Risk Analytic Approach and Cost Analysis for Interworking on the New Secured IMS Architecture

Hamid Allouch, Mostafa Belkasmi
MohammedV-Souisi University SIME Laboratory
ENSIAS, Rabat
Morocco
hamid.allouch@gmail.com, belkasmi@ensias.ma

ABSTRACT: *The IP Multimedia subsystem (IMS) is the technologies of convergence and interworking environment, with services flexibility, it‘s more than technical issue, it will prevail as core of Next Generation Network (NGN). The challenge and strategies of IMS architecture come from this convergence and the complexity of these technologies. In this work we present a novel design of architecture, that turns up some challenges of new IMS architecture and security system with optimal cost. The proposed architecture provides a robustness, reliability, scalability and strategy for extension in the future and responds to the security challenges. The architecture introduce clustering database HSS with automatic storage of data file that give a secure database. This paper respond to a most frank discussion about risk, investment and taking a security approach in IMS network issues, clearly we present the formula of the risk in IMS network and the comparison presented the impact of the cost signaling interworking with and without securing Gateway (SEG) with access network (AN) interworking between WiMAX and UMTS based on the new approach of secured architecture IMS. The result show the cost without Security Gateway (SEG), for signaling IMS traffic is lower than the cost with SEG, and the cost is increased by increasing arrival rate, there is a tradeoff between the level of increasing system security and the potential cost incurred .we conclude that this architecture is suitable for operators and services providers to protect against every conceivable threat, attacks , vulnerability and Denial of services.*

Keywords: IMS, SIP, SEG, Security IMS, Distributed Architecture, Cost Architecture

Received: 3 June 2012, Revised 21 July 2012, Accepted 30 July 2012

1. Introduction

The goal of IMS is the convergence: Everywhere, Anytime, and with any terminals for voice, data communication services, video, messaging and web-based technologies, the challenge of IMS architecture come from this complex and convergence of technologies. IMS is a standardized by third Generation Partnership Project (3GPP) [1] and European Telecommunications Standards Institute (ETSI) [1] as the part of the 2G/3G/4G of wireless and wire-line environment, which will enable and give a brief specification of the IMS.

By it convergence, and based on SIP as mechanism signaling support the data communication services, voice, video, messaging and web-based technologies ,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.

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 and security system, hence the fundamental contribution include the flowing aspects:

- Security classification and analysis for different element in IMS network.
- Giving and modeling by formula the risk in IMS
- Designing the secured architecture of IMS.
- Evaluating the proposed architecture by cost analysis.

The paper is organized as follows. Section 2 gives an overview of the standard architecture of IMS and architecture security. In Section 3, we present IMS Security classification and proposed risk formula that critical to know, In Section 4, we present our proposed secured architecture of IMS. The methodology to analysis the interworking between WiMAX and UMTS based on IMS with SEG of the proposed architecture and security is presented in section 5. Finally, we give some result and benefits of interworking and conclusion and perspective.

2. Overview of Standard IMS Architecture and Security

2.1 Backgroud about IMS

IMS is 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].

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:

2.1.1 A database HSS (Home Subscriber Server)

HSS is the main database used by the IMS, it contains and store user profiles, Stores all subscriber, service-related data and the users of a domain. It provides the location and authentication information based on requests from the I- or S-CSCF, or the AS. HSS database is the same as the HLR in the existing mobile network.

2.1.2 Application Server (AS)

Application Servers provide application services including IP telephony, multimedia applications, voice call and video conferencing applications (e.g. Presence, PTT, Instant Messaging, Supplementary Services, conferencing,).

IMS Application Servers (AS) provides SIP-based IMS services:

- May act as SIP-UA, SIP-Proxy, and SIP B2BUA.
- AS are invoked by the S-CSCF via the SIP-based ISC interface.

The different AS types are defined:

- SIP-AS (SIP-Application Server)
- IM-SSF (IP Multimedia Service Switching Function)
- OSA-SCS (OSA Service Capability Server)

2.1.3 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 principal functions performed by the P-CSCF are forwarding a received SIP register request from the UE to another entry point using the home domain name.

- Forward SIP messages received from the UE to the P-CSCF or the SIP server (e.g. S-CSCF) that say the registration procedure.
- Ensure that the SIP messages received from the UE to the SIP server (e.g. S-CSCF) contain the correct or up to date information about the access network type currently used by the UE, when the information is available from the access network.

- Forward the SIP request or response to the UE.
- Generation of CDRs.
- Maintain a Security Association between itself and each UE, as defined in TS 33.203 [18].
- Should perform SIP message compression/decompression.
- Authorization of bearer resources and QoS management. For details see TS 23.203 [19].
- Detection and handling of an originating or terminating IMS MPS session establishment request.
- Detect and handle an emergency session establishment request.

Based on operator policies, and the availability of the user location information and/or UE Time Zone from the access network, ensure that relevant SIP messages contain the correct or up to date information about the user location information, and/or UE Time Zone provided by the access network currently used by the UE.

2.1.4 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, There may be multiple I CSCFs within an operator's network, the principal functions performed by the I-CSCF are.

Registration: Assigning a S-CSCF to a user performing SIP registration.

Session-related and session-unrelated flows that:

- Route a SIP request received from another network towards the S-CSCF.

- Translate the E.164 address contained in all Request-URIs having the SIP URI with user=phone parameter format into the Tel: URI format of IETF RFC 3966 [25] before performing the HSS Location Query. In the event the user does not exist, and if configured by operator policy, the I-CSCF may invoke the portion of the transit functionality that translates the E.164 address contained in the Request-URI of the Tel: URI format to a routable SIP URI.

- Obtain from HSS the Address of the S-CSCF.

- Forward the SIP request or response to the S-CSCF determined by the step above.

- Based on local configuration, the I-CSCF may perform transit routing functions. If the I-CSCF determines, based on an HSS query, that the destination of the session is not within the IMS, it may forward the request or it may return with a failure response toward the originating endpoint.

- Charging and resource utilization by Generation of CDRs.

2.1.5 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, it Forward the SIP request or response to the UE and Generation of CDRs. The Serving CSCF (S CSCF) performs the session control services for the UE. It maintains a session state as needed by the network operator for support of the services.

S-CSCF Verify that the request coming from the AS,P-CSCF is an originating request, determine the served user and apply procedures accordingly.

Based on local configuration, the S-CSCF may be provisioned as the contact point within an operator's network for transit IMS scenarios and may perform transit routing functions.

Charging and resource utilisation by generation of CDR

- Ensure that the content of SIP request sent or received by the destination end point matches the determined IMS communication service definition, based on terminating user's subscription.

For Session-related and session-unrelated flows:

It shall reject IMS communication to/from Public User Identity(s) that are barred for IMS communications after completion of registration, May behave as a Proxy Server, May behave as a User Agent, Provide endpoints with service event related information, Forward the SIP request or response to a BGCF for call routing to the PSTN or CS Domain, the S CSCF attempts translation of the E.164 address in the SIP URI to a globally routable SIP URI, and Reflect in the charging information that an AS has initiated the session on behalf of a served user.

2.1.6 Media Gateway control Fonction(MGCF)

MGCF Connects the media plan of PSTN/PLMN to IMS media plan and provide interworking between IMS and PLMN/PSTN.

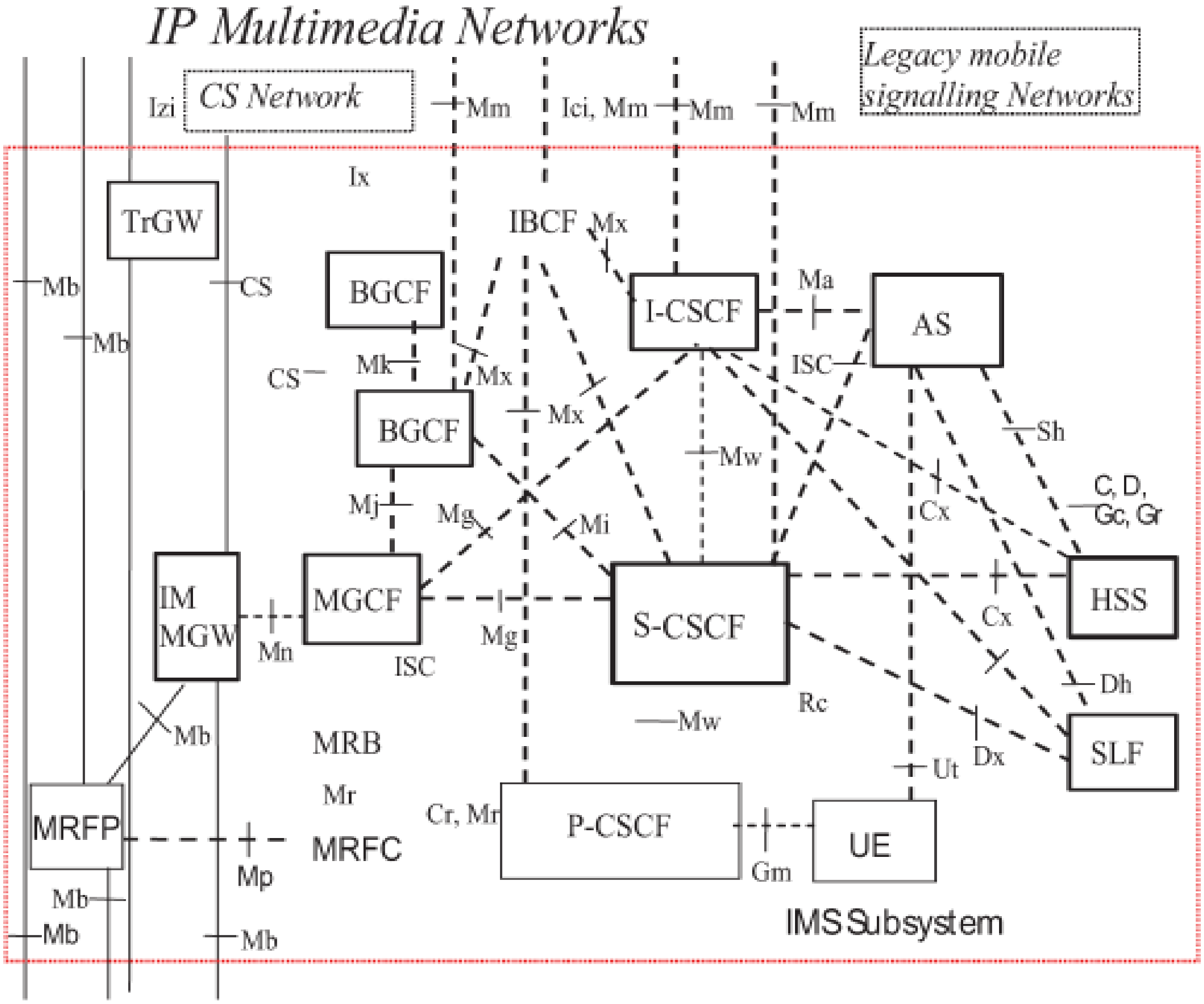

Figure 1. Standard IMS architecture from [1]

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, no repudiation, authentication and availability.

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:

2.2.1 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).

2.2.2 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.

2.2.3 Provides security within the network domain

Secure domain internally for the Cx-interface. TS 33.210 cover this security association.

2.2.4 Provides security between different networks

Provide security between different networks for SIP capable nodes. TS 33.210 cover this security association.

2.2.5 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).

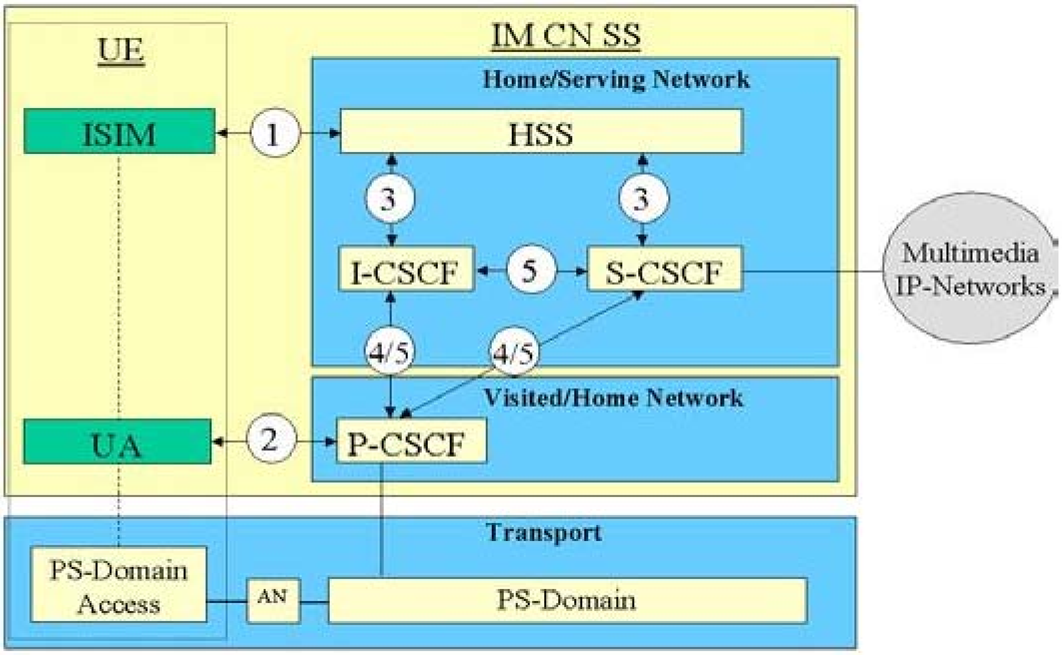

Figure 2. IMS Security Architecture [2]

3. Proposed IMS Classification Security and Moduling Risk Formula

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 proposed IMS system could be divided into five aspects of securities (as figure 3): mechanisms, attacks, threats, vulnerability and services.

3.1.1 Security mecanism

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:

3.1.1.1 Security prevention

The goal of implantation of this security is to audit and monitor any violations of security attacks in the network.

3.1.1.2 Security detection

The goal of security detection is to detect any attempts to violate security policy.

3.1.1.3 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.

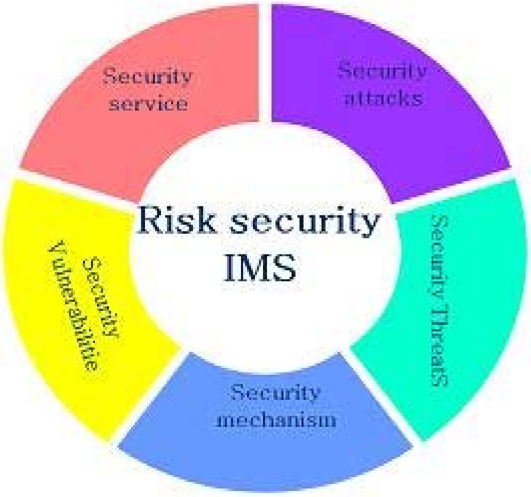

Figure 3. IMS Security Risk

3.1.2.1 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.

3.1.2.2 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 behavior 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.

3.1.2.3 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), various 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:

3.1.3.1 Accidental attacks
These come from failure of some component of IMS, or user error.

3.1.3.2 Passive attack
This 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 .

3.1.3.3 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. We distingue four categories of effect of these attacks as shown in figure 1:

a. *Interruption:* An intruder attacks availability by blocking or interrupting system resources.

b. *Interception:* the illegal party rightfully accesses System resources. This attacks confidentiality.

c. *Modification:* To create an anomaly in the network, an illegal party transmits spurious messages. This affects authenticity.

d. *Fabrication:* An unauthorized party transmits counterfeit objects into the system and causes an attack on authenticity.

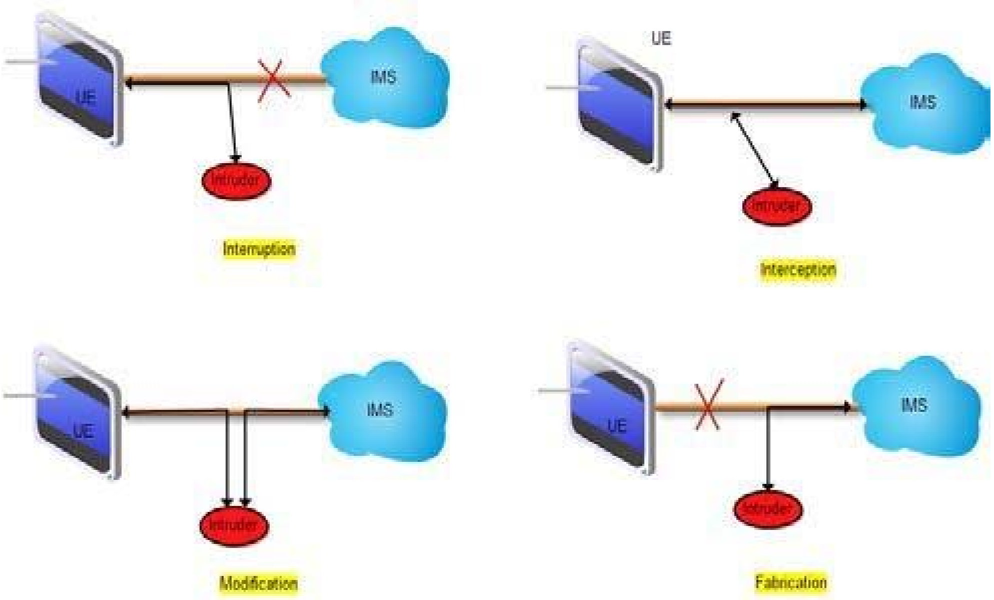

Figure 4. Security threat categories

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 distingue that security service in IMS ,can be classified as follows:

3.1.5.1 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.

3.1.5.2 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.

3.1.5.3 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.

3.1.5.4 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.

3.1.5.5 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.

3.1.5.6 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 Proposed 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):

$$R_{risks} = \left(\frac{T_{Threats} \times V_{Vulnerablities} \times S_{Service\_Sensitivity} \times A_{Attacks} \times M_{Mecanics}}{CM_{Counter\_Measure}} \right) \qquad (1)$$

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).

4. Proposed Architecture IMS Network

In this section, we introduce the proposed designed compact architecture; the details of the proposed architecture are presenting in this section in figure 4. The goals of architecture are implementing efficient infrastructure with high availability to face for any security attack. With distributed and secures communication on IMS network, the proposed solution is based on definition of security Gateway, SSL communication and IPSec tunnel for interworking between IMS networks.

4.1 Design architecture motivations

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

$$IMS_{Total\_size}(Max\_Workload) < IMS_{Component\_size}(Max\_Workload) \quad (2)$$

Therefore, the entire workload is evenly spread across all nodes at any point in time.

Then comes the idea of distributed design of the IMS network, the proposed distributed architecture x-CSCF provides the benefits:

a) Provide higher performance or better Cost/performance ratio than a centralized computer.

b) Provide higher system security,avalability ,reliabilty and scalability .

c) The system can survive any time ,any crash ,attack than a centralized computer.

d) Facilitate the communications for acceding any application severs .

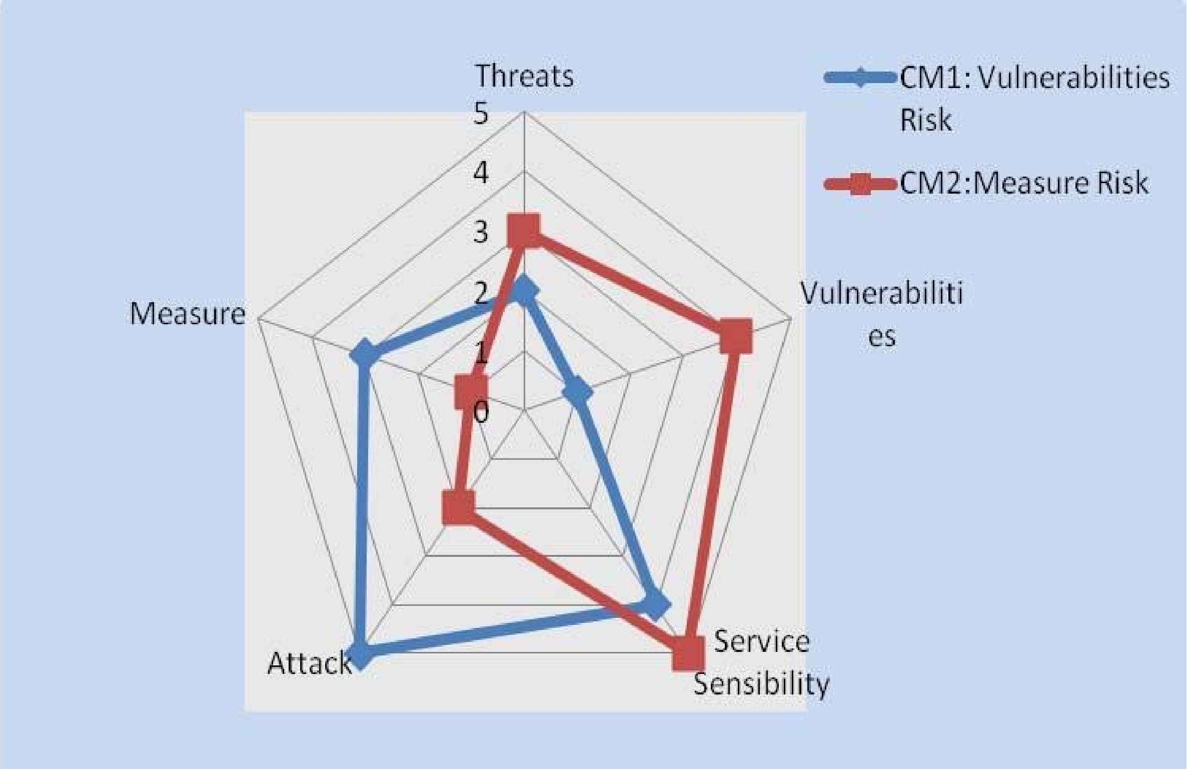

Figure 5. Example “*Kiviat*” Chart of Risks

The HSS architecture proposed provide Load Balancing, Scalability and high availability , the storage is centralized but the instance or temporary data is implanted in each node of distributed architecture compact distributed Systems.

4.2 Limitation of centralized IMS architecture

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 signaling towards a network, this attack can make a network unused.

We can illustrate this limitation by equation (3) and (4)

$$\sum_{i=1}^{N}(R_i S_i) \leq Bandwidth_{IMS} \tag{3}$$

$$\sum_{i=1}^{N}(R_i S_i) \leq Capacity_{IMS} \tag{4}$$

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, S_i is Network Bandwidth of the IMS, S_i is the size of packet of SIP in the IMS and $Capacity_{IMS}$ is The processing capacity of the IMS network.

4.3 Distributed proposed IMS compact architecture

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

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.

4.4 Security Architecture IMS analysis

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.

	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

Table 1. IMS Modular Security Plane

Some of important protocol using in our architecture are:

4.4.1 The Secure Shell (SSH)

Designed protocols SSH provide a secure Telnet-style console interface, as well as several other remote access services. This is a highly useful tool for creating secure remote configuration interfaces, since it geared toward remote shell functionality.

4.4.2 IPSEC

IPsec is a protocol designed to work at the IP layer, and is widely used for implementing Virtual Private Networks. IPSEC is a security framework similar to SSL, but with a bit larger scope. The IPSEC protocol, described in RFC 2401, consists of various security mechanisms and policies that are used to build different kinds of secure tunnels between devices.

4.4.3 The firewall

The IMS networks proposed with a firewall, that filters communications, it has configured as a barrier. A firewall must decide packet by packet, with a small chance, while a firewall effective against subtle attacks must be able to make things more complicated.

Configuring a firewall is to write specific rules to determine the allowed packets and packets prohibited; each packet is characterized by few parameters:

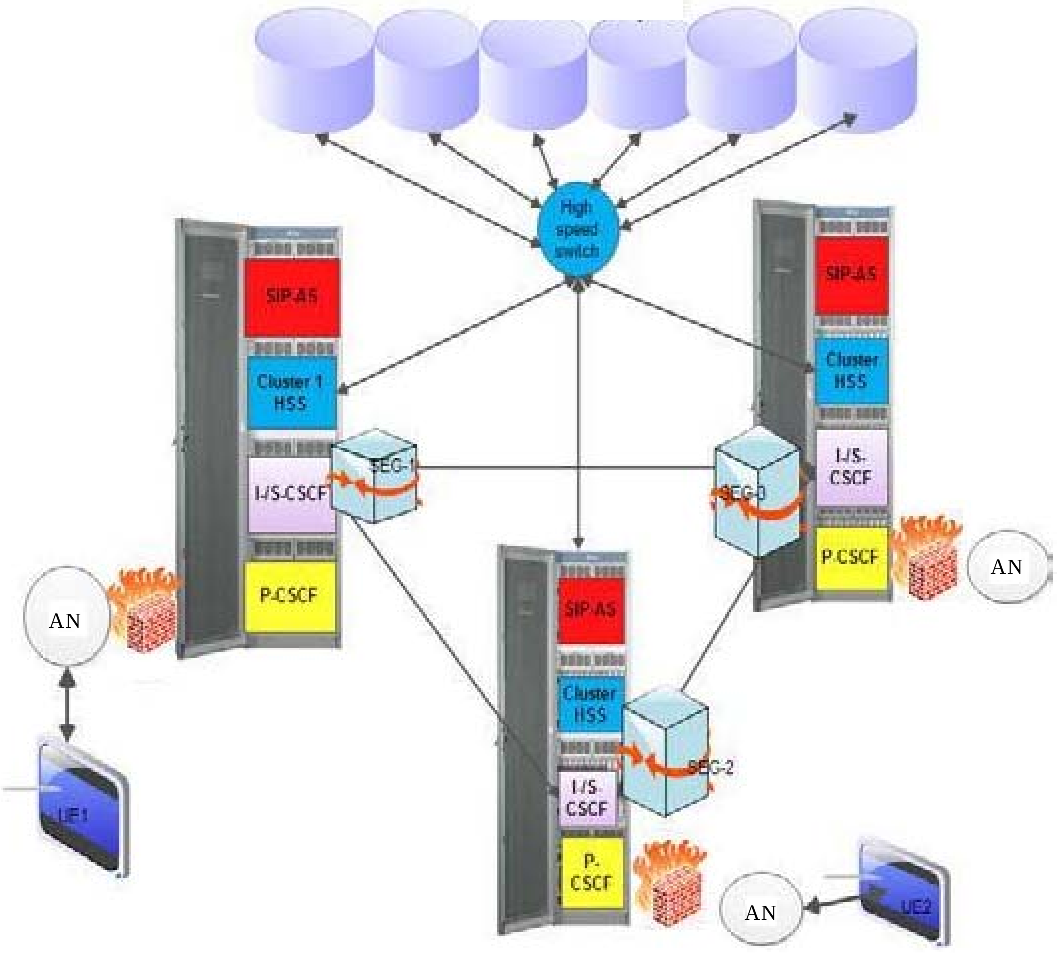

Figure 6. Consolidate into Low Cost Servers using components of real cluster of IMS

a. The IMS network interface on which the packet arrived, a firewall has at least two interfaces, one connected to the private network and the other connected to the Access network like mobile or the Internet network;

b. The fact that the package is shown on the interface from within the firewall or from the network;

c. The protocol which the packet belongs, as mentioned in the IP header;

d. The addresses of origin and destination, mentioned in the IP header of the packet, the port numbers of origin and destination, mentioned in the TCP header or UDP;

e. In the case of a TCP packet, the sequence numbers and acknowledgment, allow reconstructing the sequence of packets of a TCP connection.

These parameters are used to identify the type of communication which the packet belongs, and possibly to reconstruct a sequence. The simple filtering by port results in the writing of simple rules.

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

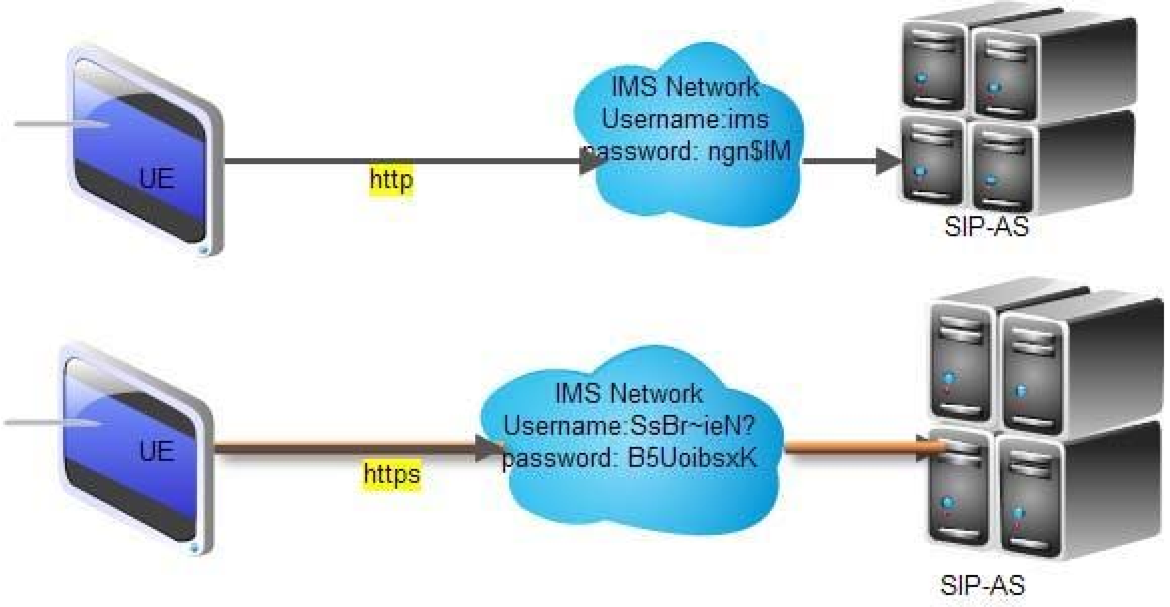

Figure 7. Authentication in http and https

5. Analysis Cost of Our Secured IMS Architecture

We use IPsec protection to secure the IP SIGNALING traffic and 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 (5);

5.1 Session set-up in IMS with two different Access netwok

In the following analysis, we consider the case of a user in a wireless network WiMAX trying to communicate with a user in a UMTS cell base on IMS of our proposed architecture.

The proposed architecture is capable of supporting all the 3GPP interworking scenarios. Users that access services from WiMAX are capable of communicating with users residing in the UMTS and vice versa .the figure 7 give the flow involved in the session setup between the WiMAX and UMTS in IMS.

5.2 Cost analysis

In this section, an analytical model for cost analysis is presented to evaluate the performance of the proposed architecture. The total cost C_{IMS} for establishing the session between two users belong IMS with two different networks access(AN) is calculated by the sum of the accumulated costs for the transmission of signaling and traffic flow data IMS, encapsulation, decapsulation of packets and routing packets in each entity of IMS. This cost can be given by:

$$Cost_{IMS}(P_{Packet\_routing(\alpha)}) = \sum_{j=1}^{n} \sum_{i=1}^{3} Cost_{Component\_IMS}(P^{j}_{i(\alpha)}) \qquad (5)$$

Where for i =1, 2 and 3 denote respectively the transmission cost, the processing cost and the queuing cost respectively.

As in figure 9 the three costs is giving by the following formula Transmission cost signaling with SEG:

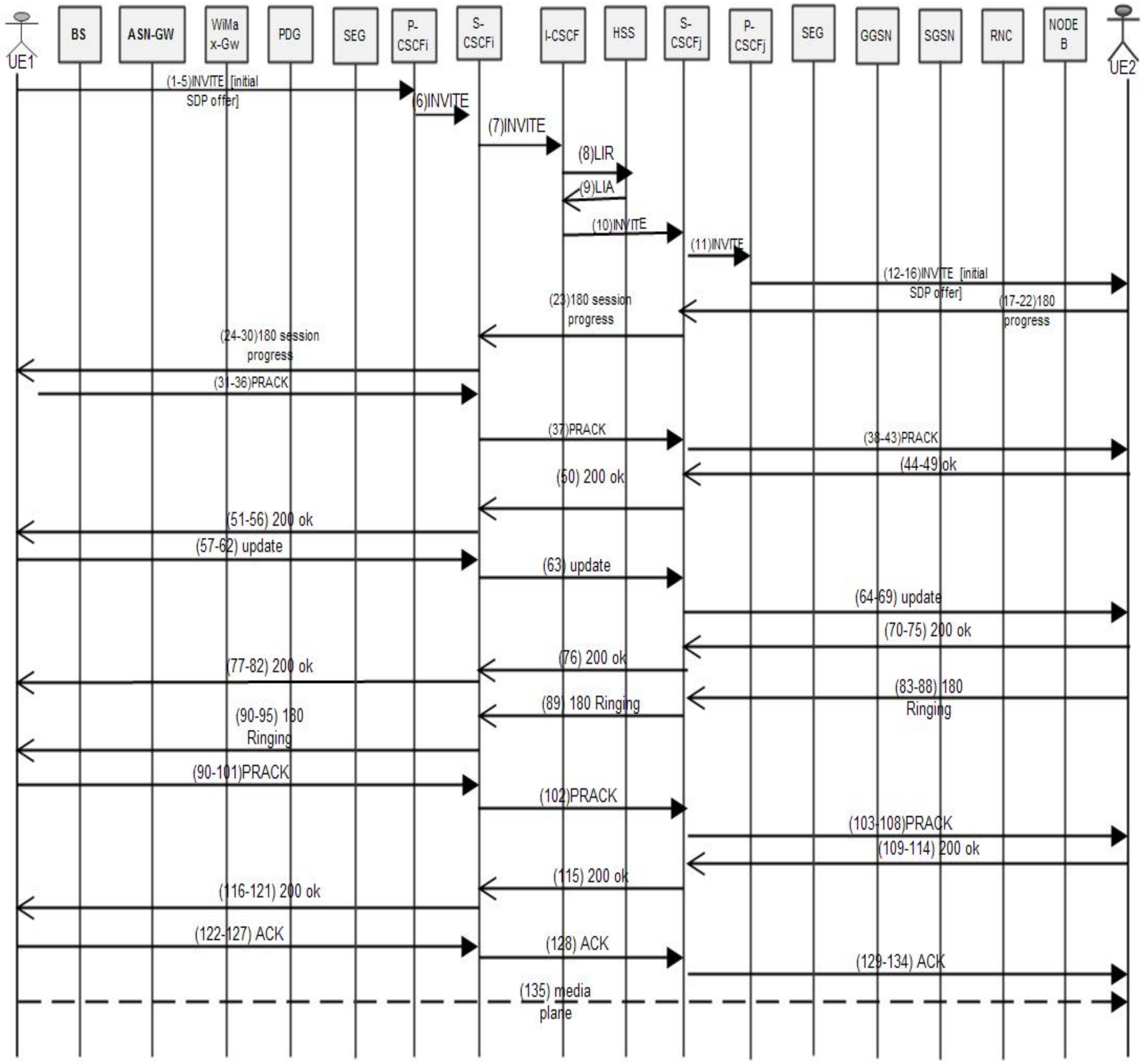

Figure 8. The WiMAX→UMTS session setup based IMS process signalling

$$C_{Transmission} = \lambda l \left[2 \times \mu_{wireless} + \mu_{wired} \left[\begin{array}{l} 10 \times d_{BS\text{-}ASGW} + 10 \times d_{ASGW\text{-}WIMAXGW} + 10 \times d_{WIMAXGW\text{-}PDG} \\ + 10 \times d_{PDG\text{-}SEG} + 10 \times d_{SEG\text{-}PCSCFi} + 10 \times d_{PCSCFi\text{-}SCSCFi} + 6 \times d_{SCSCFi\text{-}ICSCF} \\ + 2 \times d_{ICSCF\text{-}HSS} + 8 \times d_{ICSCF\text{-}SCSCFi} + 10 \times d_{PCSCFj\text{-}GGSN} \\ 10 \times d_{GGSN\text{-}SGSN} + 10 \times d_{SGSN\text{-}RNC} + 10 \times d_{RNC\text{-}NODEB} \end{array} \right] \right] \quad (6)$$

where d_i denote the number of hops or the number of messages between two entities.

The Processing cost signaling is giving by:

$$
\begin{aligned}
C_{Processing} = {} & 10 \times C_{BS} + 10 \times C_{ASGW} + 10 \times C_{WIMAXGW} + 10 \times C_{PDG} \\
& + 10 \times C_{SEG_i} + 10 \times C_{p\text{-}CSCF_i} + 10 \times C_{S\text{-}CSCF} + 10 \times C_{S\text{-}CSCFj} + 4 \times C_{I\text{-}CSCFj} \\
& + C_{HSS} + 10 \times C_{GGSN} + 10 \times C_{SGSN} + 10 \times C_{RNC} + 10 \times C_{NODEB}
\end{aligned}
\tag{7}
$$

Queuing cost signaling is giving by:

$$
\begin{aligned}
C_{queue}^{data} = {} & 10 \times E\,[\eta_{bs}] + 10 \times E\,[\eta_{ASGW}] + 10 \times E\,[\eta_{WIMAXGW}] + 10 \times E\,[\eta_{PDG}] \\
& + 10 \times E\,[\eta_{SEG_i}] + 10 \times E\,[\eta_{P\text{-}CSCFi}] + 10 \times E\,[\eta_{S\text{-}CSCFi}] + 10 \times E\,[\eta_{I\text{-}CSCF}] \\
& + E\,[\eta_{HSS}] + 10 \times E\,[\eta_{GGSN}] + 10 \times E\,[\eta_{SGSN}] + 10 \times E\,[\eta_{RNC}] + 10 \times E\,[\eta_{NODEB}]
\end{aligned}
\tag{8}
$$

5.3 Numerical results

In this section, we present numerical results of our proposed secured architecture in some use cases.

In our architecture, we consider a network that consists of two networks WiMAX and UMTS network.

The numbers of users in each type of network are:

$$N_{UMTS} = 700;\ N_{WIMAX} = 600$$

We also assume that each GGSN supports three SGSN, each SGSN supports four RNCs and each RNC controls two Nodes. The cost of transmitting the packets of the unit links in the wireless $\mu_{wireless}$ and the wire connections μ_{wired} are made to 3.84×10^6 and 0.1 respectively. The hop distances for GGSN is d_{GGSN} and for the RNC d_{RNC} are set to 4, while the other hop distances are set to 2. The length L of the IP address and the size of the machine word S is set to 32 bits.

In addition, the system value k is selected to be 5. The weighting factor is set at, and the delay time is increased to 100 ns for each memory access. The service rate for all entities of the network is set to 250 packets /s. In addition, the unit cost of treatment for all network entities is fixed at 4×10^3 except for the SGSN and the GGSN that the cost of processing unit for all network entities are set to 8×10^3.

Figure 8 depicts the transmission cost, figure 10 the processing cost of signaling in IMS and figure 11 depict Queuing cost for signaling for different values of IMS arrival rates with and without SEG cost security.

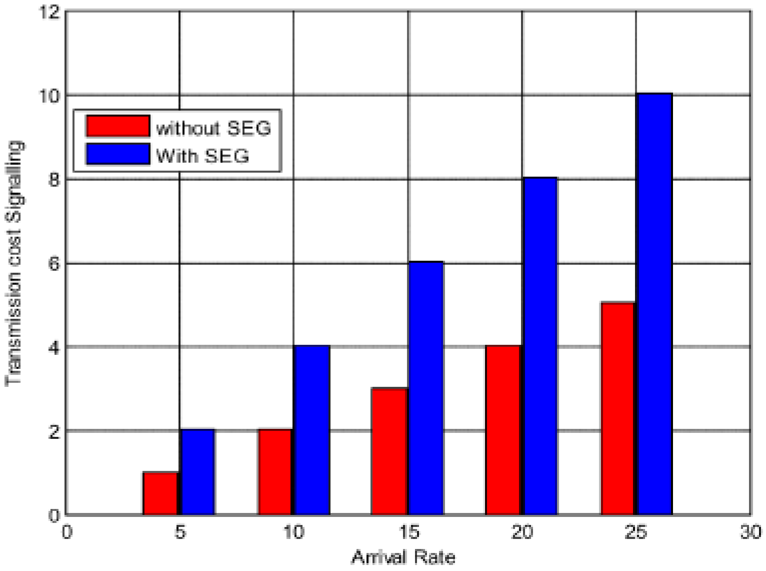

Figure 9. Trnasmission Cost of IMS with and without SEG

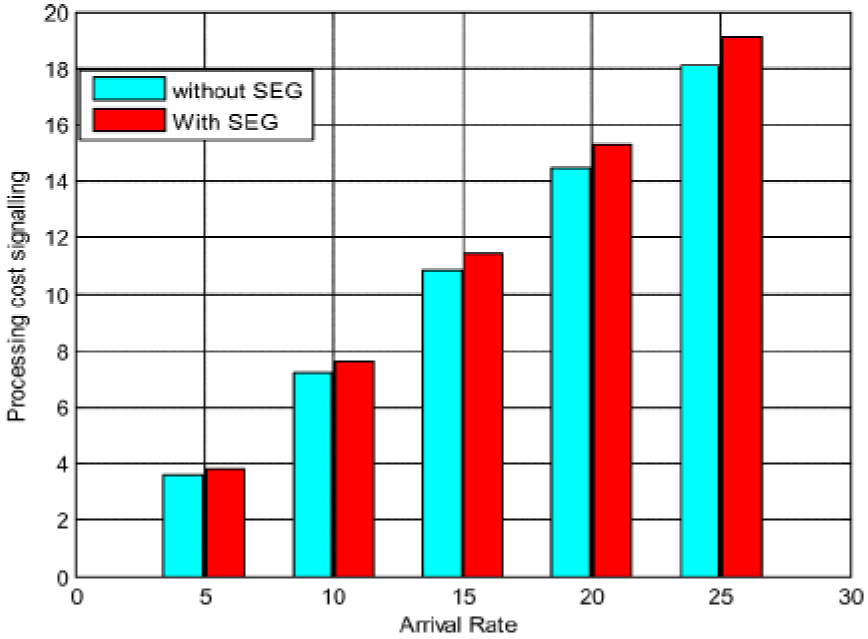

Figure 10. Processing cost of IMS with and without SEG

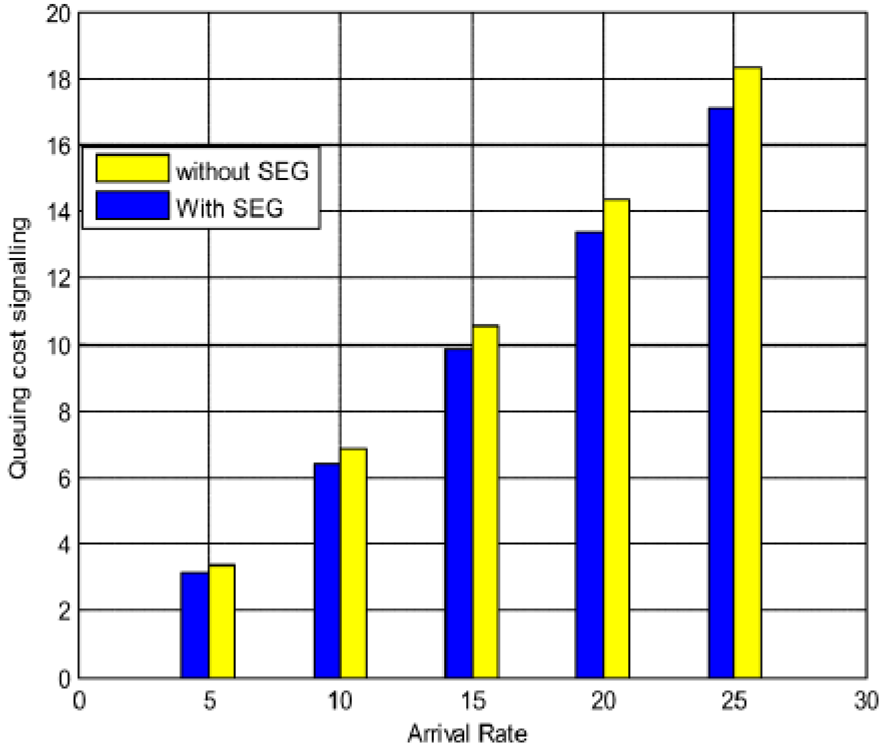

Figure 11. Queueing Cost of IMS with and without SEG

Figure 12 depicts the global cost of transmission and the processing for Signaling, for different values of IMS arrival rates λ. More specifically, the labels Csig_without and Csig_withSEG denote respectively the Global values of cost without SEG and with SEG.

As it was expected the cost for signaling IMS traffic without SEG is lower than the transmission cost for IMS traffic with SEG, but

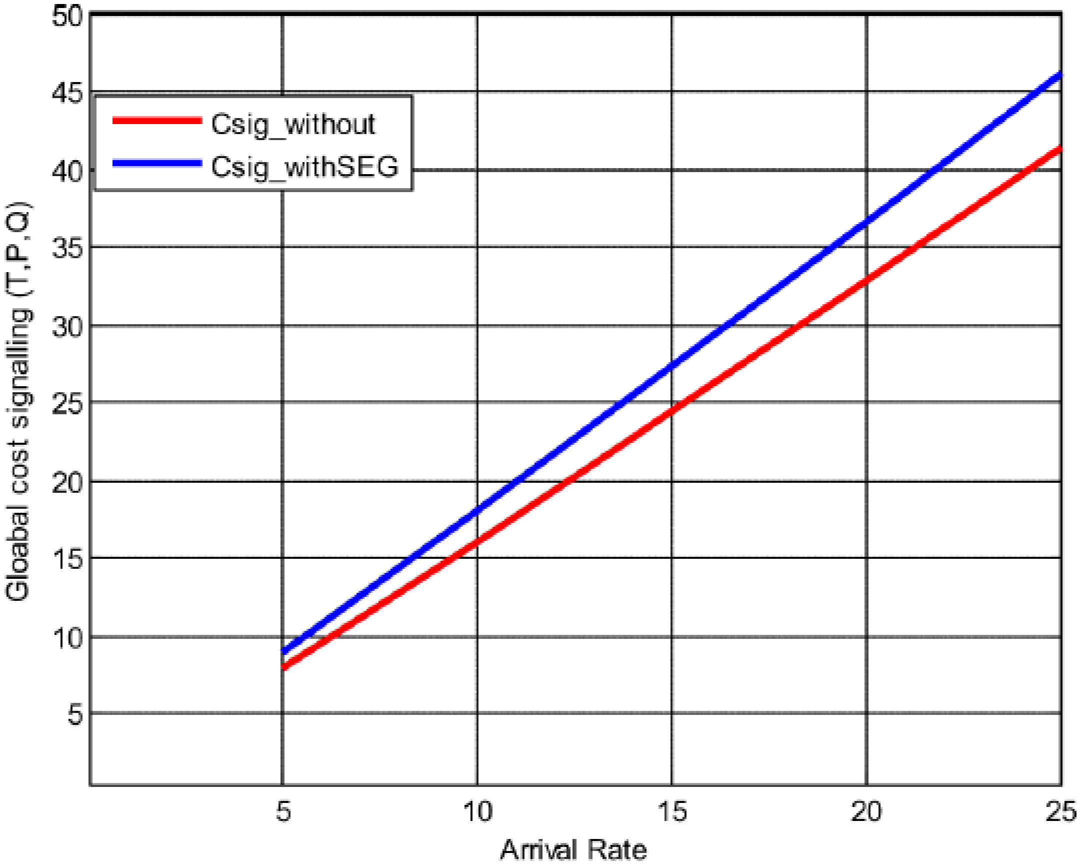

Figure 12. Globale Cost of IMS signalling with and without SEG

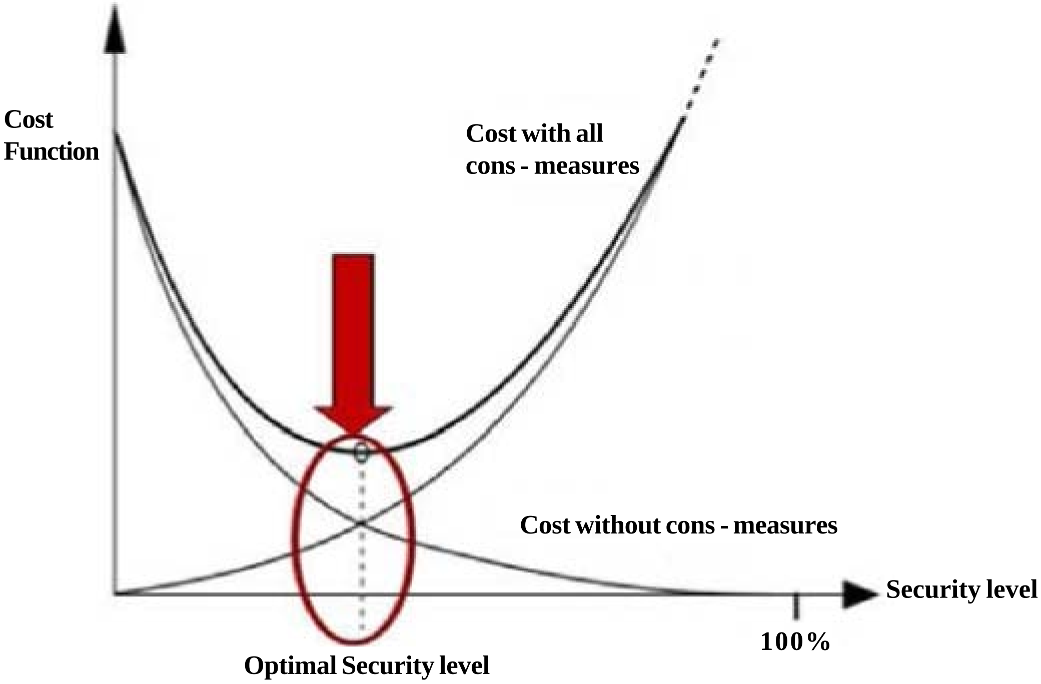

Figure 13. Cost function of a secured IMS system

the cost is increased by increasing arrival rate. As it is shown in the figure the difference of cost for signaling IMS traffic is increased for arrival rate higher and by increasing the cons measure. From This figure 12 the difference is kept constant and negligible independently of the value of the arrival rate λ.

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

For most systems, the cost for security increases exponentially with an increase in the security level toward the 100% level from Figure 13. We show that there is a tradeoff between the level of increasing system security and the potential cost incurred.

For Building optimal cost security level, we addressed the proliferation and magnitude of risks, the organizations need to consider a more automated, proactive approach to security.

6. Conclusion

By increasing and interconnecting complex systems of telecommunication Access Network (AN) in IMS ,the risk increase exponentially, our proposed architecture and formula are technical and functional issues for decreasing the compounding the risk factors .our idea is to give a design of secured and distributed IMS, by classification and evaluation of costs for this distributed and secured architecture IMS network . the proposed architecture giving the intelligence security side for incorporate the best secure business and respect different aspect of security like vulnerability, threats and attack model, a detailed analysis in different layers of IMS is giving. Also we give in the paper for the business to incorporate security intelligence as our approach of risk.

The proposed design reduce the cost to optimal level, we give a policy for securing the network IMS system by modeling the Risk as formula (1), The common formula denominator requires that Security today is more than a purely technical issue. It requires a frank discussion about risk, investment and taking a preventative approach to security issues. This paper addressed in a cost-effective manner, numerical result of signaling with and without SEG element in the IMS.

Clearly, more than ever, each component of architecture IMS and by our formula of risk make member of the enterprises owns a significant stake and a powerful role in securing the data and intellectual capital that flows through the network.

References

[1] 3GPP, GSM, ETSI. (2011). TS 23.228 IP Multimedia Subsystem (IMS); Stage 2 (Version 11.6.0, Release 11)

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

[3] Harri Holma, Antti Toskala. (2011). LTE for UMTS: Evolution to LTE Advanced, Second Edition. P344 Edittion.

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

[5] Al Shidhani, Leung, V. (2009). Pre-authentication schemes for umts-wlan interworking, Eurasip J. Wirel.Commun.Netw, pp.5:1–5:16, February . [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] Islam, S., Grégoire, J.-C. (2011). Multi-domain authentication for IMS Services,Computer Networks 55 Published by Elsevier, 2689–2704.

[8] Chen, C.-Y., et al. (2008). An efficient end-to-end security mechanism for IP multimedia subsystem, Computer Communications Published by Elsevier.

[9] Psimogiannos, N., et al. (2011). An IMS-based network architecture for WiMAX-UMTS and WiMAX-WLAN interworking, Computer Communications 34 Published by Elsevier, 1077–1099.

[10] Camarillo, G., Garcia-Martin, M. A. (2006). The 3G IP Multimedia Subsystem (IMS), second ed., Wiley.

[11] Measurements and Analysis of M/M/1 and M/M/c Queuing Models of the SIP Proxy ServerSureshkumar V. Subramanian, Rudra Dutta IP Communication Business Unit, CISCO Systems, Research Triangle Park , USA.

[12] Agrawal, P, Hung yeh, J., Chen, J.-C., Zhang, T. (2008). Ip multimedia subsystems in 3gpp and 3gpp2: overview and scalability issues, *IEEE Communications Magazine*, 138–145.

[13] Mani, M., crespi, N. Inter-domain qos control mechanism in ims based horizontally converged networks networking and services (icns'07), 9–25 june, p. 82.

[14] 3gpp ts 23.234 v8.0.0 (2008). 3gpp system to wireless local area network (wlan) interworking; system escription, release 8, december.

[15] Munir, A., Wong, V. (2007). Interworking Architectures for IP Multimedia Subsystems. *ACM/Springer Journal on Mobile Networks and Applications*, 12 (5) 296–308, December.

[16] IEEE (2006).Comparative Study of M/Er/1 and M/M/1 Queuing Delay Models of the two IP-PBXs Alireza Dehestani, Pedram Hajipour (ANSS'06) 2006 IEEE

[17] Rosenberg, J., et al. (2002). SIP: Session Initiation Protocol, IETF RFC 3261,June.

[18] 3GPP TS 33.203: Access Security for IP-based services.

[19] 3GPP TS 23.203. Policy and Charging Control architecture.

[20] 3GPP TS 23.107. Quality of Service (QoS) concept and architecture.

[21] 3GPP TS 29.162. Interworking between the IM CN subsystem and IP networks.

[22] 3GPP TS 26.114. IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction.

[23] 3GPP TS 29.328. IP Multimedia (IM) Subsystem Sh Interface; Signalling flows and message contents.

[24] 3GPP TS 23.380. IP Multimedia Subsystem (IMS); IMS Restoration Procedures.

[25] IETF RFC 3966: "The tel URI for Telephone Numbers.