# Design of Transparent Distributed IMS Network: Security Challenges Risk and Signaling Analysis

HAMID ALLOUCH[1], MOSTAFA BELKASMI[2]

[1]University Mohamed V SOUISSI, ENSIAS Rabat, MOROCCO
Hamid.allouch@gmail.com
[2]University Mohamed V SOUISSI, ENSIAS Rabat, MOROCCO
belkasmi@ensias.ma

***ABSTRACT***

*The IP Multimedia subsystem (IMS) based on SIP as mechanism signalling and interfaces with other servers using OSA (Open Service Access) and CAMEL (Customized Applications for Mobile network Enhanced Logic).Is responsible for the interconnection of IP packets with other network, IMS support data communication services, voice, video, messaging and web-based technologies. In this work we present a distributed design of architecture that turns up some challenges of transparent mobility on the secured IMS architecture. We introduced the architecture with clustering database HSS and automatic storage of data files that give a secure access to database. This paper gives an overview of classification of security in IMS network and we show delay analysis comparison in signalling interworking with and without securing Gateway (SEG) in the registration of any UE in access network based IMS. We show that there is a trade-off between the level of increasing system security and the potential delay incurred by mobility in Access Network .we conclude that this architecture is suitable for operators and services providers for the new business models delivering ,the services based IMS Everywhere, anytime and with any terminals.*

***KEYWORDS***

*IP Multimedia subsystem (IMS); session initiation protocol (SIP); distributed architecture, signaling analysis, mobility*

## 1. INTRODUCTION

The new framework IP Multimedia Subsystem (IMS) firstly is specified for mobile networks especially for Universal Mobile Telecommunications System (UMTS) networks [release 5]. It has been introduced and standardized by the Third Generation Partnership Project (3GPP) and European Telecommunications Standards Institute (ETSI) ,actually (November 2012) [1] in phase of release 11 for providing Internet Protocol (IP) telecommunication services. The goal of IMS is the convergence: it will make Internet technologies such as the voice; data communication services, video conferencing, messaging and web-based technologies Everywhere, Anytime, and with any terminals, the challenge of IMS architecture come from this convergence.

By it convergence, The IMS provides better quality of service, charging infrastructure and security. IMS provide a single interface to different traditional or to new generation mobile architectures allowing better working environment for the end users. Research is in progress in various fields especially in security and QoS, where the protocols IMS provide better performance. The complexity of the design architecture and convergence raises significant security concerns IMS network.

DOI : 10.5121/ijngn.2012.4401 

Many requirements of this architecture stipulate that a mobile user should follow a multi-process to access IMS services. This is because the inherently open nature of IP-based networks exposes the User Equipment (UE) and service providers to security attacks.

This paper comes for turns up some challenges of IMS architecture, mobility and security system, hence the fundamental contribution include the flowing aspects:

- Easy user registration and setup of multiple services in a single session or multiple simultaneous synchronized sessions with securing the architecture.
- Easy user mobility in IMS network for different Access Network by proposing the framework Handover Manager (HOM) for monitoring and managing the resource allocation.
- Security classification and analysis for different elements in IMS network.
- Provide the Quality of Service (QoS) required for enjoying, rather than suffering, real time multimedia sessions by designing and evaluating the performance of the proposed architecture by delay analysis.

The paper is organized as follows. Section 2 gives the overview of standard IMS architecture and security. In Section 3, we present our IMS Security classification that critical to know , In Section 4, we present proposed our secure architecture of IMS with HOM, the methodology to analysis and analysis are performed to evaluate the proposed of architecture and security in section 5. Finally, we draw some benefits and conclusion.

## 2. STANDARD IMS ARCHITECTURE AND SECURITY OVERVIEW

IMS is standard based on SIP and IP protocols, as shown in Figure 1; this standard defines a generic architecture for offering Voice over IP (VoIP) and multimedia services [1].

### 2.1. Background about IMS:

IMS provides integrated services to its end of users, and a platform for application providers to host their content on its servers. The core network consists of the following elements:

*A database HSS (Home Subscriber Server) :* is the main database used by the IMS, it contains user profiles and subscription data. It provides the location and authentication information based on requests from the I- or S-CSCF, or the AS, The HSS holds the databases of subscriber's public and private identities, security variables, and location information. It contains the HLR (Home Location Register), EIR (Equipment Identity Register), and AuC (Authentication Centre).

*Application Server (AS):* Application Servers Communicates with S-CSCF and HSS and provide application services including IP telephony, multimedia applications, voice call and video conferencing applications. all IMS services are implemented in Application Servers.

*Proxy Call Session Control Function (P-CSCF):*
P-CSCF is first point and the gateway to UEs to the IMS network. PCSCF is a SIP enabled proxy server and all user requests, signaling and control information passes through it. The P-CSCF primary role is to exchange SIP traffic and provide the Security and Signal compression.

*Serving Call Session Control Function (S-CSCF):*
S-CSCF is the most important element of IMS core. Most of its functions are related to registration, session and application services. Registration requests from end users are

received by the S-CSCF and authenticated by contacting the HSS for user security and authentication parameters. It Acts as the SIP registrar, Performs Service Invocation and Routes the SIP signaling to the AS.

*Interrogating Call Session Control Function (I-CSCF):*
I-CSCF acts as the point of contact for user connections and sessions, regardless of whether a user belongs to the same network or a roaming user from another network. it Performs DNS lookup to identify the address of the SIP server and Consults HSS and finds out the S-CSCF.

*Media Gateway control Fonction(MGCF):* connects the media plan of PSTN/PLMN to IMS media plan and provides interworking between IMS and PLMN/PSTN.

*Access/Interface Network :*

- Acts as Interface to the User Equipment.
- Any UE can be attached to it.
- Based on the UE the access network makes access with the core IMS backbone.
- Various Interfaces: UMTS, CDMA, 802.11, VoIP, Wireline.

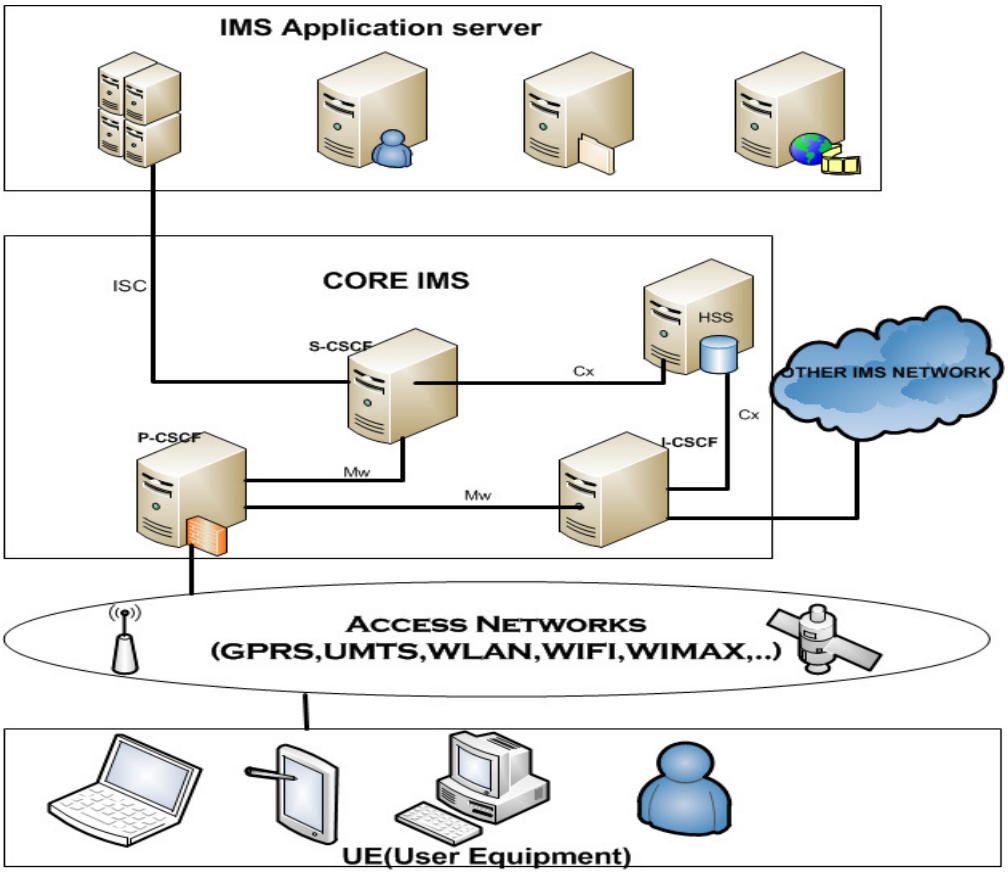


Figure 1. IMS architecture adopted from [1]

## 2.2. IMS architecture security

A secure IMS system architecture is extremely important that needs to be capable of protecting its associated elements with respect to confidentiality, integrity, non repudiation, authentication and availability.

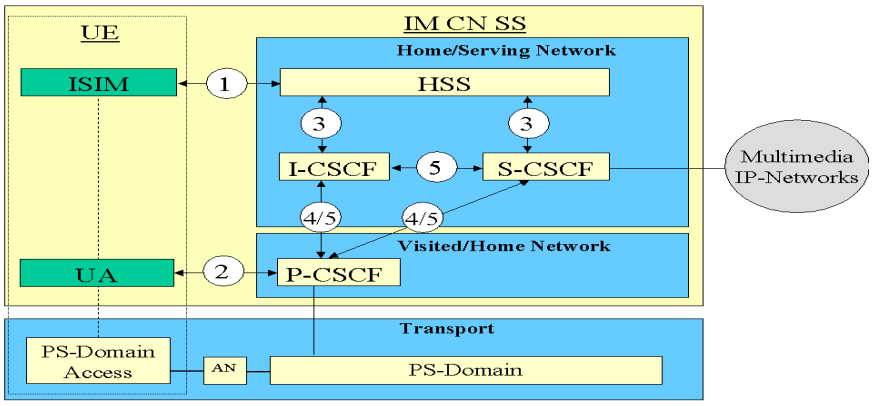


Figure 2. IMS Security Architecture [2]

The IMS Security architecture is presented in figure 2 [2], it provide insight into the interactions between the CSCFs and both internal and external components of the IMS.

The diagram show five different security associations and different needs for security protection for IMS and they are numbered by 1, 2, 3, 4 and 5 described below:

① **Provides mutual authentication.**
The HSS delegates the performance of subscriber authentication to the S-CSCF. The long-term key in the ISIM and the HSS is associated with the IMPI. The subscriber will have one user private identity (IMPI) and at least one external user public identity (IMPU).

② **Provides a secure link and a security association:**
The secure link and association is between the UE and a P-CSCF for protection of the Gm reference point.

③ **Provides security within the network domain:**
Secure domain internally for the Cx-interface. TS 33.210 cover this security association.

④ **Provides security between different networks:**
Provide security between different networks for SIP capable nodes. TS 33.210 cover this security association.

⑤ **Provides security within the network:**
Provide security internally between SIP capable nodes. TS 33.210 cover this security association. This security association applies when the P-CSCF resides in the HN.
Security from 2-5 are the interest link as they correspond well to the network interfaces between the HSS and CSCF components, and are thus useful attack vectors (VA).

## 3. IMS CLASSIFICATION SECURITY

We give in this section our view for classify the security in IMS network, and formula for detecting the risk

### 3.1. IMS classification security

The different side of security defined in the IMS system could be divided into five aspects of securities: mechanisms, attacks, threats, vulnerability and services.

#### 3.1.1. Security mechanisms:

A mechanism security is designed to detect, prevent, or recover from a security attack, also the mechanisms system IMS can be categorized by three types:

*Security prevention:* The goal of implantation of this security is to audit and monitor any violations of security attacks in the network.
*Security detection*: The goal of security detection is to detect any attempts to violate security policy.
*Recovery:* The goal of recovery is to restore and recover the IMS system after been detected security violation threats, attacks and vulnerabilities. This policy may be declared in the first implementation IMS by configuring the parameter of time to recover until failure, this parameter is very critical if we decide that an availability is 24/24 is important.

#### 3.1.2. Security Threat:

With the increase of user IMS, cell phone subscriptions and internet users consequently increasing the amount transferred and the data connections, security problems are increasing in number and scope. There are three major categories: external threats, internal threats and compliance requirements.

*a. External threats :*
These threats are becoming increasingly critical because of its continuous growth, there are groups of organized criminals, hackers, and there are criminal enterprises, even state-sponsored entities. The Motivations for attackers are no longer limited to the profit, but sometimes may include prestige. These attacks targeted databases of corporate customers, through to listen in the network, and end up by damaging a material of communications Systems.
*b. Internal threats :*
These can be dangerous than the external attacks. In many situations, insiders perpetuate breaches in information security. Insiders today can be employees, contractors, consultants and even partners and service providers. These breaches range from careless behaviour and administrative mistakes to deliberate actions taken by disgruntled employees, such as giving away their passwords to others, losing back-up tapes or laptops or inadvertently releasing sensitive information,.
*c. Compliance requirements :*
The provider or operators of IMS are invited to respond to an ever-reporting requirement for IMS security and privacy standards, Such as Sarbanes-Oxley (SOX), and ISO/ IEC international standards. Indeed, these standard agencies often take a significant amount of time and effort to prioritize issues, develop policies and appropriate controls, and monitor compliance.

**3.1.3. Security Attacks:**

The security attack is any action to compromise the security of information in the system. There are three types of attacks, which may affect the IMS network system:

*Accidental attacks*: These come from failure of some component of IMS, or user error.
*Passive attack:* is in which an unauthorized attacker monitors or listens to the communication between UE and IMS network. The goal of the attacker is to obtain the information transmitted, if the intruder obtain the information about system, he can know it vulnerability to exploit in another attack like DoS.
*Active attack*: this is a serious and dangerous attack like data modification. The most critical and serious active attack can be categorized in four groups: Replay, masquerade, modification of message, and denial of service.

**3.1.4. Security Vulnerabilities:**

Most of vulnerabilities in IMS, allows the holes and security faults in the system, mostly due to a configuration problem at IMS. There are three major categories of vulnerabilities:

a. *Vulnerabilities of IMS Networks*
b. *Vulnerabilities of Service Provider Networks or AN*
c. *User Equipment Vulnerabilities*

The authentication policy or mainly vulnerable weaknesses in the system allows for threats and attacks, as a result of this flaw update security policy and security threats can be considered as potential violations of the safety, and exponential growth of the use of IMS communication is likely to have increased access to malicious intruders in the network.

For solving this issues, it recommended to have the system IMS network, application server and user Soft Equipments updated periodically.

**3.1.5. Security service:**

Is a service that enhances the security of the data processing systems and information transfers of a system, these services are used to counter security attacks, and they make use of one or more security mechanisms ,We distinguish that security service in IMS ,can be classified as follows:

a. *Confidentiality security:*
Confidentiality ensures that the information is accessible only to authorized entities. Transmission of sensitive information in IMS networks requires confidentiality. Disclosure of such information to enemies could cause devastating consequences. Routing information (control packets) must also remain confidential to certain extent, since the enemies to identify and locate their attacking targets can use such information.
*b. Authentication security :*
Authentication ensures that the origin of a message is correctly identified and its identity

is not forged. Without authentication, the malicious node could impersonate other node to gain unauthorized access to resource and sensitive information.

*c. Data Integrity security :*

Data integrity ensures that only authorized identities are able to modify system assets and transmit information. A message could be corrupted because of link failure, or malicious attack.

*d. Non repudiation security :*

Non-repudiation ensures that the origin of a message cannot deny having sent the message. It is very useful to detect and isolate compromised nodes.

*e. Access control security:*

Access control ensures that access to information resources may be controlled by or for the target system. To achieve this control, each entity trying to gain access must be first identified, or authenticated, so that access rights can be tailored to the individual.

*f. Availability:*

Ensure that network elements do not provide information pertaining to the end-users network activities (e.g., denial-of-service attacks).

a. *Data Confidentiality:*

Protect end-user data that is transiting a network element or communications link, or is resident in an offline storage device against unauthorized access or viewing. Techniques used to address access control may contribute to providing data confidentiality for end-user data.

b. *Communication Security :*

Ensure that end-user data that is transiting a network element or communications link is not diverted or intercepted as it flows between the end points (without an authorized access)

In general, it is very hard to detect passive attacks since they do not disturb the system. But active attack we can detect it by traffic analysis, auditing, monitoring network traffic, CPU, disk usage and Encrypting messages such as measuring the length, time and frequency of transmissions. These mechanisms can help in predicting or guessing network activities and give the idea about the architecture to design for high security network.

### 3.2. Risk formula in IMS

We conclude this classification , that we modulate a security in IMS network by satisfaction a formal 1 ,there are six parameters influence a list of risk ,these list check considering a security initiative designed to evaluate and improve the availability of an information system. It will compile a list of risks, associate each of these risks to threat, vulnerabilities, sensitivity, attack and we consider the mechanisms and counter-measures, which we can develop to protect IMS network, according to a formula (1):

$$\mathrm{R}_{risks} = \left( \frac{\sum_{t} T_{Threats} \times \sum_{v} V_{Vulerabilities} \times \sum_{s} S_{Service\_sensitivity} \times \sum_{a} A_{Attacks} \times \sum_{m} \mathrm{M}_{Mecanisms}}{\sum_{i=1}^{5} \mathrm{CM}_{Counter\_Measure}} \right) \quad (1)$$

Formula (1) and "Kiviat" chart figure. 4 are giving the fact that attackers become more and more creative, so there is an urgent need for more effective and carefully designed counter-measures (CM).

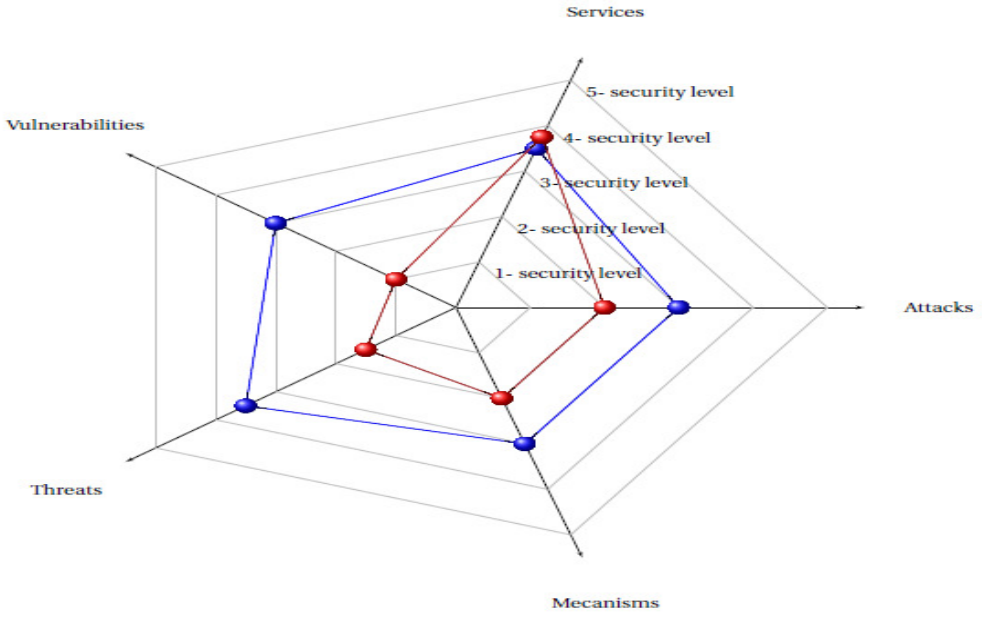


Figure 3. "Kiviat" diagrams of Risks, blue line is low risk(more than 3 of security level) ,maroon line show a risk for low level of securities

## 4. SECURED ARCHITECTURE IMS NETWORK

In this section, we introduce the architecture of IMS; the details of architecture are presenting in this section in figure 4. The goals of architecture are implementing efficient infrastructure with high availability to face for any transparent mobility in IP networks based on SIP and security attack. With the distributed and secures communication on IMS network, the architecture is based on definition of security Gateway, Handover Manager(HOM) make a mobility transparent to users IMS , the communication SSL and IPSec tunnel for interworking between IMS networks.

### 4.1. Design architecture motivations:

The motivations of our framework are responding in the most section of availability ,mobility, security, and scalability. We have the Maximum total workload used for system IMS sizing is limited by the size of all max components.

The centralized architecture of IMS has a limitation of capacity of resource, because of single server and limitation of bandwidth; we can see this limitation in security if some attacker or intruder wants DoS of centralized IMS by directing a attack by huge amount of SIP signalling towards a network, this attack can make a network unused.

We can illustrate this limitation by equation (2) and (3)

$$\mathrm{IMS}_{\mathrm{Total\_Size}}\left(\mathrm{Max\_Bandwith}\right) = \sum_{i=1}^{N=\max}\left(R_i S_i\right) \le IMS_{\mathrm{Components\_Size}}\left(Bandwith_{\max}\right) \quad (2)$$

$$\mathrm{IMS}_{\mathrm{Total\_Size}}\left(\mathrm{Max\_capacity}\right) = \sum_{i=1}^{N=\max}\left(R_i S_i\right) \le IMS_{\mathrm{Components\_Size}}\left(Capacity_{\max}\right) \quad (3)$$

The equation show the limitation of centralized of bandwidth and the capacity processing, the total bandwidth do not exceed the max bandwidth and maximum number of user in the some IMS. Where $N$ define the Number of user in the IMS , $R_i$ is The rate of SIP packet from IMS users, $Bandwith_{\max}$ is Network Bandwidth of the IMS, $S_i$ is the size of packet of SIP in the IMS and $Capacity_{\max}$ is The processing capacity of the IMS network

### 4.2. Distributed proposed IMS compact architecture

The HSS instance can be in each node but the storage can be in another location. HSS have redundant information in each instance that can serve every node.

We introduce the entity Handover manager which play important role in monitoring and management of user handover in IMS network, our idea is to facilitate the mobility and transparent pour access network to allocate the resource and bandwidths.

In our design we have deployed also a firewall and multi x-CSCF entities in each Access network, firewall could help in filtering packet and other full functionalities.

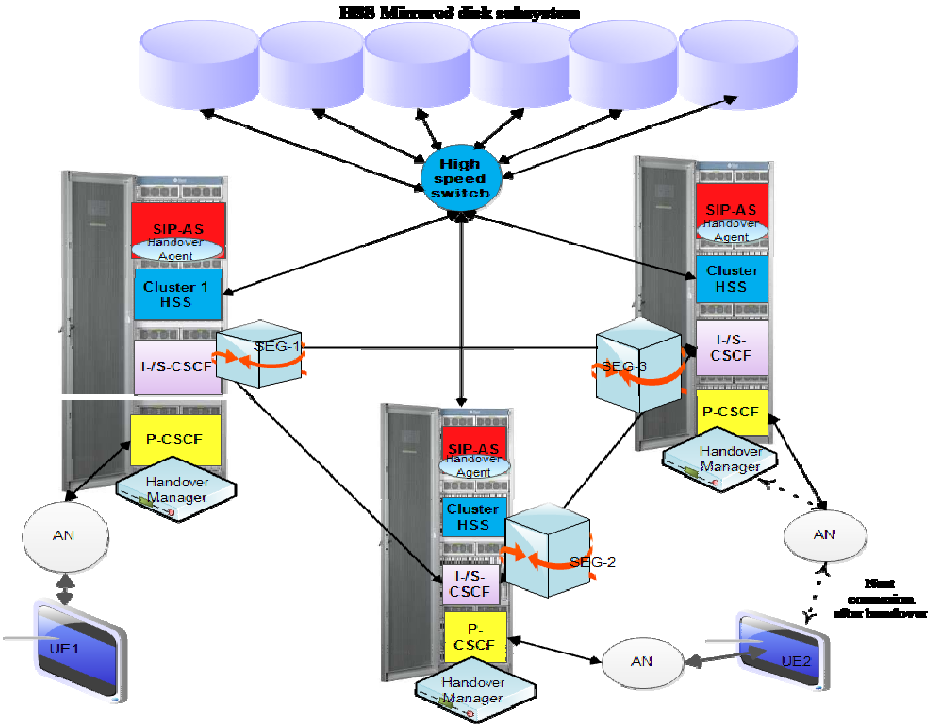


Figure 4. Consolidate into Low Cost Servers using components of real cluster of IMS

The architecture proposed with different elements is described in figure 4 , the signification of different element is described in first section ,here we give the description of security element in IMS ,we can see that different type of attacks may be done between UE and network IMS or in the network of IMS

The different element of architecture that introduced is dressed in table I organized by layer and three planes, the security IMS must be grouped according to it particular security layer and plane ,as shown to table I the IMS vulnerability analyze may be exposed by different type of attacks .

TABLE 1. IMS MODULAR SECURITY PLANE

| | **Management plane** | **IMS plane** | **End User plane** |
|---|---|---|---|
| **Application layer(AL)** | SSH, http/https, SMTP, FTP, DHCP, Telnet | SIP, Diameter | VOICE,IM |
| **Service Layer(SL)** | Diameter ,COPS | SIP/SDP ,Diameter ,H248 | RTP/RTCP, User profile |
| **Access Layer (AN)** | TCP/IP,UDP, ARP, PDF, IPsec | X-CSCF, AS, DNS, MGCF, SLF… | HSS, UE,IM-MGW,MRFP |

In figure 5, we show that HTML stream via HTTP/HTTPS is the secure communication between UE and IMS network.

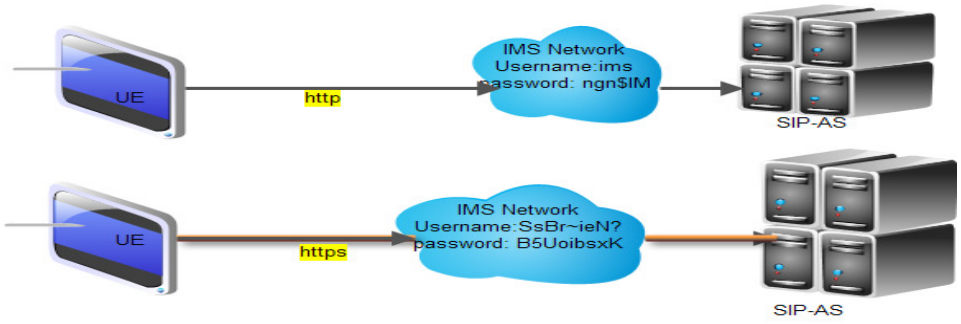


Figure 5. Authentication in http and https

## 5. The IMS Registration Procedure of the proposed architecture.

In order to provide for registration analysis, we briefly describe the registration procedure [1], the IMS registration step numbers correspond to the numbers in figure 7.

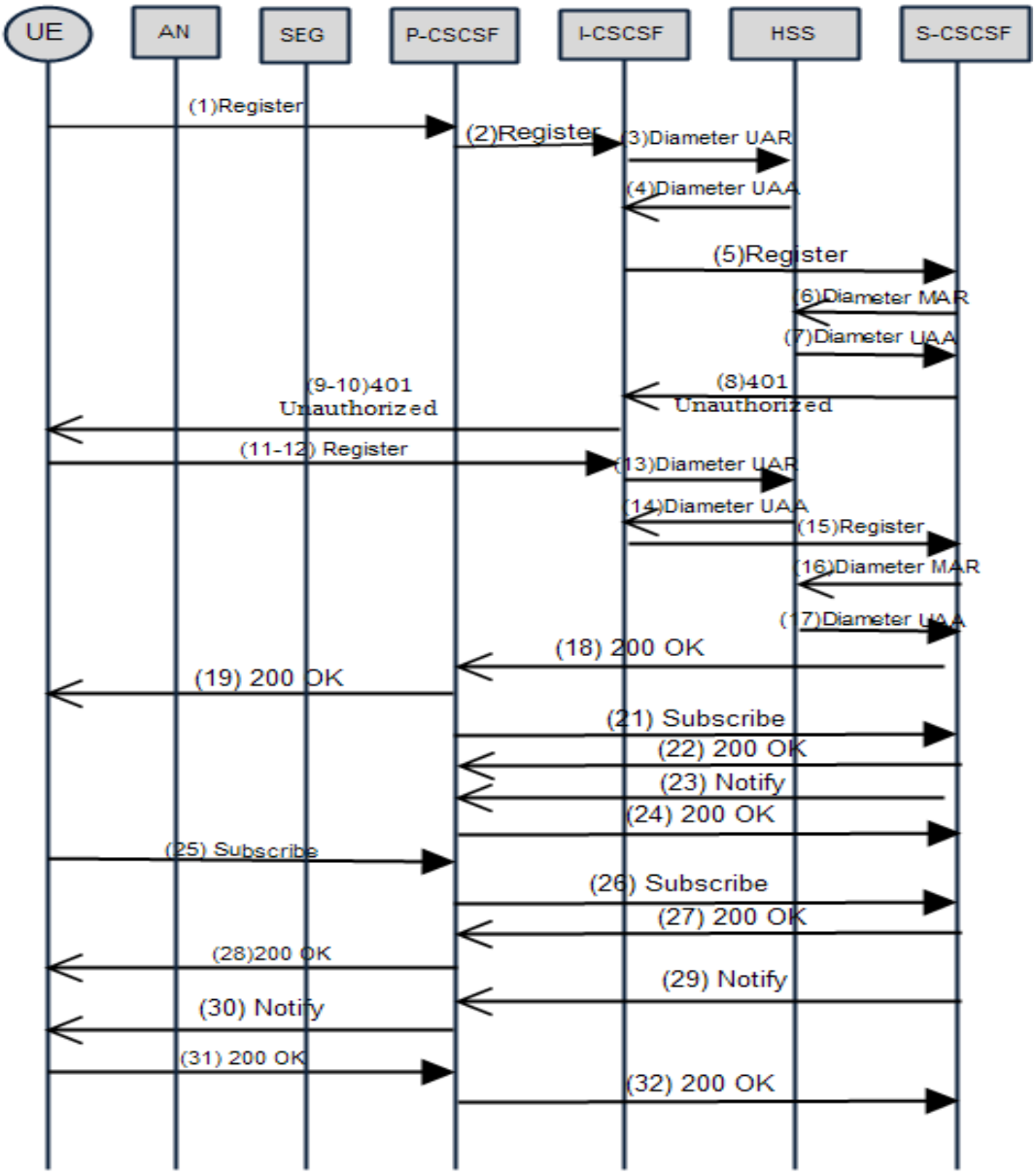


Figure 6. Registration process in IMS (adapted from [1],[2])

The IMS registration is a mandatory procedure in which the IMS user requests authorization to use the IMS services and consists of the following steps (Fig. 6): 1) The IMS registration begins with a UE (User Equipment (UE) is a generic term of source Network) SIP REGISTER request sent to the AN (UMTS, LTE, WLAN or other Access Network or Core Network (CN)), AN to SEG and SEG to P-CSCF. 2) The P-CSCF forwards the SIP REGISTER request to the I-CSCF in the user's home network. 3) The I-CSCF sends a Diameter User-Authentication-Request (UAR) to the home subscriber server (HSS) for authorization and determination of S-CSCF already allocated to the user. 4) The HSS authorizes the user and responds with a Diameter User-Authentication-Answer (UAA). 5) The I-CSCF forwards the SIP REGISTER request to the S-CSCF. 6) The S-CSCF sends a Diameter Multimedia-Authentication-Request (MAR) message to

the HSS for downloading user authentication data. The S-CSCF also stores its uniform resource indicator (URI) in the HSS. 7) The HSS responds with a Diameter Multimedia-Authentication-Answer (MAA) message with one or more authentication vectors. 8)-10) The S-CSCF creates an SIP 401 Unauthorized response with a challenge question that the UE SN must answer. 11), 12), and 15) The UE answers the challenge question in a new SIP REGISTER request response. 16) If authentication is successful, the S-CSCF sends a Diameter Server-Assignment-Request (SAR) to inform the HSS that the user is registered and the HSS can download the user profile. 17) The HSS replies with a Diameter Server-Assignment-Answer (SAA). 18)-24) The S-CSCF sends a 200 OK message to inform the user of successful registration. The subscription to a reg event state provides the user with his/her IMS network registration status. 25) and 26) The UE sends a reg event SUBSCRIBE request to the P-CSCF, which then proxies the request to the S-CSCF.
27) And 28) The S-CSCF sends a 200 OK after accepting the reg event subscription. 29) and 30) The S-CSCF also sends a NOTIFY request containing registration information in extensible mark-up language (XML) format. 31) and 32) The UE finishes the subscription to the reg event state process by sending a 200 OK message. Note that steps 21) to 24) represent the reg event state subscription process for the P-CSCF and follow the same procedure as in steps 25)-32).

# 6. INTERWORKING PERFORMANCE IN SECURED IMS ARCHITECTURE ANALYSIS AND NUMERICAL RESULT.

IMS introduce important advantages for users of different access networks like 3G (UMTS), WLAN or 4G. For securing IMS from malicious users and any possible degradation of quality of service, we followed procedure to eliminate the Risk (giving in section 2).

So we use IPSec protection to secure the IP SIGNALING traffic and for forwarding the data between IMSs Network. The tunnel is terminated by the SEG in the receiving IMS, which in turn uses IPSec to pass the data to its final destination. The end-to-end schema implies that an IPsec is established between the two IMSs. To calculate the cost of register and setup time we use the follows formula:

$$Delay_{IMS}(P_\alpha) = \sum_{i=1}^{n} Delay_{Components\_IMS}\left(P_\alpha\right) \quad (4)$$

Fig. 6 depicts the global cost of transmission and the processing for Signalling, for different values of IMS arrival rates $\lambda$. More specifically, the labels Cost_sig_w/o and Cost_sig_with denote respectively the values of cost without SEG and with SEG.

As it was expected the cost for signalling IMS traffic without SEG is lower than the transmission cost for IMS traffic with SEG, but the cost is increased by increasing arrival rate. As it is shown in the figure the difference of cost for signalling IMS traffic is increased for arrival rate higher and by increasing the cons measure. From This figure the difference is kept constant and negligible independently of the value of the arrival rate $\lambda$.

The performance overhead of our design is optimal; even we add the effect of cost of securing element SEG in IMS.

## 7. 1 IMS DELAY: TRANSMISSION DELAY WITH RLP

When transmitting message over UMTS, Radio link Protocol (RLP) is used, the flowing parameters are considering in our analysis:

P: is probability of an RLP frame being in error in the air line;

K: number of frames in a packet transmitted over the air;

D: end-to-end frame propagation delay over the air line (typical values of the order of 100 ms).

T : interface time of RLP (typical values of the order of 20 ms for GPRS).

$C_{ij}$ Represent the first frame received correctly to the destination at the ith retransmission of the jth retransmission trials. That is, the missing frame has been lost up to the (j-1)th retransmission trial and up to the (i-1)th retransmissions in the jth trial.

The effective packet loss Pf seen at the transport layer, with RLP operating underneath, is given as:

$$P_f = 1 - p + \sum_{j=1}^{n} \sum_{i=1}^{j} P(C_{ij}) = 1 - p(p(2-p))^{\frac{n(n+1)}{2}} \quad (5)$$

$n$ : is the maximum number of RLP retransmission trials.
Considering the RLP retransmissions, the transport delay in transmitting a packet over the RLP is given by:

$$D' = D + (k-1)\tau + \frac{k(P_f - (1-p))}{P_f^2} \times \left( \sum_{j=1}^{n} \sum_{i=1}^{j} P(C_{ij}) \left( 2jD + \left( \frac{j(j+1)}{2} + i \right) \tau \right) \right) \quad (6)$$

Then the transmission Delay for UMTS with RLP $D_{with\,RLP\_UMTS}$, is following.

$$D_{with\,RLP\_UMTS} = D' + \left( \frac{2Dq(1-q)}{(1-q^{N_{TCP}})} \right) \times \left[ 1 + \left( \frac{4q(1-(2q)^{N_{TCP}-2})}{1-2q} \right) - \left( \frac{1-q^{N_{TCP}}}{1-q} \right) \right] \quad (7)$$

When $D'$ denotes the packet delay when RLP is used and q denotes the RLP packet loss rate when q is given as:

$$q = 1 - P_f{}^k = 1 - \left( 1 - p(p(2-p))^{\frac{n(n+1)}{2}} \right)^k \quad (8)$$

Where p is the probability of frame being in error in the air line and k is the number of air-link frames contained in TCP segments.

The IMS registration procedure, including, subscription to reg event state, consists of eight

message exchanges between the UE and IMS network P-CSCF server (fig. 6).

3 G networks improve frame error rate (FER) with RLP.

The IMS registration transmission delay in 3G networks $D_{t\_reg\_ims\_3G}$ is:

$D_{t\_reg\_ims\_3G} - 8 * D_{with\,RLP\_UMTS}$

### 7.2 IMS Delay: Processing delay:

The main processing delays for network nodes in the IMS signaling is modeling by address lookup and during packet encapsulation and de-encapsulation at network layer . The tables addresses in IMS database contains the users record based on IP addresses:

$$D_p = (4d_{p-sn} + 4d_{SEG} + 10d_{p-p\mathrm{csc}f} + 6d_{p-i\mathrm{csc}f} + 4d_{p-hss} + 8d_{p-s\mathrm{csc}f}) \rightarrow ns \quad (10)$$

$$where\ d_j = \left( d_{p-const} + 100\left( \log_{k+1} N_j + \frac{L}{S} \right) \right) ns$$

- $N_j$ : Number of all network users in HSS.
- $L$ :denote the length en bit of IP address (32 IPv4 or 128 IPv6)
- $S$ : size en bit of machine word (32 or 64bits)
- 100 ns: denote the multiplication factor accounts for the fact that address lookup time increase in each memory access.

### 7.3 IMS Delay: Queuing delay:

The queuing delays are giving by (11). Different parameters used are listed [17], The corresponding transmission delay for a SIP message, $D_{q-imsreg}$ can be calculated in the same manner as $D_{q\ imsregUMTS}$ is given as follows.

$$D_{q-imsreg} = 4E[w_{sn}] + 4E[w_{SEG}] + 10E[w_{p\mathrm{csc}f}] + 6E[w_{i\mathrm{csc}f}] + 4E[w_{hss}] + 8E[w_{s\mathrm{csc}f}] \quad (11)$$

With $E[w_i] = \frac{\rho_i}{\mu_i(1-\rho_i)}; and\ \rho_i = \frac{\lambda_i}{\mu_i}$

### 7.4 Performance evaluation results and discussions:

In this section, we present the numerical results for IMS registration session of access network UMTS, we show the interworking architecture cost by delay analysis of SIP based signaling. Different architectures cause the IMS registration signaling messages (sent from the IMS terminal (UE) to the first point of contact with the IMS network) to flow between different architecture-specific nodes. More specifically, for different architectures, different network nodes will be along the path Between the UE and the P-CSCF. To aggregate total delay, these differences require specific modeling of the network nodes involved. The total delay from the SN to the P-CSCF in a UMTS network includes the delays incurred at the base station, SGSN, and GGSN. In this paper we considered in our study the tightly architecture, because delays incurred in the Loosely architecture ,specially at Access Network element like the station (BS), SGSN, and GGSN constitute the additional delay from the SN to the P-CSCF in a 3G network.
We show three interesting numerical result for cost of delay analysis of signalling IMS registration and mobility for our architecture.

#### a. Effect of p on IMS Delay

The figure 7 show the effect of frame error probability on IMS signaling of cost of delay for different UMTS channel rates access Network.

By increasing the channel rates we show decreasing delay signaling, also by increasing the channel frame error Rate for different ,so we can conclude that in mobility situation ,it's important to delivering high throughput for assuring a good connectivity.

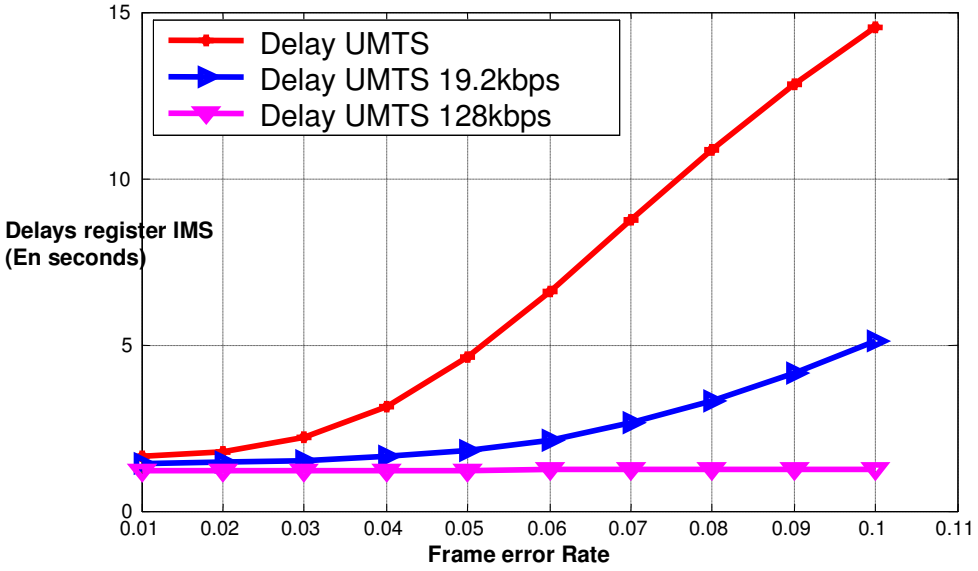


Figure 7. IMS Registration Signaling Delay For Various UMTS Channel Rates

**b. Channel rate effects on IMS Delay**

Figure 8 show IMS registration signaling delay in seconds versus by varying channel rate, we show that the IMS signalling delay decrease by increasing channel rate ,also we show that the delay with SEG is higher than with SEG for lower channel rate ,but for high channel we don't see the difference .

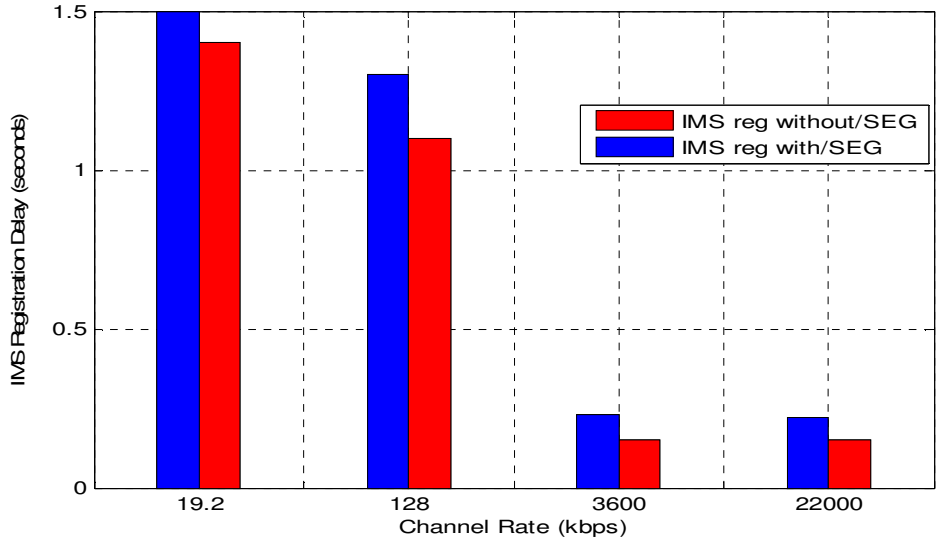


Figure 8. IMS Registration signalling Delay with and without SEG for different value of channel Rates for fixed arrival rate and fixed error probability.

### c. Global effects cost of arrival Rate λ on IMS Delay

The figure 9 show that by increasing the Arrival Rate λ , the Global delay of signalling increase and cost delay with SEG is increasing with arrival and it 's slightly higher than cost without SEG delay.

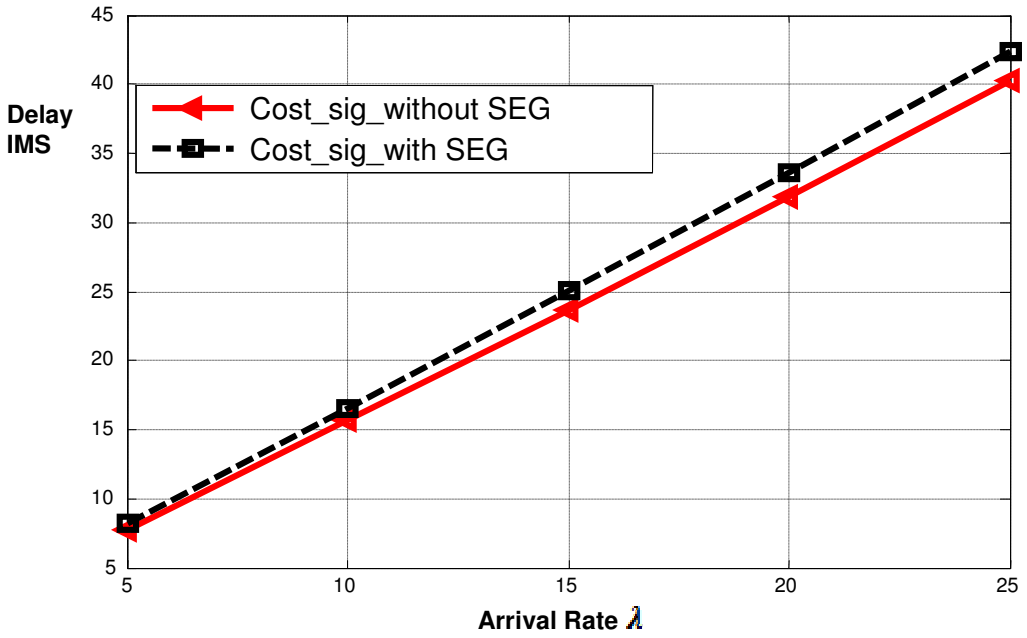


Figure 9. Global Cost of delay in IMS with and without SEG.

### d. Discusions

As we see in our last figure (7), (8), and (9), for most systems the cost of delay for security increases exponentially by increasing the security level toward the 100% level (in Figure 10). We show that there is a trade-off between the level of increasing system security and the potential cost incurred, especially for mobility of user network where the channel rates decrease.

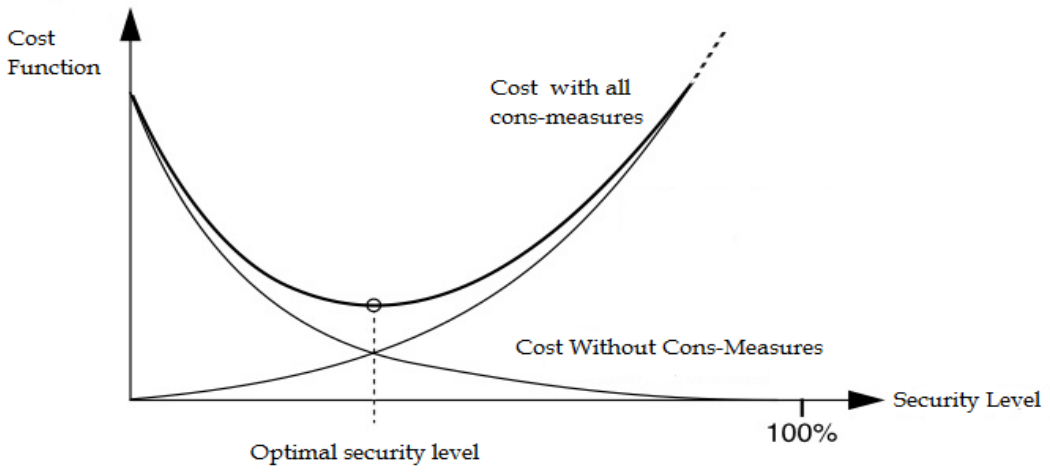


Figure 10. Cost function of a secured IMS system

## 6. CONCLUSIONS

Deploying and designing IMS network, it‘s the issues to solve the problems of interworking, mobility and security in IMS, the challenge is by decreasing the network load and securing signalling of Session Initiation Protocol (SIP) message and the flow session delay.The IMS architecture flexibility and functionalities and it convergence anytime, anywhere and anyway create new challenges of security and strategies for giving all services in one network.

The Core IMS network migration Trend to become mature, this paper gives Security Design and distributed IMS Scheme, so we give the classification of risk and evaluation of costs of delay for this proposed distributed and secured architecture IMS network.The motivation of the proposed architecture respects different aspects of security like vulnerability, threats and attack model, a detailed analysis in different layers of IMS is giving.

That makes sense and utility to this architecture, the proposed design reduce the delay to optimal level. We give a policy for securing the network IMS system by modelling the Risk as formula (1). This paper gives numerical result for the cost and delay signalling with and without SEG element in the IMS, and with HOM the element in our architecture that manage the handover .

## REFERENCES

[1] 3GPP, GSM, and ETSI, “TS 23.228 IP Multimedia Subsystem (IMS); Stage 2 (Version 11.4.0, Release 11)”

[2] M. Hunter, R. Clark, F. Park "Security Issues with the IP Multimedia Subsystem (IMS): A White Paper”, 2007.

[3] Hamid Allouch and Mostafa Belkasmi “Risk Analytic Approach and Cost Analysis for Interworking on the New Secured IMS Architecture” Journal of Information Security Research Volume: 3 , Issue: 3 (September 2012) Page: 130-147 lien : http://www.dline.info/jisr/v3n3.php.

[4] Greene, Tim. “Worst-case projected cost of Epsilon breach: $4B.” html NetworkWorld. May 1, 2011. http://www.networkworld.com/news/2011/050111-epsilon-breach-costs.

[5] Al Shidhani and V. Leung, “Pre-authentication schemes for umts-wlan interworking,” Eurasip J. Wirel.Commun.Netw, pp. 5:1–5:16, February 2009. [Online]. Available: http://dx.doi.org/10.1155/2009/806563.

[6] Han Yuexiao , Zhang Yanfu "The Building of Multimedia Communications Network based on Session Initiation Protocol "Published by Elsevier 2012 International Conference on Solid State Devices and Materials Science
[7] S. Islam, J.-C. Grégoire « Multi-domain authentication for IMS services » Computer Networks 55 Published by Elsevier (2011) 2689–2704.
[8] C.-Y. Chen et al. "An efficient end-to-end security mechanism for IP multimedia subsystem" Computer Communications Published by Elsevier (2008).
[9] N. Psimogiannos et al. "An IMS-based network architecture for WiMAX-UMTS and WiMAX-WLAN interworking" Computer Communications 34 Published by Elsevier (2011) 1077–1099.
[10] [IMS 02] Camarillo G., García-Martín M., "The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds", John Wiley & Sons, 2006, ISBN 0-470-01818-6.
[11] Open IMS Core, Open Source implementation of Open IMS Core, http://www.openimscore.org/.
[12] E. Mohammed and all. "ENHANCED TELECOM OPERATION MANAGEMENT SCENARIOS FOR IMS NETWORKS" journal IJNGN Vol.3, No.2, June 2011
[13] The European Telecommunications Standards Institute, http://www.etsi.org.
[14] S.K. Das, E. Lee, K. Basu, S.K. Sen, Performance optimization of VoIP calls over wireless links using H.323 protocol, IEEE Transactions on Computers 52 (6) (2003) 742–752.
[15] N. Banerjee, W. Wu, K. Basu, and S. Das, "Analysis of SIP-Based Mobility Management in 4G Wireless Networks," Elsevier Computer Comm., vol. 27, no. 8, pp. 697-707, May 2004.
[16] L. Kleinrock, QUEUING SYSTEMS vol. I: Theory, Wiley, New York, 1975.
[17] G. Ruggeri, A. Iera, and S. Polito, "802.11-Based Wireless LAN and UMTS Interworking: Requirements, Proposed Solutions and Open Issues," Elsevier Computer Networks, vol. 47, no. 2, pp. 151-166, Feb. 2005.
[18] C. Liu and C. Zhou, "HCRAS: A Novel Hybrid Internetworking Architecture between WLAN and UMTS Cellular Networks,"Proc. IEEE Consumer Comm. and Networking Conf. (CCNC '05), Jan.2005.
[19] H. Mahmood and B. Gage, "An Architecture for Integrating CDMA2000 and 802.11 WLAN Networks," Proc. IEEE Vehicular Technology Conf. (VTC '03), Oct. 2003.
[20] Q. Nguyen-Vuong, L. Fiat, and N. Agoulmine, "An Architecture for UMTS-WIMAX Interworking," Proc. First Int'l Workshop Broadband Convergence Networks (BcN '06), Apr. 2006.
[21] D. Kim and A. Ganz, "Architecture for 3G and 802.16 Wireless Networks Integration with QoS Support," Proc. Int'l Conf. Quality of Service in Heterogeneous Wired/Wireless Networks (QShine '05),Aug. 2005.
[22] Ahmed Barnawi and all." Security Analysis and Delay Evaluation for SIP-Based mobile MASS examination system" IJNGN mars 2012 vol4 N°1
[23] H.-T. Lin, Y.-Y. Lin, W.-R. Chang, and R.-S. Cheng, "An Integrated WiMAX/WiFi Architecture with QoS Consistency over Broadband Wireless Networks," Proc. IEEE Consumer Comm. And Networking Conf. (CCNC '09), Jan. 2009.
[24] A. Munir and V. Wong, "Interworking Architectures for IP Multimedia Subsystems," ACM/Springer J. Mobile Networks and Applications, vol. 12, no. 5, pp. 296-308, Dec. 2007.
[25] Andreea and all."Preventing Distributed Denial-of-Service Attacks on the IMS Emergency Services Support through Adaptive Firewall Pinholing" IJNGN 2010 vol2 N°1

## Authors

**Hamid ALLOUCH** Received his Telecommunication & Informatics engineering from INPT (Institute of National for Posts and Telecommunications), Rabat, Morocco in 2003. Currently he is doing his PhD in Computer Science and Engineering at ENSIAS (Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes), Rabat, Morocco. His current research interests IMS network architecture and security, heterogeneous networks and NGN interworking, mobile and wireless 3G/4G mobility network , and Information and Coding Theory,.

**Mostafa BELKASMI** Is recently a professor at ENSIAS (Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes); head of TSE (Telecom and Embedded Systems) Team at SIME Lab .He had PhD at Toulouz University in 1991. His current research interests Information and Coding Theory, IMS network architecture and security, heterogeneous networks and NGN interworking, mobile and wireless 3G/4G mobility network.