Project Number:	**CELTIC / CP7-011**
Project Title:	Mobile Networks Evolution for Individual Communications Experience – MEVICO
Document Type:	PU(Public)

Document Identifier:	<D2.1>
Document Title:	**Advanced EPC architecture for smart traffic steering**
Source Activity:	WP2
Main Editor:	ALU
Authors:	see dedicated section
Status / Version:	1.2
Date Last changes:	11.14.2011
File Name:	D2.1- Advanced-EPC-architecture.doc

Abstract:	This document firstly points out the problems with network functions distribution and multiple network accesses management. Then, this document goes through the specific functions that the architectures, defined in MEVICO/WP1, should support for an enhanced mobility management and smart traffic steering. It can be new functions, or functions which inherit from current 3GPP and IETF procedures. However, it is argued that current mechanisms do not allow to optimally address issues raised in this document. Finally, considering problem statement and applicability of current mobile networks capabilities, this document gives, at a first glance, the main directions to MEVICO/WP2.

Keywords:	Mobility, multiple paths and interfaces, network functions distribution, flat mobile architecture

Document History:	
06.23.2011	Initial version based on IR-2.2
20.07.2011	Added Section 6.1.1: BME-MIK demonstrator for reauthentication delays
10.08.2011	Added ALU testbed description
18.10.2011	Added NSN LTE emulators in validation part
28.10.2011	Added CEA testbed description
02.11.2011	Added Section 6.1.7 Turk Telekom
03.11.2011	Added Section 4.6 France telecom
10.11.2011	Revised text in 7.2 Ericsson
14.11.2011	Added text ALU (executive summary, introduction)

Table of Contents

Authors

Partner	Name	Phone / Fax / e-mail	
NSN	Johanna Heinonen		
		Phone:	+358407586791
		e-mail:	johanna.heinonen@nsn.com
NSN	Pekka Korja		
		Phone:	+358407665979
		e-mail:	pekka.korja@nsn.com
BME-MIK	Zoltan Faigl		
		Phone:	+3614633420
		e-mail:	zfaigl@mik.bme.hu
BME-MIK	Laszlo Bokor		
		Phone:	+3614633420
		e-mail:	bokorl@hit.bme.hu
France Telecom	Hassan Ali-Ahmad		
		Phone:	+33 2 99124813
		e-mail:	hassan.aliahmad@orange.com
CEA	Michael Boc		
		Phone:	+33(0)169083976
		e-mail:	Michael.boc@cea.fr
ALU	Erick Bizouarn		
		Phone:	+33130772724
		e-mail:	erick.bizouarn@alcatel-lucent
ALU	Jean-Luc Lafragette		
		Phone:	+33130772738
		e-mail:	jean-luc.lafragette@alcatel-lucent
AVEA	Engin ZEYDAN		
		Phone:	+90 216 987 6386
		e-mail:	engin.zeydan@avea.com.tr
AVEA	Çağatay EDEMEN		
		Phone:	+90 216 987 6386
		e-mail:	cagatay.edemen@avea.com.tr

TURK TELEKOM	Salih ERGÜT		
		Phone:	+90 212 309 9976
		e-mail:	lih.ergut@turktelekom.com.tr

TURK TELEKOM	Ahmet Serdar TAN		
		Phone:	+90 212 309 9975
		e-mail:	ahmetserdar.tan@turktelekom.com.tr

Ericsson AB	Rashmi Purushothama		
		Phone:	+46 10 715 5964
		e-mail:	rashmi.purushothama@ericsson.com

Ericsson AB	Jörgen Andersson		
		Phone:	+46 10 719 7013
		e-mail:	jorgen.andersson@ericsson.com

Ericsson AB	Conny Larsson		
		Phone:	+46 10 714 8458
		e-mail:	conny.larsson@ericsson.com

CWC	Jani Pellikka		
		Phone:	+35 88 553 2965
		e-mail:	jpellikk@ee.oulu.fi

Executive Summary

The deliverable D2.1 [44] from MEVICO proposes to address challenges of mobile traffic evolution with distribution of the 3GPP/EPC network entities. However, this approach may impact current mobility management procedures and new problems may occur. Trying to take benefit of the simultaneous usage of different interfaces may also lead to specific terminal management issues. This document describes these problems that the WP2 should address in order to achieve smart traffic steering in a distributed and multiple accesses mobile architecture. Then, there is a description of the chosen topics on which each partner will focus on, and how they will realize the implementation to validate it.

Simultaneous usage of different interfaces typically leads to IP configuration issues but, also to more complex problems such as which radio interface should be selected. According to current IP model, some configuration objects are global to the terminal, while they should be, sometimes, local to the interface in a heterogeneous access system (e.g. it could be necessary to bound DNS servers to particular interface). In a multiple interfaces situation, the problem of interface selection is crucial but can be extremely difficult because of the various criteria to be taken into account (e.g. user preferences, quality of the link, application requirements and so on).

The distribution of network functions implies multiplication of gateways and, thus, it adds complexity to the gateway selection problem. It is also suspected that multiplication of access gateways, and thus the increased probability of handover, may have an impact on current security management. In such a distributed architecture, current IP mobile architecture should be also rethought since maintaining centralized anchoring for mobile IP traffic may lead to unoptimized routing.

The proposed network evolution may be also the opportunity to revisit some basic mobility procedures. Typically the paging process could be improved to take benefit from the multiple access contexts and the distribution of gateways. Also, dynamic IP mobility management is proposed to be introduced together with distribution of traffic anchoring point. Dynamic mobility management aims in saving network resource by setting up IP mobility processes only when IP handover is to be performed.

The IETF RFC 2101 (1997) [9] says: “Identifiers should be assigned at birth, never change, and never be re-used. Locators should describe the host's position in the network's topology, and should change whenever the topology changes”. This requirement sounds like common sense, however IP networks still

do not met it. Today, both identifier and locator roles are handled by the IP address. As a consequence, separation of locator and identifier in future mobile network is an important evolution expected to meet, at least, one of the fundamental IP network requirement.

Then, this document goes through the specific network functions that the architectures, defined in MEVICO/WP1, should support for an enhanced mobility management and smart traffic steering. It can be new functions, or functions which inherit from current 3GPP and IETF procedures.

This document studies how current inter-system and intra-system mobility management may be impacted by distribution. If current mobility management could apply, it is argued that mechanisms do not allow to optimally address issues raised in this document. For instance, P-GW relocation is an option to be studied for reaching optimal routing in a distributed mobility architecture.

Finally, this document gives a description on all the proposed MEVICO demonstrators that have a link to the mobility and routing topic. These demonstrators will be used to validate the different WP2 technology solutions described in IR2.5 [47] .A demonstrator may be either a testbed, or a simulation or an analytical solution.

List of acronyms and abbreviations

3GPP	3rd Generation Partnership Project, based on GSM Technology
AAA	Authentication, Authorization, Accounting
ANDSF	Access Network Discovery and Selection Function
AP	Access Point
API	Application Programming Interface
APN	Access Point Name
AR	Access Router
AS	Application Server
ASN-1	Abstract Syntax Notation One
B2BUA	SIP Back-to-Back User Agent
BEX	HIP Base Exchange
BS	Base Station
BSD	Berkeley System Distribution
BTS	Base Transceiver Station
CAPEX	Capital Expenditure
CDN	Content Delivery Networks
CN	Correspondant Node
CPU	central processing unit
CQI	Channel Quality Information
CSCF	Call Server Control Function
CTS	Clear To Send
DeNB	Donor eNB
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
DSCP	DiffServ Code Point
DSMIPv6	Dual Stack MIP v6
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
eNodeB	evolved Node B (eNB)
EPC	Evolved Packet Core
EPS	Evolved Packet System
ERP	EAP Reauthentication Protocol
FMIPv6	Fast MIP version IPv6
FW	Firewall
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
GUTI	Globally Unique Temporary Identity
GW	Gateway
HA	Home Agent
HI	Host Identifiers
HIP	Host Identity Protocol
HIT	Host Identity Protocol
HNP	Home Network Prefixes
HO	Handover
HSS	Home Subscriber Server
HTTP	hypertext transfer protocol
IA	Intermediate Anchors
I-CSCF	IMS proxy node

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFOM	IP flow Mobility
IKEv2	Internet Key Exchange (IKEv2) Protocol
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISMP	Inter-System Mobility Policy
ISRP	Inter-System Mobility Policy
KPI	Key Performance Indicator
LFN	Local Fixed Node
LMA	Local Mobility Anchor
LTE	Long Term Evolution
LTE-A	Long Term Evolution – Advanced
LU	Location Update
MA	Mobility Anchor
MAC	Media Access Control
MAG	Mobile Access Gateway
MAPCON	Multi Access PDN CONnectivity
MIH	Media independent handover
MIMO	Multiple Input Multiple Output
MIP	Mobile IP
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MN	Mobile Node
MPLS	Multi-Protocol Label Switching
MPTCP	Multipath Transmission Control Protocol
NAT	Network Address Translation
NEMO	Network Mobility
NMIP	Non MIP
OFDMA	Orthogonal Frequency Division Multiple Access
OPEX	Operational Expenditure
OSI	Open System Interconnection
PBA	Proxy Binding Acknowledgments
PBU	Proxy Binding Updates
PCC	Policy Control
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy-CSCF
PDN	Packet Data Network
P-GW	Packet Data Network (PDN) Gateway
PMIP	Proxy Mobile IP version 4
PMIPv6	Proxy Mobile IP version 6
PoA	Point of attachment
POP	Point of Presence
PPP	Point-to-Point Protocol
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network

RAT	Radio Access Technology
RFC	Request for Comments
RN	Relay Node
RO	Routing Optimization
RSTP	Rapid Spanning Tree Protocol
RTS	Request To Send
RVS	Rendezvous Server
SCC	Service Centralization and Continuity
S-CSCF	Serving CSCF
S-CSCF	IMS proxy node
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
S-GW	Service Gateway
SIM	Subscriber Identity Module
SINR	Signal to Interference and Noise Ratio
SIP	Session Initiation Protocol
SMS	Short Message Service
SPI	Security Parameter Index
SxS_GW	SIPcrossSCTP Gateway
TA	Tracking Area
TCP	Transport Control Protocol
TEHO	Traffic Engeneering Handover
TEID	GTP tunneling endpoint identifier
UE	User Equipment
UFA	Ultra Flat Architecture
UMTS	Universal Mobile Telecommunication System
UPE	User Plane Entity
VLR	Visitor Location Register
VPN	Virtual Private Network
Wi-Fi	“Wireless Fidelity” a trademark of the Wi-Fi Alliance (IEEE 802.11 certified devices)
WLAN	Wireless Local Access Network

1. Introduction

As shown in MEVICO IR1.1 [1], a huge increase of mobile data traffic is expected for the next few years. Among the different ways to address the issue is the offloading. Basically, this approach consists in offloading the mobile network towards fixed accesses (e.g. Wi-Fi accesses). For a better efficiency, offloading should leverage on dynamic usage of the different access networks (i.e. it should be possible to perform handover of ongoing session), thus leading to inter-systems mobility management. Initially, mobility has been managed through cellular technologies and dedicated to voice services. Once addicted to mobile voice services, users also got used to mobile data services. A challenge for the coming years is to anticipate the inevitable growth of demand on the required network resources, especially on the radio link, for such bandwidth consuming data applications. The arrival of handsets capable of being attached to multiple access technologies (e.g., 3GPP, Wi-Fi) allows to partially overcome the issue by using alternatively or simultaneously more than one access network. Additionally, in order to offer a better quality of experience to the user with an optimised management of scarce radio resources, the network operator may want to maximise the benefit of the multiple-accesses environment through a dynamic mapping of data sessions on the most appropriate accesses. These mapping strategies are derived from various criteria, including the application type (e.g. voice or data), the QoS available on each access network, the user preferences, the terminal environment... This flexibility in heterogeneous networks management requires the deployment of specific inter-access mobility architectures enabling the simultaneous use of multiple accesses and the transfer of ongoing sessions among access networks with no impact on the user experience.

EPS architecture, at least in its current release, i.e. R10, supports inter-system mobility architecture but is missing some key features that an optimal mobility solution should offer, such as network-assisted mobility management solutions (i.e., the network assists the user equipment in the access discovery, the access selection and the mobility triggering). The user equipment implements connection manager capable of handling multiple interfaces (e.g.., defines a predictable and stable behaviour of the user equipments when combining operator policies, user preferences, service requirements…).

However, smart traffic steering could potentially add a significant complexity on the host to estimate the most optimal path for a flow based on different input criteria. Although the host has access to a lot of input parameters for access decision it could be easier in some cases for the host to get a predefined set of rules downloaded. Depending on the available access technologies different rules would be applied to make a decision on which interface to send the packet and/or to be reachable.

The selection of the more appropriate mobility management strategy is also one of the main challenge for mobile network evolution. Heterogeneous access network architecture may lead to cohabitation of several mobility protocols (e.g., MIP, GTP, SIP) being used in a harmonized and flexible manner (e.g., dynamic re-selection of pertinent mobility anchors, PGW versus SCC AS in 3GPP). Some applications can survive to an IP address handover, i.e. manage IP mobility and inter-access handovers. In a such a diversified environment, the mobility management should take into account these various situations. However, the selection of the mobility mechanism may be quite complex as it shall be based on a combination of service requirements, user equipment capabilities, available network features, and so on.

Considering all above challenges, this document will address evolution of mobile architecture according to two main drivers:

The importance of both the functional segmentation (i.e., initiation, decision, execution) and the dynamicity (or auto-configuration) of the mobility architecture.

The purpose is to facilitate the network evolution, the flexibility of the mobility management and the mutualization of equipments, the need of distribution and flattening (i.e., fewer levels in the network hierarchy). Less centralised inter-access mobility architectures choice is done to optimise the traffic flow management; as per in MEVICO/WP1 recommendation [2].

2. Problem Statement

The document MEVICO IR1.3 [2] proposes to address challenges of mobile traffic evolution with distribution, or flattening, of the 3GPP/EPC network entities. However, this approach may impact current mobility management procedures and new problems may occur. Trying to take benefit of the simultaneous usage of different interfaces may also lead to specific terminal management issues. This section describes these problems from the WP2 perspective, i.e. problems that the WP2 should address in order to achieve smart traffic steering in a distributed and multiple accesses mobile architecture.

2.1 Smart Traffic Steering in Multiple Paths Environment

Mobile broadband networks are expected to experience significant data traffic growth in the future [1]. As said in the introduction (section 1), efficient use of heterogeneous access networks may be part of the solution space. Heterogeneous network capabilities introduce among others multiple simultaneous available paths for user data to traverse in the network. Besides, 3GPP has defined in Rel-10 three capabilities that address traffic steering across multiple accesses (and/or APNs), namely IP Flow Mobility (IFOM), Multi Access PDN CONnectivity (MAPCON), and Non-seamless WLAN offload. In this context, optimal mapping of traffic over candidate paths is a key issue which requires mechanisms for smart traffic steering to be defined.

Smart traffic steering requires to optimize initiation, selection, configuration and use of multiple access network interface capabilities both in mobile device and in network side. Various criteria should be taken into account to allow efficient use of the multiple available paths in the network, different radio access technologies and gateways. The need for traffic steering granularity may vary on access technologies and interface depending on the needs: IP connection, IP flow and application level. Smart traffic steering allows balancing signalling and data communication within Evolved Packet Core (EPC).

On devices supporting multiple interfaces operators may convey different types of policies. For instance in 3GPP, ANDSF framework may be used to assisted access network selection using Inter-System Mobility Policy (ISMP) and traffic offloading to WLAN via Inter-System Routing Policy (ISRP). Policies may also be local in scope and user defined. In Rel-10 3GPP ANDSF policies are not designed to support dynamically changing situations in the network such as network load evolution and to be able to support different applications such as those sharing the same port numbers. Besides interfaces selection mobile device shall cope with complex selection and configuration issues. Typically, source address selection, address overlap or DNS selection, cannot be solved by simply modifying configuration rules [14].

2.2 Impact of Mobile Network Evolution

Mobile network evolution is going on new design to avoid excessive traffic concentration on a single gateway and centralized anchors (potentially resulting in non-optimized routes) and to distribute the traffic anchors across the network. For instance, 3GPP has defined in Rel-10 methods, such as SIPTO, for optimization of traffic distribution across the network and selection of optimal gateways (S/P-GW).

This is also the guideline for architecture design in MEVICO/WP1 [2]. Additionally, local caching and Content Delivery Networks (CDN) may benefit from the ability of the network to distribute traffic across the network as close as possible to end user device.

Current trend in network evolution is thus to distribute data anchoring in local gateways. So, maintaining centralized mobility anchoring, as per current solutions (reminded in [4]), in such architecture would lead to non-optimal routing. Actually, with centralized mobility management the traffic shall be always forwarded to the local mobility anchor, while data traffic is locally anchored.

2.3 Useless “always-on” IP Mobility Management

In today’s mobile networks, more often than not, mobile devices remain attached to the same IP point of attachment. In other words, some applications are launched and complete while connected to the same point of attachment. In this case, a specific support for IP mobility management, expected to provide IP session continuity in case of hypothetic IP subnet handover (e.g. inter-access handover), is not required. However, current IP mobility solutions [4] do not take this into account. Actually, current mobility solutions have been designed to be always on and to maintain the mobility context (e.g Mobile IP binding) for each mobile subscriber as long as they are connected to the network. So, when the mobile devices remains attached to the same point, this can result in a waste of resources and ever-increasing costs for the service provider. On the contrary, devices located in vehicles will suffer from frequent handovers and may require optimized mobility procedures.

In addition, it is possible to have the intelligence for applications to manage change of IP address (e.g. in case of inter-access mobility) without needing help from the network. If so, it is a waste to provide network mobility support and maintain mobility context for applications or devices which don't need it.

Infrequent mobility and intelligence of many applications suggest that mobility support can be provided dynamically, thus simplifying the context maintained in the different nodes of the mobile network.

Smart traffic steering and mobility procedures optimization could take into account awareness of applications types and requirements (e.g. by means of traffic management and DPI), device location and movement in the network, device type, subscription type, load in the network (by means of traffic management), and various policies defined by the operator and end-user.

2.4 Impact on Terminal

Multiple path management requires the terminal to be simultaneously linked to several interfaces. And among them some links may be setup for very specific purposes such as VPN. In this situation the terminal shall be able to select the best interface according to plethora of criteria such as applications requirements, network conditions, user preferences, and so on. Even with assistance from the network, e.g. policy based selection with 3GPP ANDSF [7], selection may be an heavy computation task for the terminal. Moreover, the terminal may have to face to complex configuration issues (e.g. routing, policies conflict) [14], which may require more computation effort.

2.5 Performance of Current Intra-system EPC Procedures in Distributed Architecture

When offloading through other access networks is not possible, optimization of intra-EPS traffic routing is the main and immediate solution to accommodate the expected traffic growth. In this situation smart traffic steering should allow to add greater control and flexibility on flows data paths.

Depending on EPC deployment scenario described in IR1.3 [2], some problems may arise. Here are problems identified for examples of deployment scenarios.

- Case 1: The P-GW is centralized and the S-GW is distributed (e.g. scenarios 1B or 2A in the deliverable IR 1.3) [2]. The data traffic of two communicating users associated to close-by eNBs would undergo an important indirection towards the centralized P-GW (located in national POP) before coming back to the destination. This indirection would highly reduce performance of flows and also unnecessarily increase the load in the EPC. A centralized solution has however some advantages. In this context, the P-GW could gather all required knowledge to enable network-based smart traffic steering. The outcome would be a better management of resources and rapid improvements of data traffic performance.

- Case 2: All of the EPC elements are distributed (e.g. scenario 2C or 3 in the deliverable IR 1.3) When all EPC elements are distributed, particularly the P-GW, current EPC mobility procedures can be used. However, they are not optimal especially for moving users. Indeed, the user will remain anchored in the initial P-GW through which the call has been initiated, while he is connected to a base station, which could be far from the initial P-GW. This means that we have to configure the path between the base station and the P-GW, leading to higher configuration and transport link costs.

2.6 Challenges of Identifiers and Locators

In current IP networks locators of network elements and end-nodes are IP addresses. Due to mobility, network renumbering and smart traffic steering, the end-points of traffic flows might change frequently. Hence, locators are short-lived. On the other hand, network nodes, end-nodes or users need persistent identifiers, not depending from the mobility events. An important challenge in mobility, traffic, network management functions is how to bind efficiently locators to identities.

Future routing solutions (e.g., georouting) may require new locator namespaces and routing mechanisms. Introduction of new locator types and routing mechanisms in specific intra-domains should be supported independently from the identifiers used in the service stratum, and without influencing inter-domain routing.

The optimal routing path should depend only on locators and not on the identifiers.

For scalable routing, topologically routing entries that may be aggregated, should be used in inter-domain routers.

The downside in separating the identifier and locator roles of the IP address is that tracking traffic flows becomes easy for 3rd parties. It is a mundane task for an eavesdropper to map traffic flows to an identity if the identity information is carried in every packet transmitted over the network; whether this ID is some identifier string (e.g. HIT in Host Identity Protocol) or a Security Parameter Index (SPI) tag associable with the identity. For this reason, incorporating ID/locator split in mobile networks requires a mechanism to blind the real identities from eavesdroppers or to distribute/generate verifiable pseudonym identities.

ID/Locator separation schemes offer different possibilities to deal with these problems. On the other hand, some of these solutions support IP mobility management as well; hence they are interesting also in the mobility research domain. [Annex 9.1] discusses in details the advantages and drawbacks of ID/Locator separation.

2.7 Security Considerations

In current 3GPP networks, non-3GPP access is protected by IKEv2 and IPsec protocols. Seamless inter-system handover between non-3GPP accesses is not supported.

Flattening the core network leads to the increase of inter-GW handovers. In case of inter-GW handovers, the identity of the GW is changed. This can not be handled by current IPsec security association negotiation protocols such as IKEv2 or HIP. These protocols can only deal with non simultaneous locator changes of the endpoints. Handover to new gateways induces the need of establishing new security associations between the MN and the new GW. Currently, IKEv2 or HIP would re-establish the security associations, causing high overhead in case of frequent IP address changes.

Another question is handling handovers between heterogenous access networks where re-authentication and key agreement on multiple layers could result in serious deteriorations in ongoing communication sessions. Cross-layer optimizations could be used for fast re-authentications during handovers.

The authentication methods of different L2 access technologies should be made compatible with an ERP-like (EAP Reauthentication Protocol) fast reauthentication method. ERP basically enables a simple two-message authentication procedure for re-authentications in case of EAP-based authentication methods. This approach could be applied for other authentication methods. With cross-layer authorization the overhead of full authentication and key establishment procedures on L3 could be minimized by saving the cost of Diffie-Hellman key exchanges or other computationally demanding cryptographic operations. However, in ERP, this would need the L2 and L3 endpoints to be located in the same physical entity that is only true for the MN. At the network side the L2 and L3 security association endpoints may be separated. In that case a new security protocol is needed to provide the keying material to L3 in the distributed gateway.

An alternative to cross-layer authorization is to harmonize the authentication and authorization processes and perform it only on either of the layers, i.e. L2 or L3. This could effectively reduce the number of used authentication protocols/methods in the network and could also possibly reduce the signalling and delay overhead from the multiple layer-specific signalling as done in today's networks. The ubiquitous nature of the IP protocol speaks for harmonized L3-based authentication and authorization. This means that the bootstrapping is performed by an IP-based authentication protocol before the UE acquires IP addresses or connects to any services in the access network.

The current use of IKEv2 in EPC can lead to overlapping (encapsulated) IPsec connections. E.g., in case of initializing an IMS session through a 3GPP Wi-Fi access, an IPsec association is established both on the network level and on the SIP signalling level, resulting in overprotection and signalling overhead between the MN and ePDG. In a distributed architecture the IPsec establishment could be managed.in a hop-by-hop manner, without unnecessary encapsulations, where the intermediate hops would be the distributed gateways.The problem with the cryptographic algorithms used in the current authentication protocols such as HIP is that they require a great deal of processing-power. Especially, the signature and encryption algorithms are quite memory and CPU hog. Thus, using such algorithms can be too heavy for the resource constrained mobile devices we have today, and introduce unacceptable delays in service when run during handovers.

For this reason, mobile devices and mobile networks require use of lighter protocols in authentication in order to provide better performance and quality of experience for user. For example, replacing signatures

with cipher-based message authentication and using more lightweight Elliptic Curve Cryptography (ECC) could solve the problem. However, using such techniques has downsides, e.g. lost of non-repudiation.

2.8 Unoptimized Routing due to Centralized Firewalls

One additional concern is security concerning traffic from one UE to another. In current networks, mobile to mobile traffic is usually routed via firewalls – not inside or between the GW elements. A resulting question is whether to distribute the firewall functionality as well? Or is straight mobile to mobile traffic acceptable in the mobile operator's access network? Centralized FW will cause unoptimized routing the same way as centralized GW elements.

2.9 Reachability/Paging

This section deals with UE incoming calls that occurs currently in interpersonal communications such as voice, SMS, MMS, instant messaging, and represents statistically half of the calls of this type of service.

One of the big differences between fixed and mobile networks is that for the latter the service, in case of UE incoming calls, can be provided although the network does not know in advance the precise location of the UE. This is made possible through a couple of procedures, namely paging and location update. The attached UE, before any active session, is roughly located at Tracking Area[1] (TA) level. The TA is defined as a group of cells covering a certain geographic area. An incoming call is possible via the paging of the concerned UE in all the cells of the TA. Thanks to the paging response of the concerned UE, the network is aware of its precise location, i.e. at cell level. It can then notify it for session setup.

The TA size, in terms of number of cells, follows from a trade-off between signaling and radio load of paging and signaling and radio load of TA updates at TA border. These procedures allow – to the cost of a widely sent but on demand paging message – to avoid updating the location of every idle mode UE at every cell change, which would lead to a prohibitive cost in terms of signaling and radio load, in addition to UE battery life.

These procedures arise from the idle mode that enables both to spare battery life and to limit radio load. In this UE state, even if the "always on" IP connectivity has been setup from the start, i.e. the attachment procedure, the connection to the radio network is not permanent. In other words, a GTP tunnel is permanently established between e-Node and PDN-GW but the radio bearer is systematically released on inactivity basis.

- Multiple technologies should require a solution based on common management:

Paging and Location Update (LU) procedures should take into account the requirement of multiple gateways and multiple interfaces to extend and improve the performance of IDLE mode management procedures.

- Gateways distribution impact: the MME distribution should be concerned at first.

If the P-GW is distributed, there will be more frequent IP address changes for the MN. Nevertheless this should not impact directly the paging procedure, since it is initiated by the MME on another temporary identifier basis, the GUTI.

- Dynamic mobility management: it may introduce a big challenge. Procedures enabling reachability represent a cornerstone of the mobile networks, and the notion introduced as "dynamic mobility management" will have to cope with the always reachable capability of the UE.

2.10 Transport Network Topology in Distributed Architecture

Transport network topology commonly used in the access networks is a tree topology. In current mobile networks with centralized GW elements the traffic is flowing mainly between the base stations and core network elements. Therefore the tree topology in the mobile backhaul is optimal.

[1] The 3GPP, for equivalent notions, names "Location Area" for CS domain in 2G and 3G, "Routing Area" for PS domain in 2G and 3G and "Tracking Area" in 4G (so for PS domain),

In the distributed architecture the GW elements are in the access network. In this scenario, the traffic is often flowing between two elements located in the leaves of the transport network tree. This can lead to the situation where the logical routing path is optimized (not going anymore via centralized GW) but the physical path is not.

2.11 Support of Moving Networks

In the current 3GPP EPC core, the support of moving networks is not specified by network-based mobility management protocols, e.g., PMIPv6. It is expected that the importance of moving networks communications will increase in the next years thanks to the maturity of vehicular communications and the current deployment of wireless access networks in airplanes. If one considers the operation of PMIPv6 [11] in the 3GPP EPC core, only UE mobility is managed. The routing procedures and the data structures have then to evolve in order to provide the support of moving networks at the IP level.

3. Architectures scenarios

The MEVICO IR1.3 [2] derives distributed architecture scenario according to the following assumptions:

- Functional EPC architecture remains unmodified.
- Organic distribution of EPC entities with possible function co-location (e.g. S and P-GW)
- Control plane (MME/ANDSF) may or may not be distributed

According to WP1 scenarios, the EPC can be distributed at different parts of a mobile network. Because centralized services can still be offered, centralized gateways can also cohabit with distributed gateways. The global picture brought by WP1 is depicted on Figure 1.

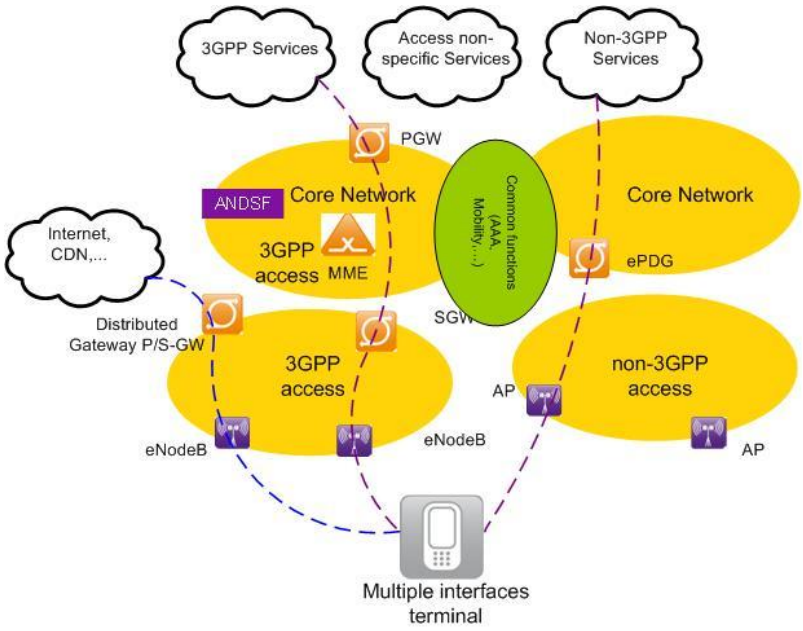


Figure 1: distributed architecture

Scenario 3 of MEVICO IR1.3 [2] is a distribution pushed at its limit. This scenario can also be referred as a flat architecture. A flat architecture as opposed to the hierarchical architecture presents fewer levels or fewer node types in the functional network architecture either in the user plane only, in the control plane only or both in the user and control planes. Figure 2 below illustrates a flat architecture where S/P-GW functions are split between centralized and flat entities. A possible split would be to implement data path management functions in the flat gateways (e.g. IP address allocation, routing) and control plane functions in light gateways (i.e. that are not flattened). For instance, packet marking may stay centralized in the core network. The section [Annex 9.2] discusses the functions which could be distributed/flattened. However, this document will not definitely state which functions should be distributed/flattened and which function should remain centralized. It should be clear that, the answers will be given by the result provided by the demonstrators.

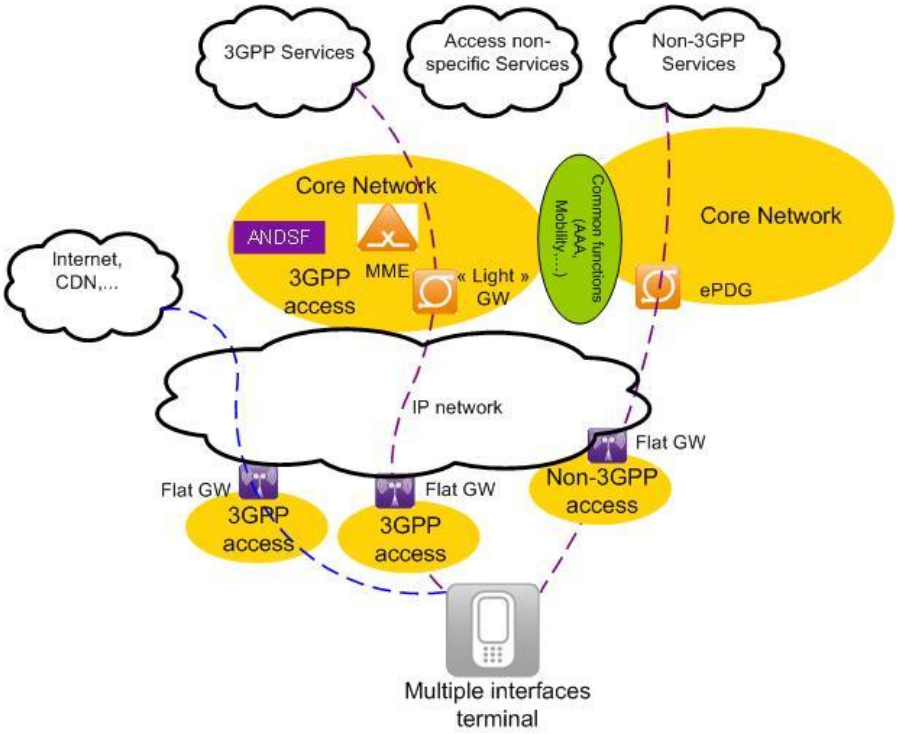


Figure 2: flat user plane architecture

4. Functions for Smart Traffic Steering in Multiple Access Context

Smart traffic steering is obviously related to the selection of the best path according various criteria. It includes also all functions required to apply the decision and related functions such as security or QoS management. This section lists the functions that may be impacted by distribution or multiple accesses feature.

4.1 Naming and Addressing Functions

The UE is generally characterized with an identifier/locator couple:

- The identifier, the identifier is permanent and is meant to uniquely identified the UE;
- The locator is dynamic; it depends on the current location of the UE within the network; it is used to route data towards/from the UE.

In the current multi-access context, different access network technologies coexist and apply dissimilar principles. Thus, different identifiers may be found at different network levels: MAC addresses, IP addresses, DNS names, SIP URIs (Public User Identity in IMS network), IMSI (International Mobile Subscriber Identity) and and IMEI (International Mobile Equipment Identity) in GSM/3G, public key and so on. In some architectures, these different identifiers may also be used to locate the UE (e.g., IP address, MAC address) thus leading to a naming/addressing separation issue when dealing with inter-access mobility (section 2.6)

Long term multi-access architectures should consequently globally rework the identifier/locator couple, so that the identifier stays unique per UE independently of the access network topology and the locator provides network topology information whatever the access technology.

4.2 Multiple Interfaces Terminal Configuration

A multihomed node can be simultaneously connected to several interfaces (physical and/or virtual); e.g. wired Ethernet LAN, a IEEE 802.11 LAN, a 3G cell network, one or multiple VPN connections. Current smartphones typically have multiple access network interfaces that may be simultaneously connected to networks.

In such an environment, a multihomed host processing attachment (or reattachment in idle mode) receives node configuration information from each of its access networks, through various mechanisms such as DHCP, PPP or IPv6 router advertisements. Some received configuration objects are specific to an interface such as the IP address and the link prefix. However, some others are typically considered as being global to the node, such as the routing information (e.g. default gateway), DNS servers IP addresses and access selection policies.

When the received node-level configuration objects have different values for each access network, such as different DNS servers IP addresses, different default gateways or different access selection policies, the node has to decide which ones to use or how to combine them.

4.3 Selection

4.3.1 Access Selection

In a multiple access context, the node may handle simultaneously multiple domains with disparate characteristics, especially when supporting multiple access technologies. Selection is simple if the application is restricted to one specific provisioning domain: the application must start on the interface if available, otherwise the application does not start. However, if the application can be run on several interfaces, a smart selection function is required. Selection can be made upon various criteria, such as in [5]:

- Preferences provided by the user,
- Policies provided by network operator,
- Quality of the radio link,
- Network resource considerations (e.g. available QoS, IP connectivity check...),
- The application QoS requirements in order to map applications to the best interface
- Security considerations (supported authentication schemes, security level, application requirements)

4.3.2 Gateway Selection

The Gateway selection function has an important role in the distributed architecture because there are a large number of Gateway elements in the network. In practice this could mean that distributed Gateways have to be cheap equipment with limited capacity. This has impact on the GW selection procedure as well.

In current 3GPP networks the Gateway selections is based mainly on the target network, suitable location and possibly load balancing issues. In the distributed architecture the Gateway selection algorithm will be much more complicated since additional criteria have an impact. For instance, the following criteria may come into play. in addition to usual location and load balancing considerations:

- GW capacity
- UE mobility requirements
- Application requirements
- Roaming user
- Location of CDN/Cache
- Subscription data
- Device type
- Cell type
- Access type

Gateway selection during a possible Gateway relocation procedure may still have additional requirements. In order to take full advantage of the distributed architecture, the goal of the Gateway selection algorithm should be to provide for each mobile user, application or flow, the required quality of service with optimized network resources allocation.

Gateway selection problem becomes harder when centralized and distributed gateways co-exist.Typically, there might be cases when distributed architecture does not bring any benefits or centralized gateways are more optimal choice especially if the operator already owns centralized gateway elements. In case data packets of the roaming users are always routed to the GRX network: the centralized gateway close to the border gateway element might be an option. Another issue is that centralized gateways might have features (e.g. DPI) that distributed gateways do not have due to economical reasons.

4.3.3 Source Address Selection

The IETF defines default Address Selection specification [10] defines algorithms for source and destination IP address selections. It is mandatory to be implemented in IPv6 nodes and dual-stack nodes.

However, this function becomes crucial and much more complex in multiple access system where dynamic mobility management is a must (section 2.3). When using anchored based IP mobility management applications, which do not need mobility must use the local address instead of the anchored

address (Home Address in MIP or Home network prefix for PMIP). Here, the problem is to know the type of address "anchored vs. not anchored", especially with PMIP where the mobile node is not supposed to be aware of the mobility management. The system can expose the type of address to the application which decides, or not, to use an anchored address the system may also deal with selection complexity on behalf to application,

4.4 Reachability Management in a Multi-access Context

The reachability management allows a UE to stay reachable by any correspondent user while moving and changing its network attachment point, even if no session is engaged.

In future perspectives of generalized multi-access architectures, the reachability management may be fully reworked taking into account existing mechanisms, namely the paging function

4.5 Policy Provisioning

The distribution of configuration policies (e.g. address selection, routing, DNS selection...) to end nodes is being discussed both within the IETF and 3GPP (e.g. ANDSF in [7] and some DHCP options [15]). Consistent Policy provisioning must be implemented in multiple access system (e.g. 3GPP and Wi-Fi). Actually, if independent provisioning mechanisms come into play on each access, policies may conflict and bring issues to the multihomed node.

4.6 Mobility Management Functions

4.6.1 Mobility Anchor Discovery

During bootstrapping operation, the mobile node needs to select its mobility anchor. Incoming communication must discover the mobility anchor where the mobile node, to be reached, is attached. The problem is that these operations can be complex in a distributed architecture where mobility anchors are multiplied. So, one of the most significant issues with distribution of mobility anchor, is that a special mechanism is needed to identify the exact mobility anchor that maintains the mobility binding of each mobile node.

4.6.2 Location Update

This function should not be mixed up with the location management specified in cellular mobile networks and directly tied to paging mechanisms. However, it generally consists in informing any network entities or correspondent users of the new mobile UE location leading to either signalling path modification or data packet reforwarding, or both.. For instance, with IMS Service Continuity, the SIP protocol is used both for the UE to maintain its reachability for any new incoming session (by sending SIP REGISTER requests to the registrar server, S-CSCF) and to update the control and transfer planes of an ongoing session, by informing a correspondent node of the new UE location (by sending SIP INVITE requests). Similarly, a Mobile IP Binding Update message between a mobile UE and its mobility agent updates the identifier/locator (i.e. permanent IP home address/local Care Of Address) mapping maintaining the UE reachability and generates a direct data reforwarding towards the new UE location through the mobility agent.

4.6.3 Initiation

This function triggers handover decision function. The handover initiation function may be **controlled by the** UE or the network and may be based on **different layer events,** or triggers, monitored inside the mobile UE:

- either **layer 2 events**, "loss of radio signal" is one of the most common layer 2 events used; they generally require the support of continuous radio scanning mechanisms within the UE;
- **layer 3 events** (e.g. Router Advertisements),
- **applicative events** ;

There is also a need of network introspection. The network should have, for example, the knowledge of all radio accesses information. It may be static information as the description of each antenna localization or dynamic information such as resource availability. Other kind of information like TEHO should be used to optimize the traffic management. The events that trigger mobility management are: QOS/QOE unacceptable value, forecasted throughput above required level, policy rules enforcement (like in ANDSF)…

Protocols defined in IEEE 802.21 [37] enable handover initiation by **the mobile UE but also by the network**, allowing a better network resource control; for instance, information like network capabilities in term of QoS may be taken into account through the MIH Information Service. However, IEEE 802.21 mechanisms restrict the definition of triggers to link events only; now, the choice of a target access for

handover may pertinently consider other kinds of trigger, like application needs, operator and user preferences, depending the user and network environments..

The **distribution of the handover initiation** among several entities requires a control function to establish the link between these entities and the entity(ies) implementing the decision function. In IEEE 802.21, a discovery procedure is defined and the decision function has the possibility to subscribe to any proposed triggers.

4.6.4 Decision

This function is similar to the access selection described in section 4.3.1 and corresponds to the handover decision phase, that principally triggers the handover execution step including the "control plane update" as well as the "transfer plane update". It includes a decision algorithm that selects the best target access the mobile UE has to be reattached to as well as the way the handover decision is provided to handover execution entities (e.g. handover command).

Decision may be based on classification among all available paths. For instance, it may take into account of each network status, like resources availability. For example, Call Admission Control mechanism should be used to check if the move to this eNodeB is realistic. On GW global throughput is a selection criteria. Once again policy rules may be used to select the right path. It supposes the system capable of maintaining a knowledge plan based on information gathered from the initiation function.

Contrary to the handover command protocol, the decision algorithm is considered out of OSI layers. The handover decision may also include the pre-selection of candidate cells in order to trigger a handover preparation phase improving the handover latency. At least, three different models may be adopted:

- Either a **terminal-centric** model: the UE makes a decision based on local measurement, user preferences and potentially static pre-configured operator policies; for instance, an iPhone with multiple access capabilities and implementing an adaptative HTTP streaming would be able to solely detect a network congestion through packet reception monitoring performed at the application layer and decide an inter-access handover;
- Either a **network-assisted** model: the UE makes a decision based on local information (measurement, user preferences, pre-configured operator policies…) with a network assistance; a network entity is then required to provide the UE with additional dynamic information monitored by the network (e.g. network load indication) or with a pre-defined list of appropriate networks; local information need to be updated/provisioned in this network entity.
- Or a full **network-controlled** model: the network selects the access network and enforces the decision to the handover execution function, which can be implemented in the UE or in the network; the network needs to have accurate dynamic information related to local access network availability and conditions.

4.6.5 Execution

The execution function covers transfer plane update, including any function having an impact on the transfer plane during the mobility management, i.e. any function that allows forwarding data flows through target accesses and potentially modifies transferred data (e.g. according to DSCP treatment rules on the target network); it includes any **context reconfiguration** along the data path as well as the **data forwarding** itself and routing tables modified accordingly.

1) Context Reconfiguration

The behavior of network nodes along the data path is updated / configured as the result of a handover procedure (i.e. including handover execution and handover preparation): layer 2, layer 3 (e.g. IP address), layer 4 (e.g. SCTP parameters), application context activation/deactivation, lifetime update; modified DSCP, modified ciphering.

2) Data Forwarding

For each solution, data forwarding may include the following operations:

- Destination media address update at the level of a SIP correspondent node for instance
- Tunnel endpoints setup/deletion ; new anchor setup ; data encapsulation
- Temporary tunnel forwarding (e.g. FMIPv6.)
- Data packet buffering

5. Applicability of Current Solutions in Distributed Architecture

5.1 Intra-3GPP Mobility Management

One of the main drivers for mobile network evolution is the expected huge data traffic growth which put pressure on scalability requirements. Possible means for improving the situation are distributed network architecture and possibility to offload traffic to an offload/transport network at a network node close to UE's point of attachment. The transition from the current 3GPP specified network architecture to a distributed one could introduce remarkable changes even if the basic functionalities, network elements and procedures remained the same. So, this section discusses the intra-3GPP mobility management in distributed/flat architectures. The goal is to figure out how EPC mobility procedures can match flattening requirement.

According to WP1 [2], the distributed architecture has several implementation options. Among them is the distribution of data plane as summarized in section5.1.1,.In this scenario, it is assumed that S- and P-GW elements, as current 3GPP specification, are distributed to the access network but the MME is centralized. It is also envisaged to co-locate S and P-GW with the eNB. However, in this case, collocation of current P/S GW at the eNodeB level could be nonsense from the economical point of view and, thus, a distribution of the GW functions should be studied (section 3). It is also possible that the network has both centralized and distributed GW elements (scenarios 1, 2, 3 from IR 1.3). In section 5.1.2, it is assumed that the QoS is controlled through PCC architecture and that the PCRF and P-CSCF are distributed in addition to the P-GW, S-GW and MME (scenario 2C from IR 1.3).

5.1.1 S/P GW Distributed and MME Centralized

A mapping of EPC entities from centralized architecture to distributed and flat architectures is depicted in the following figure.

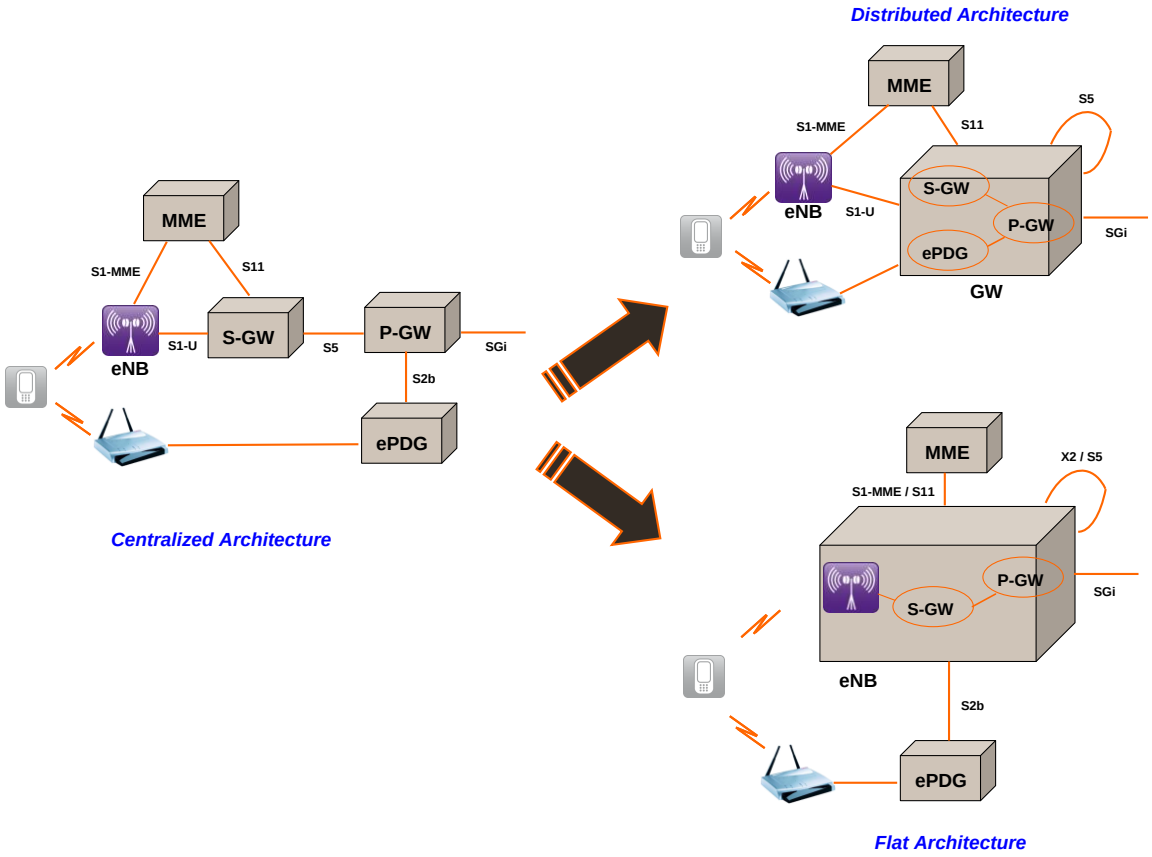


Figure 3: EPC Architecture Evolution.

The distributed and flat architectures lead to delete interfaces between entities (these interfaces become internal within a network node), or to merge interfaces (e;g. S1-MME and S11).
The co-location of several entities within a network node impact more and less functions and procedures as defined currently in 3GPP specifications, such as:

- Merging of the S-GW and P-GW selection functions,
- Handover function and S-GW relocation function.

And the modification of reference points may lead to modify highly a protocol and even to make a protocol obsolete or unsuited (e.g. S1-MME/S11).

5.1.1.1 Interfaces

Distributed architecture has impact on 3GPP specified interfaces. If the P- and S-GW elements are co-located somewhere in the access network (but not co-located with eNBs), the current interfaces and procedures can be used – but some optimizations might be required. One issue is S-GW relocation procedure and visible S5 interface. If standard procedures are used, this might lead into situation where a UE needs two GW elements close to each other (Figure 4). Typically, If standard S-GW relocation procedure is used (i.e. the user remain anchored in the initial P-GW and the S-GW is changed according to its movement), this would require that a given S-GW is linked to a local P-GW and to distant neighboring P-GW ensuring the anchoring, which impacts configuration and transport costs. A solution for this problem is to specify and introduce in 3GPP a P-GW relocation procedure.

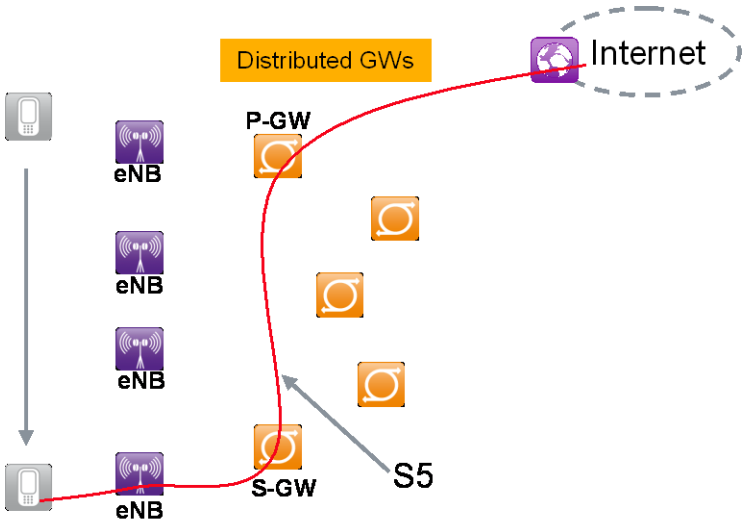


Figure 4: S5 Interface in Distributed Architecture.

If GWs are co-located with eNBs, several 3GPP specified interfaces may become invisible i.e. they might be internal to a certain network element. This kind of collapsed architecture has a major impact on many procedures and functionalities in the network: either they become obsolete or they have to be optimized to the distributed network architecture. It depends on the grouping of functionalities and the level of the distribution which interfaces will become invisible.

Figure 5 presents the flat architecture, which can be seen as an extreme case of distribution: S-GW, P-GW and ePDG elements are co-located with eNB. In this case the only visible interfaces will be S1-C, S11, SGi and S5 in case of S-GW relocation.

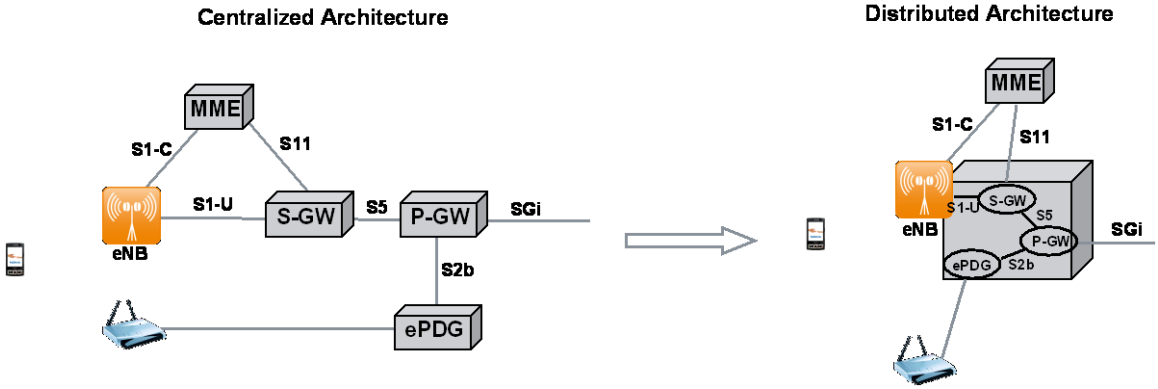


Figure 5: Centralized vs. flat architecture

There are many consequences because of such flat architecture. The most important is maybe the fact that the SGi interface starts straightly from the eNB and native IP packets are routed in the access network. In current 3GPP networks mobility protocols (GTP or PMIPv6) operate below the P-GW element but here, with flat architecture, it is no more the case. If the UE is motionless, pure IP routing is enough to route the user data packets to the right destination (unless a handover is done based on some other reason than mobility). Mobility management in SGi interface means also traffic steering on flow level (or UE IP address level if the UE owns multiple IP addresses); PDN connections and bearers are specified only up to the P-GW.

5.1.1.2 Mobility Management Procedures

The mobility management procedures in the distributed architecture can be categorized into three classes:

1. Current procedures that are used as such.
2. Current procedures that require modifications and optimizations. The optimization of the mobility management procedures is essential because in distributed architecture the signalling traffic should not be proportional to the traffic flows (IR2.1 requirement).
3. Totally new procedures.

In this section the most common 3GPP specified mobility management procedures are introduced and the suitability of them in the distributed architecture is discussed. The purpose is to give pointers to the steps where optimization is required.

5.1.1.2.1 Attach

A UE has to register itself to the network in order to access services. The registration is done during an attach procedure, at the same time an always-on IP connectivity for the UE is enabled by establishing a default bearer. The attach procedure can be divided into the following parts:

1. An Attach request message is sent from the UE to the core network. When the MME receives the message, it identifies and authenticates the user.
2. After the authentication is executed successfully the MME contacts the HSS and fetches the subscription data.

If S/P-GW is not collocated with eNB, the MME performs the GW selection procedure according criteria listed in section 4.3.2.

3. Based on the subscription information the MME starts the default bearer activation procedure. If dynamic IP address allocation is in use, the PDN-GW allocates the UE IP address.
4. The MME forwards this information to the UE in an attach accept message.

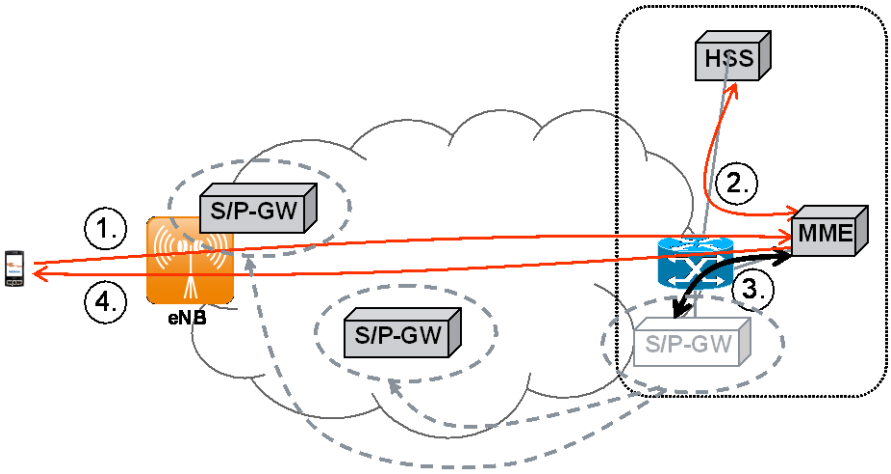


Figure 6: Attach Procedure.

Attach procedure is presented in Figure 6. It presents the steps 1-4 of the standard attach procedure and visualizes the movement of the GWs from core site either to the access network or to the same element as eNB.

Optimization issues:

- Signaling traffic between MME and GWs
- Default bearer activation procedure. The role of default bearer when GW is co-located with eNB. Because of invisible interfaces the only meaning of this might be the IP address allocation.

5.1.1.2.2 Handover

A Handover is a process of transferring an ongoing data session uninterrupted from one eNB to another.

The steps are the following (apart from the very 1st step which is the detection of the need based on UE measurement report):

1. The source eNB makes the handover decision. It asks the target eNB to reserve the needed resources by sending a handover request message.
2. The source eNB sends a handover command to the UE.
3. The UE confirms the handover and connects to the new eNB.
4. The path switch procedure reconfigures the GTP tunnel and updates the new location to the core network elements.

The handover procedure is presented in Figure 7. This picture gives the steps 1 to 4 of the standard handover procedure and visualizes the movement of the GWs between a centralized architecture and a distributed one.

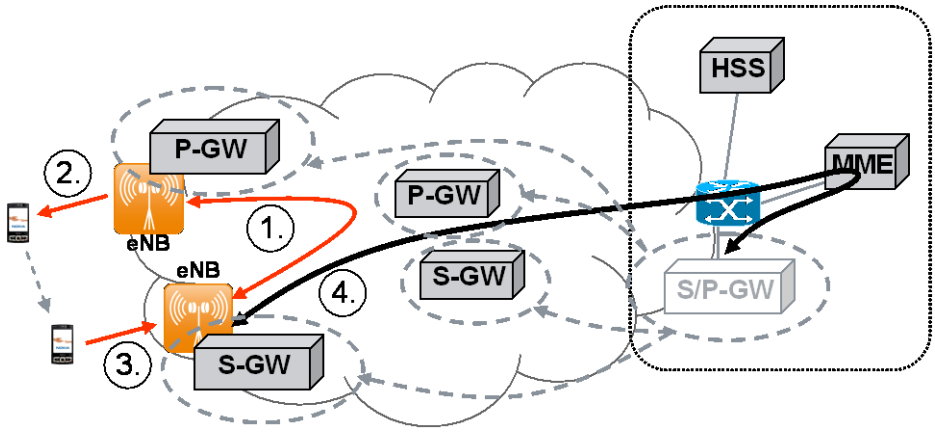


Figure 7: inter-eNodeB handover management.

The following identifies rooms for optimization for the handover management in distributed architecture:

- Path switch procedure. If S1 interface is virtual (SGW colocated with the eNodeB), there is no GTP-U tunnel to come into play.
- If the GWs are in the access network, the S-GW relocation procedure might lead to an unoptimized solution where the UE has two GW elements possibly very close to each other. For these two cases, an inter P-GW relocation mechanism could be more efficient.
- the seamless mobility is not required for motionless UE (e.g. fixed sensors)

5.1.1.2.3 Paging

When a data packet arrives in the network and is addressed to an idle mode UE, paging is required to reach this UE. The procedure is presented in Figure 8.

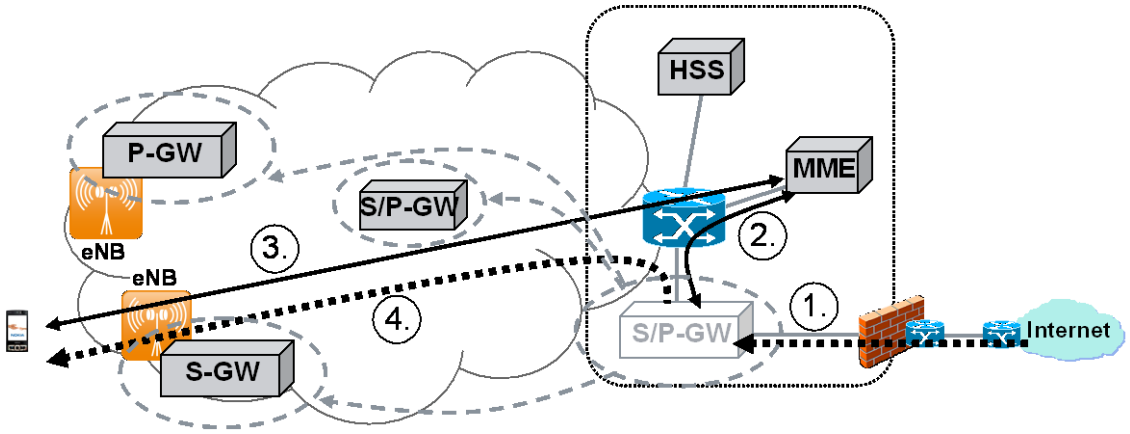


Figure 8: Paging procedure.

The following steps are included in the paging procedure:

1. Downlink data packet arrives to the S-GW.
2. The S-GW sends a paging notification to the MME.
3. If the UE is registered in the MME, the MME sends a Paging message to each eNodeB belonging to the tracking area(s) in which the UE is registered.The step is described in detail in TS 36.300 and TS 36.413. The UE responds with a service request procedure.
4. Downlink data packets can be routed to the UE.

Optimization issues:

- Paging procedure could be optimized for permanently motionless UEs (e.g. static sensor).
- When downlink data packet arrives to the S-GW which is in the access network or co-located with eNodeB, it is not optimal if the centralized MME still does the paging which will page that exact eNodeB.

5.1.1.3 EPS Bearer Model

An EPS bearer uniquely identifies traffic flows that receive a common QoS treatment between a UE and a PDN GW. A default bearer is activated during an attach procedure and it enables always on IP connectivity. In addition to default bearer one or more dedicated bearers may be activated. Traffic flow templates (TFT) in the UE and PDN-GW are used for mapping traffic to an EPS bearer. This is presented in Figure 9.

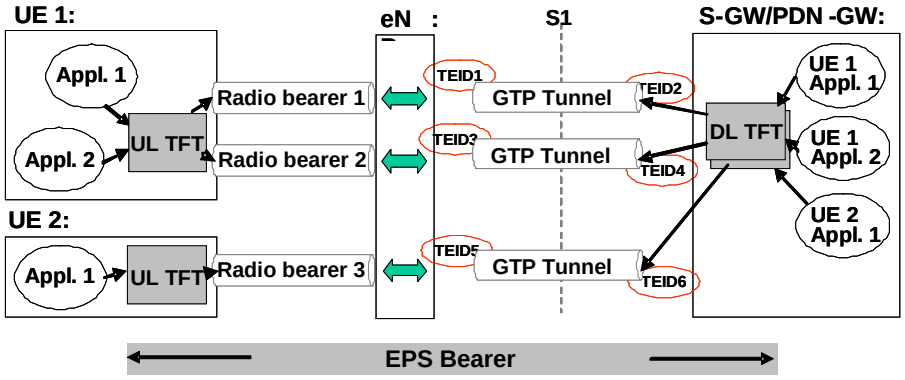


Figure 9: EPS Bearer Model (distributed architecture).

It has to be noticed that in 3GPP specification the QoS solution is strictly tied to the EPS bearers: GTP tunneling endpoint identifier (TEID) is used to separate the bearers of a certain user from each other. In distributed architecture this model has not the same meaning than in centralized architecture due to the fact that several interfaces below PDN-GW (S1/S2/S5) may become invisible, only the radio bearers are

not affected. In this case, the EPS bearer fits exactly to the EPS bearer for PMIP-based S5/S8 (traffic flow between UE and S-GW) as defined currently in 3GPP specifications. Therefore the role of QoS in distributed architecture has to be rethought. One option could be to utilize IETF specified differentiated services architecture.

With the flat architecture, the EPS bearer is limited to the radio bearer after the attachment to the network and the S1 bearer (GTP tunnel) does not exist in this case. Hence, the QoS management should be reviewed.

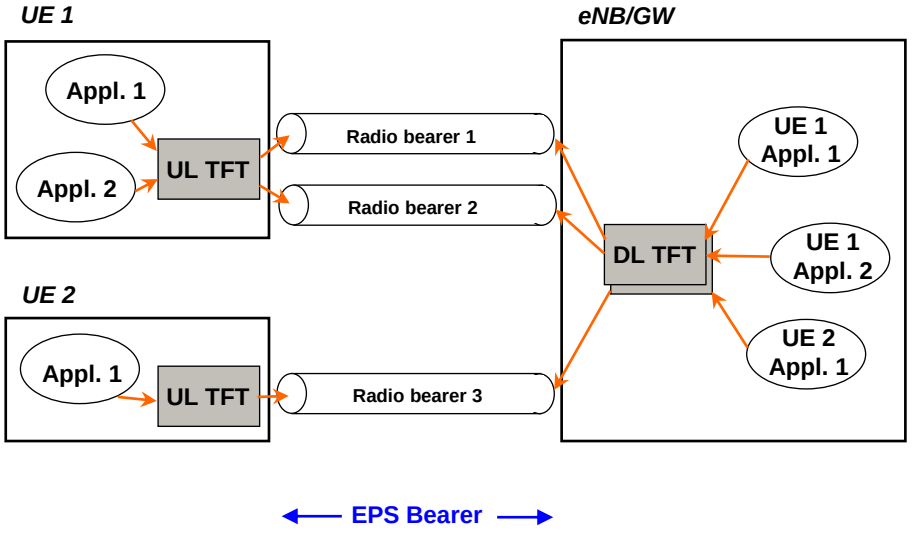


Figure 10: EPS Bearer Model (flat architecture).

On the other hand the concept of PDN connection defined as "an association between a UE represented by one IPv4 address and/or one IPv6 prefix and a PDN represented by an APN" is still valid. Access point name (APN) is a contact point to the external networks and therefore the UE IP address can be allocated by the mobile network operator or it might be received e.g. from a corporate network.

5.1.2 S/P GW, MME, PCC and IMS Nodes are Distributed

Scenario 2c in WP1 [2] suggests to distribute PCC and IMS nodes in addition to S/P GW and MME. In that case, the probability that a user changes, during mobility, of P-GW, S-GW, MME, PCC (PCRF) node and IMS node is high. The last sections have highlighted the need for inter P-GW relocation mechanism. Solutions that come to mind for this inter P-GW relocation can be MIP-based (RFC 3344) or SIP-based (3GPP TS 23.237). In that case, the necessary phases for inter P-GW mobility execution are (figures below):

- Phase 1: authentication/registration to the network and to IMS through the P-GW2. During this phase, the MN is allocated with a new IP address (@IP2), discovers P-CSCF2 and updates its SIP signaling route in the P-CSCF2 and the S-CSCF (SIP Register).
- Phase 2: the MN establishes a SIP dialog though GW2 towards P-CSCF2. This dialog aims at establishing a context in the P-CSCF2 and at informing the P-CSCF2 about the description of the service (SDP) willing to be established through P-GW2. After dialog establishment, policy rules will be enforced by from P-CSCF2 to the P-GW2 that will establish a bearer.
- Phase 3: depending on the mobility execution, the MN IP address will be updated in the network or in the Correspondent Node (figures below). This allows the traffic to go through the P-GW2 and the bearer2.

These phases occur each time the MN mobility induces a P-GW change, in a break before make manner. Indeed, as the P-GWs are distributed, it is very likely that they offer the same type of a physical access (e.g. through the e-NB). Therefore, to execute phase 1, 2 and 3 the MN should have broken the link with the P-GW1. As phases 1, 2, 3 take time, the handover performance will be impacted. Therefore, a more optimal solution to handle mobility in such case has to be defined. Such solution may be found in [8]. Indeed by concatenating the P/S GW, MME, PCRF and P-CSCF functions in the same equipment (the UFA-GW) and simplifying them, it becomes easier to perform a handover with a limited delay, thanks to a proactive step and a network controlled handover execution.

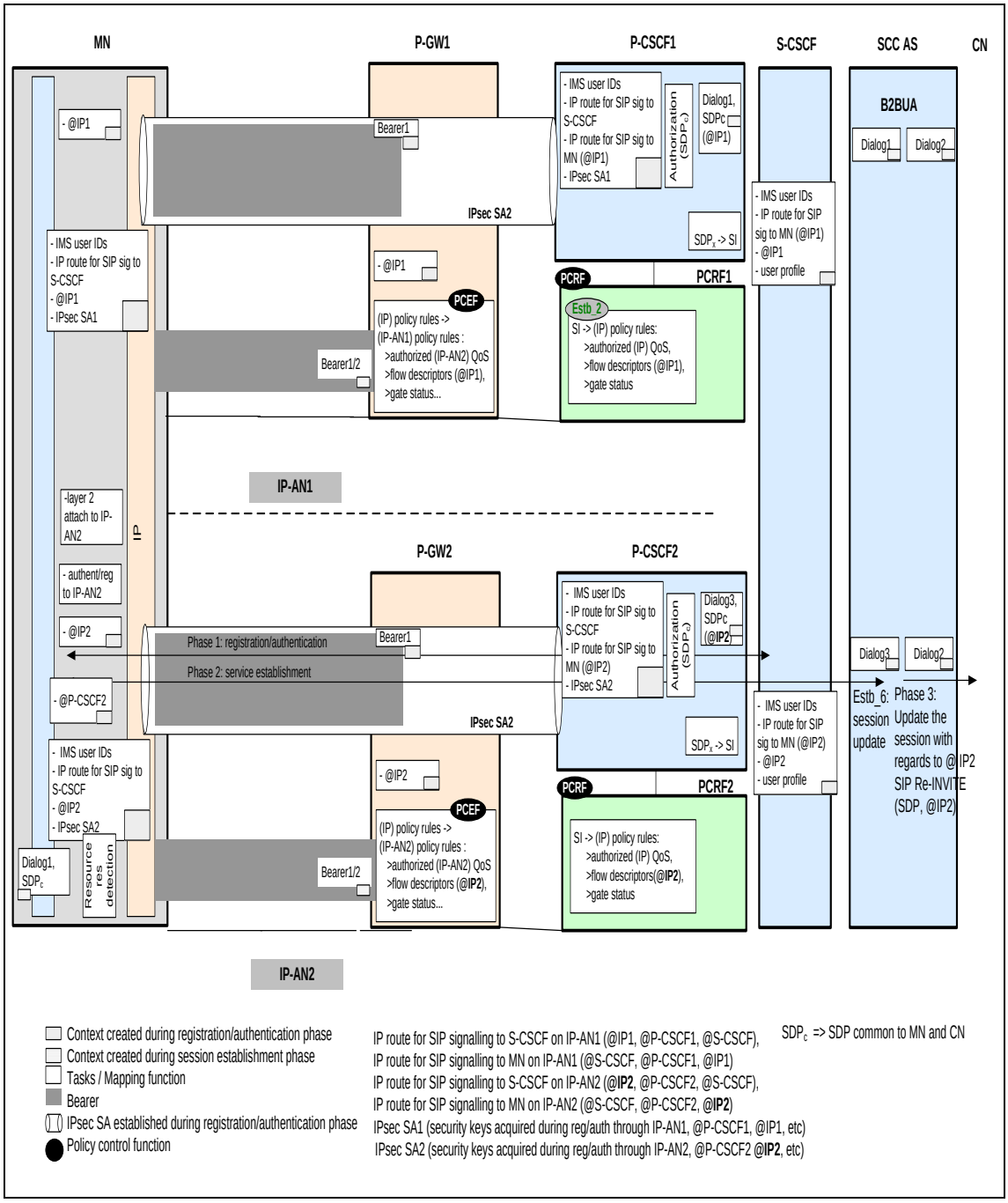


Figure 11: inter P-GW mobility using ISC solution (3GPP TS 23.237).

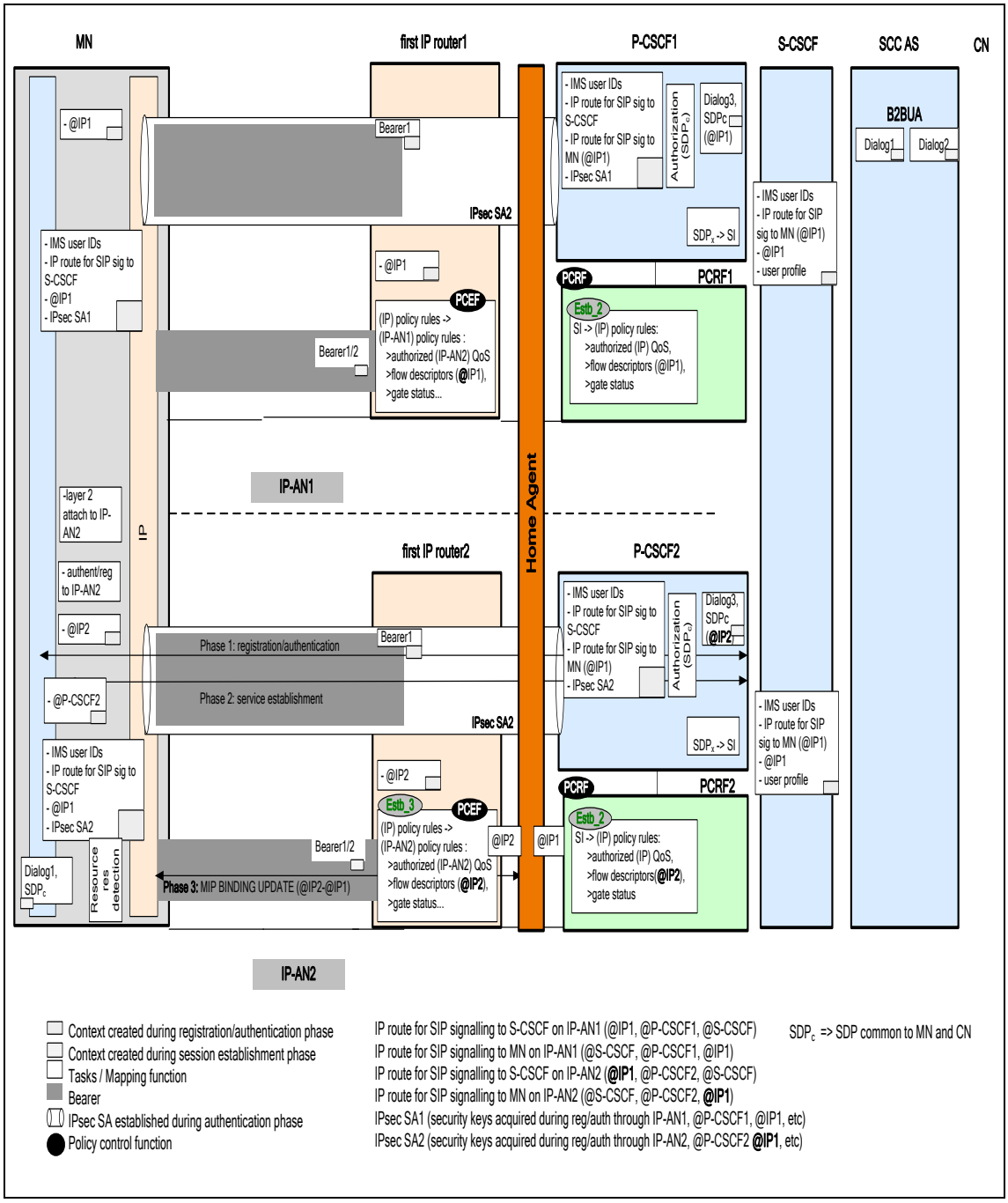


Figure 12: inter P-GW mobility using MIP solution.

5.2 IETF Based Solutions

5.2.1 IP Anchoring Based Mobility Management

The IETF working group MEXT (Mobile IPv6 EXTensions) has been rechartered to work on distributed mobility management [48]. The working group will work on setting up Mobile IPv6 networks so that traffic is distributed in an optimal way. Even if the working group has not adopted a document yet, several drafts are on the table. These documents describe the problem, the architecture scenarios and solutions. So, this section gives a summary of this work, knowing that this work can evolve in a close future.

The architecture scenarios are described in [16]. This document explores different ways for distribution of mobility functions in the Ip mobile architecture. Basically this draft distinguish the fully distributed approach from the partial distribution, principles of dynamic mobility management are also covered.

5.2.1.1 Fully Distributed Architecture

In a fully distributed approach, the distribution scheme is applied to both control and data planes. The Figure 13 gives a possible deployment of MIP, or PMIP, in a fully distributed architecture. Here, each access router implements a mobility anchor (MA), i.e. HA or LMA.

Note that, according to [16], less flat deployment is also possible.

If an MN attaches to an MA and initiates an IP communication with a CN, the traffic is anchored to this MA. When performing a handover to another MA, regular MIP, or PMIP, operations come into play, e.g. the UE sends a binding update to its HA (i.e. the previous access router), which updates its routing state. The previous access router can then forward packets to the new location of the UE. Location updates to the control function can be initiated by the UE (a la MIP) or controlled by the network (a la PMIP).

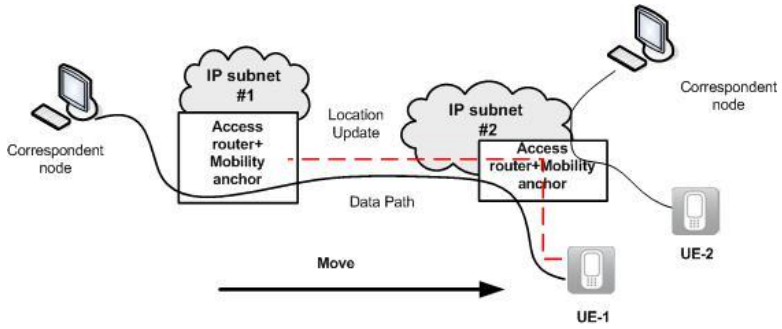


Figure 13: fully distributed mobility management.

The UE can potentially be attached to more than one mobility anchor. So, one of the most significant issues of the distributed control plane (e.g., distributed HAs), is that incoming communication requires a special mechanism to identify the exact mobility anchor that maintains the mobility binding for the targeted UE.

5.2.1.2 Partially Distributed Architecture

Mobile IP or Proxy Mobile IP combine the control and data planes, which means that all signaling packets and data packets follow the same path and go through the HA or local mobility anchor. However, considering that the volume of data traffic is much higher than that of control traffic, it should be possible to achieve effective traffic distribution by separating the control and data planes and applying a distributed architecture only to the data plane.

A partially distributed mobility management scenario is depicted in Figure 14. The architecture supports multiple mobility anchors (MA) in charge of the routing function. In Figure 14, the mobility anchor is confined with the access router, but according to [16], less flat architecture is also possible. So, in the example of Figure 14, when UE-1 attaches to MA1 and initiates an IP communication with a CN, the traffic will be anchored to MA1. If UE-1 attaches to MA1 and initiates an IP communication with a CN, the traffic will be anchored to MA1.

When UE-1 performs a handover to MA2 (Figure 14/step 1), the UE updates its location up to the centralized control function (Figure 14/step 2). Then, the control function updates the routing state of MA1 and MA2 in order to forward packets to the new location (Figure 14/step 3). This approach is to be compared to centralized mobility management reminded in Figure 15 (more details can be found in [4]).

The location update may also be initiated by the network. An example of separating control plane and data plane using PMIP is proposed in [18]. In this document, the data plane of PMIP is distributed while the control plane remains centralized.

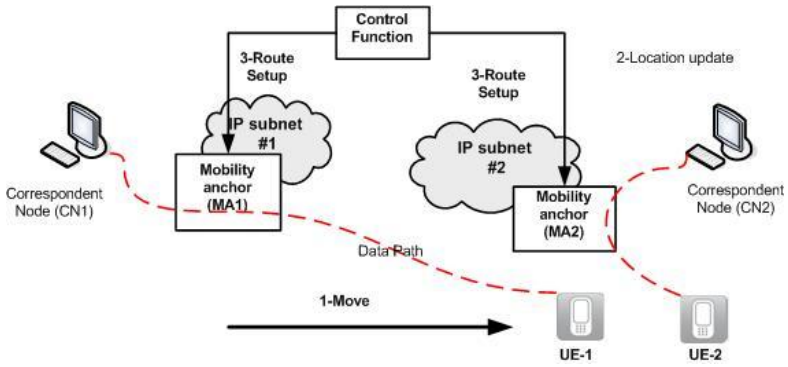


Figure 14: partially distributed mobility management.

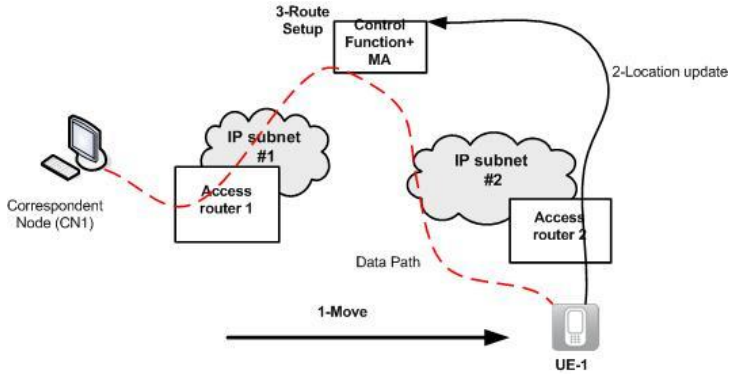


Figure 15: centralized mobility management.

Obviously, because of the planes separation, current MIP and PMIP protocols cannot apply without modification. If the location update mechanism is unmodified, a new piece of protocol is required on the interface between the control function and the mobility anchor.

5.2.1.3 Dynamic Mobility Management

As explained in section 2.3, one of the purposes of dynamic mobility management is to provide mobility support only to those applications and to those MNs that really need it.

Some applications can survive to an IP address change, i.e. applications can manage IP mobility. It is thus inefficient to play IP mobility management for that application, i.e. it useless to maintain a mobility context (i.e. mobility binding) for that IP flow, it sub-optimal to anchor the traffic of that application to the mobility anchor. One scenario to avoid providing mobility support to applications not needing mobility support is to rely on source address selection. The IP stack of the mobile node can potentially deal with, at least two IP addresses [4]: the anchored address (e.g. the Home address with Mobile IP [12]) and the local address (e.g. the Care-of-address with Mobile IP [12]), which is a non-anchored address. The idea is simply to use the non-anchored address as source address for mobility capable applications and the anchored address for applications needing the IP mobility support [19]. As a consequence, the type of address should be exposed to the application making the address selection. However, it is sometimes difficult for the IP stack to know if an IP address is anchored or not, especially with Proxy mobile IPv6 [8] where the mobile node obtains the Home Network Prefix in the same manner that a local address.

Another purpose of dynamic mobility management is to avoid providing mobility support for IP session beginning and ending while the mobile node remains attached to the same point of attachment (section 2.3). One scenario providing such a dynamic mobility management is depicted on Figure 16. Here, each access router implements the mobile anchor function. This is a basic deployment, maybe not optimal but without requiring modifications of current anchored based IP mobility protocols (MIP/PMIP).

Consider a MN attached to the access router AR1 (Figure 16/step 1). MN acquires an IP address (IP1) from the local access router (AR1). If the MN initiates a flow (flow#1), flow#1 uses IP1 and is routed in a standard way as long as the MN remain attached to AR1.

If the MN performs handover to a new access router, AR2 (Figure 16/step 2):

- The MN obtains another IP address (IP2) in the new IP network
- flow#1 remains anchored to AR1, which now plays the role of HA. Data are tunnelled between AR1/HA1 and the MN , or between the AR1 and AR2 if using PMIP.

If the MN initiates a new flow (flow#2) (Figure 16/step 3):

- flow#2 uses IP2 and is routed in a standard way as long as the MN remain attached to AR2.

In other words, the MN plays with an IP flow anchored to AR1 (flow#1 initiated while attached to AR1) and an IP flow via AR2, flow#2, which uses the address obtained from AR2 (i.e. local address).

If the MN performs handover to a new access router, AR3 (not drawn in the picture), while maintaining both communications, two mobility anchors will come into play: AR1/HA1 anchors flow#1, initiated via AR1, and AR2/HA2 which anchors flow#2, initiated via AR2.

In other words, both flows are anchored to two different HAs (flow#1 on AR1/HA1 and flow#2 AR2/HA2). The MN can use several home addresses:

- Flow#1 served by HA1/AR1 uses IP1
- Flow#2 served by HA2/AR2 uses IP2

If one IP flow stops, mobility context (binding) and resources (tunnel, routing state) are released (Figure 16/step 4).

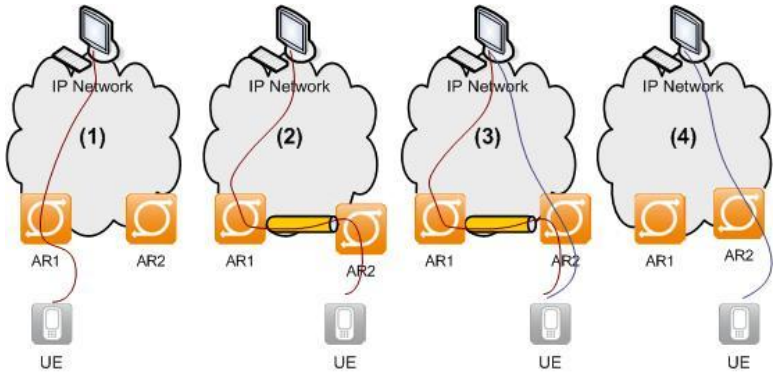


Figure 16: Dynamic mobility anchoring.

An example of dynamic mobility management using PMIP and MIP are proposed in [17] and [18] respectively.

5.2.1.4 Principle of Routing optimization

IP anchoring based mobility management such as PMIPv6 or DSMIPv6 are both standardized at the IETF, respectively RFC 5213 and RFC 5555, and supported in 3GPP architecture. In a PMIP domain, it is specified that bearers are activated only in the access network on the radio and S1 interfaces [7]. Intra-EPC forwarding, as well as inter-systems service continuity, can be ensured over IP legs through MIP/PMIP specific routing procedures.

Considering the operation of PMIP in a centralized architecture, e.g., the P-GW located in a national POP and S-GWs distributed in regional/local POPs (IR1.3 scenario 1B [2]), the S-GW plays the role of MAG and the P-GW the role of LMA. Each UE is associated to its first IP router, which is a MAG (S-GW). IP addresses are assigned by the LMA where they are topologically anchored. Data coming from outside the PMIP domain will be routed naturally towards the LMA and then a PMIP-specific procedure will deliver the data to the destination UE.

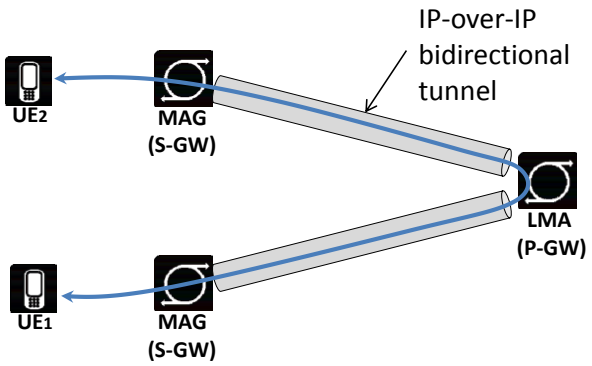


Figure 17: Data path between UE1 and UE2 in a PMIP domain.

Within the PMIP domain, data are transferred in bidirectional IP-over-IP tunnels established between the LMA and the MAGs through S5/S8 interfaces (see Figure 17). PMIP related signalization rely on the S5/S8 interfaces but are not tunnelled. PMIP deployment has been specified for a wide range of access networks. For instance, the ePDG in a Wi-Fi access network as well as the ASN-GW in a WiMAX access network may play the role of MAG in a PMIP domain.

In such a context there are two main subjects of optimization: the first (O1) is on the indirection of the data path that has an impact on the communication performance (see Section 2.5). The second (O2) is on the centralized anchor (the LMA), which represents a single point of failure and a point of concentration of all data flows.

The constraints of the O2 problem may be relaxed by distributing the traffic load through distributed P-GWs; for instance by confining P-GWs with S-GWs in the access network or in local POP (IR1.3/scenarios 2C, 3 [2]). In such architecture, MIP and PMIP operations may not be affected as with the fully distributed approach described in section 5.2.1.1.

Obviously, with distribution, the number of clients anchored at an LMA should decrease and so the number of handled flows. At the attachment, the UE may be anchored at the P-GW collocated with its S-GW. The Figure 18 depicts the data path for an inter-UE communication (the mobility anchor is collocated with the S/P-GW). Note, that the S5/S8 interfaces [7] are hidden and that the LMA (P-GW) is on the data path towards the destination UE2.

For a moving UE however, the S-GW may change (as depicted on Figure 19). The on-going session of UE1 undergo an indirection as it remains topologically anchored on the previous LMA. In such a case, a P-GW relocation is a possible solution to keep the P-GW as close as possible of moving UEs. So far, such an approach is only possible when the data session is finished as it may require an IP re-assignement. Therefore the problem O1 remains in a distributed architecture and different solution(s) should be proposed to achieve optimized data paths.

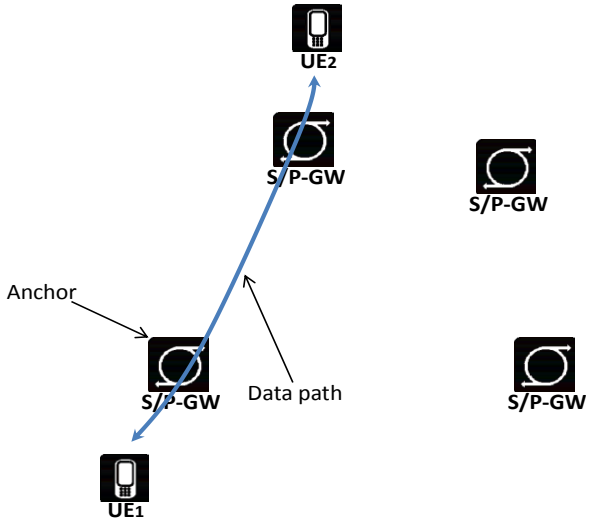


Figure 18: Data Path in a PMIP Domain for a Non-Moving UE

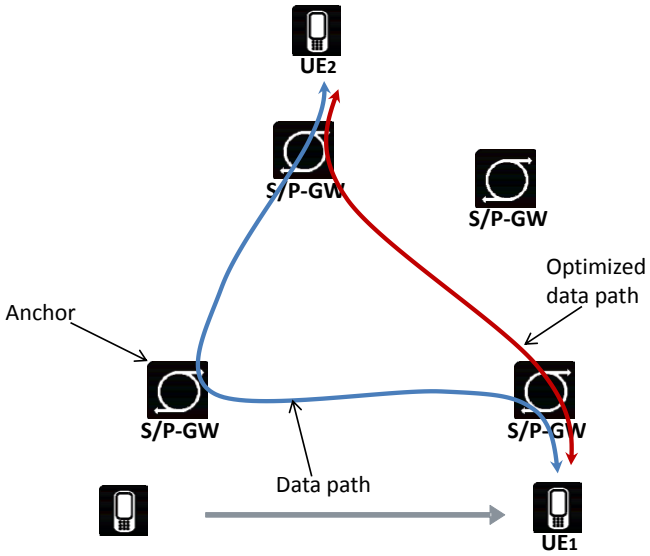


Figure 19: Non Optimized and Optimized Data Path in a PMIP Domain for a Moving UE.

As depicted on Figure 19, the data path undergoes an indirection (the blue arrow) considering the end-to-end data shortest path (the red arrow). One solution to address this issue is to rely on intermediate anchors (IAs) deployed in the domain between S-GWs and P-GWs. The basic idea is to allow the UE1's LMA, which remains the anchoring point of signalling messages, to delegates the role of data anchor to the most appropriate IA(s) to optimize the data traffic, at least temporarily. The resulting data path may pass through one IA or through a chain of IAs without having to cut off on-going communications.

Data anchoring is a subset feature of the LMA, which also (1) assigns and releases IPv6 prefixes (Home Network Prefixes "HNPs"), (2) advertises the assigned prefixes towards the Internet, and (3) store the current points of attachment (MAGs) of all UEs under is responsibility through the Proxy Binding Updates (PBUs) and Proxy Binding Acknowledgments (PBAs) signalling messages. Hence, the IA function is a subset feature of the LMA that becomes mobile, i.e., the resulting data paths can be adapted to the UE mobility and the corresponding node as well.

In a distributed architecture several P-GWs deployed in different (local/regional) POPs may share the same APN. At the first association, the UE will be associated to one P-GW in the current POP. The UE moving between different POPs will have its communications anchored to the first starting POP. In this scenario, the solution will be able to select the most appropriate P-GW (in the POP where the UE is currently attached) as IA to anchor the UE data traffic. Without loss of generality, the IA functionality may be deployed on any type of entity or even as a standalone server.

In this solution the LMA remains signalling anchor for two main reasons: the first is because it advertises the IPv6 prefixes towards neighboring routers. It means that traffic coming from the Internet first arrives at the LMA. It is then important that the LMA remains aware of the current status of assigned prefixes through PBUs and PBAs. The LMA is able to releases the assigned IPv6 prefixes because it can detect the UE's disconnection. The second reason is that it is able to control the IAs' selection. This point is important as it can help to prevent routing loops.

5.2.2 Anchorless Mobility Management

NMIP [25] is designed as a light mechanism to provide a connection mobility and migration in area where mobility protocols such as IP Mobility Support for IPv4 [RFC3344] or ipv6 [RFC3775] are not desirable or applicable. NMIP is an end to end protocol and it does not require mobility agent such as a Foreign Agent (FA) and Home Agent (HA) to be present in the network to provide session. Both UE and its correspondent need to be NMIP compliant.

In the NMIP protocol when the UE has to change its IP address, it notifies its peers by sending it new address. This is done on a connection basis, in order to keep the connection update with their current IP address of the correspondent node.

A TCP connection between two hosts is maintained in each host using a lookup key that depends on the source and destination IP address of its end-point. Whenever a host decides to change it's current IP address for a connection, it sends to the other host an order to "rehash" the connection with the new

address prior to pursue activity. Nat and firewall traversal have to be take into account. Figure 20 depicts the NMIP anchorless mobility management.

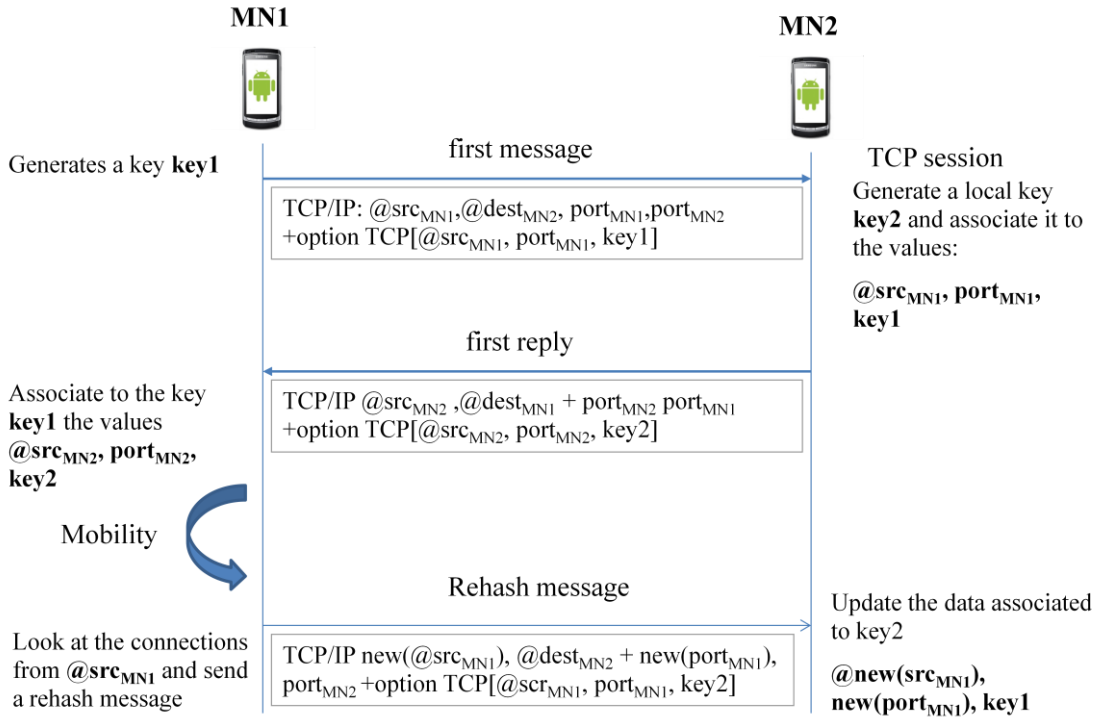


Figure 20: NMIP Anchorless Mobility Management Overview.

5.2.3 SIP and SCTP Deployments in New Flat and Distributed Architectures

The distribution of SIP based architecture is addressed in documents [20][21] where the new mobile network architecture called UFA (Ultra Flat Architecture).

UFA is based on **SIP** to provide service control for all services during service access and mobility procedures. Thus, non-SIP native services are extended to be controlled by SIP protocol. In UFA, a specific attention has been given for non-SIP native applications transported over **SCTP** on the user plane. Controlling non-SIP native services by SIP has required an interaction between SIP protocol, these services and SCTP in the Mobile Node (MN) and the Correspondent Node (CN).

UFA is constituted of 6 network nodes: the e-NB, the I-CSCF (IMS proxy node), the S-CSCF (IMS proxy node), the HSS and two new nodes, that are:

- UFA Gateway (UFA_GW): the UFA_GW is the main node in UFA. It gathers the classical LTE/EPC node functions (MME, S-GW, P-GW), policy control (PCC) functions [23], P-CSCF functions, SCC AS functions [22] [24] and new introduced functions that control the service access and mobility procedures. This means that the UFA_GW controls the session and offers IP connectivity (UFA_GW is the first IP router) to users. **It has to be noted that the UFA_GW is not just a co-location of functions and equipments, but an optimal combinaison of functions in unique equipment. Thus, the use of the term "flat" here is not the same as the one defined in section 3 i.e. with the UFA_GW we reduce the number of network levels but we don't necessarily include them with the e-NB level.**

- SIPcrossSCTP Gateway (SxS_GW): this node handles, for non-SIP native services, the cases where the interaction between SIP protocol and non-SIP native services is not supported in the CN.

5.2.3.1 UFA Nodes and Control Functions

Most of the UFA control functions are within the network, specifically in the UFA_GW. The MN and the CN act as slaves to the network intelligence.
We describe hereafter the UFA_GW, emphasizing on its control functions. We also detail the other UFA nodes on the control and transfer planes (Figure 21).

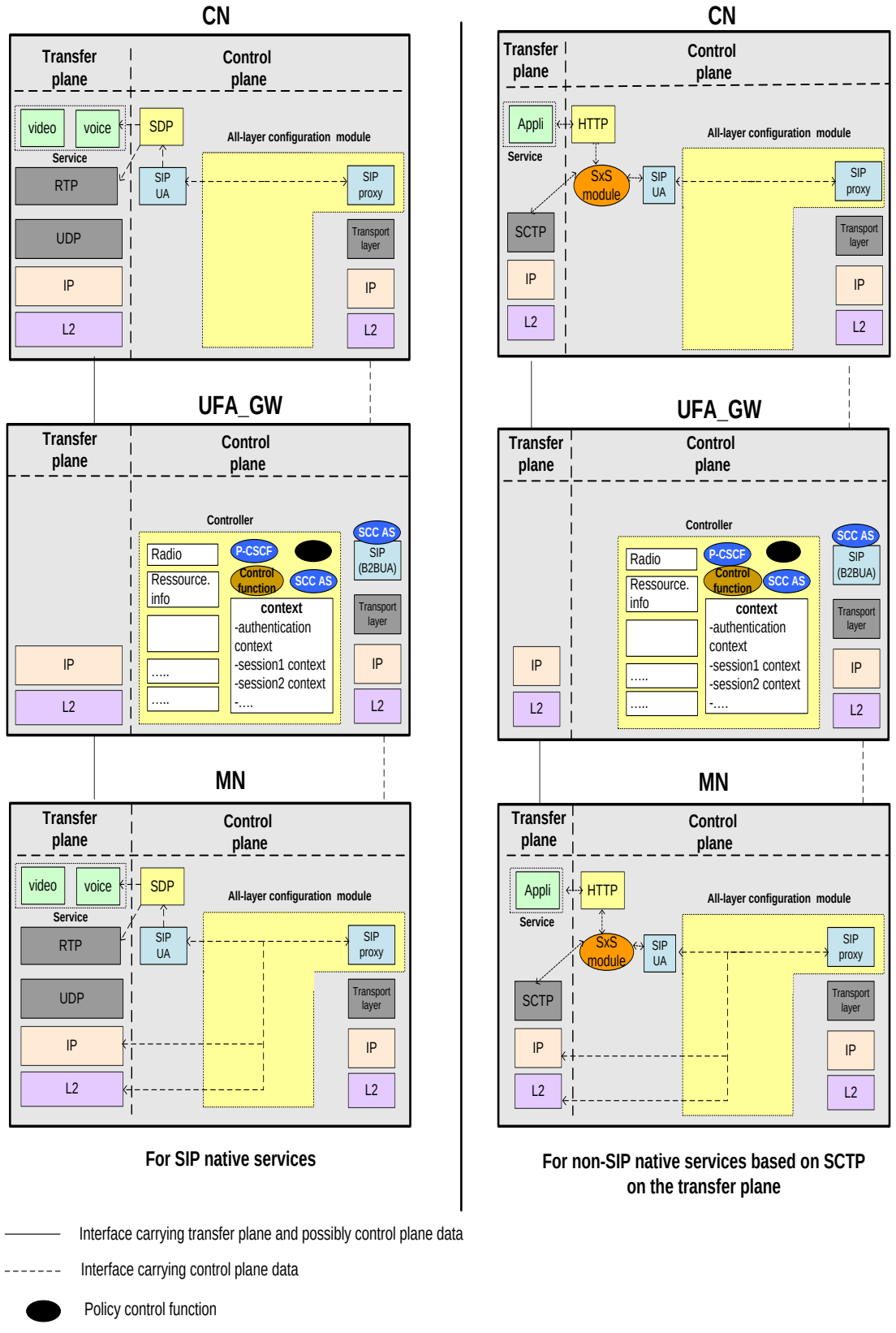


Figure 21: UFA Control and Transfer Planes.

UFA Gateway

The UFA Gateway (UFA_GW) control functions are within a controller module. This module generates decisions regarding the service access and mobility procedures. Decisions are enforced by acting on SIP messages, thanks to the SIP Back-to-Back User Agent (B2BUA) (see Figure 21).

• The **Controller** contains the SCC AS function, the IMS functions, the policy control functions, and other control functions adding more intelligence to the UFA_GW. These control functions enable to:

– Decide on mobility from the current UFA_GW to a target UFA_GW in case of coverage loss, current overload or better conditions detected on the target UFA_GW. The interaction with the SCC AS functions enables to decide whether the handover decision is compliant with the the home operator policies.

– During service establishment phase or mobility procedure, determine:

* The **service configuration** for SIP native services, or the **SCTP layer configuration** for non-SIP native services transported over SCTP, the CN should have:

- The **service configuration** for SIP native services contains the new MN IP address and the **service adaptation** (i.e. downgrade or upgrade), based on the (target) UFA_GW available resources.

- The **SCTP layer configuration** for non-SIP native services contains the new MN IP address and the **SCTP congestion control parameters**. It is assumed that non-SIP native services, transported over SCTP on the transfer plane, do not need service adaptation. They adapt their bitrate to the available bandwidth. However, to use efficiently the available bandwidth, SCTP layer needs to be configured with optimal values for its congestion control parameters.

* The **all-OSI layer configuration** the MN should have. It includes, among other things, the MN IP address and the service configuration for SIP native services or the SCTP layer configuration for non-SIP native services.

The Controller then communicates these configurations to the B2BUA, which sends them within SIP messages to the MN and CN.

To trigger the previous actions, the Controller receives and treats inputs coming from other internal sub-modules (Figure 21). The Radio sub-module collects the radio measurements, sent by the MNs about their current UFA_GW and neighboring ones. These measurements enable to trigger a handover based on coverage criterion. The Resource information submodule calculates the UFA_GW available resources in order to trigger a handover based on load criterion or to adapt the service.

The controller also stores the contexts generated following the service access procedure.

• The **Back-to-Back User Agent (B2BUA)** is quite similar to the SCC AS B2BUA with added/modified features. Like the SCC AS B2BUA, it terminates the SIP dialog (dialog1) initiated by the MN and establishes a second SIP dialog (dialog2) with the CN. Unlike the SCC AS B2BUA, it modifies the content of SIP messages exchanged between the MN and the CN or builds SIP messages that are sent to the MN and CN based on decisions and configuration information received from the Controller.

Terminal (MN/CN)

In addition to the classical SIP UA responsible for controlling applications, the MN/CN implements UFA specific modules on the control plane. As shown in Figure 21, these modules are:

• **SIP Proxy**: As described in the previous section, SIP messages received from the UFA_GW may contain configuration information. The SIP proxy in the MN/CN is responsible for filtering and extracting the different layer-related configuration information and relaying them to the all-layer configuration module.

• **All-layer Configuration Module**: It receives the different layer-related configuration information from the SIP proxy and relays each part to its concerned layer (layer 2, IP, SIP UA). For non-SIP native services, the SIP UA relays the received information to the SIPcrossSCTP module.

• **SIPcrossSCTP Module (SxS module)**: This module within the UFA_GW is specific to non-SIP native services. It is responsible for the interaction between the service, SIP and SCTP. It has a central role in making non-SIP native services controlled by SIP. It locally detects the service related events (establishment, release) and triggers the equivalent events on the SIP level. For example, when a service is going to be launched, it establishes a SIP session and fills equivalent SDP fields (service name, flow descriptors).
It receives from the SIP UA, the SCTP-related configuration information sent by the UFA_GW, and relayed to it by the all-layer configuration module. Then, it enforces this configuration by interacting with SCTP.

SIPcrossSCTP Gateway (SxS_GW)

The support of non-SIP native services in UFA requires that the MN and the CN implement both SIP and SxS module. However, if the CN lacks these functions, to handle non-SIP services over UFA, a proxy network node, called SIPcrossSCTP Gateway (SxS_GW), is needed. When the MN initiates a non-SIP native service, SIP signaling is sent to the CN. The SxS_GW, intercepts this signaling and translates it to service specific signaling (e.g. RTSP or HTTP), that it sends to the CN. Thus, the SxS_GW anchors the control plane traffic. It also anchors the data plane traffic.

5.2.3.2 Mobility Procedure in UFA

In the LTE/EPC model, as described in section 5.1.2, the mobility procedure induces a high handover delay and does not enable service adaptation. Even solutions with proactive step execution and/or context transfer cannot solve efficiently these problems.

UFA mobility procedure solves the above problems and brings additional advantages:

• Mobility is controlled, decided and executed by the UFA_GWs. It takes into account different kinds of inputs.

• Mobility is based on a proactive context transfer. It is efficient as all of the contexts to be transferred are co-located in the UFA_GW. Mobility procedure includes two phases as shown in Figure 22:

– A preparation phase initiated by the UFA_GW_S to the UFA_GW_T, aiming at predetermining:

* The **service configuration** for SIP native services, or the **SCTP layer configuration** for non-SIP native services, the CN should have after the MN handover.

* The **all-OSI layer configuration** the MN should have after its handover.

– An execution phase aiming at providing the MN and the CN with the predetermined configurations.

Hence mobility procedure enables service adaptation for SIP native services or SCTP congestion control parameters tuning for non-SIP native services, according to the UFA_GW_T available resources.

• Mobility procedure is the same for SIP and non-SIP native applications and uses SIP protocol. For applications transported over SCTP, SIP replaces m-SCTP use and enables in addition to tune SCTP congestion control parameters.

• Mobility procedure is is independent of the radio technology. It can be intra-technology or inter-technology depending on whether the UFA_GW_S and the UFA_GW_T implement the same radio access technology or not.

• Mobility is performed on a per-service basis meaning that: (1) if a given MN has many ongoing services, for each service the MN will receive a dedicated service configuration or SCTP layer configuration, (2) when handover is inter-technology, the UFA_GW_S may decide to only transfer a set of services to a UFA_GW_T.

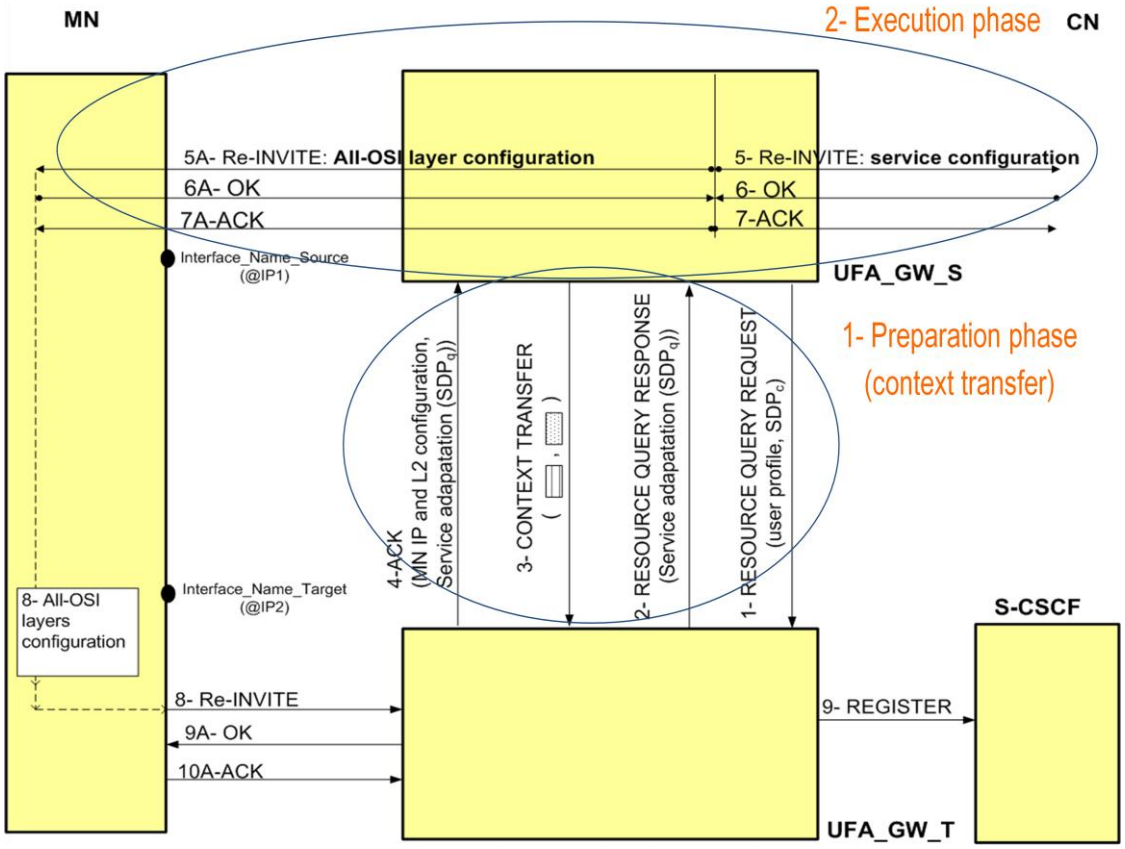


Figure 22: UFA Mobility Procedure.

5.2.4 HIP Deployment in New Flat and Distributed Architectures

The separation of locator and identifier information is probably one of the main evolution trends of the future Internet. As a consequence, MEVICO WP2 should describe challenges, benefits and how to introduce such a revision of the naming and addressing in EPC architecture. The main advantages and disadvantages of ID/locator split have been described in Section 2.6 and Annex 9.1.

The Host Identity Protocol (HIP) is a security control protocol providing true ID/locator separation, IP-mobility and multihoming. In HIP-enabled nodes, applications use persistent host identities instead of IP addresses for addressing. Mobility is hidden from the application and transport layer. The HIP signaling is performed over IP layer, and it provides among other services non simultaneous IP mobility management and IPsec transport for the transport and user plane. HIP has been described in section 2.5 of IR 2.3 [4].

HIP is an instance protocol providing a logical overlay for ID/Loc separation with cryptographic IDs (i.e., Host Identifiers - HIs) generated from a new, statistically globally unique namespace called Host Identity. In this namespace a Host Identifier is the public key of an asymmetric key-pair which is thus self-certifying, making possible the integration of strong security features such as authentication, confidentiality, integrity and protection against certain kind of Denial-of-Service (DoS) and Man-in-the-Middle (MitM) attacks. Several extensions have been defined to the base HIP protocol, e.g. advanced mobility and multihoming support, service registration, Rendezvous Server (RVS) extension, source address validation for authentication and access control, configuration provision for merging HIP with DHCP, and relay mechanisms for NAT traversal. Together with other proposals for DHT-based distributed name services and overlay routing mechanisms HIP also enables tackling scalability issues of current architectures by reducing anchors.

In current 3GPP networks, non-3GPP access is protected by IKEv2 and IPsec protocols. HIP could replace IKEv2 currently defined for non-3GPP access as network access security protocol, if it performs better in L3 re-authentication and IPsec security association establishment procedures.

Seamless inter-system handover between non-3GPP accesses is not covered by current 3GPP standards, however HIP could also support seamless inter-system handover between non-3GPP access networks.

As described in section 5.1.1.2, in a distributed 3GPP architecture, PGW relocation procedure is highly needed because when the MN moves to a new eNodeB, not only the EPC bearer path between the SGW and eNodeB must be relocated, but if the current P-GW is changed, the complete EPC bearer must be established between the new eNodeB and new PGW. If the PGW, SGW and eNodeB are collocated, than

the EPC bearer becomes virtual, there is no need for the GTP tunnel, just IP address allocation for the MN. In distributed or flat architectures, containing multiple distributed P-GWs, intra-3GPP mobility will lead to frequent inter-PGW handovers. HIP can provide secure L3 attachment and handover execution procedures for the MNs, and enables IP-level reachability of the MNs from correspondent nodes.

Scenario 2c in WP1 [2] suggests to distribute PCC and IMS nodes in addition to S/P GW and MME. In that case HIP can also provide mechanisms for L3 handover preparation and execution instead of MIP, m-SCTP or SIP-based solutions.

The performance and functionalities of HIP must be optimized for large-scale operator-driven environment. Hence its default certificate-based authentication must be changed to more lightweight authentication procedures, e.g. shared secret-key based procedures and Elliptic Curve Cryptography algorithms. Currently HIP follows an end-to-end approach between communicating peers. However, in the 3GPP architecture the endpoints must be the MN and the first GW in the network in order to enable network operations on plain data. Currently HIP does not support handover to new peer without complete re-establishment of the HIP host association and IPsec security associations. New solutions such as delegation-based HIP [29][30], enabling handover to new GWs must be used.

As a summary of pros and cons, the HIP-based L3 handover preparation and execution has the following advantages for 3GPP architectures:

- It is a partially distributed mobility management protocol, anchorless in the user plane, and centralized (using HIP Rendezvous extension, RFC 5203) or distributed (using the Host Identity Indirection Infrastructure (Hi3)) in the control plane
- Mobility is transparent for the application and transport layer, i.e., SIP and non-SIP enabled applications are supported. However application-level session parameters and QoS parameters must be updated by the applications. In case of SIP-based applications, SIP-based mobility management is the most appropriate solution. However seamless mobility can still be supported by the HIP-based handover procedure because it fulfills real-time service-interruption delay constraints [30].
- In case of flat or distributed 3GPP architecture, as depicted in Figure 2, a considerable part of the operator traffic, which was previously located in trusted domains, will go through untrusted IP networks. HIP provides automatic and flexible VPN configuration to securely reach femtocells and distributed GWs in the access networks.
- Multipath transmission (i.e., traffic is sent through multiple interfaces of a HIP-enabled node) of application flows is supported. In case of multipath transmission, TCP friendliness of multiple flows versus other flows in the network can be supported using mHIP [26] by HIP-level congestion control.
- Flow mobility and simultaneous multiaccess is supported by HIP extensions described in, e.g., in [28]. They describe mechanisms for flow identification and carrying filter rules (i.e., policy transfer) in HIP signaling in order to support the above behavior.

Disadvantages of HIP-based mobility management are the followings:

- In case of HIP delegation-based services, support of non-HIP enabled peers must be solved. Currently there is an ongoing work to guarantee transparency between HIP and non HIP-enabled hosts [28] using HIP proxies.
- One HIP host association maps to one IPsec security association, which leads to the selection of the most strict security preference of the transported data. E.g., if IMS signaling requires integrity and confidentiality protection than all user plane data must be protected in the same level between the MN and the GW, because there is one IPsec SA pair under one HIP host association pair. If higher granularity of security choices is required, multiple IPsec SA establishments per HIP host association should be implemented. However, this would highly increase he complexity of HIP, and HIP may lose its performance cost advantages versus IKEv2.
- User and network authentication and key agreement procedure of HIP should be light-weightened to better adapt to large-scale operator-driven networks.

5.2.4.1 General HIP-based Mobility Architecture in UFA

Compared to the SCTP-based solution proposed in section 5.2.3, the HIP-based Ultra Flat Architecture alternative is independent from the transport layer mechanisms.

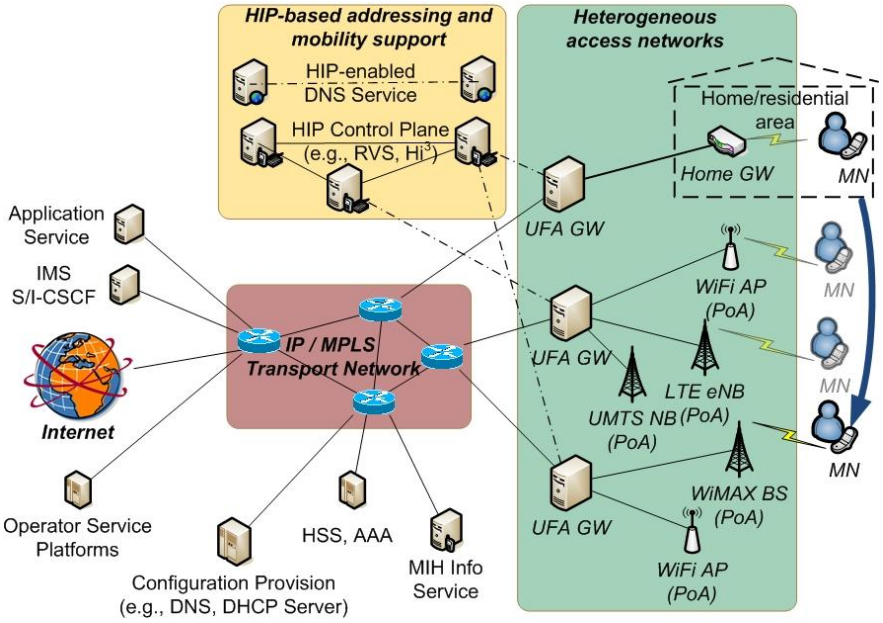


Figure 23: A HIP-based Ultra Flat Architecture.

The HIP-based Ultra Flat Architecture [8][29][30] depicted in Figure 23 comprises four main parts:

1. several access networks,
2. an IP/MPLS transit network,
3. a handover preparation and initiation subsystem (e.g., based on IEEE 802.21 MIH [31])
4. a HIP-based control network.

In this scheme centralized IP anchors between Point of Access (PoA) nodes and correspondent nodes are totally removed, and network functions are placed at the edge of the transit and access networks (close to the Point of Access (PoA) nodes) in the Ultra Flat Architecture Gateways (UFA_GWs). The main tasks of the HIP-capable UFA_GWs:

1. performing fast cross layer (L2 and HIP-level) access authorization
2. actively interacting with hosts through delegation-based HIP and IPsec association management and context transfer for optimized message exchange in HIP-based UFA mobility and multihoming operations. (Note that this framework transports end-to-end flows between MNs and CNs in a hop-by-hop manner. The middle-hops are the UFA GWs, i.e., the delegates of the end peers).
3. performing the actual mapping/routing between outer header IPsec tunnels based on inner header identifiers.

The control network in the upper part of Figure 23 (HIP-based addressing and mobility support) contains a HIP-compatible Domain Name System [33] for resolving domain names to host identities and/or locators depending on the actual situation. In addition there is the HIP Control Plane which stores and distributes dynamic and presumably frequently changing binding information between host identities and locators of all actively communicating (mobile) hosts in UFA. This control plane might be a conventional RVS [34] park or a complete distributed HIP signaling architecture like Hi3 [35]. The records managed here are provided by the UFA GWs using their own global locators as location information to be bounded with identities of their actively interacting partners.

The control of the above functions brings cross-layer HIP modules in the UFA GWs, MNs and Correspondent Nodes (CNs). HIP Base Exchange (BEX) and Update procedures deal with dynamic negotiation of IPsec security associations between the MN and the UFA_GW to protect user data and mutually authenticate the MN and the network. The handover execution procedure is started by the UFA_GW_S. HIP and IPsec contexts are established between the UFA_GW_T and the MN's CNs, furthermore, between the UFA_GW_T and the MN, using the mediation of the UFA_GW_S. This is possible due to the delegation of HIP signaling rights from the MN and from the UFA_GW_T to the UFA_GW_S [29]. Context Transfer Protocol [36] is used to transfer the HIP and IPsec contexts from the UFA_GW_S to the UFA_GW_T and the MN. As the contexts are in their place the MN is notified by the

handover preparation and initiation subsystem to attach to the new PoA. The handover preparation and initiation subsystem handles handover preparation issues and relating signaling tasks in order to initiate proactive HIP handover procedures in the UFA and to support both network and mobile controlled handover decisions.

6. Smart traffic Steering Demonstrators

6.1 Demonstrators Description

From the requirements put in the IR2.1, were defined some challenges that should represent the most promising and interesting topics in the mobility and routing area. These challenges are described in [44]. Partners have proposed some technology solutions that are aimed to solve some aspects of the challenges. These technology solutions will be implemented on demonstrators that can be either a testbed or a simulation or an analytical solution. The results of these demonstrators will be used in the MEVICO validation process that will allow comparison between close topics and will give valuable information on the improvement that can be expected for each challenge. It will also give some answers on the preferred architecture that should be selected and the level of distribution of the network elements.

6.1.1 Performance Evaluation of Different L3 Authentication Methods (BME-MIK)

The aim of this demonstrator will be the evaluation and demonstration of the differences between the performance costs of different L3 authentication methods in different architectural scenarios. This topic is related with the performance problems described in Section 5.1.2, i.e., the first phase of service continuity during inter-GW handover. The results are expected to support our decisions on which technologies and authentication methods should be selected in distributed EPC where the first IP gateway is located at different parts of the network.

Several reference scenarios for different distribution levels of the core network will be considered. The most important cases are the centralized, distributed and/or flat use cases. These use cases will be emulated using network emulators such as Network Emulator (netem) and KauNet [44].

The key performance indicators of L3 authentication and security association establishment procedure are the message complexity of the authentication methods, the application-layer delay caused by reauthentication, and the CPU utilization cost at the UE, the P-GW/authenticator, and the AAA server by the reauthentication process. Reauthentication delay is important from a user perspective, whereas utilization is relevant for network dimensioning and planning

Figure 24 illustrates the structure of our experimental network.

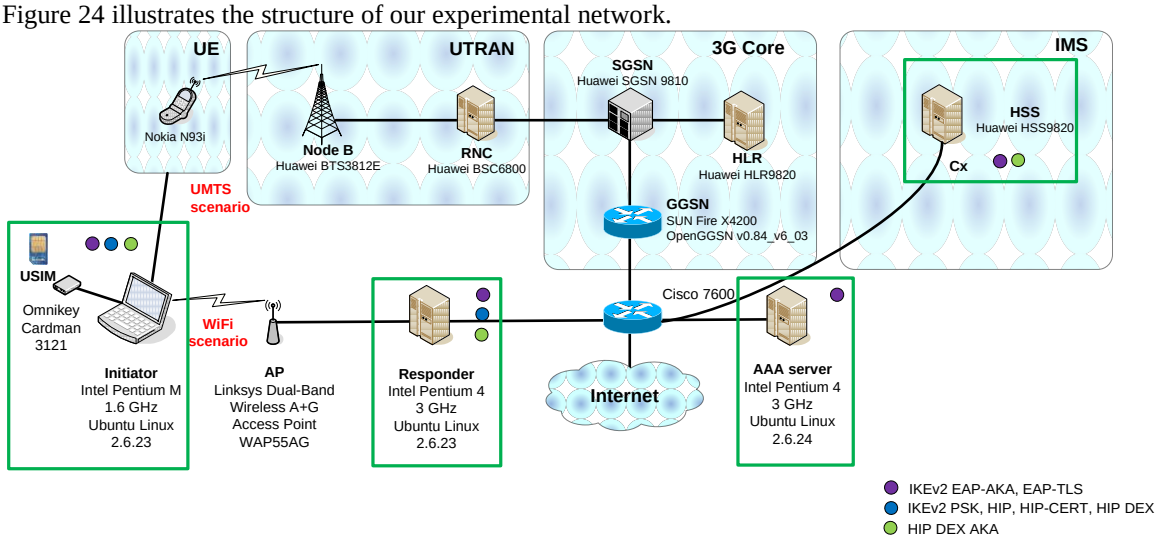


Figure 24: Testbed for Reauthentication Measurements.

In the experimental setup, the initiator (UE) is realized using a laptop with Intel Pentium M 1.6 GHz CPU with fixed CPU frequency. The responder (distributed P-GW) and the AAA server are realized two desktop PCs with Intel P4 3 GHz CPUs. All computers run the Ubuntu Linux operating system with a 2.6.23 version kernel at the initiator and the responder, and a 2.6.24 kernel at the AAA server. The AAA server is realized with freeRADIUS version 1.1.7 and openSSL.

Preliminary results have been made on this testbed for different IKEv2 reauthentication methods using the ikev2-2.0beta1 implementation from the IKEv2 project [41]. The results have been described in [40], and it shows the CPU cost and network utilization costs of different EAP-based methods in partially emulated reference scenarios, i.e., Wi-Fi, UMTS, far-close, bandwidth-limited, and close-far scenarios.

The Wi-Fi, UMTS, close-far, and bandwidth-limited scenarios represent the cases where IKEv2 is used as a mechanism to provide integrated network access authorization for various RANs. The responder is one or a few hops away from the initiator, and functions as authenticator and enforcement point providing access to the Internet.

The UMTS, Wi-Fi and bandwidth-limited scenarios represent situations where the initiator get access through a RAN close to its network access service authorizer, i.e., the AAA server.

In the close-far scenario, the transfer delay between the responder and the AAA server is large, emulating situations where the initiator gets network access in a visited network far from its access service authorizer.

In the MEVICO project we plan to compare the Strongswan Charom [42] IKEv2 implementation with different EAP methods, furthermore, the HIP for Linux (HIPL) implementation [43], and a new HIP Diet exchange implementation. New reference scenarios will be applied to emulate different topologies. Since LTE network is not available for the testbed, LTE connections could be simulated using KauNet, a network emulation tool for BSD and Ethernet connection between the initiator and the responder.

This demonstrator fits well for validations but not for demonstrations. For demonstration purpose some part of the testbed, e.g. the UE and the responder, should be moved to the demonstration place. It might be possible to demonstrate the effect of different reauthentication procedures e.g., on multi-flow measurements or a video on demand application. This demonstration opportunity will be further investigated during the project.

6.1.2 Performance Evaluation of HIP-Based Authentication and Bootstapping (CWC)

The point of this demonstrator is to study the feasibility of using HIP Diet Exchange, a more lightweight security negotiation scheme in (1) user and host re-authentication, (2) and bootstrapping in the operator controlled Wi-Fi accesses. The performance cost in terms of number of messages, CPU load, memory usage, processing and network delay, and throughput in various inter-GW handover scenarios will be examined. The measurements are expected to share light as to what kind of architecture suits the future mobile networks the best. Delay in bootstrapping and (re-)authentication is crucial from the end-user perspective, while the CPU and memory utilization is relevant information for network dimensioning and planning, as mentioned above in the previous section. The measurements will be contrasted with the current authentication and bootstrapping schemes in 3GPP networks, e.g. EAP-AKA and IKEv2.

We will also intend to perform measurements with various resource constrained devices such as Android-based handhelds. At later time, the testbed will also be extended with Femtocell access points, or a simple Femtocell backhaul network, and perform above described measurements when mobile host roams from Femtocell access point to another. The testbed is illustrated in Figure 25 below.

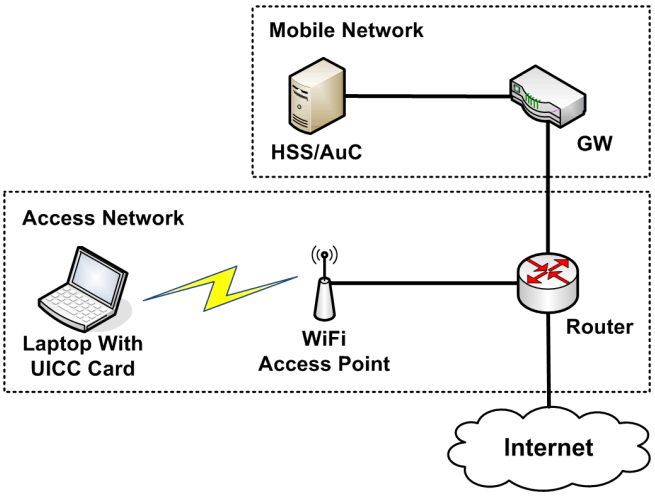


Figure 25: Testbed for Authentication and Bootstrapping Measurements.

UE is a Dell Vostro 3300 laptop with 64-bit GNU/Linux operating system running kernel version 2.6.38. The laptop is equipped with an internal Broadcom 802.11b/g/n wireless network adapter and uses Dekart DK38T SIM card reader with vendor supplied drivers. The laptop is also incorporated with 2.8 GHz Intel Core i7 CPU and total system memory of 4 GB. Later we will intend to use Android-enabled smart phones as UEs in the testbed to evaluate the performance impact of our authentication scheme on real-life device with scarce resources.

The Wi-Fi AP in Figure 4 that the UE connects through is a Netgear WNDR3700 gigabit wireless router with all L2 security mechanisms (i.e. WEP/WAP) disabled and has no authentication requirements towards connecting clients. The router, which separates the Internet, access networks and the core mobile network, is NexGate NSA1086 with 8 Gigabit Ethernet ports installed with GNU/Linux 2.6.38 kernel and configured to act as an IPv4 and IPv6 router.

The GW and HSS/AuC machines are Dell PowerEdge SC1435 servers with 64-bit and 32-bit GNU/Linux operating systems running 2.6.38 kernel, respectfully. Both machines incorporate 2.6 GHz AMD Dual-Core Opteron processor, 8 GB system memory, and two gigabit Ethernet network adapters. OpenSSL library version 1.0.0d is installed for cryptographic algorithms.

The GW at the border of core network runs a daemon application responsible for listening and accepting incoming connections from UEs wishing to connect to the mobile network, and performing HIP-based authentication.The same daemon is run in the UE as well but operates in the Initiator role and accesses the USIM application during the authentication process.

For the time being, the testbed is used as an implementation and verification platform for solutions developed in the MEVICO project. Main validations are performed with a testbed (described in section 6.1.1) provided by BME-MIK. Our testbed is not suitable as a demonstrator per se but requires tweaking in order to compress it into two portable devices and an access point. It may well be, however, possible to modify our testbed for portable demonstrator use, as in practice full-fledged 3GPP devices are not needed to demonstrate our HIP-based 3GPP authentication and bootstrapping scheme.

6.1.3 Performance Evaluation of HIP based Ultra Flat Architecture (BME-MIK)

In order to provide an extensible, full and precise model for the HIP based Ultra Flat Architecture, we extend and enhance the IPv6 based Host Identity Protocol simulation framework called HIPSim++ [49][50]. This model is built on the top of the 20090325 version of INETwithMIPv6 which is an extension and TCP/IP model collection of the component based, modular OMNeT++ 4.x discrete event simulation environment.

Transparency of the novel HIP layer, extendability and proper implementation of the UFA functions and the integrated IEEE 802.21 MIH mechanisms are the most important requirements which will be guaranteed for evaluation and demonstration purposes. Full implementation of IPSec and relating algorithms is not part of our simulation model: our simulations will not possess properly realized Diffie–Hellman mechanisms, RSA engine, cryptographic hash functions and puzzles because mapping of all the security algorithms is out of scope of our current research efforts. The main design goal of the UFA extensions of HIPSim++ is to accurately simulate HIP based UFA instruments focusing on the advanced proactive mobility and multihoming capabilities and wireless behaviour of the scheme and providing only skeleton implementation of the above mentioned mathematical and security apparatus.

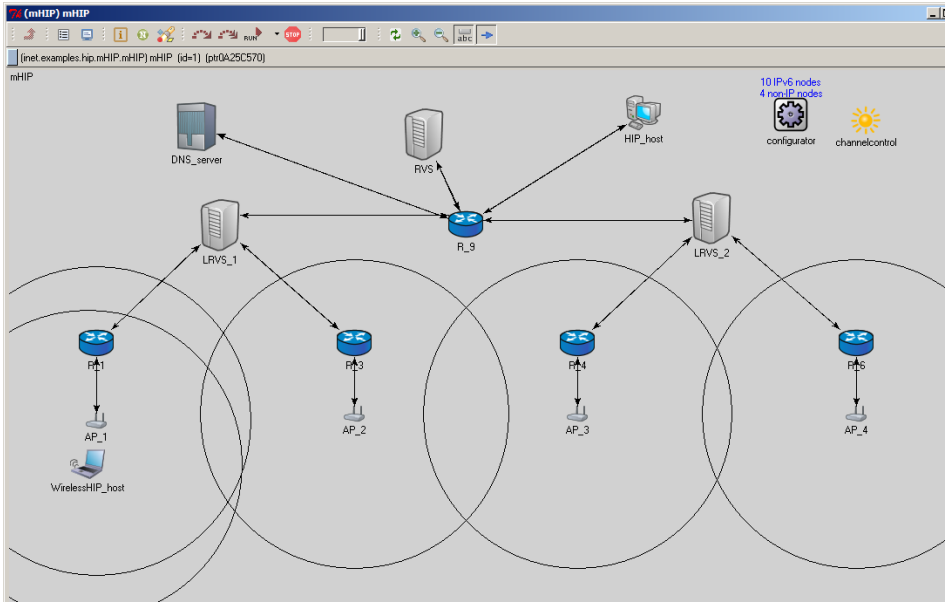


Figure 26: Example simulation scenario within the HIPSim++ framework.

Our base model, the INET collection contains detailed and accurate implementations for IPv4, IPv6, TCP, UDP, SCTP, MPLS, RSVP, LDP protocols and several applications like telnet, video streaming, Voice over IP, etc. INET also includes link-layer models as PPP, Ethernet and 802.11b/g (both ad-hoc and infrastructure modes), WiMAX, etc. This rich base protocol collection enables HIPSim++ to execute the widest scale of measurements and analysis: all the pros and cons of applying HIP based UFA in a mobile network can be evaluated as in HIPSim++ the whole INET simulation model set can be easily used and even modified in case of need.

Within this complex framework we will evaluate and demonstrate the efficiency of the proposed HIP based UFA scheme. The network topology to be applied for the analysis will consist of three main parts. We will set up a domain for the correspondent node(s), the core network with the DNS, RVS systems and router parts, and also a domain for the air interface containing the wireless access points with the UFA-GWs and the mobile nodes. The MNs are able to migrate between different APs with different mobility models such provoking handover events (e.g., Fig. 26). Inducing independent handovers during simulation runs we can measure for example:

- Handover latency – 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
- UDP packet loss – the number of lost UDP packets during a handover in the HIP based UFA system while transmitting different UDP traffics
- TCP throughput – throughput of a defined time interval experienced at different handover frequencies

The simulations are expected to show the power of applying HIP in future distributed and flat mobile environments and highlight the benefits of the UFA scheme in general.

6.1.4 Performance and Evaluation of Different Mobility Schemes using LTE (ALU)

The aim of this demonstrator will be to evaluate different mobility schemes, using the same equipments.

First, some comparisons will be made on IEEE 802.21 (MIH) and the 3GPP ANDSF protocols. These two protocols are designed to provide some helpful information about HO, especially on the HO preparation step in order to optimize it. It can also give propositions on some new networks opportunities access to the user equipment. The measurement to check the interest of these solutions will be based on HO efficiency: HO preparation duration, HO execution duration and HO success rate.

To test MIH implementation, a Point of Service (PoS) an additional functionality will be embedded within the MME. There is also a need to embed two Points of Access (PoA), one within untrusted access and the second within the eNodeB. A MIH client will be implemented in the user equipment, this client will be able to exchange messages with PoS and PoA and use information to trigger HO.

ANDSF implementation only needs an ANDSF server embedded in the MME and an ANDSF client within the User Equipment. This client will receive some rules from the server and will propose to a connection manager to apply this information to improve user equipment network access.

Then protocols such as NMIP, MPTCP and SCTP will be studied. For this comparison there is no need of additional network equipment, these protocols being end to end. We plan to examine wireshark traces from UE, access point and eNodeB to evaluate bit rate, latency and jitter using all these protocols.

Preliminary results have been made using Ethernet link, Wi-Fi and 3G access. In MEVICO project we plan to evaluate these protocols using LTE access.

Next step will allow us to distribute some of the EPC network elements (SGW, PGW, MME) by using the open platform PlanetLab in order to evaluate our mobility schemes

The measurements are expected to highlight what kind of architecture suits the best using these protocols and to evaluate each of them.

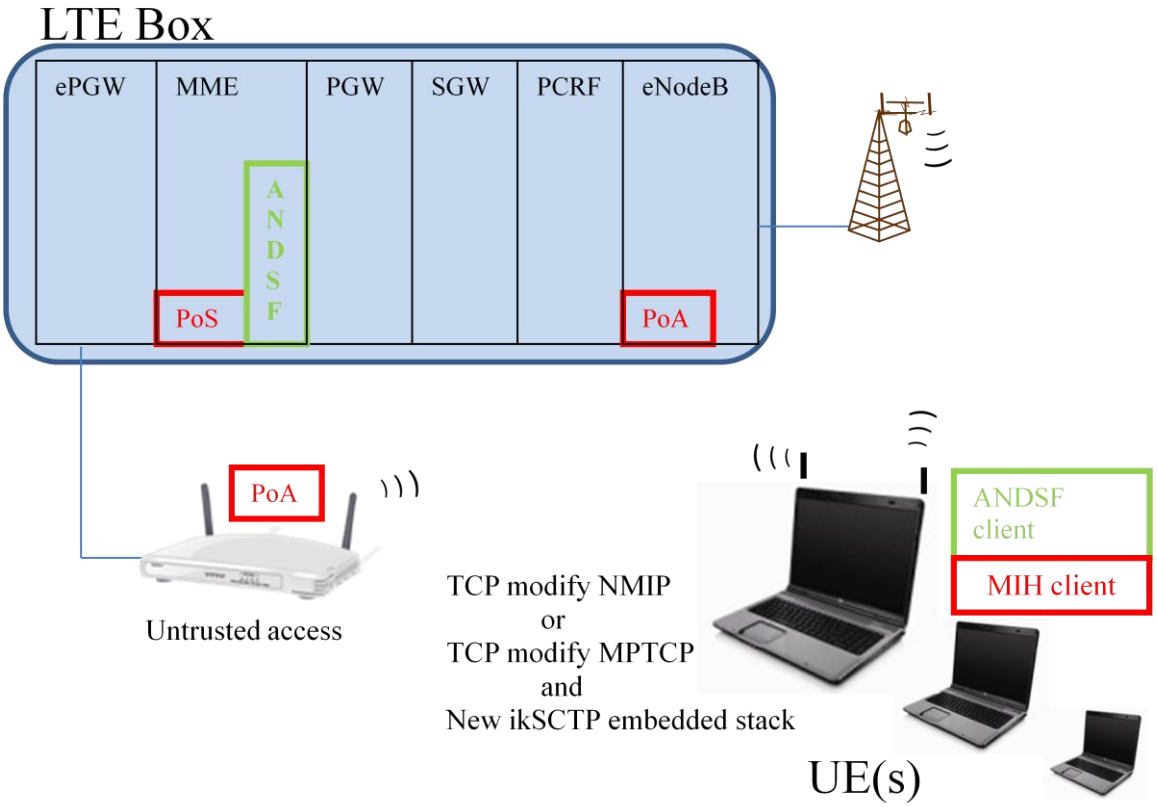


Figure 27: Testbed for Different Mobility Schemes.

6.1.5 Evaluation of Different Mobility Using LTE Emulators (NSN)

The aim of this validation environment will be the evaluation and demonstration of performance, scalability and cost of EPC (Evolved Packet Core) in different architectural scenarios for GW relocations and mobility management.

This validation environment is based on NSN internally developed LTE Linux emulators, which are currently used in R&D demo-concept and trial development projects conducted NSN. LTE emulators based on a combination of 3GPP specifications and implements following:

- Network elements:
  - Multiple UEs
  - Multiple eNBs
  - Two MMEs
  - Two UPEs (User Plane Entity)
  - One HSS
  - One PGW

- One PCRF, as a stand-alone and separate tester
- One SGSN, as a stand-alone and separate tester
- One VLR, as a stand-alone and separate tester

- Interfaces:
  - Uu
  - S1-MME
  - S1-U
  - S4
  - PMIP based S5 GTP based S5
  - S6a
  - S7 (Gx/Gxc), in the context of PCRF stand-alone and separate tester
  - S10
  - S11
  - SGs
  - X2
  - Gn
  - Gi

NSN LTE emulators are implemented in C language, using CVOPS and ASN.1 tools and run on Linux operation system.

LTE emulators system setup for this project shown in Figure 1 is deployed on 7 servers running on standard Linux OS combined in test network. Dell PowerEdge 210 with quad-core Xeon /4GB RAM servers are used in this setup.

Figure 1 shows NSN LTE Emulator configuration for GW relocations and mobility management demonstration. Application running in UE_1 is working with Application in Network (e.g. video streaming). UE may have different operations in control and user plane:

-Handovers from eNB_1 to eNB_2 – within MME_1 control scope

-Handovers from eNB_1 to eNB_3 – involving change control MME

- Gateway relocations in different control scopes

Application performance can be monitored and messages flow in control plane can be studied during those operations. Using scenarios with multiple UEs and eNBs, system scalability and performance can be studies for different architectural solutions.

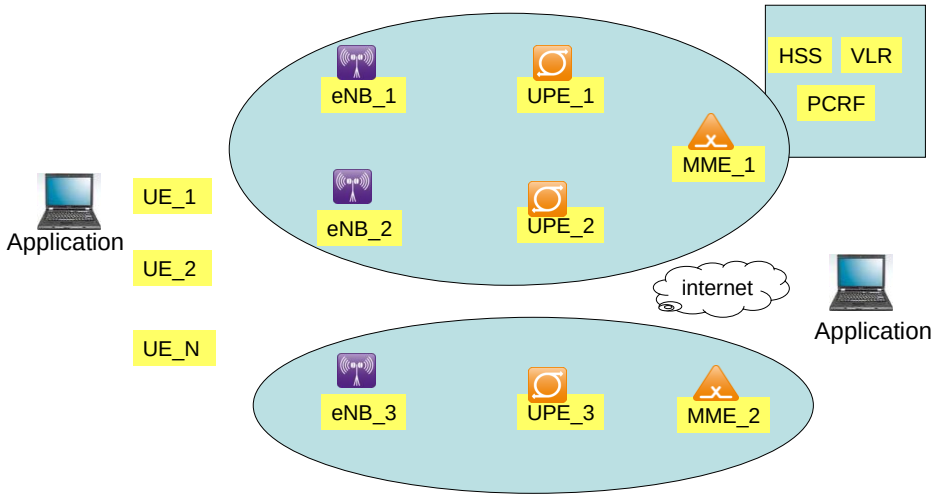


Figure 28: NSN LTE Emulator configuration for GW relocations and mobility management study.

.

6.1.6 Evaluation of Session Layer Mobility Extension to SCTP Protocol

The aim of this demonstrator is to demonstrate the session 'suspend' and 'resume' functionality with the session layer extension to the SCTP protocol. It enables applications to request suspension and resumption of communication at any given time, for surviving long disconnection periods, and for re-establishing the previous communication upon reconnection. The evaluation is performed based on the interaction of the session layer and a file transfer application under various mobility scenarios. A file transfer application is developed for session layer's testing purpose which is explained later**.** The evaluation environment is illustrated below.

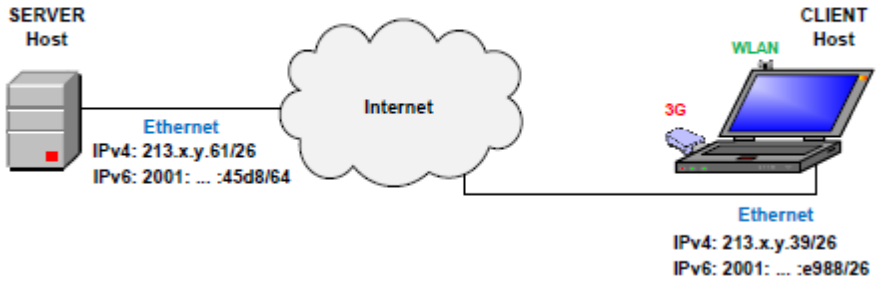


Figure 29: Evaluation environment for testing the session layer.

The evaluation environment consists of a server host and a client host, both connected to the Internet as shown in the above Figure 29. The server host has a single network interface with both IPv4 and IPv6 addresses configured. The client host can have multiple network interfaces configured, such as Ethernet interface (with both IPv4 and IPv6 addresses configured), a wireless LAN interface, and a 3G interface (using a 3G USB modem). The client host can be connected only through one network interface since the purpose of the test scenarios is to show that the session layer survives from long disconnection periods and re-establishes communication upon reconnection.

The file transfer application implemented to test the session layer is a graphical client-server application where the client requests the download of a specific file from the server. Initially, both the server and the client establish network communication and initiate a session through their Ethernet interface. After the session establishment, the client starts downloading the particular file. The client requests the content from its session layer using the Session layer API.

At this stage, either the client or the server application may request suspension and resumption of communication at any given time. Session layer messages are sent to the server if the client application requests for a suspension and vice versa. This demonstrates mobility on demand from the applications. The other mobility scenarios that can be tested are suspend and resume from short and long network disconnections. In this case, network disconnectivity (mobility event) is generated by unplugging the Ethernet cable.

6.1.7 Evaluation of PMIPv6 Routing Optimization and Support of Moving Networks (CEA)

The aim of this demonstrator is to validate two extensions to Proxy Mobile IPv6 (PMIPv6): the first extension implements the routing optimization procedure (PMIP-RO) through the use of new signalling messages and one (or several) intermediate anchors (see Section 5.2.1.4). The second extension provides the support for moving networks (PMIP-NEMO) by extending PMIPv6 data structures and routing procedures (see Section 2.11).

The validation environment is based on a CEA LIST PMIPv6 in-lab platform. PMIPv6 has been implemented from scratch and support only IPv6. The set of entities composing the testbed is presented in Figure 30. The core PMIPv6 platform runs on off-the-shelf laptops running the latest Ubuntu Linux operating system. PMIPv6 has been implemented following the RFC5213 using the C programming language at the user space. All functional entities composing PMIPv6 has been implemented as well as signalling messages, namely: The LMA that is collocated with the P-GW and the MAGs collocated with RANs' gateways, i.e., S-GWs, ePDGs, ASN-GWs, etc. Communications links between MAGs and the LMA refer to the S5/S8/S2a/S2b interfaces.

The current evaluation environment considers:

- The radio access points as Wi-Fi access-points. At some points, the radio access-points may be remplaced by typical wired 100Mb/s Ethernet links. The aim will be to reduce the impact of radio links quality variation on the performance of the core platform.
- The MAGs interconnected to their respective Wi-Fi access-points by 100Mb/s Ethernet links
- Interconnection between MAGs and IA(s) through 100 Mb/s Ethernet links
- One hub to interconnect MAGs to the LMA
- One 100 Mb/s Ethernet link to interconnect the LMA to the multimedia server

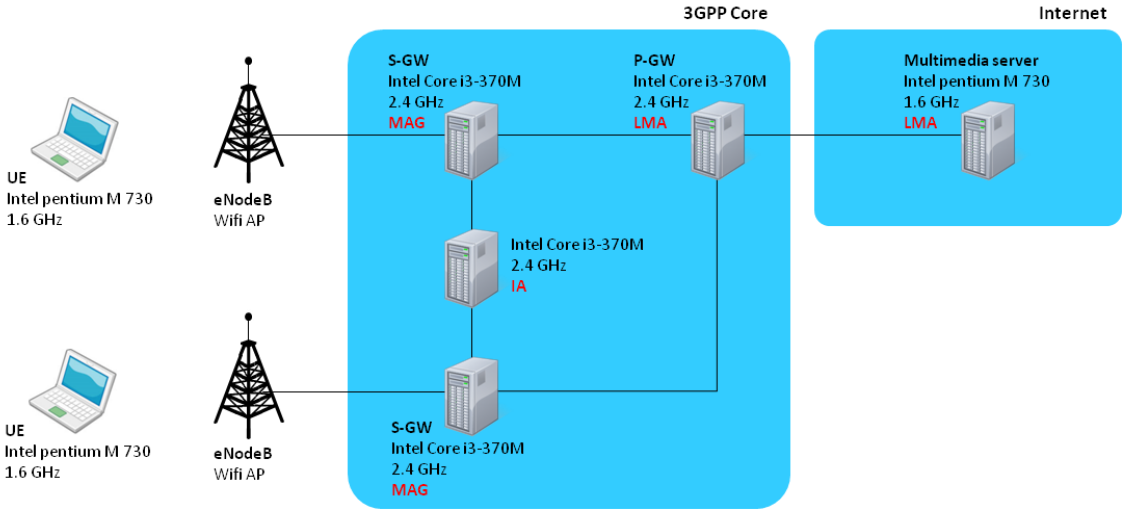


Figure 30: Evaluation Environment of PMIP-RO and PMIP-NEMO.

A typical PMIP-RO evaluation will be based on the use of one LMA centralized and at least two MAGs. One multimedia server will be located beside the LMA in what is considered as the Internet. At least two UEs will be connected to their respective access-points and will initiate data traffics towards the multimedia server. A third UE may be considered to generate background traffic and/or to increase the load at the LMA.

The principle is to generate background data traffics between UEs and the multimedia servers so that one reaches the maximum capacity at the LMA. By initiating a new flow between two UEs, this flow will be, directed to the LMA (following the standard PMIPv6 procedures) and will suffer performance degradation. The PMIP-RO extension will then starts the routing optimization procedure by anchoring this new flow at the IA close to UEs' respective MAGs. The outcome is improved data traffic performance and increased overall network capacity.

PMIP-RO performance during handover is not planned. Several interconnections with IA(s) will be considered such as mesh-like connections with MAGs or a tree-like hierarchical topology.

A typical PMIP-NEMO evaluation will be based on the depicted PMIPv6 plateform. The moving network will be composed by one mobile router implementing NEMO and one client as local fixed node (LFN). However, modifications will be introduced to neither the mobile router nor the LFN. The extension has an impact on PMIPv6 only. The validation scenario will consider data traffic between the LFN and one UE. Evaluations will take into account the impact of handovers on the traffic performance.

In all scenarios, data traffics will be initiated through the iPerf performance evaluation tool. Both TCP and UDP traffic performance will be evaluated considering the iPerf server on the multimedia server and the iPerf clients on the UEs. The to-be-optimized data stream (in PMIP-RO) between UEs will be initiated using on iPerf server instance on one UE and one iPerf client instance on the other UE.

6.1.8 Evaluation of Support for User Cooperation in Mobile Relaying (AVEA and TURK TELEKOM)

Relaying techniques are considered as an alternative solution to enhance capacity for the cell network, to extend coverage in specific locations, to increase throughput in hotspots or to overcome excessive

shadowing. It gives important advantages such as ease of deployment and reduced deployment cost compared to deploying regular Base Station (BS).

The fourth generation (4G) technologies call for very high data rates (such as 100 Mbps for mobile and 1 Gbps for fixed environments) with a robust relay and backhaul architecture [45]. However, the current technologies suffer from reduced data rate at the cell edge where the signal to noise and interference levels are typically lower. The improvements in the current LTE technologies like MIMO, OFDMA enhance the throughput under different conditions, but cannot sufficiently mitigate the problems of the UEs at the cell edge. Therefore, it is necessary to look at the solutions that will enhance the performance of UEs at the cell edge.

One solution is using LTE relaying techniques. Relay technology is an important aspect and one of the key technologies taken into consideration during the standardization process of 4G technologies like LTE-Advanced. Relaying is studied as an architectural discussion in 2009 as study item on LTE-Advanced and standardized during 2010 in LTE Release10 [45].

Relaying promises coverage-area and data rate extensions for the cell edge users. This is especially useful because LTE will operate on high carrier frequencies, i.e. 2.6 GHz which will result in ultra-dense deployment of network nodes, the transmit power is limited when transmitting broadband at the cell edge and the most of the traffic is generated indoor. Moreover, relay deployment is easier, lower power, and cheaper than base station (BS) deployments. The main objective is to provide Quality-of-Service (QoS) support for the edge users with low signal-to interference and noise ratio (SINR) using mobile relays and to build a strong interface for smooth communication between radio access network components and core network components. We will mainly look at some of the important issue in relay-assisted legacy networks for LTE-Advanced technologies like relay node selection or pairing schemes, number of relays, power allocation to the BS and relay node and relay planning.

Covered challenge is C.Mo.10 *Support for user* cooperation. Improvements in system throughput, edge user throughput and coverage are major KPIs to be looked while simulating mobile relay-assisted cellular structures and its communication with UE and eNB. Other KPIs related to mobile relaying are signalling overhead, OPEX/CAPEX, the decrease in power consumption, handover frequency and delay. The scalability of the mobile relaying can be measured using these KPI values.

We consider a test scenario in MATLAB where the mobile nodes are randomly distributed as shown in figure below. Mobility and relay models as well as other parameters like channel models are based on LTE test standards. In our model, each mobile node can also act as a mobile relay. The objective is to find the most suitable relaying node for the edge-user in order to increase its QoS parameters. The parameters that need to be considered are interference, channel quality, bandwidth and power limitations.

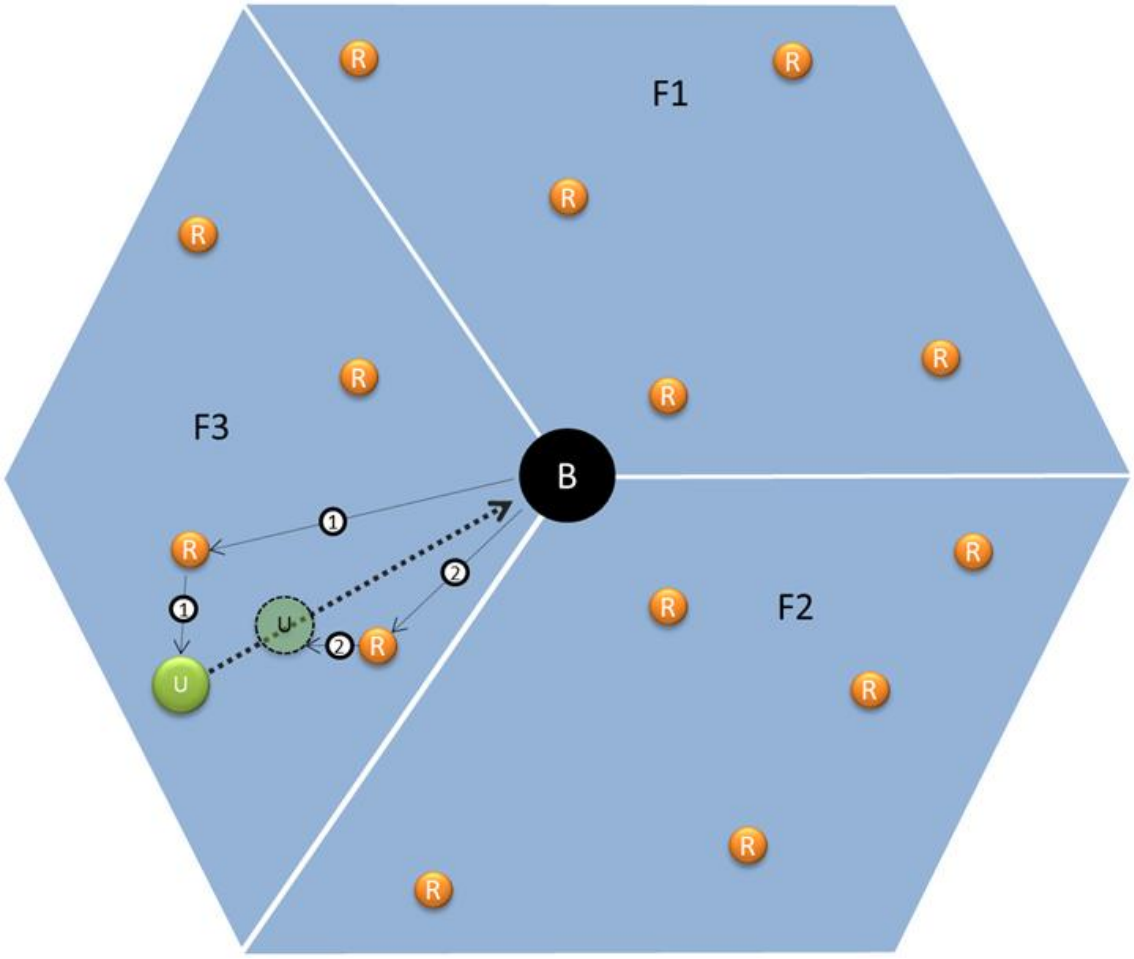


Figure 31: Considered scenario and MATLAB simulation illustration. A cell is divided into 3 sectors and mobile stations are distributed randomly in the region

The proposed algorithm will consist of two phases. In the first phase, it will try to pair the relay nodes (RNs) with their corresponding UEs. The detailed analyses of the first phase are explained below.

Phase 1: Pairing Scheme for the Selection of Relay.

In order to achieve relay gain, pairing of UEs with their corresponding relay nodes must be done efficiently.

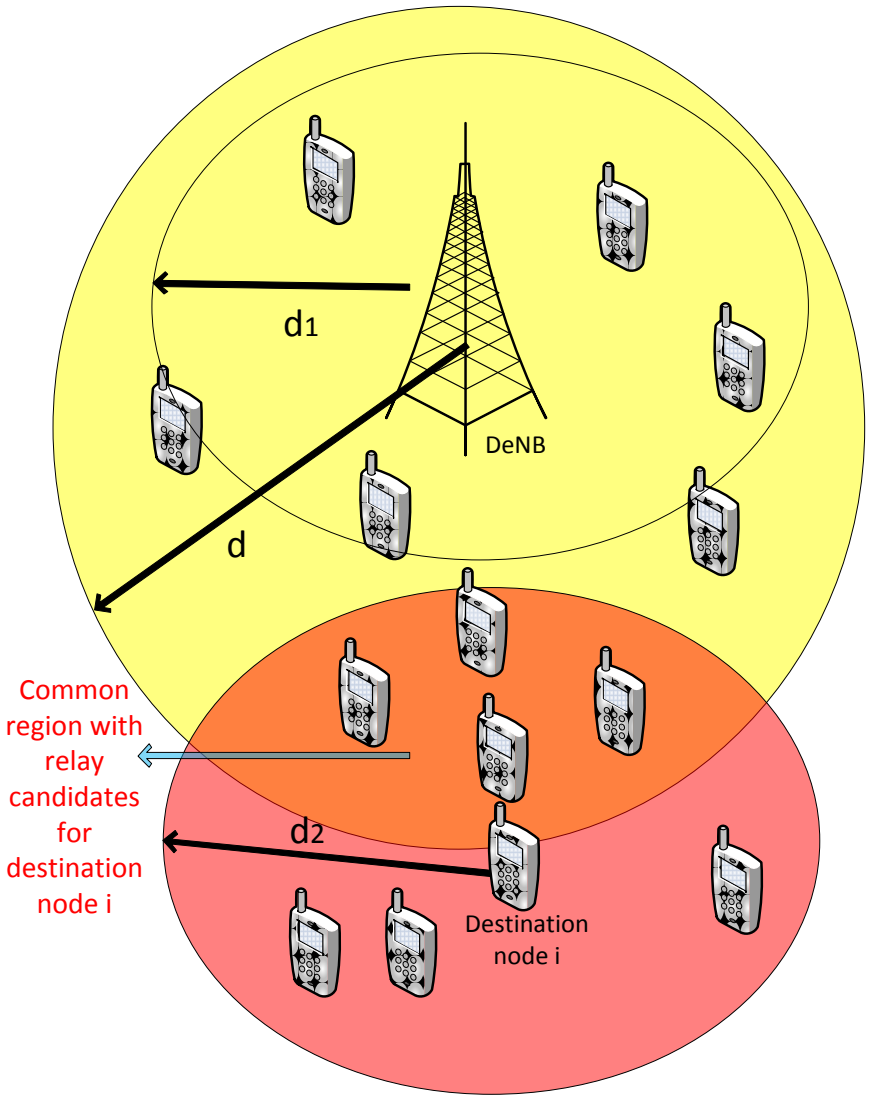
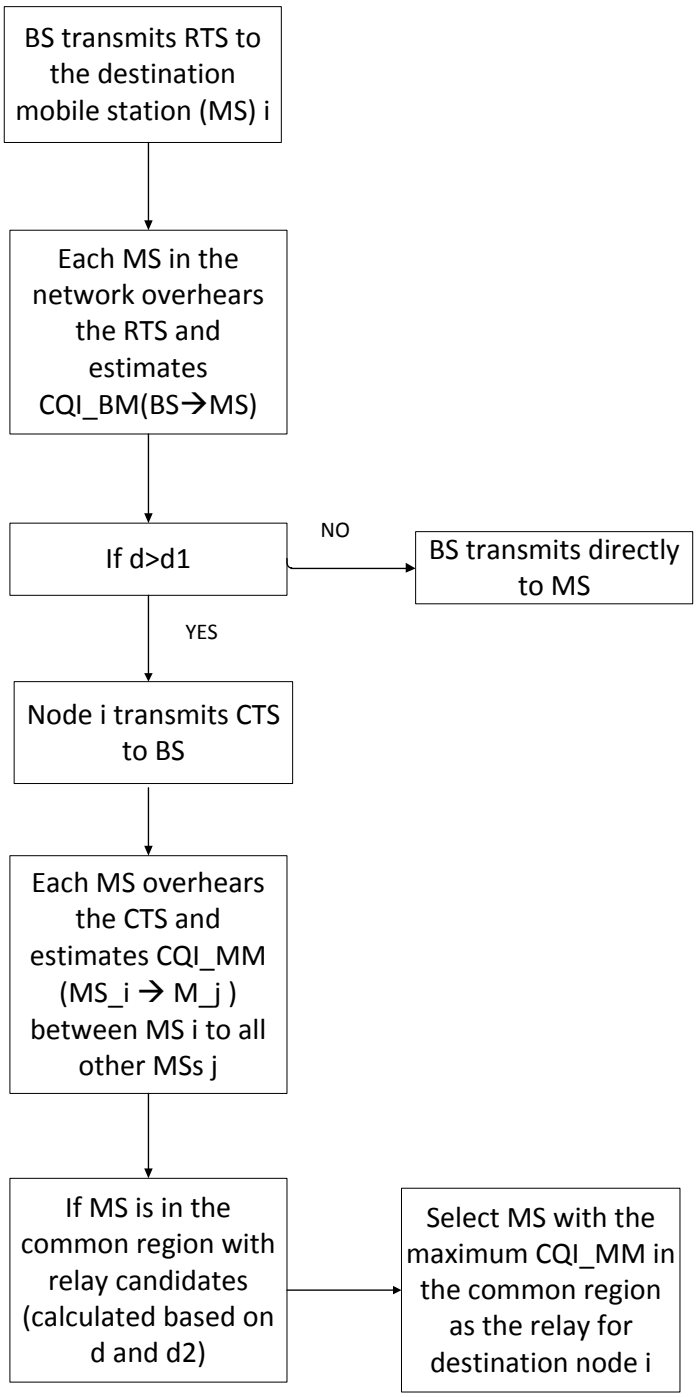


Figure 32: Illustration of the relay candidate selection algorithm using CQI values.

In the figure above, first we define the three related parameters d, d1 and d2 which are the cell radius, threshold distance for users with high channel quality information (CQI) values between base station and mobile station (CQI_BM) and relay candidate threshold distance for users with low CQI_BM values respectively. Moreover, we assume that we can measure the CQI values between mobile stations CQI_MM. Mobile stations (MSs) located outside the threshold distance d1 are considered as users with low CQI and need to find the related nodes to pair with. The MSs located between radius d and d1 are considered as users with low CQI. Note that due to shadowing, fast fading and path loss effects, the users will have different CQI values. Therefore, the CQI values, which are values between 1-32, will be selected randomly.

The corresponding measurements for CQI_BM and CQI_MM can be done during RTS and CTS packet transfer between the BS and the destination mobile i. See the flowchart below for a detailed relay selection mechanism.



Flowchart 1: Distributed relay selection mechanism using RTS and CTS packets to estimate CQI_BM values (CQI values between BS to each MS) and CQI_MM values (CQI values between destination MS i to each MS).

Phase 2:

In the second phase of the mobile relaying, we will investigate different protocols' (for example, load balancing and cooperative relaying, etc.) performance and compare them with current traditional solutions without relays.

MATLAB test environment will be used to simulate the proposed mobile relaying algorithm. The proposed algorithm will use the real LTE network parameters.

The cell structure consists of three sectors. Each sector has 10 users with a total of 30 users. 20 users are distributed to have good channel quality indicators (CQIs) and 10 users to have lower CQIs. Cell radius d is 1 km. Each user is uniformly distributed in the Cartesian coordinates.

The MATLAB figure below is the simulation model of the above proposed relay selection mechanism.

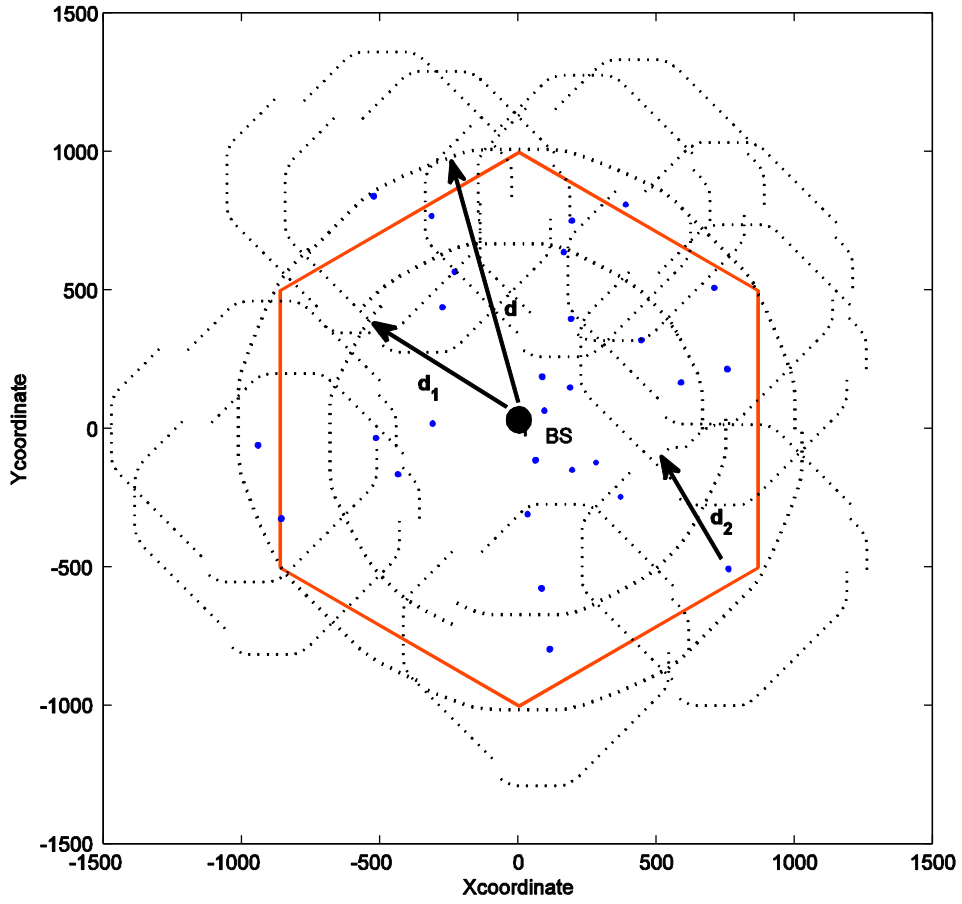


Figure 33: Figure showing the proposed user-relay pairing scheme according to proposed algorithm: d1 is selected as 666m and d2 as 500 m, the blue dots are mobile nodes.

The test results will indicate the performance results of the proposed algorithm compared with the other solutions in the literature. A brief investigation of the performance gains will also be mapped into gains in the core network.

Our algorithm will primarily investigate edge-user throughput improvements over possible deployment of relay nodes and its impact on the core network performance. The other KPI parameters like delay, signalling overhead etc. will be investigated with combination of WP1 packet results.

The signalling overhead of relay deployment is not considered as significant compared to data traffic in the backhaul or core network. It is estimated that core data traffic requirements will increase to 130 Gbps (Current core bandwidth requirements are less than 40 Gbps) in Europe [46].

i) Relaying in LTE-Advanced E-UTRAN Architecture:

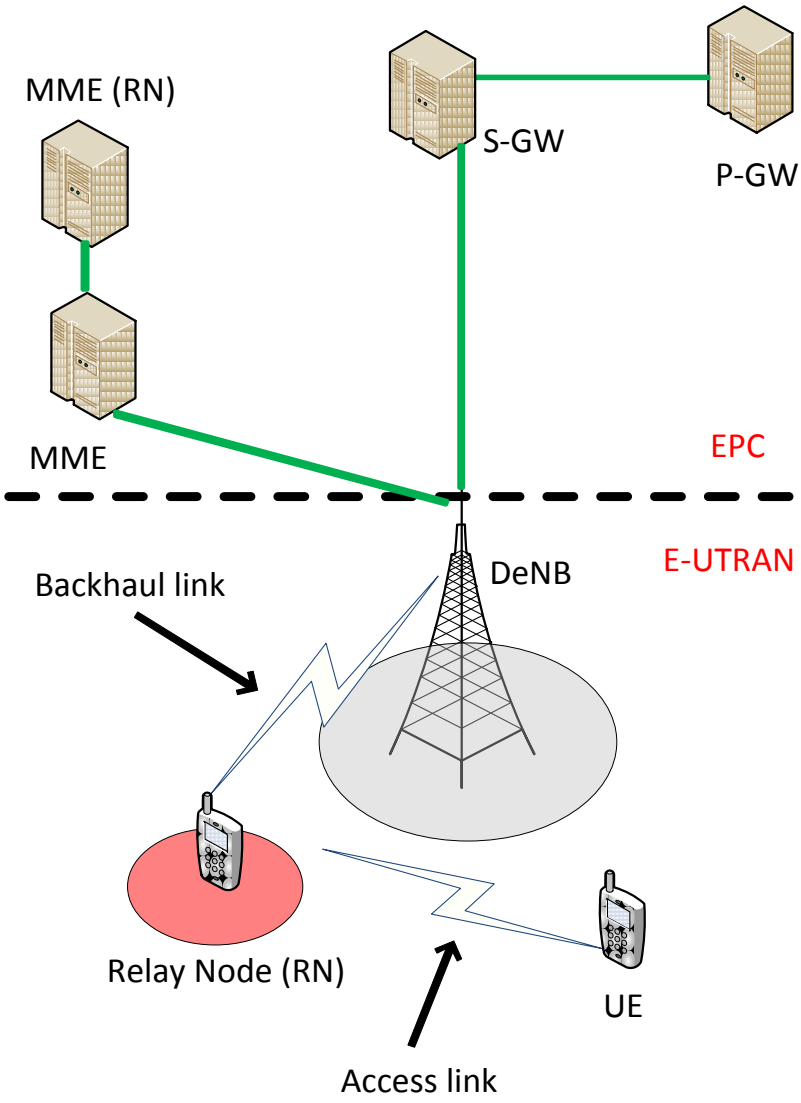


Figure 34: Evolved Packet Core (EPC) and Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)

Depending on the relaying strategy, a relay node (RN) may i) Control its own cell structure ii) Be part of the donor cell.

In the above architecture, the relay node (RN) (which is also a UE as well in our configuration) is seen as a new cell under Donor eNB (DeNB). Under S1 interface, the DeNB appears as an MME and under X2 interface, DeNB appears as an eNB to the RN. Therefore, DeNB hides the relay node (RN) that serves the UE from MMEs/GWs by providing the proxy functionalities.

In fact, DeNB acts as a gateway for RN. It creates sessions for RN and manages the EPS virtual connection for the RN, i.e. provides a transport service with specific QoS attributes. The functionality of MME (RN) is supported by MMEs.

The evolved packet core network will contain control planes MME and MME (RN) with S1 control plane (S1-c) traffic and user plane gateways with S1 user plane (S1-u) traffic.

The presented mobile relaying solution is “backhaul capacity improvement” in WP1.

ii) Impact of mobile relaying on EPC architecture

We envision two cases of deployment for the mobile relay assisted communication for EPC architecture. First, MME (RN) (or MME directly) and DeNB cooperation will be required. In this case, MME will store the location information of the UE and it will choose the appropriate relay for UE.

In the second case, DeNB will initiate relay signalling with target UE and the relay UE. In this case, DeNB will handle all coordination. This will simplify the load on EPC and will also increase the complexity of DeNB.

6.1.9 Comparison of Different Mobility Approaches Based on Mobility Costs Analysis (France Telecom)

The objective of our study is to compare analytically the performance of the classical mobility management approach which is centralized, and that of the distributed dynamic mobility management approach. In order to achieve this objective, we first define several types of mobility costs and then compare the performance of the two approaches based on these costs.

We consider three types of mobility costs:

- Signalling cost
- Tunnelling cost
- User's data packet delivery cost

Where each cost includes two parts:

- The cost of transmitting some data through the network
- The cost of processing this data at the related network entities

After expressing these costs in details for each mobility approach, we would then define some scenario in order to compare the costs of the two approaches.

7. Conclusions

From the mobility and smart traffic steering perspective, the architectures defined in section 3 should support specific functions as listed in section 4. One could argue that current 3GPP and IETF procedures may apply. However, as shown in section 5, current mechanisms do not allow to optimally address issues raised in the problem statement (section 2). Considering problem statement and applicability of current mobile networks capabilities, it is possible, at a first glance, to give some directions to MEVICO/WP2. The following sections propose work items expected to be relevant for efficient smart traffic steering in distributed and multiple-accesses mobile networks.

7.1 Handover Preparation and Decision Methods

The focus here is to optimize vertical handover, i.e. between LTE access and another radio access like Wi-Fi. Several kind of improvement is possible as neighboring access points discovery, energy saving, reauthentication speedup …

3GPP ANDSF and IEEE 802.21 standards are the main target for these topics. The corresponding testbed will give some hints about the improvement capacity.

7.2 Offloading

The use of alternate radio access like Wi-Fi will help to solve bootleneck issues of the LTE radio access.

The decision of which radio access to use may be realized either by the operator or the mobile node. The advantages of having operator managing Wi-Fi are to provide unified services anywhere, to ease optimization of radio ressources and to benefit from better indoor Wi-Fi coverage. Another benefit with the operator managed Wi-Fi solution proposed in this project is that it is possible to use existing infrastructure (fixed broadband access and modified AP) and use the UE as any other device in the home environment.

These criteria will be demonstrated in the convergence Wi-Fi testbed.

7.3 Dynamic Mobility Anchoring

Three architectures proposals have been done in D1.1 [44], from the current one that is a centralized architecture to a completely flat architecture where most of the network elements are pushed to the edge. The increase of PGW number has created the need of an optimize PGW selection.

Two demonstrators will be deployed to check the best way to select the right PGW.

7.4 End to End Transport Protocols

One main issue on mobility is a need of centralized anchor point. Some transport protocols allow to avoid the use of such anchor point. They have little or no interaction with core network element and thus be considered as end to end protocols. The protocols studied here are SCTP, NMIP and MPTCP.

Performance of each protocol will be analysed on the two demonstrators.

7.5 Flat and Distributed Mobility Management

The evolution from a centralized to flat or distributed mobility architecture has an influence on the current mobility management protocols performance. The distribution of gateways (HA in MIP or LMA in PMIP for instance) and the increase of core routing path lengths between communicating UEs create new challenges for protocols procedures, e.g., gateway selection and relocation, unoptimized data paths, load balancing, etc. Route optimization, moving networks and mobility management based at application level solve some issues tied the level of network element distribution.

Demonstrators' results will give information about the level of the optimal distribution of network elements and an overview of performance improvements as well. They will also allow comparison between similar protocols (NEMO).

7.6 User Access Authentication

Mobile network needs to authenticate the user when she initially connects or changes the point-of-attachment to the network. The problem with the current mechanisms performing the mutual authentication between the operator's network and the user is that they induce a tremendous signaling overhead, and thus are not suitable for mobility scenarios where frequent handovers occur, e.g. in scenarios with frequent inter-gateway mobility events. The current solutions also include cryptographic schemes that require a great deal of computing power from the terminal, and therefore can quickly decrease the battery life or even slowdown other operations of the device. Therefore there is a high need for new authentication mechanisms that are lightweight (i.e. suitable for resource constrained devices and

other legacy devices) and induce as less signaling overhead between the terminal and mobile network elements as possible. The demonstrators described in sections 6.1.1 and 6.1.2 address these problems and demonstrate how they can be solved with Host Identity Protocol (HIP), namely its lightweight version called HIP Diet Exchange (DEX) combined with an existing user authentication mechanism defined by 3GPP.

7.7 Support for User Cooperation

Mobile relaying allows extending cell coverage by using help of mobile nodes that are closer to the antenna. This will be helpful to achieve a fast and complete deployement solution.

The demonstrator will give indication about mobile throughput improvement. The added signaling, needed to manage relaying, will be analysed.

8. References

[1] CELTIC/MEVICO IR1.1; “Network usages and traffic scenarios”; November 2010.

[2] CELTIC/MEVICO IR1.3; “System Definition and Innovation”; March 2011.

[3] CELTIC/MEVICO IR2.1; “Requirements and constraints for smart traffic steering”; October 2010.

[4] CELTIC/MEVICO IR2.3; “Current Trends and Developments in Mobility Protocols”; October 2010.

[5] 3GPP TS 23.234;” 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 10)”; Technical Specification Group Services and System Aspects; 3rd Generation Partnership Project, 2010.

[6] 3GPP TS 23.401; “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 10)”; Technical Specification Group Services and System Aspects; 3rd Generation Partnership Project, 2010.

[7] 3GPP TS 23.402; “Architecture enhancements for non-3GPP accesses (Release 10)”; Technical Specification Group Services and System Aspects; 3rd Generation Partnership Project, 2010.

[8] Z.Faigl, L.Bokor, P.Neves, R.Pereira K.Daoud, P.Herbelin, "Evaluation and Comparison of signalling protocol Alternatives for the Ultra Flat Architecture", in proceedings of the fifth international conference on systems and networks communications (ICSNC) 2010.

[9] IETF RFC 2101; B. Carpenter; “IPv4 Address Behaviour Today”; February 1997

[10] IETF RFC 3484; R. Draves; “Default Address Selection for Internet Protocol version 6 (IPv6)”; February 2003

[11] IETF RFC 5213; Gundavelli et al..; “Proxy Mobile IPv6”; August 2008.

[12] IETF RFC 3775; D. Johnson et al.; ”Mobility Support in IPv6”; June 2004.

[13] IETF RFC 5555; H. Soliman et al.; ”Mobile IPv6 Support for Dual Stack Hosts and Routers”; June 2009.

[14] IETF Internet draft; “Multiple Interfaces Problem Statement”; http://tools.ietf.org/html/draft-ietf-mif-problem-statement; work in progress.

[15] IETF Internet draft; “DHCPv6 Route Option”; http://tools.ietf.org/html/draft-ietf-mif-dhcpv6-route-option; work in progress.

[16] IETF Individual draft; “Use case scenarios for Distributed Mobility Management”; http://tools.ietf.org/html/draft-yokota-dmm-scenario-00; work in progress

[17] IETF Individual draft; “Dynamic Mobility Anchoring”; http://tools.ietf.org/html/draft-seite-netext-dma; work in progress

[18] IETF Individual draft; “Distributed Mobility Management”; http://tools.ietf.org/html/draft-liu-distributed-mobility; work in progress

[19] IETF Individual draft; “Connection Manager requirements”; http://tools.ietf.org/html/draft-seite-mif-connection-manager; work in progress

[20] K.Daoud, P.Herbelin, K.Guillouard, N.Crespi, "Performance and implementation of UFA: A SIP-based Ultra Flat Architecture Mobile Network Architecture", in proceedings of IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2009.

[21] K.Daoud, K.Guillouard, P.Herbelin, N.Crespi, "A Network-Controlled Architecture for SCTP Hard Handover", in proceedings of Vehicular Technology Conference (VTC-fall), 2010.

[22] 3GPP, "IP Multimedia Subsystem (IMS)", TS 23.228, Release 9.

[23] 3GPP, "Policy Control and charging architecture", TS 23.203, Release 9.

[24] 3GPP, "IP Multimedia Subsystem (IMS) Service Continuity", TS 23.237, Release 9.

[25] IETF Individual draft:”NMIP” ; http://tools.ietf.org/pdf/draft-mongazon-tcpm-tcp-rehash-00.pdf ; work in progress

[26] Tatiana Polishchuk, Andrei Gurtov, "Improving TCP-friendliness and fairness for mHIP", Infocommunications Journal, February 2011, Vol III, Num 1, pp. 26-34.

[27] J. Melen, J. Ylitalo, P. Salmela, Host Identity Protocol-based Mobile Proxy, draft-melen-hip-proxy-02, February 2010.

[28] Pierrel, S., Jokela, P., Melen, J., & Slavov, K. "A Policy System for Simultaneous Multiaccess with Host Identity Protocol", IEEE ACNM2007. Munich, Germany, 2007.

[29] Bokor, L., Faigl, Z., Imre, S., "A Delegation-based HIP Signalling Scheme for the Ultra Flat Architecture", Proceedings of the 2nd International Workshop on Security and Communication Networks (IWSCN 2010), ISBN: 978-91-7063-303-4, pp. 9-16, Karlstad, Sweden, May 26-28, 2010.

[30] 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", Computer Networks, © Elsevier B.V., ISSN: 1389-1286, DOI: doi:10.1016/j.comnet.2011.02.005, 2011.

[31] IEEE, "IEEE Standard for Local and metropolitan area networks- Part 21: Media Independent Handover," IEEE Std 802.21-2008, Jan. 2009.

[32] J. Ylitalo, P. Salmela, and H. Tschofenig, "SPINAT: Integrating IPsec into Overlay Routing," in Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05), Athens, Greece, Sep. 5–9, 2005, pp. 315– 326.

[33] P. Nikander and J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extension," RFC 5205, Apr. 2008.

[34] J. Laganier and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension," RFC 5204, Apr. 2008.

[35] A. Gurtov et al., "Hi3: An efficient and secure networking architecture for mobile hosts," Journal of Computer Communications, vol. 31, no. 10, pp. 2457–2467, 2008.

[36] J. Loughney et al., "Context Transfer Protocol (CXTP)," RFC 4067, Jul. 2005.

[37] IEEE 802.21; "IEEE Standard for Local and Metropolitan Area Networks - Part 21: Media Independent Handover Services"; January 2009.

[38] J. Garcia, E. Conchon, T. Perennou, and A. Brunstrom. KauNet: Improving reproducibility for wireless and mobile research. In Proceedings of the 1st International Workshop on System Evaluation for Mobile Platforms (MobiEval 2007), pages 21–26, San Juan, Puerto Rico, USA, June 11–14, 2007

[39] S. Hemminger , "Network Emulation with NetEm", Linux.conf.au 2005 (LCA2005)

[40] Z. Faigl, S. Lindskog, A. Brunstrom, "Experimental Evaluation of the Performance Costs of Different IKEv2 Authentication Methods" In: Networks 2008: 13th International Telecommunications Network Strategy and Planning Symposium. Budapest, Magyarország, 2008.09.28-2008.10.02. (IEEE) pp. 1-19. (ISBN: 978-963-8111-68-5) DOI: 10.1109/NETWKS.2008.4763728

[41] IKEv2 Project, Visited: July 19, 2011. http://freshmeat.net/projects/ikev2.

[42] Strongswan Charon, Visited: July 19, 2011. http://wiki.strongswan.org/projects/strongswan/wiki/IKEv2Examples

[43] InfraHIP Project: Home, Visited: July 19, 2011. http://infrahip.hiit.fi/

[44] CELTIC/MEVICO D1.1; "Architecture Design Release 1"

[45] 3GPP Release 10: website: http://3gpp.org/Release-10

[46] "Architectural Considerations for Backhaul of 2G/3G and Long Term Evolution Networks'' Cisco White paper

[47] CELTIC/MEVICO IR2.5; "First Evaluation Report"

[48] IETF working group "http://datatracker.ietf.org/wg/mext/charter/"

[49] HIPSim++: A Host Identity Protocol (HIP) Simulation Framework for INET/OMNeT++, Official homepage: http://www.ict-optimix.eu/index.php/HIPSim

[50] 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), Tenerife, Canary Islands, Spain, Oct. 26. 2009.

9. Annexes

9.1 Identifier and Locator Separation in Mobile Networks

The main challenge of future IP networks is scalability and sustainability. The evolution of the network architecture, together with mobility, traffic and network management functions must face with highly increasing traffic demands. If end-to-end sessions in the service stratum are bound to short-lived locators, several functions like seamless mobility management, transparent network renumbering becomes complex.

In current IP networks IP addresses are used in the transport stratum for packet routing and node location, and in the service stratum for end-to-end communication by the transport and above protocols. Nodes (or users) are identified on service level by an identification scheme. Several identification schemes exist, e.g., the E.164 numbering, Unified Resource Locator, Unique name system, or the H.323, SIP, telephone and mail uniform resource identifiers. Identifiers are mapped to locators with Domain Name Service, location registrars, or similar address resolution services. Finally, IP addresses are used in the transport and higher layers to identify the sessions. Mobility of users, terminals, flows, networks causes locator changes that must be made transparent for ongoing sessions.

The ID/LOC separation architectures introduce a new namespace for identifying the nodes with NodeIDs. Hence they require a mapping function between IP addresses and identifiers. For scalability reasons the mapping function should not be centralized in the core network but distributed at the end nodes and the access networks, as proposed by ITU-T Draft Y.2015. In the core network the transport stratum can use IP addresses as locators to forward the traffic to the appropriate access network. The ID/LOC mapping function can be put in the access networks and in the end nodes to enable traffic and mobility management of service sessions based on IDs. This architectural approach also enables translation of the locators between the core and access networks if it is required by future routing mechanisms. The mapping function introduces complexity, but has the following advantages.

Advantages of ID/LOC separation architectures:

- End-user capabilities:
  - Seamless for the service level when a terminal or an application flow changes its locator due to mobility or smart traffic steering. However not every single ID/LOC solution enables efficient mobility, there are several schemes (e.g., Host Identity Protocol – HIP, Location Independent Network Architecture for IPv6 – LIN6) which provide advanced mobility management even in the most complex scenarios.
  - Easier binding of the peers to sessions due to their long-lived identities.
  - Allows IDs to be used in the long-term security and trust relationships.
- Network provider capabilities
  - We can introduce in the future scalable routing mechanisms using e.g., topologically aggregatable locators, without the influence of node identification on the routing policies.
  - Future routing solutions (e.g., georouting) that will require new locator namespaces can be introduced in the network independently from the long-term identities. By putting the ID/LOC mapping function to the access network, new locator namespaces and routing mechanisms can be introduced locally in the given access network.
  - Network renumbering in the customer premise networks, access network, or in the core will be more transparent for ongoing services (O&M)
  - ID/LOC eparation can play a role in supporting load sharing, e.g. multiple locators can be assigned t one identity.
- Service provider capabilities
  - Delivery of application services is independent from locator changes due to mobility or renumbering.
  - Session management in mobile and multihoming environment becomes simple on the service level. The ID/LOC split method can deal with multihoming on the locator level.

  Disadvantages of ID/LOC separation:
  - ID/LOC separation still needs support on the level of packet headers, in order to fully benefit from it. I.e., if we want that traffic steering, flow mobility, routing policies should identify flows based on IDs, a continuous mapping is needed between the locators (i.e., the source and destination address) together with other parameters (e.g., the ports, security parameter index (IPSec), transport protocol and application type) and the ID. This mapping could be replaced if we added a new control plane header including the the source and destination identity, and application type.

Another possibility is just to include the hash of these as an additional information into the headers, and use this has value to identify traffic flows by traffic management, routing, multihoming mechanisms.

A special case of ID/LOC separation is when cryptographic identifiers are used. In these cases IDs are derived from public keys of the nodes or the users. If the user or the node signs a message with its private key, the message will be self-certifying for any peer knowing the public key. Instead of PKI certificates, the list of authorized identities is enough to know for access authorization. Secure ID/LOC scheme can provide the basis for peer and message authentication procedures and for access authorization, furthermore it can contribute to more secure accounting services. However, for a mobile device it is infeasible to maintain a list of trusted IDs (e.g. trusted GWs), yet the mobile device needs some mechanism to verify that the identity of the peer host (e.g. a GW discovered in opportunistic manner) indeed belongs to the operator. For this purpose, some extra mechanism to verify the identities is needed. This could be, e.g. a standard shared secred-based 3GPP method that is incorporated into the ID/LOC authentication protocol.

Users may have several cryptographic identity tags, including blinded and/or temporary tags providing certain anonymity. This naturally requires some mechanism in the mobile network to track and possibly issue the temporary tags, as well as map them to the permanent identity.

9.2 Functions Distribution/Flattening: a first analysis

Section 4 gives a list of generic functions which may be impacted by distribution or multiple accesses requirement. Obviously, the EPC decline these functions and share out them between functional entities. Section 3 introduces the concept of flat architecture splitting network functions between flat and centralized gateways. However, at the time of writing, we do not have a clear view of which function to flatten or not. Even if not crystal clear yet, such an approach would allow to go further the only organic distribution. So, after having reminded the EPC network functions supported in each functional entity, he following tables provide a first analysis of the functions that may be distributed/flattened. This work is expected to be completed in next revision of that document.

EnodeB The eNodeB supports the LTE air interface and includes functions for radio resource control, user plane ciphering and Packet Data Convergence Protocol (PDCP)	User plane	Control plane	initiation	decision	execution	Proposed to be flattened
Functions for Radio Resource Management		x				Already flat
IP header compression and encryption of user data stream	x					Already flat
Selection of an MME at UE attachment when no routing to an MME can be determined from the information provided by the UE		x	x	x		Already flat
Routing of User Plane data towards Serving Gateway	x				x	Already flat
Scheduling and transmission of paging messages (originated from the MME)		x			x	Already flat
Scheduling and transmission of broadcast information (originated from the MME or O&M)		x			x	Already flat
Measurement and measurement reporting configuration for mobility and scheduling		x	x	x		Already flat

Mobility Management Entity	User	Control	initiation	decision	execution	Proposed

(MME): The MME manages mobility, UE identities and security parameters	plane	plane				to be flattened
NAS signaling and related security		x			x	
Inter CN node signaling for mobility between 3GPP access networks (terminating S3)		x			x	
Idle mode UE tracking and reachability (including control and execution of paging retransmission)		x	x	x	x	
Tracking area list management		x				
GW selections (Serving GW and PDN GW selection)		x	x	x		
MME selection for handovers with MME change		x	x	x		
Roaming (terminating S6a towards home HSS)		x				
SGSN selection for handover to 2G or 3G 3GPP access networks		x	x	x		
HRPD access node (terminating S101 reference point) selection for handovers to/from HRPD		x				
Authentication		x			x	
Bearer management functions including dedicated bearer establishment		x	x	x		
Lawful Interception of signaling traffic		x			x	
Support for Single Radio VCC and CS Fallback for 2G/3G and 1xRTT CDMA		x				

Serving Gateway (SGW) The Serving Gateway is the node that terminates the interface towards EUTRAN. For each UE associated with the EPS, at a given point of time, there is one single Serving Gateway	User plane	Control plane	initiation	decision	execution	Proposed to be flattened
The local Mobility Anchor point for inter-eNodeB handover	x					
Mobility anchoring for inter-3GPP mobility (terminating S4 and relaying the traffic between 2G/3G system and PDN Gateway).	x					
EUTRAN idle mode downlink packet buffering and initiation of network triggered service request procedure	x		x	x	x	
Transport level packet marking in the uplink and the downlink, e.g. setting the DiffServ Code Point, based on the QCI of the associated EPS bearer (through interface with PCRF?)	x				x	
Accounting on user and QCI granularity for inter-operator	x	x				

charging						
Lawful Interception	x					
Packet routing and forwarding	x				x	

Packet Data Network Gateway (PDN Gateway) The PDN Gateway is the node that terminates the SGi interface towards the PDN. If a UE is accessing multiple PDNs, there may be more than one PDN GW for that UE.	User plane	Control plane	initiation	decision	execution	Proposed to be flattened
UE IP address allocation	x				x	
DHCP functions		x		x	x	
Policy enforcement (through interface with PCRF?)	x				x	
Per-user based packet filtering (by e.g. deep packet inspection)	x				x	
Packet screening	x					
Lawful Interception	x					
Charging support	x					

ePDG	User plane	Control plane	initiation	decision	execution	Proposed to be flattened
Tunnel authentication and authorization		x				
Transport level packet marking in the uplink	x					
Policy enforcement of Quality of Service (QoS) based on information received via Authorization, Authentication, Accounting (AAA)	x					
Lawful interception	x					

ANDSF	User plane	Control plane	initiation	decision	execution	Proposed to be flattened
Discovery information		x	x			
inter-system mobility policies		x	x			

PCRF-PCC	User plane	Control plane	initiation	decision	execution	Proposed to be flattened
Policy decision		x		x		
PCC rules storage			x			

3GPP AAA server	User plane	Control plane	initiation	decision	execution	Proposed to be flattened
AAA function		x				x