next slides (UFA compared to E2E)

# of attached users : 1.3M

avg. # of sessions:

bw MNs: 4.63e-06

bw GWs (1000 GW): 7.78



# of attached users : 222

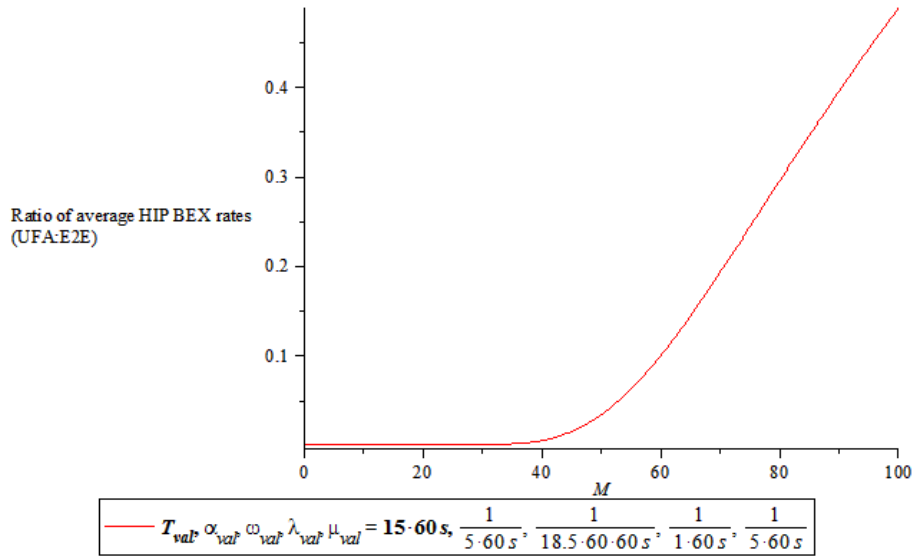
avg. # of sessions:

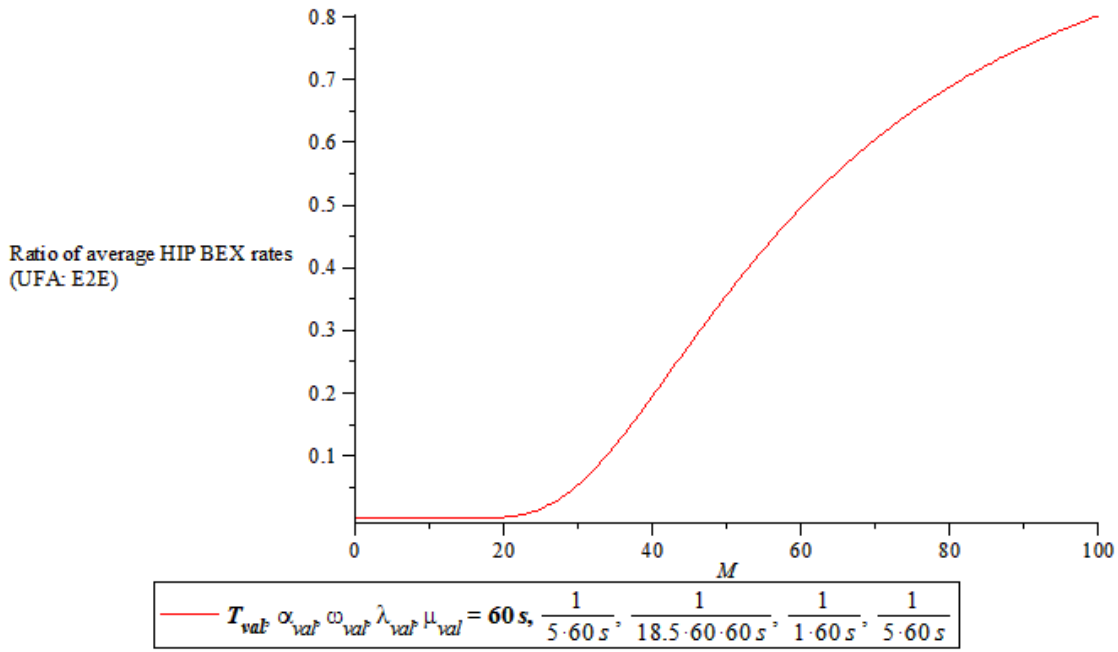
bw. MNs: 4.52e-02

bw- GWs (10 GW): 22.2

unused association lifetime:

(1) 15min, (2) 1 min





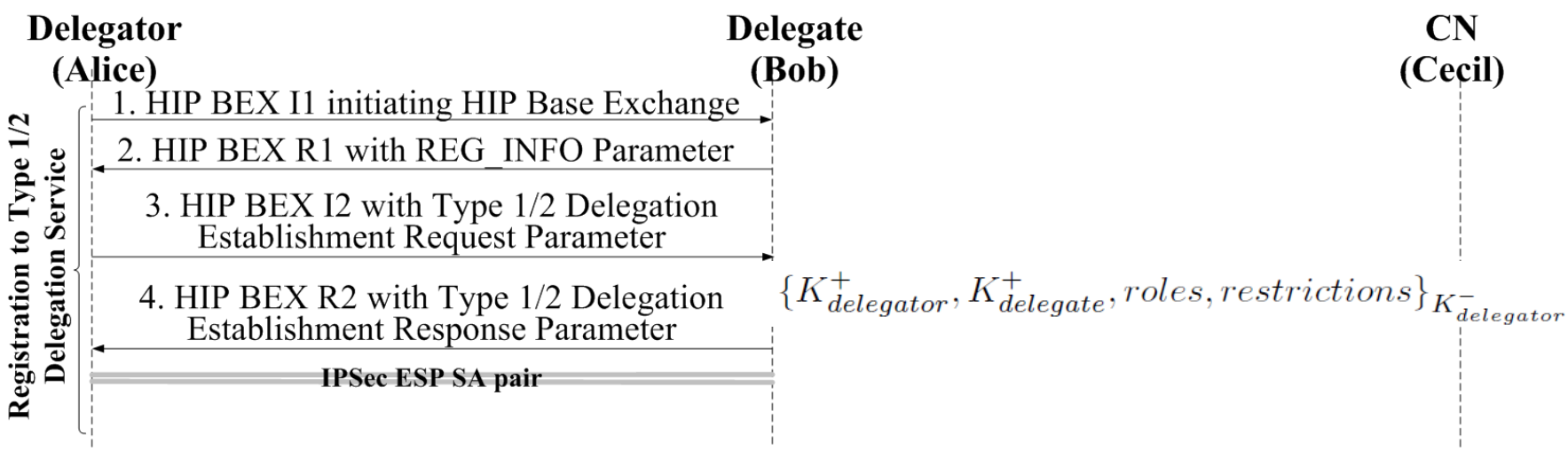
HIP delegation services

Zoltán Faigl, László Bokor, BME-MIK

[L. Bokor, Z. Faigl, S. Imre, A delegation-based HIP signaling scheme for the ultra flat architecture, in: Proceedings of the 2nd International Workshop on Security and Communication Networks (IWSCN'10), Karlstad, Sweden, 2010, pp. 9–16.]

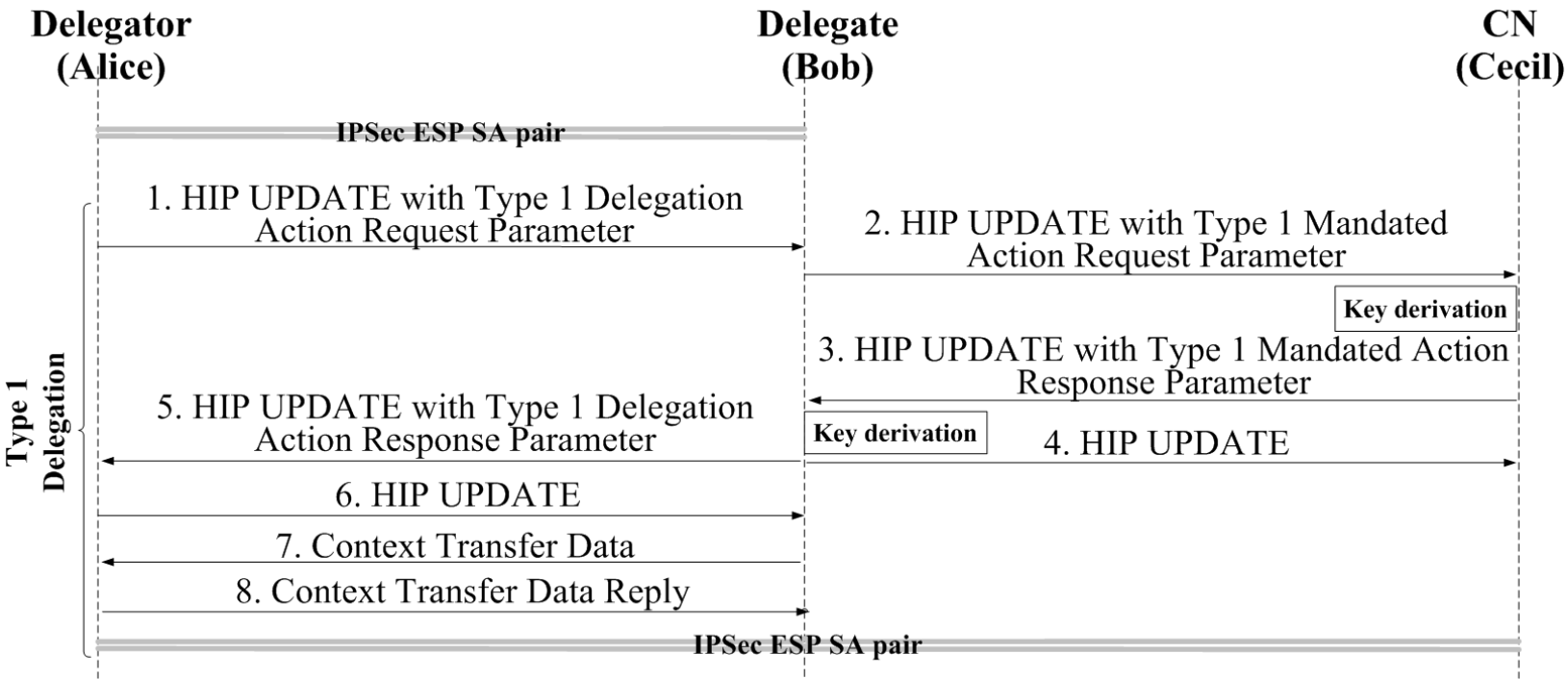
Registration to HIP delegation services

- The Delegate gets an Authorization Certificate (or Token) from the Delegator that will assure the CN that the Delegate can proceed in Delegator's name

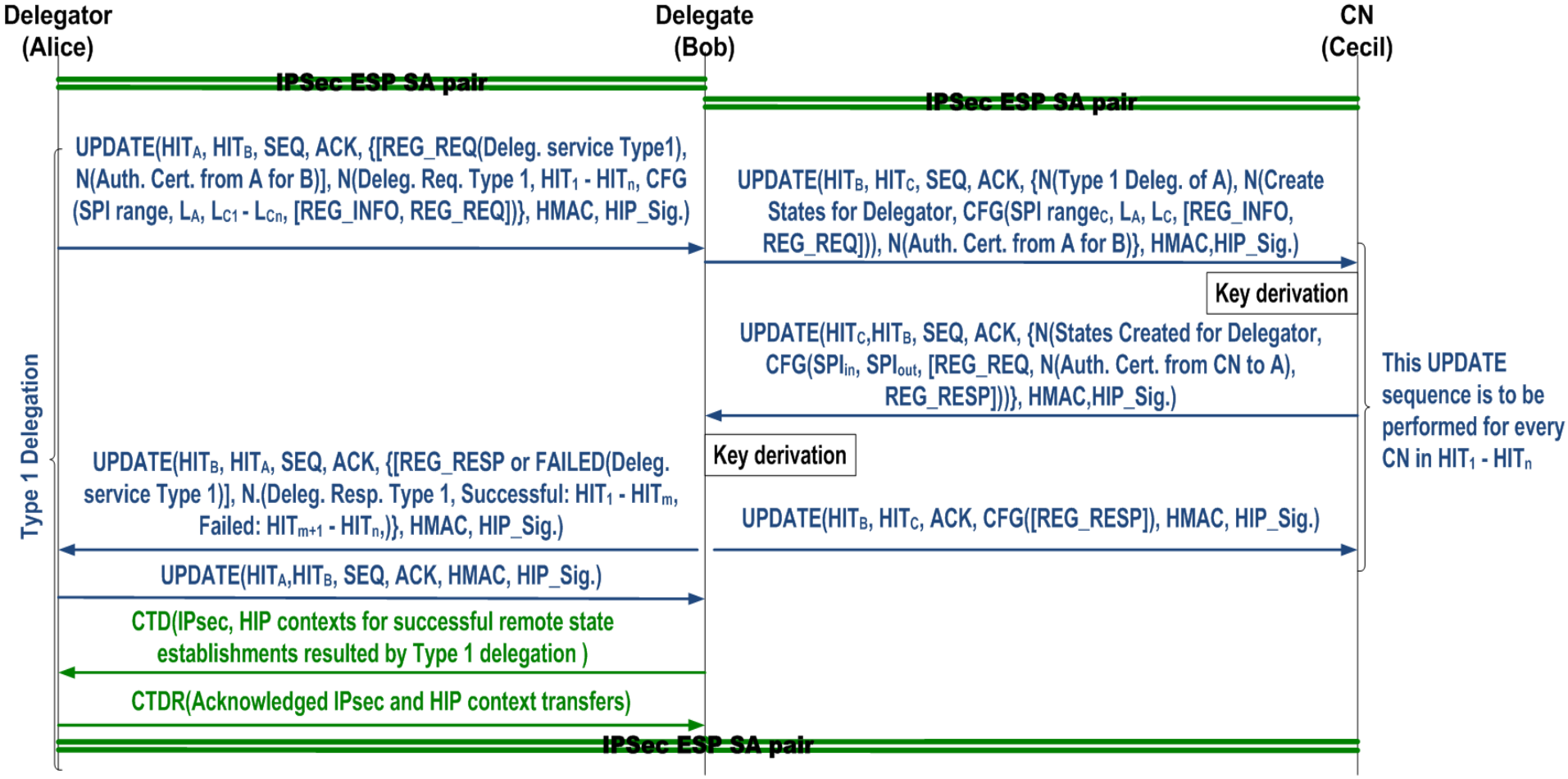


Type 1 Delegation Service and CXTP

- Type 1 Delegation Service requires
  - pre-existing IPsec SA between the Delegator and the Delegate, and
  - HIP host association between the Delegate and the CN.
- Delegate
  - establishes new HIP and IPsec SA with the CN, in the name of the Delegator. Instead of HIP BEX, simple key derivation is used.
  - sends to the Delegate the new HIP and IPsec SA contexts using CXTP protocol protected with IPsec

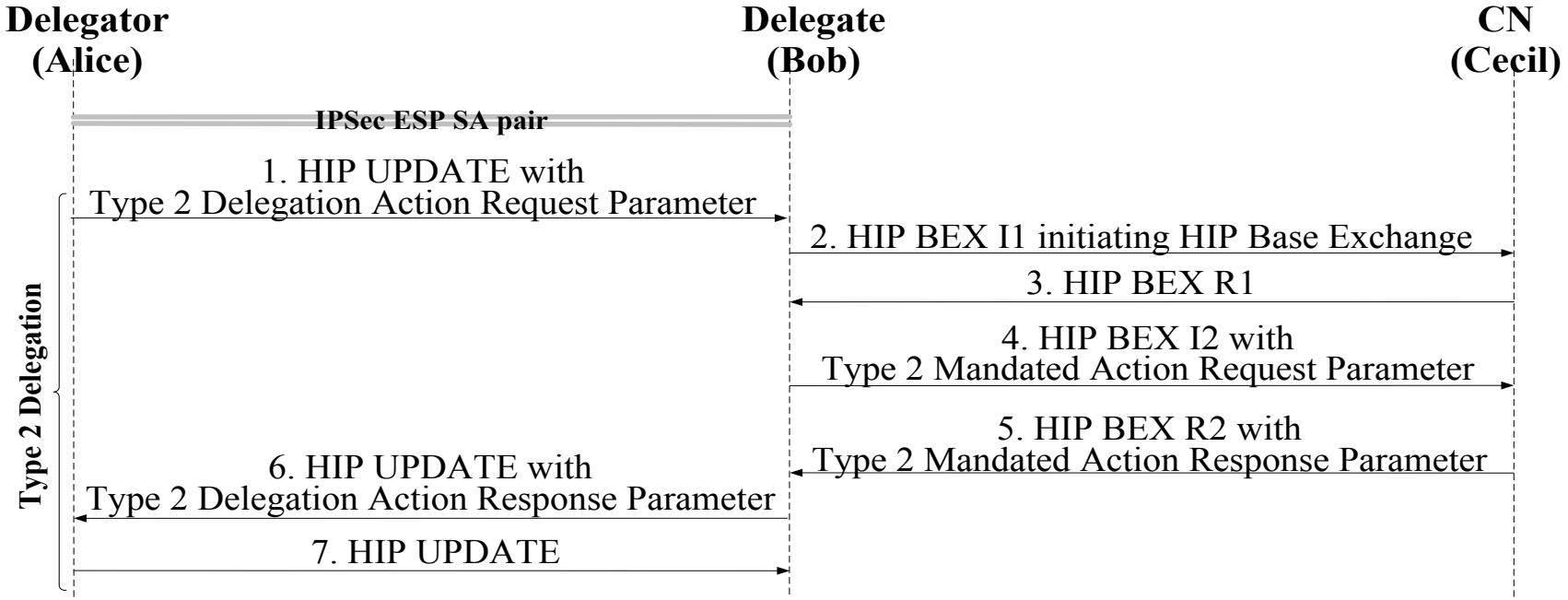


Details

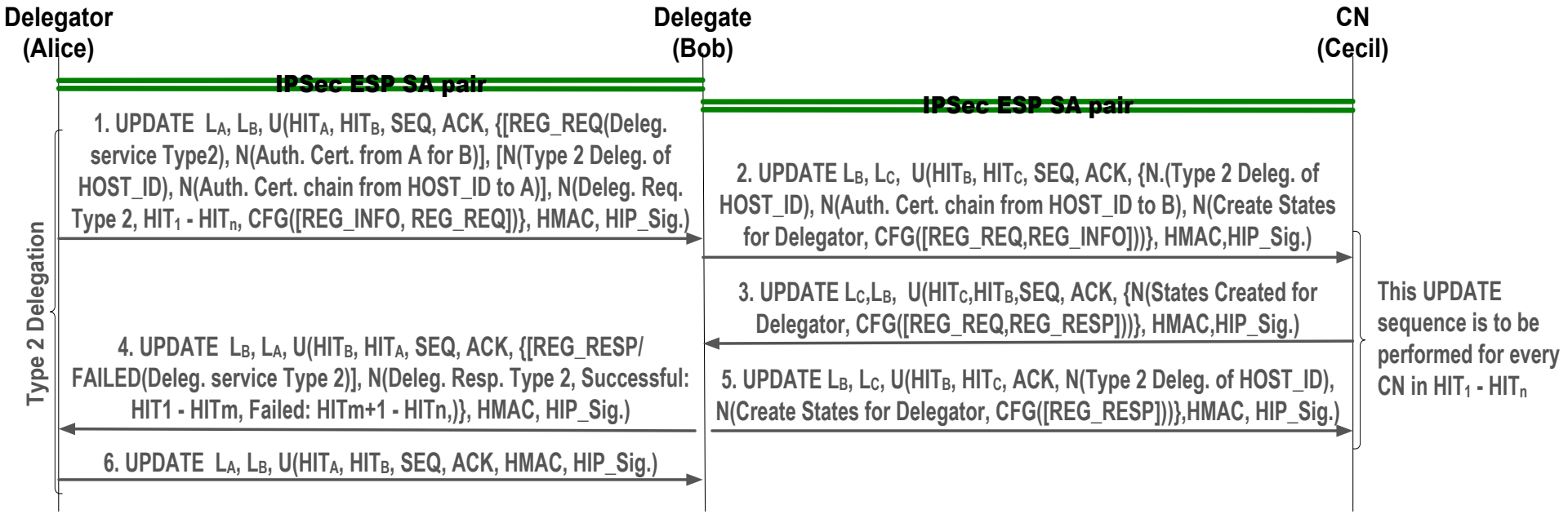

Delegator (Alice)
Delegate (Bob)
CN (Cecil)
IPSec ESP SA pair
IPSec ESP SA pair
UPDATE(HIT_A, HIT_B, SEQ, ACK, {[REG_REQ(Deleg. service Type1), N(Auth. Cert. from A for B)], N(Deleg. Req. Type 1, HIT_1 - HIT_n, CFG (SPI range, L_A, L_C1 - L_Cn, [REG_INFO, REG_REQ])}, HMAC, HIP_Sig.)
UPDATE(HIT_B, HIT_C, SEQ, ACK, {N(Type 1 Deleg. of A), N(Create States for Delegator, CFG(SPI range_C, L_A, L_C, [REG_INFO, REG_REQ])), N(Auth. Cert. from A for B)}, HMAC,HIP_Sig.)
Key derivation
UPDATE(HIT_C,HIT_B, SEQ, ACK, {N(States Created for Delegator, CFG(SPI_in, SPI_out, [REG_REQ, N(Auth. Cert. from CN to A), REG_RESP]))}, HMAC,HIP_Sig.)
Key derivation
UPDATE(HIT_B, HIT_A, SEQ, ACK, {[REG_RESP or FAILED(Deleg. service Type 1)], N.(Deleg. Resp. Type 1, Successful: HIT_1 - HIT_m, Failed: HIT_m+1 - HIT_n,)}, HMAC, HIP_Sig.)
UPDATE(HIT_B, HIT_C, ACK, CFG([REG_RESP]), HMAC, HIP_Sig.)
UPDATE(HIT_A,HIT_B, SEQ, ACK, HMAC, HIP_Sig.)
CTD(IPsec, HIP contexts for successful remote state establishments resulted by Type 1 delegation)
CTDR(Acknowledged IPsec and HIP context transfers)
IPSec ESP SA pair
Type 1 Delegation
This UPDATE sequence is to be performed for every CN in HIT_1 - HIT_n

Type 2 Delegation Service

- The Delegate
  - executes HIP Base Exchanges (BEX), HIP Updates, IPsec SA establishment in the Delegator's name, with the Delegator's authorization
  - maintains the established HIP and IPsec associations for Delegator (periodic rekeyings)
  - ~ and the Delegator notify each other in order to create the HIP host association states also in the Delegator. These HIP host associations use the existing IPsec SA bw. the Delegator and the Delegate as transport protocol.



Details


Delegator (Alice)
Delegate (Bob)
CN (Cecil)
IPSec ESP SA pair
IPSec ESP SA pair
1. UPDATE L_A, L_B, U(HIT_A, HIT_B, SEQ, ACK, {[REG_REQ(Deleg. service Type2), N(Auth. Cert. from A for B)], [N(Type 2 Deleg. of HOST_ID), N(Auth. Cert. chain from HOST_ID to A)], N(Deleg. Req. Type 2, HIT_1 - HIT_n, CFG([REG_INFO, REG_REQ])}, HMAC, HIP_Sig.)
2. UPDATE L_B, L_C, U(HIT_B, HIT_C, SEQ, ACK, {N.(Type 2 Deleg. of HOST_ID), N(Auth. Cert. chain from HOST_ID to B), N(Create States for Delegator, CFG([REG_REQ,REG_INFO]))}, HMAC,HIP_Sig.)
3. UPDATE L_C,L_B, U(HIT_C,HIT_B,SEQ, ACK, {N(States Created for Delegator, CFG([REG_REQ,REG_RESP]))}, HMAC,HIP_Sig.)
4. UPDATE L_B, L_A, U(HIT_B, HIT_A, SEQ, ACK, {[REG_RESP/ FAILED(Deleg. service Type 2)], N(Deleg. Resp. Type 2, Successful: HIT1 - HITm, Failed: HITm+1 - HITn,)}, HMAC, HIP_Sig.)
5. UPDATE L_B, L_C, U(HIT_B, HIT_C, ACK, N(Type 2 Deleg. of HOST_ID), N(Create States for Delegator, CFG([REG_RESP]))},HMAC, HIP_Sig.)
6. UPDATE L_A, L_B, U(HIT_A, HIT_B, SEQ, ACK, HMAC, HIP_Sig.)
Type 2 Delegation
This UPDATE sequence is to be performed for every CN in HIT_1 - HIT_n

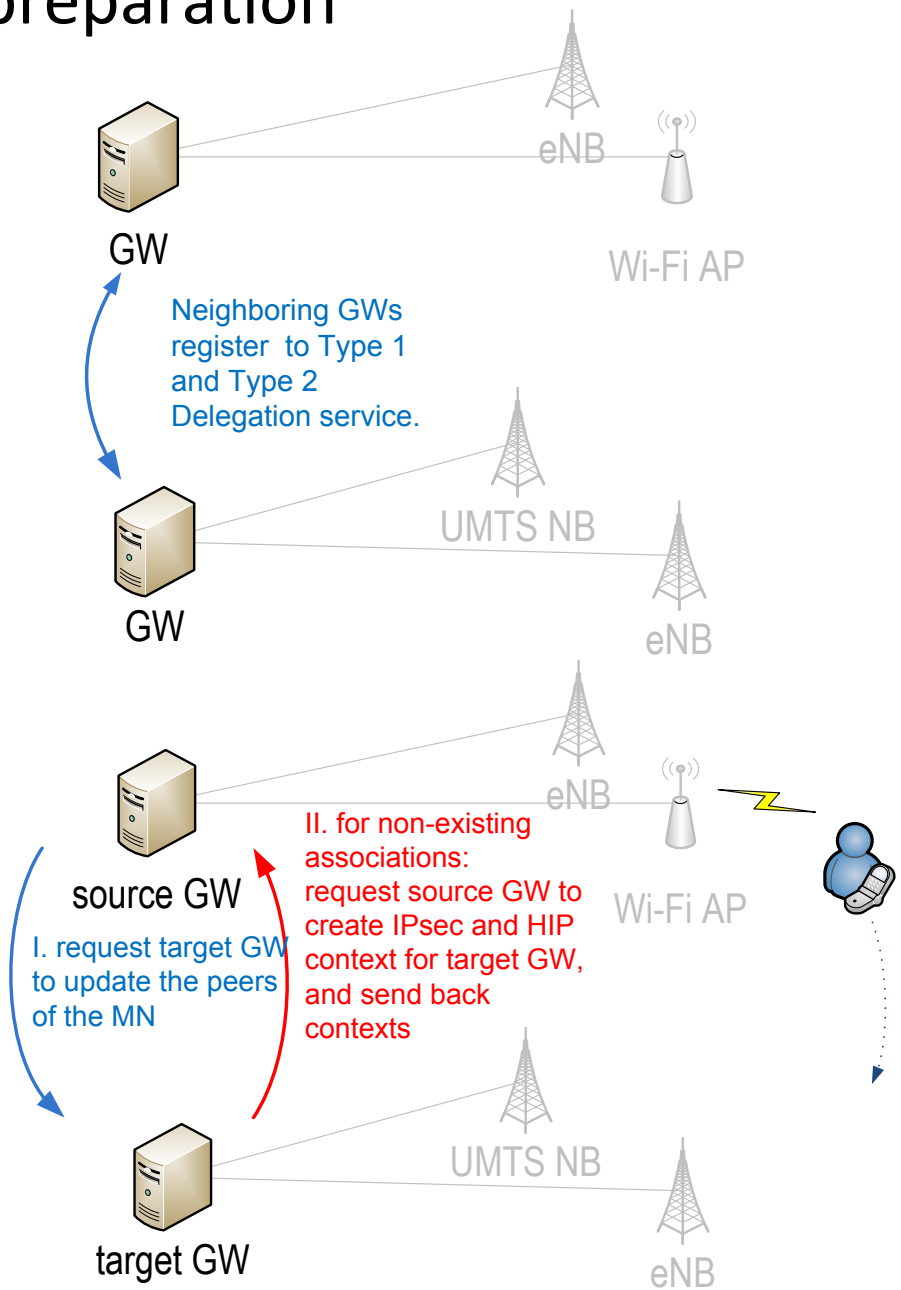
Inter-GW mobility using 802.21 and HIP delegation services

- Proactive handover procedure
  1. 802.21 initiation phase: the GW configures QoS thresholds on the MN
  2. 802.21 handover preparation phase, decide target GW: the GW queries resource information from candidate PoAs, paramters from the MIH Information service, and decides on the target GW
  3. HIP handover preparation: HIP and IPsec contexts are established for the MN - target GW, target GW - peers of the MN , traffic is routed through [MN, current GW, target GW, peers]
  4. 802.21 commit phase: establish L2 resources on target PoA and triggers physical handover
  5. Physical handover, L2 reattachment
  6. 802.21 release resources: release resources, update traffic path: [MN, target GW, peers]

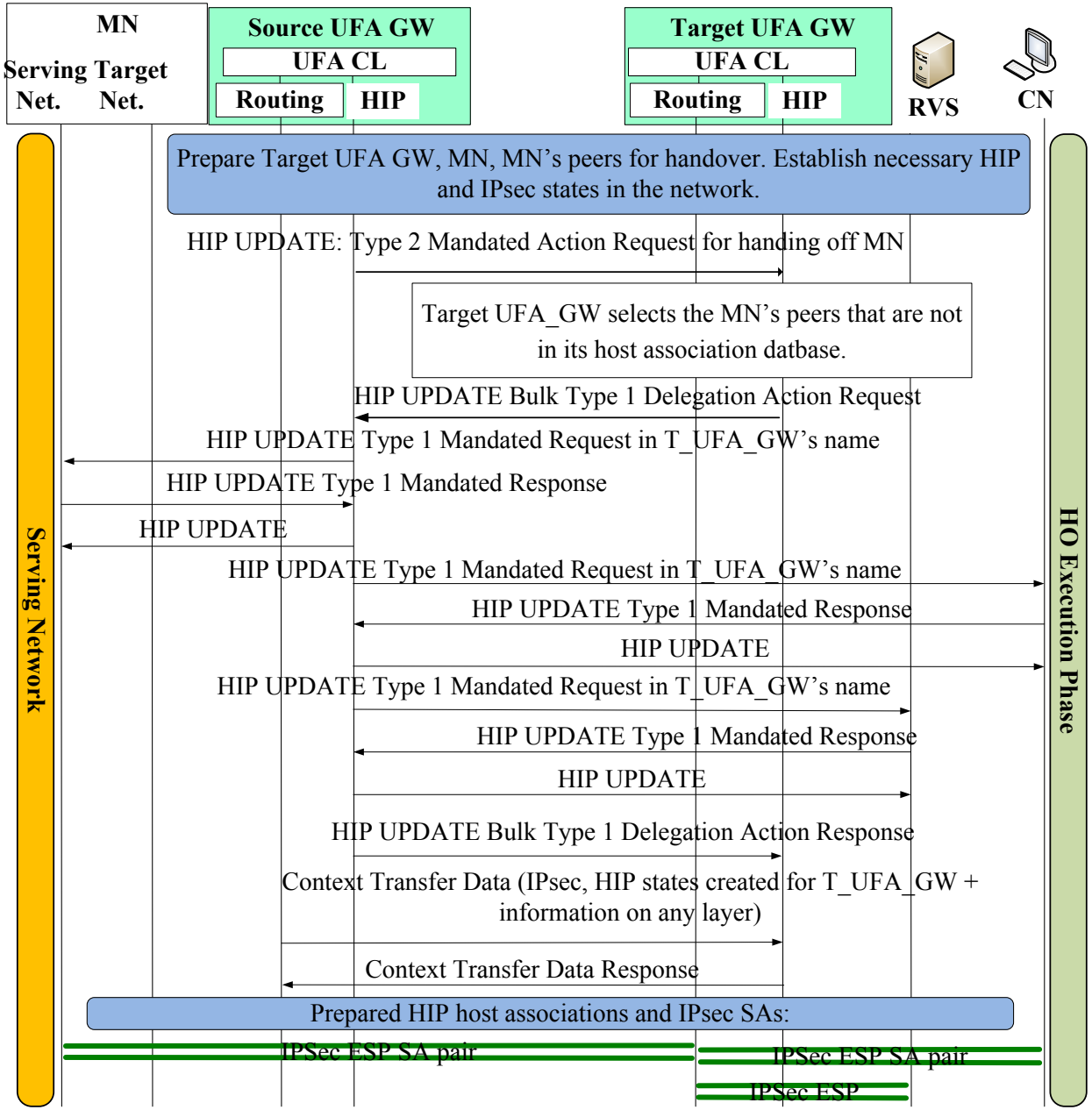
[Z. Faigl, L. Bokor, P. Miguel Neves, K. Daoud, P. Herbelin, @Evaluation of two integrated signalling schemes for the Ultra Flat Architecture using SIP, IEEE 802.21, and HIP/PMIP protocols", Elsevier, Computer Networks 55 (2011) 1560–1575]

HIP handover preparation

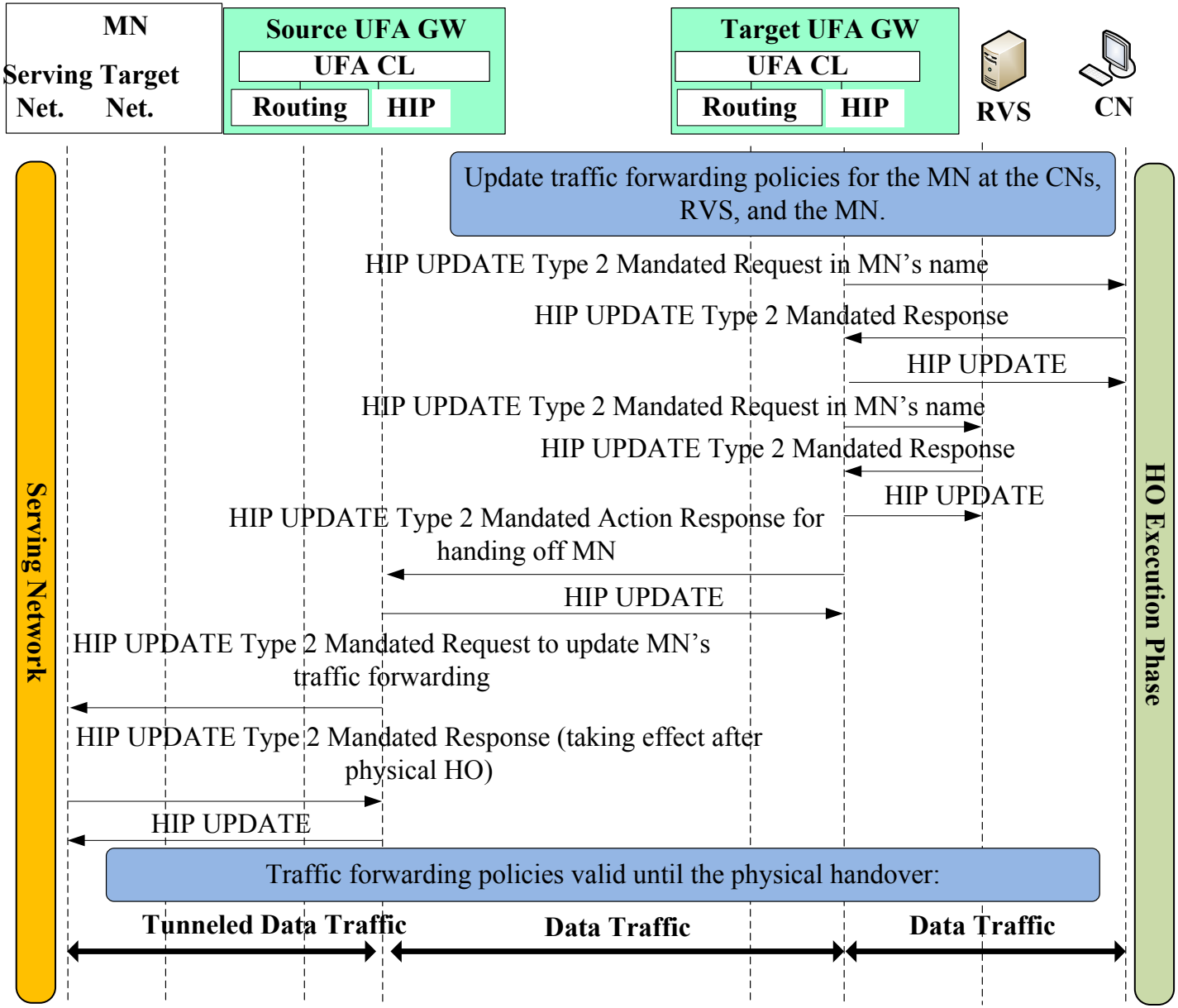
- Prerequisites:
  - the target GW registers to the Type 1 Delegation service of the source GW,
  - the source GW subscribes to the Type 2 Delegation service of the target UFA GW, HIP
- Handover preparation:
  - location update of the MN by the target GW
  - the target GW delegates HIP and IPsec association establishment to the source GW



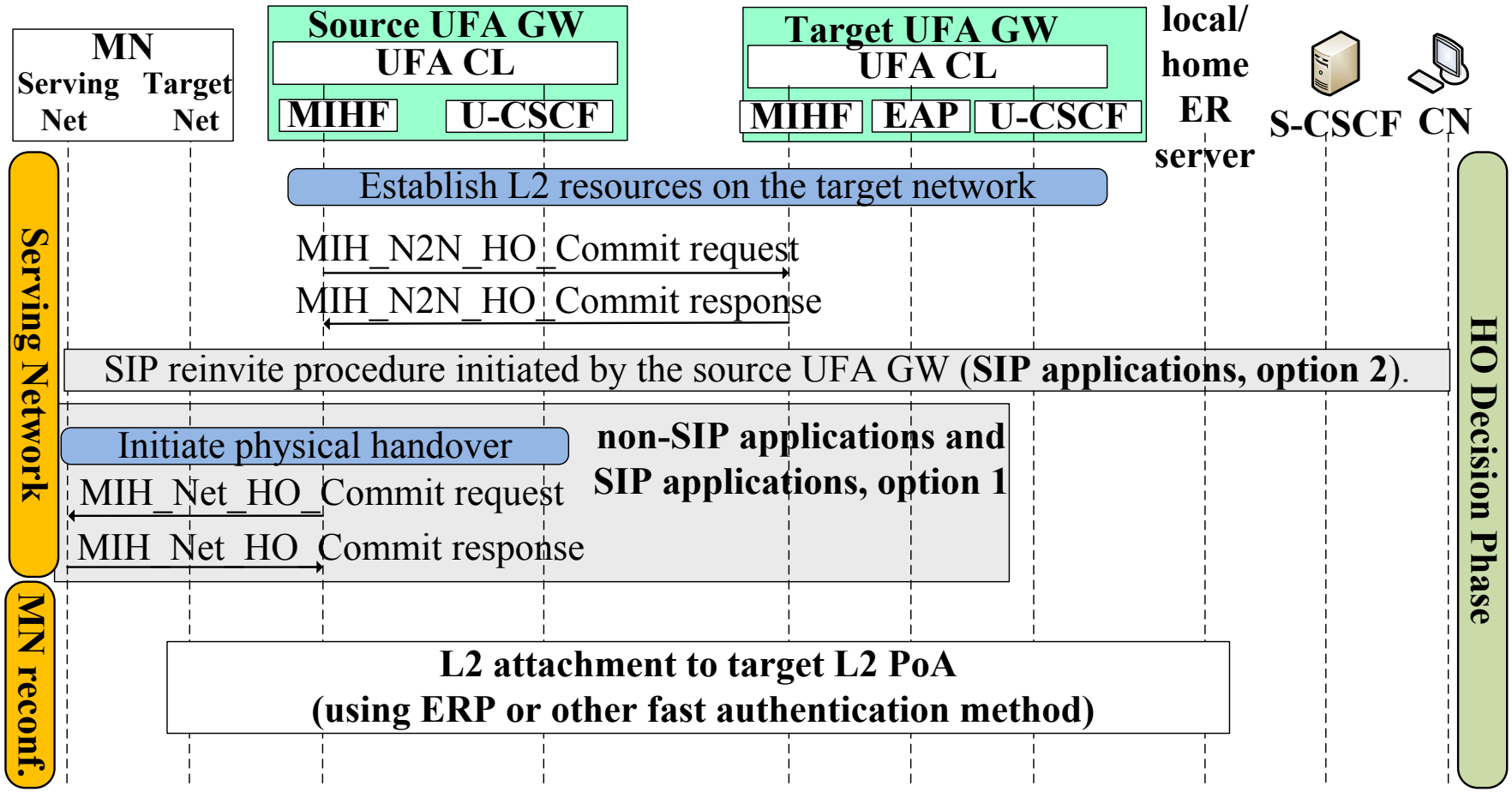
Handover preparation procedure on HIP layer



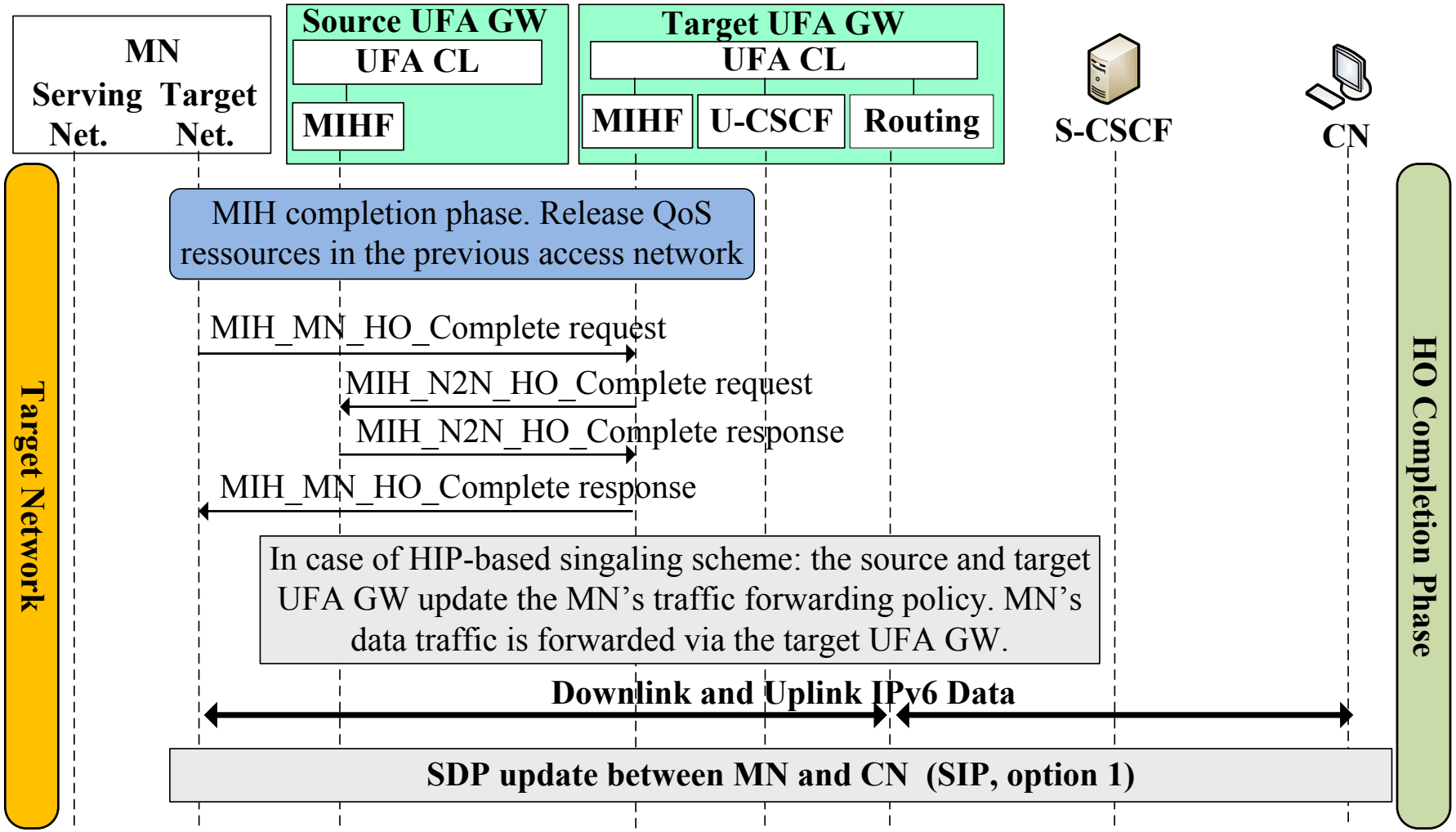
Handover preparation procedure on HIP layer



802.21 Commit phase



Handover completion phase



HIP Delegation based mobility services

- Simulation based validation (OMNeT++, HIPSim++)
- Validation status
  - Only terminal mobility
  - Delegation-based HIP implemented, 802.21 handover preparation is hardcoded, i.e., proactive handover is triggered „manually”
  - Micro-HIP and HIP mobility services are implemented for comparison (i.e. for reference results)
- Test scenarios
  - Both terminal and network mobility will be considered
  - UE is moving in the network between different access networks. Intra- and inter-PGW mobility events
  - Measurements to be done in different distribution levels of GWs, i.e. flat, distributed, centralized topologies
  - Mobile IPv6 and NEMO BS will also be used for reference

HIP Delegation based mobility services

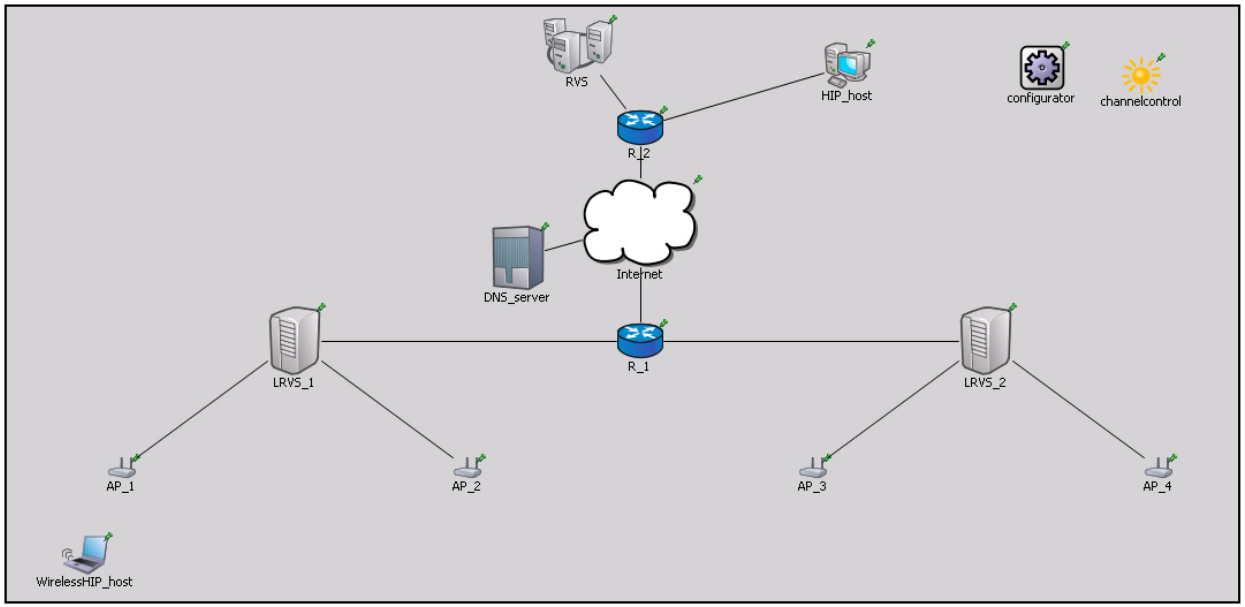
- Validation metrics, or KPIs include the following:
  - Handover delay on HIP layer
  - UDP packet loss
  - TCP throughput
  - Voice quality degradation (Perceptual Evaluation of Speech Quality - PESQ) using VoipTool
- Future work within the MEVICO project (2H11, Y12)
  - Provide different distribution-level reference scenarios for the simulation (2H11)
  - Implementation and evaluation of the delegation-based HIP-NEMO designed for flat architectures (1H12)
  - Introduce MIPv6 and NEMO BS reference models and measurements (1H12)
  - Run measurements (1H12)
  - Enhance the applied 802.21 model in INET/OMNeT++ (2H12)
  - Publish results (2H11, 2H12)

HIP-UFA Mobility simulation results

László Bokor, BME-MIK

Simulation results: Topology

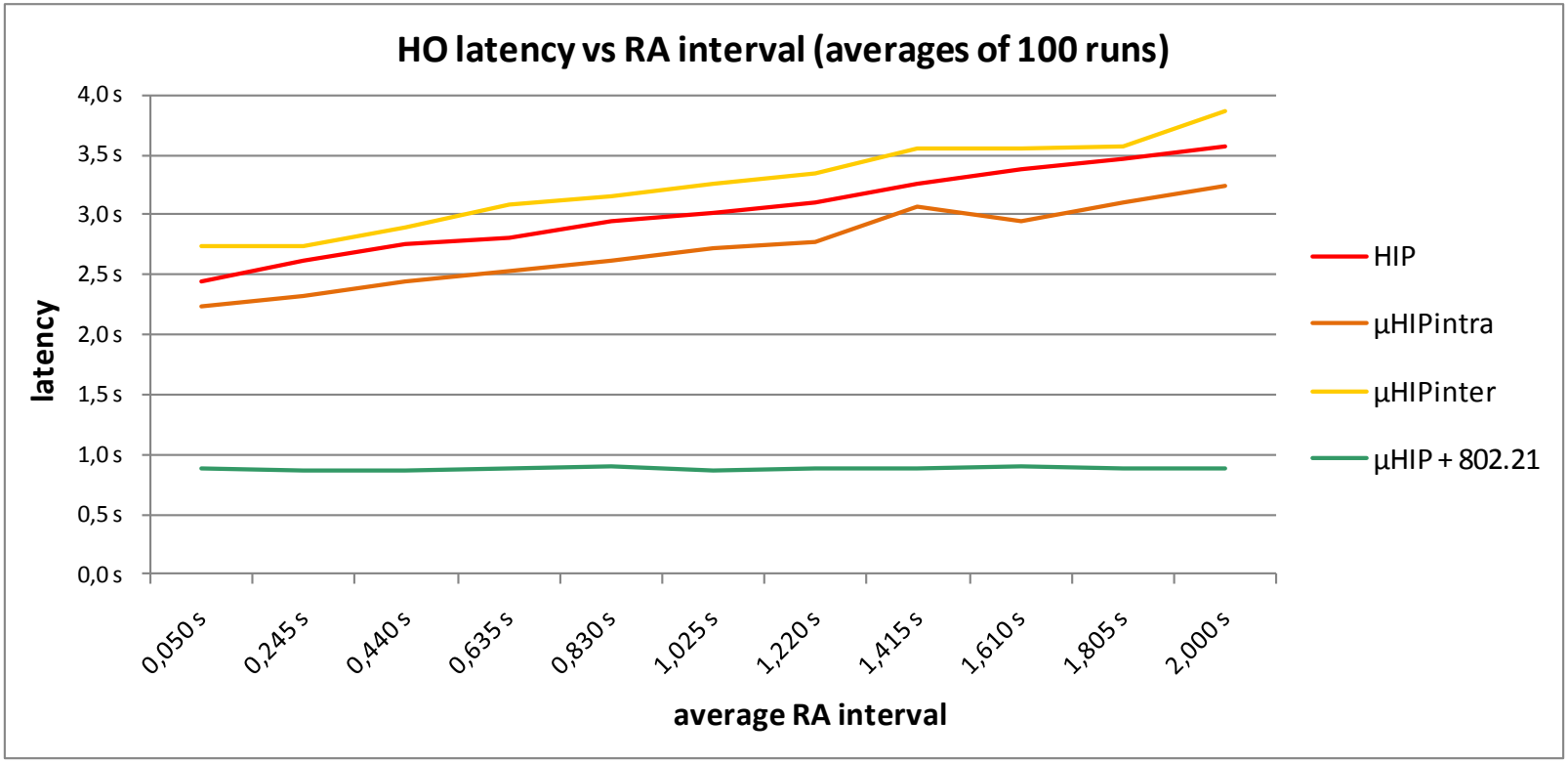
- Modeling and implementation of the integrated HIP + IEEE 802.21 MIH mechanisms and evaluation against standard HIP macro-mobility and micro-mobility solutions
  - INET/OMNeT++ based HIP simulation framework (HIPSim++*)
  - INET's Notification Board based IEEE 802.21 MIH simulation model
  - Results show the power of the integrated scheme



* [L. Bokor, Sz. Nováczki, L. T. Zeke, G. Jeney: „Design and Evaluation of Host Identity Protocol (HIP) Simulation Framework for INET/OMNeT++", in the proceedings of the 12-th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM 2009), ISBN:978-1-60558-616-8, DOI: 10.1145/1641804.1641827, pp. 124-133, Tenerife, Canary Islands, Spain, 26-30 October 2009.]

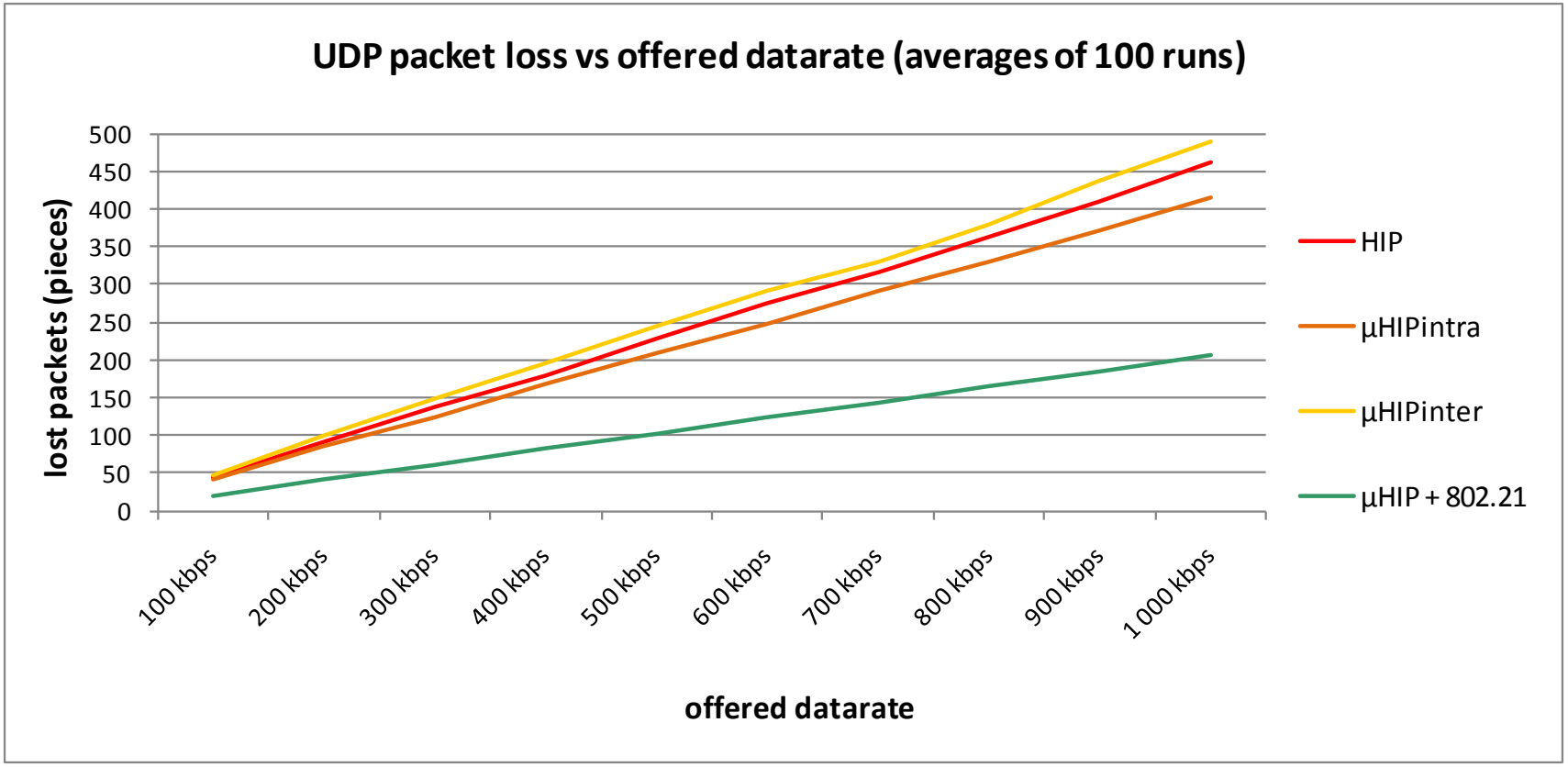
Simulation results: HO Latency

- The latency was defined here as the time elapsed between loosing the connection at the old AP and the mobile sending out the last mobility management related signalling packet (e.g., HIP UPDATE packet) while connected to the new AP
  - The integrated scheme is independent of the RA interval!



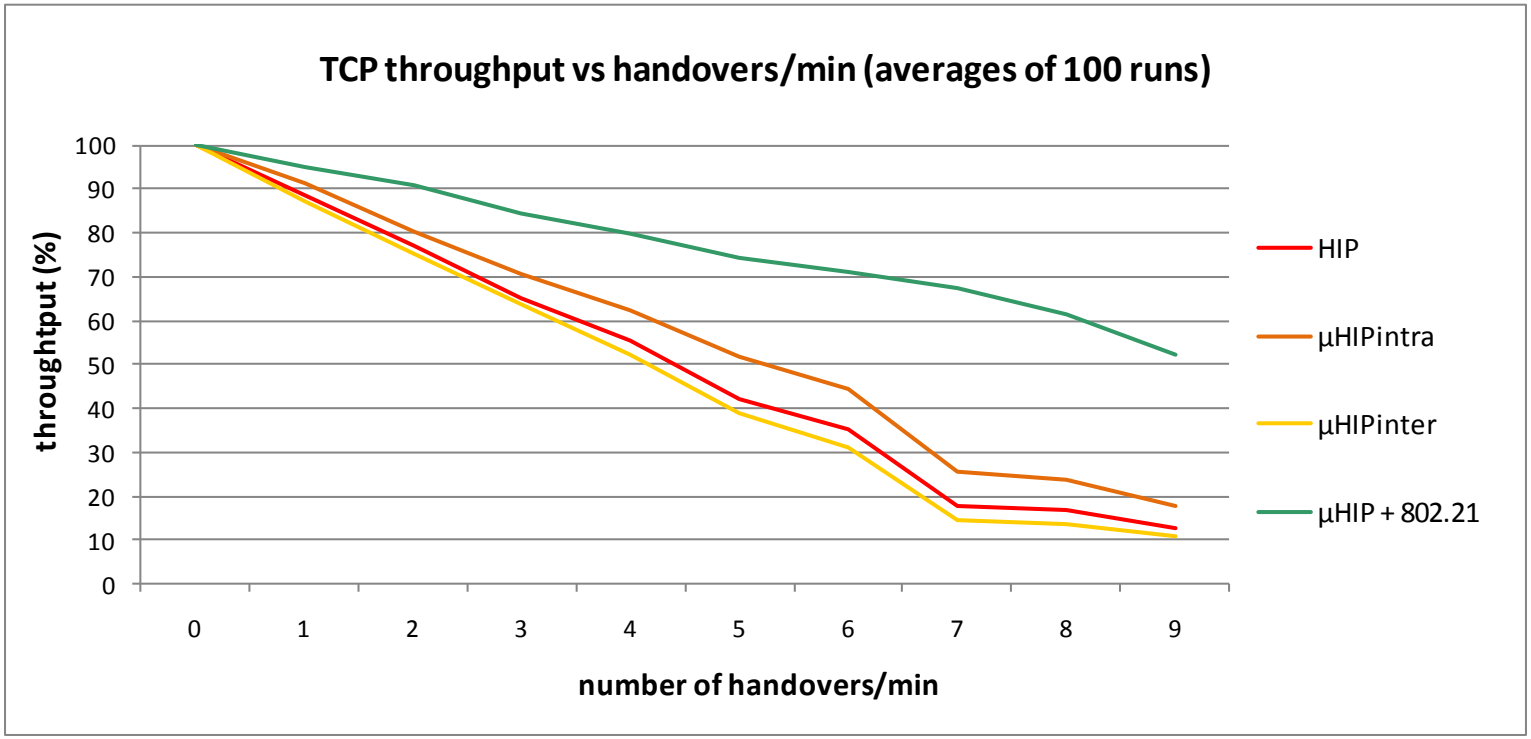
Simulation results: UDP Packet Loss

- How many UDP packets are lost during a handover in a HIP system in case of different UDP traffic?
  - UDP results are in line with the measured handover latencies and show the power of the proactive HIP+802.21 solution!



Simulation results: TCP Throughput

- TCP Reno traffic was originated between the HIP initiator and responder (i.e. the wired and wireless HIP nodes)
- We measured the throughput of one minute experienced at different handover frequencies
  - Every point represents the average throughput of 100 measurements applying the same value for the number of handovers per every minute of that series
  - Between the runs we increased the number of handovers suffered per minute form 0 to 9



Thank you for your attention!

Any questions?