

Adopting IMS in WiFi Technology

Mehdi Mani^{*}
GET-INT-Institut National des
Télécommunications
9 Rue Charles Fourier
Evry, 91011, France
mehdi.mani@int-edu.eu

Noel Crespi[†]
GET-INT- Institut National des
Télécommunications
9 Rue Charles Fourier
Evry, 91011, France
noel.crespi@int-edu.eu

ABSTRACT

IP Multimedia Subsystem which is standardized by 3GPP is an important step to improve the delivery of innovating IP-Telephony and Multimedia services to the customers in 3G and B3G networks. However, IMS is almost access independent and multiple access technologies such as UMTS, WiFi, WiMax, xDSL and Cable Technology can benefit from IMS services. In 3GPP Releases 6, an architecture for access to 3G services (including IMS services) from WLAN technologies has been standardised and the work is being completed in next releases. The goal of this architecture is to allow the 3G customers to be roamed in WLAN and access to their services in 3G domain. To this end, 3GPP has chosen a Master/Slave approach which does not bring forth IMS services directly for WLAN customers and limit the applicability to some limited scenarios such as when the WLAN and 3G domain are under control of a same operator. In this paper we propose different scenarios for adopting/adapting IMS in/for WiFi as the dominant WLAN technologies. These scenarios allow the independent WiFi operators to provide advance IP Telephony services based on IMS by themselves in addition to the broadband Internet access. These scenarios are proposed with considering the capability of various WiFi operators.

Keywords

IMS, Horizontal Convergence and IP Telephony

1. INTRODUCTION

IMS-IP Multimedia Subsystem [1] was firstly released in March 2003 by 3GPP Release 5 to provide IP based multimedia

^{*}Mehdi Mani is PhD candidate at Wireless Network and Multimedia Service Department in GET-INT. He is a member of Core Network and Service Architecture Team. His research interest is Overlay Networks and Seamless Services.

[†]Noel Crespi is professor at Wireless Network and Multimedia Service Department in GET-INT. He is leading the Core Network and Service Architecture Lab.

services in the mobile market. Based on SIP (Session Initiation Protocol), IMS is the most complete IP-based service control and management system that sets up an overlay on the under-laying transport infrastructure and provides the possibility of end-to-end IP based multimedia services.

IMS with a set of functional entities (including SIP servers and proxies) and interfaces handles establishment, modification and termination of multimedia sessions.

IMS is a significant step to improve the delivery of innovating and advanced IP-based multi-media services to customers because it simplifies the implementation of new services and reduces constraints of time to market and impacts on the existing IP networks.

IMS, according to its access independent architecture, is capable of blending different access technologies in order to achieve horizontal Fixed/Mobile convergence (FMC). The horizontal convergence is an approach in contrast with traditional vertical convergence of service-specific networks. In vertical convergence, the inter-connection is only in bearer level. However, in horizontal convergence: Firstly, the users of one domain can benefit from the services developed in other domains and secondly different technologies can combine their services to create new advanced services and more capabilities for their clients. Some examples of combined services may be: *Video on Demand (VoD) streaming to cell phone, Content Sharing between Cell Phones, Personal Video Recorders (PVR), PDA, PC and other devices, uploading the content of a daily web-log by submitting an SMS without need of additional softwares, Unified Messaging, One-Number phone service, etc.*

In 3GPP Release 6, access to packet switch 3G services including IMS services via WLAN was standardised. In the defined architecture, IMS services deployed in 3G domains will be accessible for 3G customers via WLAN. IMS services will not be accessible for WiFi customers who are not subscribed in 3G domain. Moreover, there will not be the possibility of service convergence in such approach. Therefore, such scenario will be limited for the scenarios where the 3G and WiFi accesses are deployed by the same operator or WiFi technology has very limited core network capabilities.

In contrast, such an architecture is not enough for the independent WiFi operators who own enough core network infrastructure. In fact, it is very likely that they desire to

deploy their own IMS or IMS-like services. Deployment of IMS in WiFi leads to horizontal convergence of 3G and the 802.11 broadband wireless accesses. The WiFi customers can enjoy the IP Telephony services that IMS can propose in addition to the Internet services. Moreover, the users of each domain can benefit from the services deployed in other domain. Finally IMS can yield to convergence of telecom and web services and brings out new capabilities and applications for the clients.

In this paper after introducing IMS in the next section, we investigate its independence from access technologies in section 3. We categorize the IMS elements which need adaptation according to the underlying technology and introduce the access dependent interfaces. Section 4 is devoted to the deploying of IMS in WiFi technology. The architecture specified by 3GPP for WLAN access to IMS will be discussed and then we introduce three architecture for adopting IMS in WiFi domain according to the operator capabilities. Finally the paper is concluded.

2. IMS ARCHITECTURE

The IP Multimedia Subsystem (IMS) is a SIP-based service control overlay standardised by 3GPP. It provides a clean split between services and data transport with the potential to enable control and management of services over multiple transport technologies.

Due to exploiting an IP based and flexible signaling protocol such as SIP, IMS provides the possibility for providing End-to-End IP multimedia services, increased potential for service integration and easy adoption and integration of different services such as instant messaging, presence [9] and video conferencing[8].

2.1 IMS Functional Elements

The construction of IMS architecture is based on three main *Call Session Control Functions (CSCF)*: *P-CSCF*, *S-CSCF* and *I-CSCF* which stand respectively for *Proxy-CSCF*, *Serving-CSCF* and *Interrogating CSCF*.

P-CSCF: Proxy-Call Session Control Function is the entry point of the IMS for the User Equipment (UE) and proxies the SIP messages to the proper CSCF in the core. It is also the entity that should secure the link for the client to protect the privacy of its messages. Moreover, it may support SIP compression in order to reduce the load on the radio interfaces. UE can discover P-CSCF using DHCP. *I-CSCF* (Interrogating-CSCF) is the entry point of the operator's IMS for other operators' CSCFs. It may hide topology, configuration and capacity of the domain by supporting Topology Hiding Inter-network Gateway (THIG) functionality. I-CSCF acts as a SIP-proxy by routing SIP requests received from another network towards the S-CSCF. In addition, in the registration phase, it assigns the right S-CSCF to the UE. This assignment will be carried out by interrogating the HSS to check the S-CSCF capabilities and user profile.

S-CSCF (Serving-CSCF), acts as a SIP Registrar as defined by IETF RFC 3261 [7] located in the user's home domain. It controls the session of registered users and invokes the requested services. The S-CSCF may reject communication

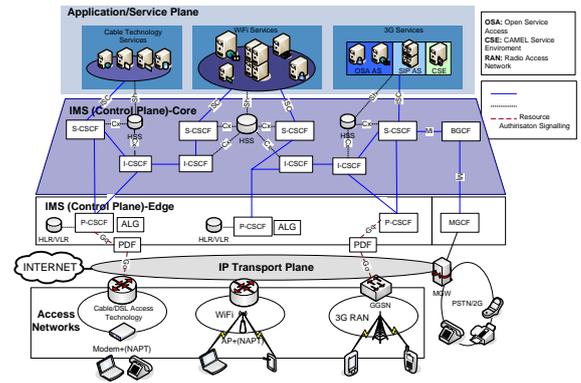


Figure 1: Architecture of IP Multimedia Subsystem

when the media parameters are not in line with the user's service profile or with the local policy.

In addition to these call session control entities, other main IMS entities can be summarized as follow:

PDF (Policy Decision Function): This is logically a centralized entity that makes the policy decision according to the policy rules and the dynamic and static information of the network. This decision will be transferred via Go interface to the edge router (ie GGSN in 3G) which plays the role of Policy Enforcement Function (PEF). Consequently, according to the PDF decision, PEF allocates the resources for the session media. In Release 5, the PDF was enclosed in the P-CSCF. But Release 6 introduces a clear separation between the P-CSCF and the PDF function and the Gq interface was defined between P-CSCF and PDF [1] as shown in Fig.1. With this extension, other non-SIP based services will also benefit from the resource control mechanisms.

HSS- Home Subscriber Server, in addition to location information, holds the user identifications and the relations between the different public and private identifiers of users for Authentication, Authorization and Accounting (AAA).

AS (Application server) gathers specially a collection of SIP Servers for basic services including *Caller-ID*, *Call Forwarding* and *Messaging* as well as advanced services such as *Presence*, *Multimedia Messaging*, *Push to talk/video* and *Conferencing*. The AS is either localized in the user's home network or in a third party domain.

BGCF which stands for *Breakout Gateway Control Function*, determines the next hop for routing the SIP message toward PSTN domain. For PSTN terminations, the BGCF selects the network in which PSTN/CS Domain breakout is to occur. If the BGCF determines that the breakout is to occur in the same network in which the BGCF is located, then the BGCF selects a MGCF which is responsible for inter-working with the PSTN/CS Domain. If the break out is in another network, the BGCF will forward IMS messages to another BGCF in the selected network.

The *MGCF*-Media Gateway Control Function is considered as a SIP endpoint. It translates ISUP/BICC messages of the PSTN side to SIP signalling of the IM CN subsystem

side and vice-versa. The MGCF performs the inter-working to the PSTN and controls the Media Gateway (MGW) for media conversions.

2.2 Access to IMS Services

In order to access to an IMS service and to establish a session, a user needs to pass five phases:

- 1) Attachment to the network and authentication.
- 2) IP connectivity
- 3) Discovering the P-CSCF.
- 4) Application level registration.
- 5) Session setup and resource reservation.

In the first three phases, the user will be attached to the network and be authenticated. Then, it will be allocated an IP address by the edge router in the domain of attachment. In the next step the user should discover the P-CSCF as the entry point in the IMS.

From this step on, the user will be able to register himself with IMS. This process is called service level registration. In this phase the user will send a REGISTER message toward its home domain. This message will be forwarded to the proper I-CSCF in home domain by P-CSCF. As the first action, I-CSCF interrogates the HSS for the user profile to verify if this user is allowed to be connected to the IMS domain via the current P-CSCF. If user profile meets the condition, I-CSCF ask HSS to assign the proper S-CSCF to the user according to its service filter criteria. Then the REGISTER message will be forwarded to this S-CSCF and the user will be localized with this server. It means that the S-CSCF will bind the current IP address of the user with its Public ID(s) (or SIP URIs). A condensed signaling flow for service level registration is depicted in Fig.2.

After registration in IMS domain, the user is able to establish a session and benefit from the IMS services. For this purpose, the user launch an INVITE request toward another party (or a server in IMS domain). This request contains the proposed session parameters by the caller and will be routed to the callee. If the session parameters were also approved by the callee, the required resources will be reserved in bearer level (ie IP transport) for the media related to this session.

However, it should be mentioned that the process of resource reservation depends on network access technology and operator policies. IMS architecture enables a policy based resource reservation approach. P-CSCF extracts the session QoS parameters and transfers these information to PDF via Gq interface. PDF according to the user profile and network policies determines the amount of resources that should be allocated to this session's media and transfers its decision to the router that supports the PEP-Policy Enforcement Point functionality. In 3G, for instance, GGSN is dedicated to support this later functionality. Therefore, Go interface is defined between PDF and GGSN. This interface is based on COPS which is defined in RFC 2748 in IETF [13].

3. ANALYSE OF IMS INDEPENDENCE FROM ACCESS TECHNOLOGY

One of the aims of 3GPP Release 6 was to improve IMS architecture to be, as much as possible, independent of the

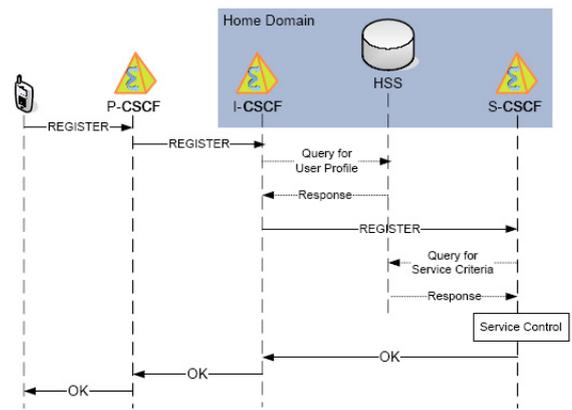


Figure 2: Service Level Registration in IMS

access technology. This enables users to access the same services when they are either under UMTS/WLAN coverage or connected to xDSL technology. Despite of this aim, there are a number of unavoidable access specific interfaces in IMS to the under-laying transport layer such as:

- Common interfaces for collecting accounting information from bearer level.
- Interfaces for coordination and enforcement of QoS to bearer level (ie Go)

Therefore, these interfaces and the IMS functionalities that are directly connected to them should be adapted to the under-laying technology characteristics. We have extracted out these IMS functions/elements. They are the functionalities which are categorized as IMS edge in Fig.1:

- *P-CSCF* is the most important IMS entity that has some functions which need to be adapted to their underlying technology. These P-CSCF functions are as follow:

SIP message Compressing Protocol: Each access technology may use different compressing protocol to reduce the IMS message sizes. For example, the compressing method used in WLAN may be different from that of UTRAN. Moreover, in the case of broad-band wire-line access technologies, compressing protocol may be simply ignored in P-CSCF.

Session Security Functions: The security level also depends on the access technology. In 802.11 because of shared medium and low intrinsic security, the operator may use IPSec tunnel between UE and P-CSCF. However in xDSL there is no need for such a strict condition. In addition the operator may use security protocol in session layer too. For example, one may use Secure SIP (SSIP) [7] to add additional security level.

QoS functionalities: In 3G, the P-CSCF will extract the session media parameters that exist in SDP in the body of SIP messages to send to PDF. These parameters describe the media type (voice, video), its codec and the required QoS level. PDF according to the mentioned session parameters, user profile, and network policies send a token to the PEP (Policy Enforcement Point) resided in GGSN. And

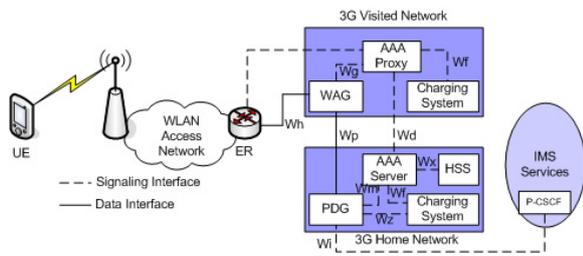


Figure 3: 3GPP Approach for Access to IMS services via WLAN

then GGSN reserve the resources for the media of the session according to the received token. However, in the case of WLAN, there is no necessarily resource reservation process. Therefore, the P-CSCF does not need to start the resource reservation process and extracting the session media parameters.

- *Application Level Gateway (ALG)* is another functional element whose existence in IMS depends on the underlying technology. ALG is required in order to modify the IMS messages which pass through NAT. There are some headers in IMS messages such as *Contact*, *Via*, *To* and *From* that contain the IP address of the end points, therefore every modification in IP address should be also carried out in these headers of SIP messages. ALG is the functionality that takes care of these modifications in IMS overlay. If the access network IP stack (ie IPv4) is different from IMS domain IP stack (ie Ipv6), or when the operator supports the users behind NAT, this functionality is required.

- *HLR (Home Location Registrar)*: For the Multi-access to IMS, it is more convenient to implement the HLR functionality separated from HSS. This is basically because the user location information required for user localization depends on access technology. In 3GPP IMS, HSS is in charge of users' localization by supporting HLR functions. For the 3G technology Cell ID indicates the user point of attachment. The 3G User devices are aware of their location and they obtain this information during their attachment phase. They put Cell ID information in a dedicated header in the REGISTER request and transfer it to their IMS home domain. Consequently, the Cell ID will be stored in HSS. However, in the case of other access technologies, there are two main concerns that support the separation idea of HLR function from HSS: Firstly, the definition of attachment point information is somehow challenging that depends tightly to the implemented technology. For instance, in WiFi, *SSID-service set identifier* may also be used for indicating the attachment point. SSID is a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. *BSS-Basic Service Set* is an *access point (AP)* which is connected to the wired network and a set of wireless stations. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. Secondly, there are some devices which are not able to capture their location information. This is an issue specially with legacy Telephone devices in fixed access technologies like DSL and Cable. Therefore,

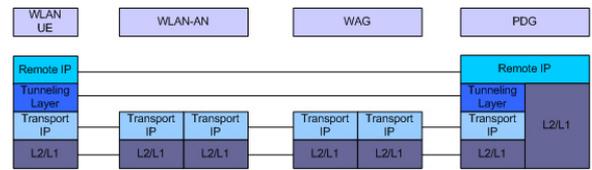


Figure 4: IP Connectivity configuration proposed by 3GPP for WLAN-3G Inter-working

other functionalities should be anticipated to add location information in the packet headers.

According to these reasons, the HLR structure and related interfaces should be adapted to access technology. The user location information will be created according to the access characteristics and be registered in HLR. Then HSS, as the main database for user profile provides a pointer to these information.

4. 3GPP APPROACH FOR ACCESS TO IMS THROUGH WIFI

Based on IEEE WLAN 802.11 protocol, WiFi technology is mainly developed to provide broad-band wireless access to Internet services in hot spots. By adopting IMS as the service control overlay, advanced telephony services can also be deployed in WiFi domains with a robust and scalable architecture. However, different WiFi operators may choose different strategies for deployment of IMS according to their network configuration, capabilities and resources. The simplest strategy is to define the proper interfaces to let the clients to have access to IMS services which are deployed in 3G domain via 802.11 WLAN and IMS will not be deployed in WiFi domain. Such architecture is called Master-Slave architecture. The 3G operator will be considered as the Master and defines all the required functionality for bearer level inter-connection as well as AAA functionality in service control layer.

The standardisation work in 3GPP for WLAN-3G inter-working in Release 6 and 7 is based on this strategy. In Release 6, in the feasibility study stage, six scenarios with Master-Slave WLAN-3G inter-working architecture are introduced[3].

In scenario one, the mobile domain users will be able to have direct access to internet through the WLAN Access Network. This is the only service in this scenario and the user will receive a single bill from its mobile operator for WLAN and UMTS access.

In scenario 2, the user is still only able to access to internet via WLAN. However, in the absence of direct connection of WLAN to internet, the user may use the IP core provided by 3G domain to access to internet services. The goal of scenario 3, on which we focus in this section, is to allow the operator to extend 3GPP system Packet Switch based services to the WLAN. These services may include, for example, IMS based services, location based services, Multimedia Broadcast/Multicast Services (MBMS), and any service that is built upon the combination of several of these components. Scenarios 4 and 5 are founded based on scenario

Table 1: WLAN and UMTS differences for access to IMS

	WLAN	UMTS
Number of actors in roaming case	Three: WLAN AN, VPLMN and HPLMN	Two: VPLMN and HPLMN
Go, policy control	This is not defined at all in 3GPP for WLAN accesses	This is defined by 3GPP for UTRAN
Notion of "tunnel for signalling"	No notion of "secondary tunnel" is defined for WLAN Interworking, which means that both signalling and data packets will use the same tunnel	The notion of Secondary PDP Context allows differentiating the PDP Context for signalling and the PDP Context for data
Support of IPv4 necessary on the Local IP layer	IPv4 must be supported on the Local IP layer because many WLAN Access Networks will only support IPv4 in early deployments, as IPv6 must be needed for IMS, this means that the WLAN UE must support the dual stack	The use of IPv6 only is possible as long as the SGSN and GGSN can support it; in such a case, the UE can be based on IPv6 only as far as IMS is concerned

3 and deal with mobility, service continuity and seamless service aspects and scenario 6 is to provide Circuit Switch (CS) domain services.

Scenario 3 architecture is depicted in Fig.3. There are four new functional elements that are defined for the purpose of access to 3G services via WLAN as follows.

3GPP AAA Proxy and Server are defined To implement the AAA functionality defined by 3GPP for WLAN accesses [4]. 3GPP AAA Server is located in the 3G home domain. It retrieves authentication information and subscriber's profile from the HLR/HSS for each user and authenticates the users based on the information received from the HLR/HSS. These information are transferred to WLAN for admission control of the users. In addition, this entity provides the Charging Information.

3GPP AAA Proxy is used in roaming situations and it works as a proxy between UE in the WLAN and the 3GPP AAA Server in the 3G home domain.

In addition to these AAA functional elements, in bearer level two new elements are defined to create secure connection to 3G domain.

WAG-WLAN Access Gateway is the entry point of the mobile network from the WLAN perspective. In the case of roaming, the UE will be connected to the WAG in the visited network. WAG (either in home or in visited network) forwards the data toward the Packet Data Gateway in home domain. WAG also transfers the bearer level charging information to 3GPP AAA Proxy/Server.

PDG- Packet Data Gateway is the edge router in the 3G home domain that establishes and controls the connection of the user to the external network and services (ie IMS overlay) located in 3G domain. It allocates remote IP (as depicted in Fig.4) to the UE and creates a tunnel between itself and UE in WLAN. Then it maps this tunnel to the external tunnels toward external networks. As shown in Fig.4, it can be noted that two IP layers are represented in this protocol stack. In fact, with such configuration, the PDG can be seen as the last hop router for the UE from the

external network view and in addition the 3G Core Network configuration has no impact on the IP connectivity of the UE in WLAN. Fig.5 shows the complete procedure to setup a session for an IMS service.

Finally it should be mentioned that according to the intrinsic differences in WLAN 802.11 and UTRAN technologies the condition of access that these two technologies provide for IMS services are not exactly the same. 3GPP has not considered resource reservation for WLAN accesses to IMS services. Therefore there is no equivalent interface for Go in WLAN case. As mentioned before, Go is an interface between PDF and GGSN in order to transfer the policy decisions for resource reservation. The differences between WLAN 802.11 and 3G technologies that should be taken into account for access to 3G services including IMS are listed in table 4.

5. GOING BEYOND THE 3GPP PROPOSAL BY ADOPTING IMS IN WIFI DOMAIN

The 3GPP approach for providing WLAN access to IMS services is satisfactory for certain operators with specific conditions such as: i) the operators that own both of WiFi and 3G access technologies; ii) WiFi operators who do not de-

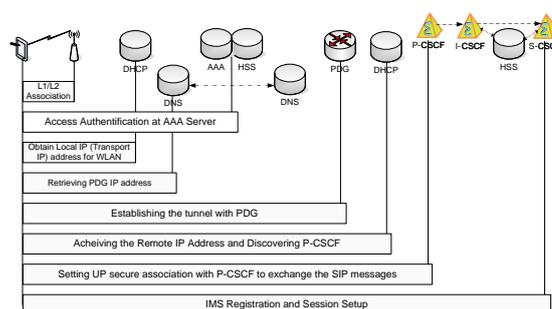


Figure 5: Different Phases of access to IMS Services from WLAN according to 3GPP approach

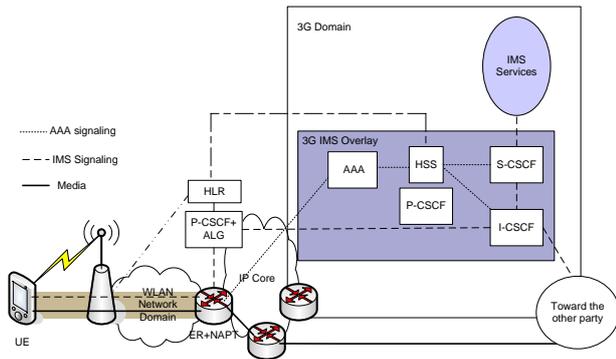


Figure 6: First phase of deploying IMS in WiFi domain

sire to invest too much for the deployment of IMS on their own domain. However for the WiFi operators who have deployed their own core network, this architecture may not be acceptable for several reasons as follows.

Firstly, from the business point of view it is unlikely that such a WiFi operator accepts that all the IMS services reside in 3G domain. Secondly, in such a Master/Slave interworking architecture, all the policy for interconnection is defined by 3G operator which is very unlikely acceptable for WiFi operators. Thirdly, the process of setting up the IMS services via WLAN will be so complicated (as depicted in Fig.5). Fourthly, the remote IP address that allows the user to be connected to IMS domain is assigned by the 3G domain. Therefore, if 3G has deployed its IMS based on IPv6 (as what is defined in standard), the end users in WLAN should support a multi-stack IPv4/IPv6 protocol.

Consequently, WiFi operators who own enough resources and desire to support IMS services may adopt IMS as the service overlay in their own domain instead of just being connected to 3G IMS.

Deployment of IMS in WiFi network domain leads to horizontal convergence of 3G and WiFi technology. In such architecture a user may be accessible by a unique number via both of UTRAN and 802.11 access technologies. Moreover, the users of each domain can benefit from the services deployed in other domains.

Nevertheless, to deploy the IMS overlay, WiFi operators may choose a step by step and evolutionary strategy to avoid a sudden huge cost for deploying the IMS services. To this end we have proposed several phases for adopting IMS in WiFi technology. In the first phase, as depicted in Fig.6, the WiFi operators may just implement the functionality of P-CSCF. The P-CSCF will define the security strategy and the compressing protocol to reduce the size of SIP messages. For inter operability with IPv6 domain, NAPT (Network Address/Port Translator) and ALG-Application Level Gateway functionalities are required. NAPT should be implemented in edge router to replace the IPv4 and IPv6 addresses at the

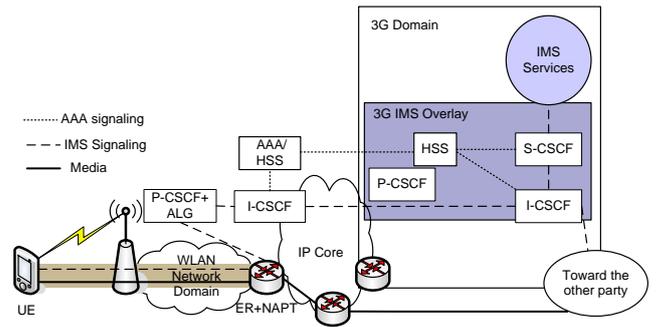


Figure 7: Second phase of deploying IMS in WiFi domain: AAA functionality in WiFi Domain

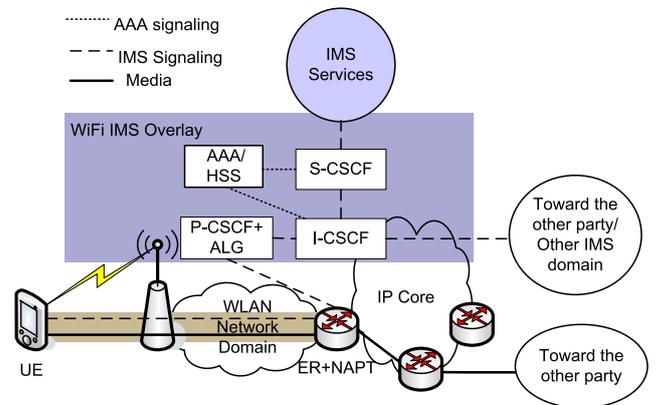


Figure 8: Last phase of deploying IMS in WiFi domain: Complete IMS

edge of the network in bearer level. ALG functionality, in this phase of IMS deployment, may be added to P-CSCF. With such architecture, the end users do not need to support multi protocol stack of IPv4/IPv6 in order to access to IMS services. Moreover, in this approach, there is no need of implementation of PDG and WAG. In fact, the WiFi operator connects its network directly to the network backbone without passing through 3G network. However for session routing, the SIP messages in this phase are still required to be routed via 3G domain.

HLR is also implemented in WiFi domain and the SSID will be considered as the attachment point information. In the next phase of IMS deployment (Fig.7), WiFi operators deploy also both of HSS and I-CSCF. In this phase, WiFi operators will be able to carry out AAA functionalities in their own domain. Therefore the WiFi operator is able to manage provides the public and private identification for their clients independent of the 3G operator. I-CSCF interrogates HSS to assign a S-CSCF to the user according to his service criteria. In this phase service triggering functions carry out in 3G domain, however WiFi is able to add some advance and combinational services to the existing services

in 3G domain in order to enrich the existing services for the clients. Finally, in the last phase as depicted in Fig.8, the IMS overlay will be deployed completely. S-CSCF in WiFi domain localizes the clients when they register for IMS services and invokes the services for them when they request. SIP based services will be implemented in this phase in IMS overlay of WiFi domain. In this phase in both of bearer and signaling level WiFi is independent of 3G and can connect to the rest of the network directly.

The step by step IMS deployment provides a smooth migration toward WiFi-with-IMS for the operators. The WiFi operators, according to their strategies and capabilities, may choose one of the proposed architecture.

6. CONCLUSIONS

In this paper different strategies for adopting IMS in WiFi technology was proposed. IMS as the most complete service control overlay can bring out horizontal convergence of different access technologies which consequently leads to advance services like unique numbering and web and telecom service convergence. We presented the challenges and limitations of the proposed approach by 3GPP for 3G-WLAN interconnection. Then to cope with this limitations, In this paper we proposed three phase-by-phase strategies of IMS deployment in WiFi technology. The defined strategies allow the WiFi operators to inter-connect their networks to 3G domain in a win-win condition. The defined strategies get over the existing problems in 3GPP approach such as Master/Slave inter-working architecture, complicated session set up process and requirement of multi stack support in end user device.

7. REFERENCES

- [1] 3GPP, IP Multimedia Subsystem (IMS), TS 23.228, Release 8, Version 8.0, March 2007.
- [2] ETSI, TISPAN, NGN Functional Architecture, ES 282 001, V1.1.1 August 2005.
- [3] 3GPP, Feasibility study on 3GPP system to WLAN interworking, TR 22.934, Release 7
- [4] 3GPP, 3GPP system to WLAN interworking, TS 23.234, Release 7, Version 7.50, March 2007.
- [5] 3GPP, Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), TS 24.228, Release 5, v5.15.0, Oct 2006.
- [6] ITU-T Rec. Y.2001, "General Overview of NGN," Dec. 2004.
- [7] IETF, RFC 3261, Session Initiation Protocol, June 2002.
- [8] 3GPP, Conferencing Using the IP Multimedia Core Network Subsystem, TS24.147, Release 7, Version 7.1.0, March 2006.
- [9] 3GPP, Messaging using the IP Multimedia (IM) Core Network (CN) subsystem, TS24.247, Release 7, Version 6.5.0, March 2006.
- [10] 3GPP, Voice Call Continuity between CS and IMS, TS 23.206 Release 7, version 1.1.0, July 2006.
- [11] IETF, RFC4566, SDP: Session Description Protocol, July 2006.
- [12] IETF, RFC 3311, The Session Initiation Protocol (SIP) UPDATE Method, September 2002.
- [13] IETF, RFC 2748, The COPS (Common Open Policy Service) Protocol, January 2000.
- [14] 3GPP, Customized Applications for Mobile network Enhanced Logic (CAMEL), Release 7, June 2006.