

Challenges to Next Generation Services in IP Multimedia Subsystem

Kai-Di Chang*, Chi-Yuan Chen**, Jiann-Liang Chen*
and Han-Chieh Chao***

Abstract—The trend of Next Generation Networks' (NGN) evolution is towards providing multiple and multimedia services to users through ubiquitous networks. The aim of IP Multimedia Subsystem (IMS) is to integrate mobile communication networks and computer networks. The IMS plays an important role in NGN services, which can be achieved by heterogeneous networks and different access technologies. IMS can be used to manage all service related issues such as Quality of Service (QoS), Charging, Access Control, User and Services Management. Nowadays, internet technology is changing with each passing day. New technologies yield new impact to IMS. In this paper, we perform a survey of IMS and discuss the different impacts of new technologies on IMS such as P2P, SCIM, Web Service and its security issues.

Keywords—IP Multimedia Subsystems, Peer-to-Peer, Web Services, SCIM

1. INTRODUCTION

The architecture of UMTS (Universal Mobile Telecommunications System) can be divided into circuit-switched networks (CS), packet-switched networks (PS) and IP Multimedia Subsystem (IMS). The services on the UMTS can be roughly divided into voice service, data service and packet-based multimedia service. When UMTS integrates with these heterogeneous wireless network technologies, such as the 802.11 series wireless local area network (WLAN) and 802.16 series network (Worldwide Interoperability for Microwave Access, WiMAX), it could offer ubiquitous services anytime, anywhere and even while mobile. Thus, it can serve to achieve the goal of next generation communication networks.

It can be argued that the architecture of IMS has already been incubating for a long time if we look at the evolutionary development of 3GPP. The IMS is a network subsystem specified by 3GPP (3rd Generation Partnership Project). 3GPP proposed R99 (Release 99) in 1999. It contains the system architecture and services of core networks with standards such as WCDMA (Wideband Code Division Multiple Access) and TD-CDMA (Time Division-Code Division

※ This research was partly funded by the National Science Council of the R.O.C. under grants NSC 98-2219-E-197-001 and NSC 98-2219-E-197-002.

Manuscript received February 14, 2010; accepted April 8, 2010.

Corresponding Author: Han-Chieh Chao

* Dept. of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan (d9807502@mail.ntust.edu.tw, lchen@mail.ntust.edu.tw)

** Dept. of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan (chiyuan.chen@gmail.com)

*** Dept. of Electronic Engineering and Institute of Computer Science and Information Engineering, National Ilan University, I-Lan, Taiwan (hcc@niu.edu.tw)

Multiple Access). The All-IP architecture was planned promptly after R99 (the forerunner of IMS). Due to the architecture being too complex, the development work was divided into R4 (Release4) and R5 (Release5) in 2000. R4 was expected not to include IMS. It focused on the specification of IP transport, and was released in 2001. R5 was completed in 2002, and brought the IMS formally into the 3GPP standard. Further IMS related functions tend toward stability in R6 (Release 6) and were released in 2005. The follow-up R7 (Release 7) also adopted the concept of fixed mobile convergence.

IMS can be regarded as the trend of future wireless communication networks. The concept of IMS is to merge telecommunication technologies, wireless networks and wired networks under the All-IP environment to provide more extensible, real-time and interactive multimedia services for 3G and even future 4G networks. IMS uses modified IETF SIP (Session Initiation Protocol) to establish the service session. The main function is to combine circuit-switched and packet-switched domains. The contents are not limited by the access medium but become more extensible to offer more value-added services to users.

This paper is organized as follows. In Section 2, we review and discuss the related works and technological background. In Section 3, we discuss the main issues which have impact on IMS service. Finally, we present the future directions of IMS in section 4 and our conclusions in the final section.

2. BRIEF OUTLINE OF IP MULTIMEDIA SUBSYSTEM (IMS)

The IMS architecture as shown in Fig.1 can be divided into three tiers: the Media/Transport plane, Control/Signaling plane and Service/Application plane. The Media/Transport plane refers

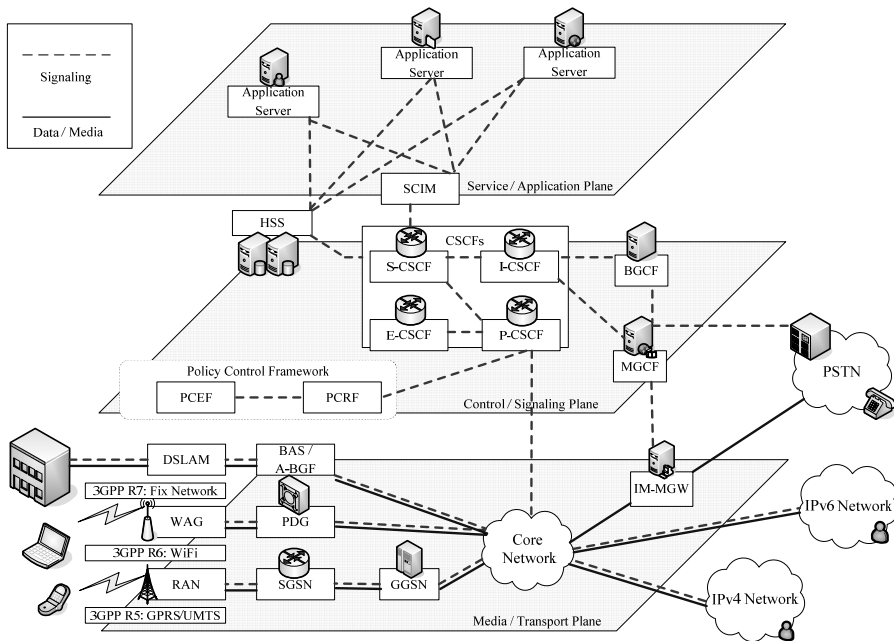


Fig. 1. Layered Architecture of IMS

to a wide range of different access technologies. Within the IP transport layer, users go through Wireless LAN, GPRS (General Packet Radio Service) or UMTS (Universal Mobile Telecommunication Systems) to acquire network connectivity. Once connected to IMS, users can access a variety of multimedia services.

There is a set of IMS core components in the Control/Signaling plane– CSCFs (Call Session Control Functions), which includes Proxy-CSCF (P-CSCF), Interrogating-CSCF (I-CSCF) and Serving-CSCF (S-CSCF). The SIP signaling will be processed and routed to the destination through this plane.

In the Service/Application plane, there are various application servers. The application servers provide users a wide range of IMS service. Operators can use the standard IMS architecture to build up their application servers.

3. CHALLENGES TO NEXT GENERATION SERVICES IN IMS

3.1 IMS meets Web2.0 World

Web services provided static pages in the past. Today, there are many dynamic pages even instant, real-time services in Web service, which is called Web 2.0. Users can interact with other people or conduct business through Web 2.0. One purpose of Web 2.0 is the same as the IP Multimedia subsystem – providing ubiquitous and various services to users any time. Thus, the IMS and Web 2.0 worlds bring many benefits. In [2], Jain et al. list the main features offered by each in Table 1.

IMS can provide many benefits by adopting Web 2.0 principles [3]. In the other words, Web 2.0 can benefit from implementing IMS functionalities [4]. Not only could IMS make Web 2.0 services better, but it could also bring new charging business models for these services.

- **Charging - New Business Models**

New business models can be promoted by using multiple charging mechanisms such as offline charging, online charging and flow based charging in IMS [5]. Moreover, by adopting IMS, Web 2.0 services could increase their users and reach them through different access offerings such as mobile, broadband, Public Switched Telephone Network (PSTN) and xDigital Subscribers Line (xDSL). This would allow the Web 2.0 service providers to realize their Web 2.0 principle of “Beyond a Single Device” such as a PDA phone or smart phone.

Table 1. IMS and Web 2.0 features

IMS	Web 2.0
Charging – New Business Models	Beyond a Single Device
Network Functionality reused	Collective Intelligence
Policy for Servers	Lightweight Programming Models
Quality of Service	User as Co-Developer
Strong Authentication	Valuable Data & Information
Service/Enablers reuse	

- **Quality of Service**

Popular Web 2.0 services such as YouTube and Google MAPs could put the core network and last mile under huge strain in the future. Service providers can use IMS to allocate different QoS levels to those services with its supported QoS mechanism and its QoS requirement. IMS can provide the important basic infrastructure for those services to guarantee their quality [6]. Web 2.0 service providers can use IMS core networks to assign policies for each service by controlling the different QoS mechanisms. For instance, policies can be applied with various bandwidth parameters and codecs for different subscribers, users and group permission levels.

- **Strong Authentication**

Apart from the QoS issues, cooperative Web 2.0 services could result in users' sensitive and private data being available to malicious users such as crackers. Web 2.0 services can prohibit these security risks [4] by using IMS's robust authentication mechanisms such as DigestAKA or security tunnels between IMS components either when registering or before sending any request.

- **Service/ Enabler reuses**

The IMS services and enablers can be opened up to the Web world. IMS services/enablers such as presence, location, conferencing, push-to-talk, IPTV and group management can be used by Web 2.0 services. The traditional telecommunications services such as Short Messaging Service (SMS) and Multimedia Messaging Service (MMS) can also be offered. The Web 2.0 service providers can increase services' value by using the service/enablers in IMS. The usage of these services, which are already well defined and tested, would reduce the cost of developing these functionalities for Web 2.0 service providers and enable them to deploy these applications in a short time.

- **Lightweight programming model**

IMS can expand its availability easily and cost efficiently by simply adopting the "Lightweight Programming Model" Web 2.0 principle. This model is based on a high level of accessibility for users, developers and/or creators and on the idea of adaptation and change towards improvement within the development process. Thus, people or service providers could open up many new services at minimal cost and in a short time.

Other successful Web 2.0 principles that IMS could take on are "users as co-developers," "harnessing collective intelligence" and "valuable data and information." IMS can allow users to be contributors to services through bringing these principles into IMS. As users can better understand what it is they require. This could result in novel applications becoming more suitable to their requirements. IMS also holds important data and information that is a core element for services. IMS could build upon Web 2.0 principles then provide its data, such as user's presence state, location information and his/her profile, to 3rd party service providers in order to combine information with a 3rd party's service. As a result, a new source of information can be created. By combining different regions such as IMS, third party providers, Web 2.0 and many novel services, the architecture can continuously evolve; see Fig.2.

In Fig.2. (a), we find that users who accesses IMS, Web 2.0 or third party provider services need to subscribe to all the domains independently. By combining these worlds, users can subscribe to one subscription and benefit from converged services, as shown in Fig.2. (b). Single

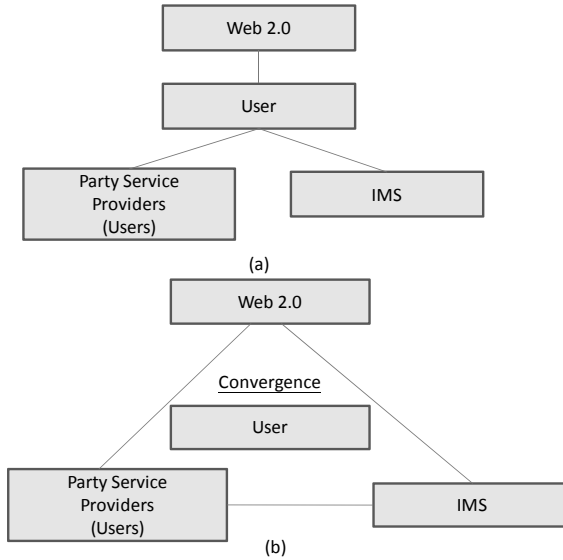


Fig. 2. User accessing services in (a) Existing world and (b) Combined IMS and Web 2.0

Sign-On (SSO) can be offered by the IMS to enhance user experience. Thus, the IMS framework can be seen as the future of telecommunication networks; the Web 2.0 world is responsible for user generated content, communities creation, auto-management, and collaboration. The 3rd party service provider is responsible for services provided to users without using IMS framework or Web 2.0 principles. By combining these worlds, it is assumed that the domains can complement each other, offer more creative applications to users and enhance users’ experience.

3.2 From IMS to IMS 2.0

When IMS meets the Web 2.0 world, the new service type will have to have influence on current IMS architecture in order to compensate for new services in Web 2.0. The concept of IMS 2.0 architecture is proposed by Jain et al. [2]. There are two main design considerations in it: The first is an “Open Service Access (OSA) framework,” the concept of OSA in IMS 2.0 is to expose the IMS assets to the Web 2.0 world, an OSA framework that carries IMS for third parties was looked into [7]. However, it is very complex to use these assets. For instance, IT developers need to have in-depth understanding of telecommunications [8]. Thus, Parlay X Web Service was proposed to solve the aforementioned problems but some telecommunication knowledge remains paramount [8]. Consequently, the combination of the kinds services from the IMS and the Web 2.0 worlds require a greater understanding of telecommunication knowledge. Moreover, different services could have adopted different Web service extensions for their security, trust and session management issues. This would result in interoperability problems that will become more critical when combing with different services. Although the Web Service Interoperability Organization is researching solutions for interoperability problems between Web services, it was felt that an easier approach needs to be adopted [9]. While in consideration of such dilemmas and in keeping with the implementation of Web 2.0 principles, another ap-

proach for opening up the IMS assets in a simpler manner was chosen.

The second design consideration is “Positioning of IMS 2.0 Service Architecture.” This consideration involves how the core components should be located in the IMS or the Web domain. As Web 2.0 services become easier to access and knowledge about telecommunications is acquired for IMS services, it would be advantageous for core components to be hosted in the IMS domain. This would improve the dynamic of composed services and make the concurrent framework leveraged according to service’s requirements. For instance, services could have different requirements for charging, authentication, QoS and policy, which can be easily distributed by the core components in the IMS domain. Finally, network functionalities of media servers and legacy services can be easily contacted and combined with existing services.

For accessing the Web world between the IMS and the Web 2.0 domain, Web 2.0 Gateway was introduced in [2]. The main design rules for their IMS 2.0 architecture are: The IMS 2.0 Web Portal serves as a unit of access for management and configuration. And only authorized users from both the IMS and Web 2.0 domain can use the Web Portal for service management. Then, by defining the different security levels, Service Level Agreement (SLA), QoS required for the service to apply charging information and policies applicable for each service. It is the interface for the system manager to access the IMS 2.0 databases (ex: Resource Database and Home Subscribe Server), which hold information such as service information, user types, user permissions and user profiles. In this architecture, Web Portal services/enablers can be added, updated or removed. Fig.3. shows the high level functionality of the IMS 2.0 Service Broker, Resource Database and Web Portal. As shown in Fig.3., service providers can specify information about the services via the Web Portal interface. Information is stored in the Resource Database. Service Brokers can access it to provide the authentication, charging mechanisms, QoS policies and other features required by each service.

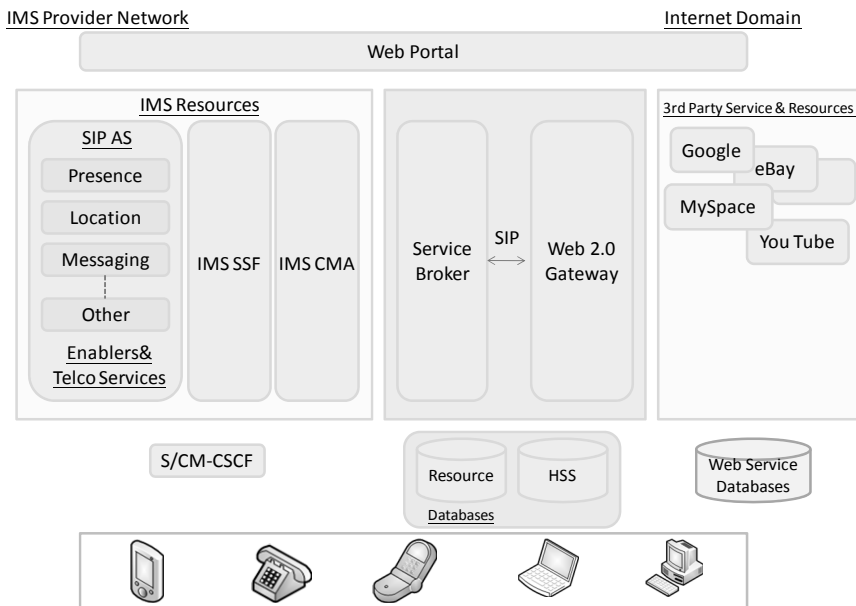


Fig. 3. The IMS 2.0 Architecture

Table 2. Authentication and Authorization Levels

IMS Users	Authenticated based on user Credentials and public user identity. Can retrieve specific info only about them.
Enterprise Users	Users are provided a single identity in order to access inform of set of users. Can retrieve info only about their users.
Service Providers	Can access only information provided by IMS 2.0 or IMS enablers. Information is provided without revealing the identity of the user
Mobile users	Using SMS to authenticate users: particular public enablers' info allowed
Guest Users	Users are limited access to enablers' info

In the proposed IMS 2.0 architecture, users have to authenticate themselves with the common AAA component. Table 2 indicates the different levels of authorization that can be offered to various groups of users. High level authorization is offered to Web users, who are also mobile users, as a method for the mobile device users to confirm their identity.

The common charging enabler could make sure that all the services used are as per the user package plan and the QoS required. Each component could send their Charging Data Records (CDR), service usage and charging mechanism to the charging enabler. The Service Broker can terminate sessions when a user's credit limit is over.

To discover resources in the Web world, a GET request is sent to the Web 2.0 Gateway by HTTP. Then the request is translated into a SUBSCRIBE message in SIP and then it's forwarded to the Service Broker. The Service Broker replies with a SIP NOTIFY message containing the resource URI and information about the discovered resources. This message is translated through the Web 2.0 Gateway and sent to the Web world by HTTP. Thus, the resources can be connected by SIP-URI. The user can progress from one state to another to discover and then get information about acquired IMS 2.0 resources. As IMS 2.0 resources can be used by HTTP URI, it would be an easy method or indicator for the users to create and publish their services. In the SIP world, resources in IMS world can be shown as:

sip:r1.resources@ims.provider.com
 sip:r2.resources@ims.provider.com
 ...
 sip:rn.resources@ims.provider.com

3.3 SCIM & Service Brokers

The concepts of Service Capability Interaction Manager (SCIM) or Service Broker were standardized in 3GPP IMS related specifications. We will describe the concept for both SCIM and Service Broker in this section.

3.3.1 SCIM

SCIM stands for "Service Capability Interaction Manager". This terminology was first proposed by 3GPP in April 2001. The purpose of SCIM was "service capability coordination" at the beginning. The concept was proposed that SCIM be a standalone component located between the S-CSCF and the IMS application servers (AS). It is connected with the S-CSCF and the application servers through the SIP+ reference point. The reason for the definition is that SCIM as

a separate entity from the S-CSCF logically belonged in the application layer. It's different with the S-CSCF, it would use non standardized data to perform its duties.

The contribution of SCIM results in some problems, as service interaction management is considered a serious matter in telecommunications. However, some vendors didn't want to start standardizing the SCIM in 3GPP due to the complexity of this issue. The other vendors thought that IMS was not simply a voice-centric network. Thus, the standardization of the SCIM was limited to be a technique for documents in 3GPP specifications. However, while the IMS was proposed, some operators started to ask for SCIM. Some cooperators started to propose "SCIM" related specifications in these years.

In the situation that the IMS application layer was not yet well-defined, the term of SCIM became a magic box that would overcome all the unresolved questions.

3.3.2 Service Broker

At the beginning of 2005, 3GPP R7 specification defined a new work item. The goal is to specify a service broker in the context of OSA/Parlay, "Enable detection and resolution of service interaction." The work item suggests that the service broker should support the IMS SCIM, but the suggestion was removed from the final version. However, the 3GPP CT5 (OSA/Parlay) technical report stated in its discussion of the works that the service broker should have the capability of brokering non-OSA applications. The motivation of the service broker was to standardize the SCIM and to make it become part of an OSA/Parlay solution.

Being a component under control of OSA/Parlay, the service broker had no opportunity to be accepted as a SCIM. IMS is standardized by 3GPP groups and 3GPP SA2 for its architecture. Some companies support the service broker and therefore proposed to extract it from 3GPP CT5 and to have it standardized by another group. 3GPP SA2 didn't want to standardize it. It was a similar situation to SCIM in 2001 but, in this case, development proceeded. The sample cases to explain the requirement of standardizing the service broker for IMS were voice-centric architecture. Thus, a clear description of the service broker role is, "service interaction management," such as the initial concept of SCIM.

Specifications about the role of service broker were documented in technique report 23.810, a part of 3GPP R8. 3GPP organization spent much effort standardizing a function. But the organization body didn't have a clear understanding of the problems to be solved. There are already some useless 3GPP specifications and there is no need to add the service broker as one of the useless specifications.

For example, a dispensable 3GPP concept is the "subsequent filter criteria". The sFCs were introduced with initial filter criteria (iFCs). It permits an application server to set filter criteria dynamically in the S-CSCF after triggered signaling through initial filter criteria. sFCs serve the same purpose as dynamic triggers in Intelligent Networks - that permit applications in Intelligent Networks to dynamically set new trigger points to change. The problem is that the functions of sFCs do not make sense with the ISC on SIP because the concept conflicts with routing mechanisms in SIP worlds.

3.4 Peer-to-Peer (P2P) Networks

Peer-to-peer, commonly called P2P, is any type of distributed network architecture group by many devices. The participants make part of their resources available to other members. This

network does not need central infrastructure (such as servers or stable hosts). Peers play both roles as consumers and suppliers for resources. This contrasts the traditional client-server model, in which the servers supply and the clients only consume.

Peer-to-peer was popularized by file sharing software like Napster, BitTorrent, eMule and eDonkey. The concept of peer-to-peer file sharing networks arouses new structures and philosophies in other areas. In this social context, the concept of peer-to-peer is like a meme which refers to fair social networking. It is currently spreading throughout society, enabled by internet technologies in general.

To provide IMS P2P service, Liotta et al. introduce a novel P2P service, the PeerMob system [10]. The peerMob system is realized as a SIP-based application, making the P2P service IMS-compatible without changing any existing IMS servers.

The PeerMob system adopts a hybrid, Super Peer and group based architecture. The structure of the P2P peer groups is determined by service semantics. Peers are organized into different groups for publishing and discovering the services or functionalities. A certain number of peers will be elected to Super Peer by the PeerMob system according to a Super Peer election algorithm. Super peers work as information switches for discovery of P2P requests in the particular group, and store the meta-adverts to the contents in the group. Simple peers store the actual data contents to be downloaded for other peers. The PeerMob system holds the service schema which effects the way peers are dynamically grouped, acting as meta-information repetitive of super peer identifiers. A detailed description of the operation of the PeerMob system is illustrated in Fig.4.

P2P services mainly rely on two functions: publish and discovery. Publishing allows a peer to broadcast its content, resources or services to make the resources shareable with other peers. Discovery allows a peer to find its interesting resources.

Liotta et al. assume that the PeerMob system has already been populated with useful content,

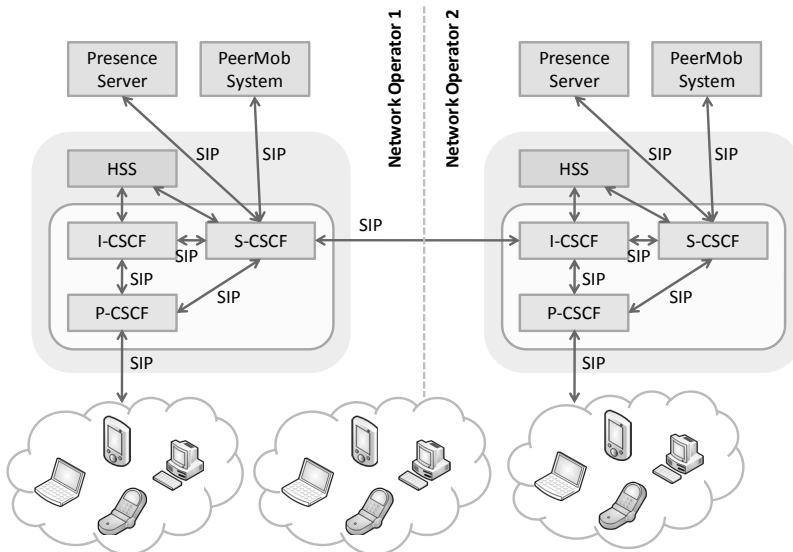


Fig. 4. P2P-IMS: PeerMob System

including digital rights management (DRM) protected content [11]. And they also assume that content in [10] has been categorized well using meta-information according to a semantic-based mechanism which was proposed in [11].

The PeerMob system has three main functions:

The first is to create groups based on semantic information attached to the data [11]. Bloom filters have been used for the corresponding discovery algorithm, which method is well-established in the area of P2P systems.

The second function is group management. In a mobile P2P scenario such as UE in IMS, the number of super peers in each group should be adaptive with the group size.

The last, disaster recovery, is an important element of PeerMob. The PeerMob system could keep track of the status of super peers, such as who can disconnect at any moment.

3.5 Mobile Clients

Nowadays, almost every person has at least one mobile device such as a cellular phone. With the rapid development of technology, there are many new communicating applications in cellular phones. For example, the cellular phone can be equipped with the 802.11 Wi-Fi, Bluetooth, GPS and radio. Thus, people can use their device as a tiny computer to surf the internet, as an audio player to listen to music and/or as a navigator for locating places. There is one thing to keep in mind, that the size of a device and its battery capacity is limited by human thought. Also, the core networks of telecommunication are on the way towards Next Generation Networks. This leads vendors to ponder the following question: How about the Mobile Client for the Next Generation Networks?

IP Multimedia Subsystems are the major component for the convergence of computer networks and telecommunication networks. Thus, the compatibility of mobile devices and the IMS becomes a very important factor of design for mobile clients. The most popular platforms for mobile devices are Symbian, J2ME and BREW. The functionality of each platform is described in Table 3.

Table 3 makes a comparison between the three most popular mobile development platforms

Tabel 3. Commonly used Mobile Development Platforms [12]

Functionality	Symbian	J2ME	BREW
Foundation Language	C++	Java	C++
Learning Curve	Difficult	Average	Difficult
Emulator	Free	Free	Limited
Debuggers Available	Good on latest version	Excellent	Need Payment
Cost for Development Tool	Varies (there are tree tools)	Free	Extensive
Cross-Platform Deployment	Compile for each target	Average	CDMA Handsets only
Developer Community and Support	Extensive	Extensive	Limited
Market penetration	Extensive	Extensive	few countries only
SIP support	Yes	Yes	Unknown
RTP Support	Yes	No	Unknown

[12]. J2ME combines a resource-constrained Java Virtual Machine (JVM) and a set of Java Application Programmable Interface (API) for developing applications targeted at small devices such as set-top boxes and mobile phones. J2ME is divided into configurations [13], profiles and optional API.

For the sake of research and development of a platform for the proposed client [14], the Java Community Project (JCP) SIP API for J2ME [15] was used. This API is specified in the Java Specification Request (JSR) 180. In [14], they intend the architecture to be used for the mobile client of the Next Generation Networks. The proposed IMS Client has the capability to initiate and process SIP requests and responses with the IMS Core. Fig.5 shows the flow-diagram of the IMS Client from when the device is turned-on. Then Fig.5 illustrates the process from performing of the registration, creation of a session and ending the session. The proposed IMS Client consists of the UA Client (UAC) and the UA Server (UAS). Thus the client could process both requests and generate responses. The proposed IMS Client has the capability to register with the IMS Core. The proposed client could establish sessions by SIP methods, negotiate media codec and QoS mechanisms through Session Description Protocol (SDP) [16] offer/answer, terminate a session and exchange text messages based on plane-text or XML. The flow of media traffic can be achieved by SIP MESSAGE method to communicate between two end users.

If the IMS gains approval quickly into the telecommunication industry, the success of Fixed Mobile Convergence (FMC) in the NGN will become reality; and the IMS Client presented in [14] will be closer to becoming a fully developed client. Table 4 compares characteristics of currently existing IMS Clients to those of the proposed IMS Client.

There was an IMS Client developed by [14] as a mobile client for Next Generation Networks. The J2ME platform was used to develop their IMS Client as J2ME is one of the most popular mobile device development environments. Though targeted towards all kinds of hand held smart-phone devices, the client was only audited using Nokia’s Emulator, which was provided by the Sun Wireless Toolkit. Demonstrations were made by performing tests on the IMS Test-bed. The paper presented that vendors could use J2ME to develop IMS Clients. J2ME based IMS Clients are light users when compared to currently existing IMS Clients which are not tar-

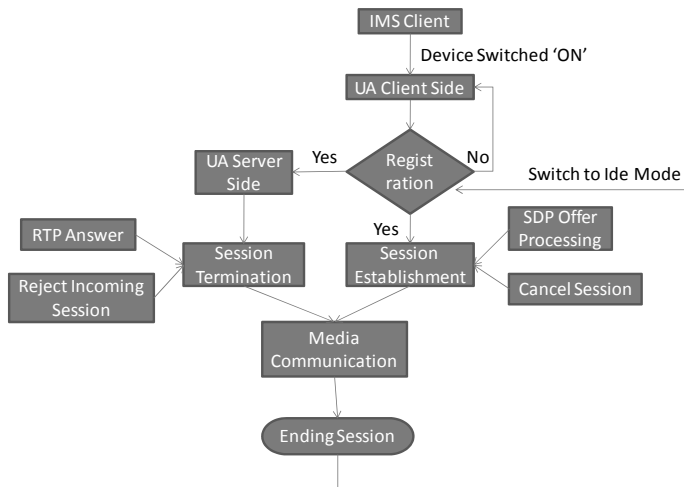


Fig. 5. IMS Client Flow Diagram

Tabel 4. IMS Client Performance Analysis

Function	Light-Weight IMS Client	FOKUS OpenIMS Client Lite	IMS Communicator
Development Platform	J2ME (CLDC)	Java (JSE) and .NET	Java (JSE)
Targeted End-User Device	CLDC Compliant Mobile Phones	Pocket PC, Laptops and Desktops	Desktops and Laptops
Memory Footprint (Excluding Libraries)	About 37 KB	About 1.3 MB	About 1.5 MB
Authentication Support	In Future	Digest-AKA	Digest-AKA (Work in progress)
Client Availability	Not Available online	Available online (No source code)	Available online (With source code)
Standard Compliance	3GPP and IETF	3GPP, IETF and TISPAN	3GPP, IETF and TISPAN
SIP Support	Yes	Yes	Yes
RTP Support	In the Future	Yes	In the Future

geted for CLDC based mobile devices.

3.6 Service Security

The IMS security mechanisms are divided into two parts: access security and network domain security. Access security, specified in 3GPP TS 33.203 [1], includes authentication related mechanisms and traffic protection between the UE and core network. Network domain security, specified in 3GPP TS 33.210 [17], includes traffic protection between network elements and takes into account roaming and non-roaming scenarios.

The IMS security architecture is shown in Fig.6. The required security associations between the User Equipment (UE) and IMS core network are specified. On the UE side, the IMS authentication key and functions are stored on a Universal Integrated Circuit Card (UICC) and the IMS Subscriber Identity Module (ISIM) indicates a collection of IMS related security information and UICC functions. The five security associations for the IMS security architecture are numbered in Fig.6 thusly:

1. Provides mutual authentication between UE and HSS. The UE must have one user private identity (IMPI) and one or more user public identity (IMPU). The pre-shared long-term key in the ISIM and the Authentication Center (AuC) of HSS is associated with the IMPI.
2. The Gm reference point provides a security link and corresponding security associations between the UE and the P-CSCF after registering.

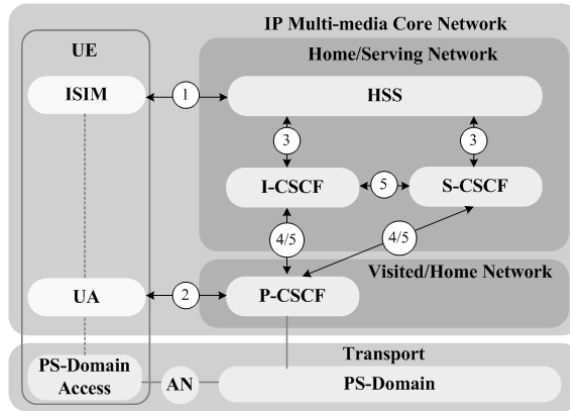


Fig. 6. IMS Security Architecture [1]

3. The Cx-interface provides security associations for the HSS Database.
4. Provides link security for network elements between different network domains. It is specified by TS 33.210, as the Za interface in Fig.7. The Za Interface applies the Encapsulating Security Payload (ESP) tunnel mode.
5. Provides link security for network elements within the same network domain. It is specified by TS 33.210, as the Zb interface in Fig.7.

Numerous well-known attacks have been perpetrated on IP networks. Security is the first challenge for communication systems migrating into the All-IP network. According to the existing attacks which have been discussed relative to IMS they can be classified into two types: Time-Dependent attacks [18, 19], and Time-Independent attacks[20-24], as depicted in Fig.8. It is easy for attackers to try exploiting the security weaknesses within the SIP methods and to cause DoS (Denial of Service) attacks to the provided services.

Besides various traditional network attacks, the forthcoming problems [25] that IMS would meet are as follows:

- Fixed-Mobile Convergence (FMC) Security Risks - Both wired networks and wireless networks can be integrated using the IMS architecture. IMS has become the architectural solu-

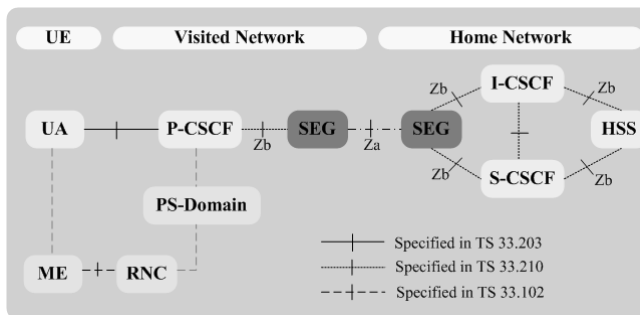


Fig. 7. IMS Network Domain Security [1]

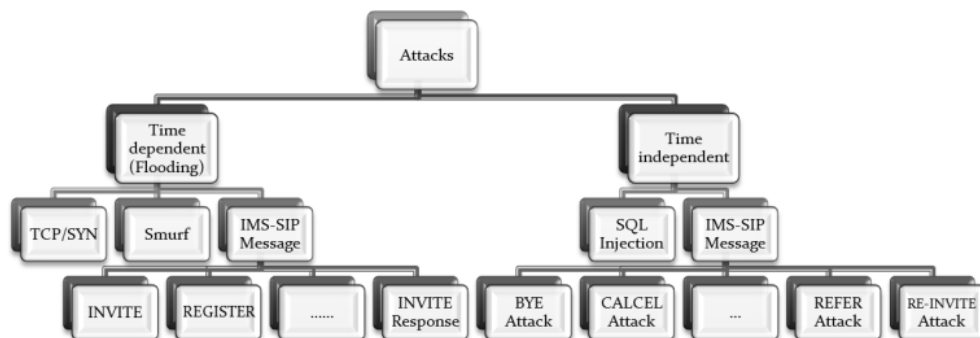


Fig. 8. Attacks Classification in IMS

tion for FMC, adopted in many different standardization solutions such as PacketCable and ETSI TISPAN. Because the environmental requirements and hardware for wireless and wired networks are different, the IMS security features may not be directly adopted by the wired networks. It is expected that the IMS core network would be accessed from both wireless and wired networks, making the related security mechanisms very important.

- **Media Plane Security** - Currently, the IMS security architecture provides security protection only for SIP signaling messages. The media plane may be protected by the hop-by-hop security associations inside the core network, however, these security mechanisms may be disabled by the provider for performance reasons. Therefore, under the above-mentioned FMC architecture, media plane security will not be guaranteed.

Recently, 3GPP proposed TR 33.828 [25] to discuss IMS media plane security, but they have just begun to specify the related requirements in this technical report. The main issues are the Lawful Interception requirements, media security and SIP related problems. In 3GPP, the preferred solutions are to perform key exchange messages in the signaling path (Session Description Protocol, SDP) and to start with RTP (Real-Time Transport Protocol) and then upgrade to SRTP (Secure Real-Time Transport Protocol).

Currently, regarding the IMS media plane security issues, most research focuses on the IMS registration authentication procedure. [26] Proposed a One-Pass Authentication Procedure for UMTS to decrease the registration traffic up to 50% and authenticate the IMS user correctly. Huang et al. [27] proposed a one-pass AKA procedure which does not lose efficiency as Lin et al.'s, and also provides mutual authentication and key agreement capability. However, when the user obtains the key from the above-mentioned procedure to establish security associations, they're only provided link security between the UE and P-CSCF. [28] Proposed an IMSKAAP key exchange protocol and fit it into the IMS session initiation procedure to achieve media plane end-to-end security. This mechanism also mitigates the impact of SPIT (Spam over IP Telephony) using Mutual Authentication, and fulfilling the Lawful Interception requirement.

- **Spam over IP Telephony** - Like the Internet spam problems, the Spam over Internet Telephony is an urgent problem for VoIP and IMS. A malicious person could send numerous unsolicited voice calls or prerecorded messages to the IMS user. Unlike the spam email problem,

the SPIT exists in real-time services. But the SPIT can be prevented through policy control, completed user authentication and a tight trust model for IMS.

4. FUTURE DIRECTIONS

From the content in section 3, we can list the related research topic to each region. We give the summary to overcome the different impacts as follows:

For Web 2.0 Worlds – The applications and several web services make the web world more and more active. It also pushes web service towards a high peak. In the future IMS world, questions as to co-existing with various services are very important when we consider the architecture combining Web 2.0 and IMS. For example, the research issues include how to enhance co-operation and make them more intimate in IMS and Web. How to reduce the overhead when translating between protocols is also a research topic.

For IMS 2.0 Architecture – When scholars propose IMS 2.0 architecture, they have to consider that it be made compatible when co-functioning within existing specifications, which are decided by the standard organizations. Due to the fact that IMS 2.0 architecture is a newly proposed architecture, which has yet to be confirmed by formal organization, the practicality of IMS 2.0 architecture is still under observation. The main difference between IMS and IMS 2.0 is that the IMS 2.0 architecture introduces the concept of “HTTP SOAP” inside. The main research about IMS 2.0 architecture can be divided into two parts. The first part is the core network architecture of IMS 2.0, the other part is users’ terminals design.

For SCIM & Service Brokers – The service reusing capabilities to implement different integrated services in next generation networks provides flexible and open service architecture. As the main portion of service delivery, the SCIM and Service Brokers play the role of middleware building blocks between the control and service layers. The concepts of both SCIM and Service Broker have advantages and drawbacks when operators chose one of them.

The goal is to provide rich services over the next generation network and reduce both costs and development time. With the Service Broker architecture, service blending can be deployed quickly and easily by its steplet. Steplets are the key elements of the Service Broker. It can forward a request to an application server and contact non-sip servers via any form of RMI/RPC protocol. The steplet engine loads and creates steplets. For any steplet, the engine creates one instance that is used for all messages. As a result, all messages in the Service Broker are handled by the same steplet. Thusly, this could enhance service delivery, negotiation and management. No matter which architecture is chosen, the compatibility between different operators and service providers must be maintained. Otherwise, the concept of Next Generation Networks (NGN) and Fixed-Mobile Convergence (FMC) would be useless.

For P2P Networks – P2P Networks not only bring the benefits for file sharing and service sharing but also some negative influence; for instance, pirated goods and bandwidth occupation. The question of how to bring the P2P advantages into full play and at maximum benefit is a topic to be studied. For example, different core networks for service control could integrate P2P architecture to distribute the traffic or the bottle neck into one core network.

For Mobile Clients – When the programmers or developers design for the Mobile Client of the next generation services they have to consider how to present the user interface in a limited display panel. Also, how to implement those complex functionalities in small user equipment

becomes a trade-off for the vendors. The most important factor is to present the concepts of next generation service. In future, the next implementation could be to layout the Real-time Transport Protocol (RTP) to allow audio and video sessions, the adding of presence functionality for instant messaging, and the deployment of the IMS Client within the relevant IMS compliant mobile devices. The lack of support for these additional IMS functions for the presented IMS Client forms the basis to classify our IMS Client as a light-weight client.

For Service Security – Regarding the different security issues, each topic is worth study in next generation services. No matter how good the technique is; the security issues always exist. Therefore, how to use the technology solution or management solution to reduce security risks is the most important goal in handling security issues.

5. CONCLUSION

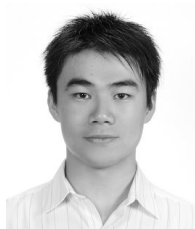
In this paper, we have highlighted impacts on the next generation's services. We discuss the new technologies as challenges to IMS. Currently, the speed of formulating specifications is much slower than rapid applications' development; therefore, considering the impact in different regions is important for next generation services.

We not only point out the impact from different regions but also indicate guiding principles for those topics. By following these guiding principles, we can establish a complete architecture for the next generation's services. In the future, regardless of the emerging services and consideration of standardization and compatibility, we can form a mature solution for next generation service in IP Multimedia Subsystem.

REFERENCES

- [1] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; 3G security; Access security for IP-based services (Release 7); Technical Specification 3G TS 33.203 2005.
- [2] Jain M. and Prokopi M., "The IMS 2.0 Service Architecture," in Proceedings of Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST '08. The Second International Conference on, 2008, pp.3-9.
- [3] What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software, <http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-Web-20.html>
- [4] Camarillo G. and Garcia-Martin M.A., "The 3G IP multimedia subsystem (IMS): Merging the Internet and the cellular worlds". Chichester, UK, John Wiley & Sons, 2004.
- [5] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging (Release 8); Technical Specification 3G TS 32.260 version 8.2.0, 2007.
- [6] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; End-to-end Quality of Service (QoS) concept and architecture (Release 7); Technical Specification 3G TS 23.207 version 7.0.0, 2007.
- [7] 3GPP, "3rd Generation Partnership Project; Open Service Access (Release 7); Technical Specification 3G TS 23.198 version 0.7.0, 2007.
- [8] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 2: Third party call (Release 8); Technical Specification 3G TS29.199-2 version 8.0.0, 2007.
- [9] WS-I "Web Services Interoperability Organization," <http://www.ws-i.org/>

- [10] Liotta A. and Ling Lin, "Managing P2P services via the IMS," in Proceedings of Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on, 2007, pp.586-600.
- [11] Liotta A., Ballette M., Lin L., Gasparoni M., Brick P. and Papadoglou N., "Service-Driven Group Management for Mobile P2P Services," 2005, pp.221-230.
- [12] Guo Fang Mao, Talevski A. and Chang E., "Voice over Internet Protocol on Mobile Devices," in Proceedings of Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS International Conference on, 2007, pp.163-169.
- [13] Li S. and Knudsen J., "Beginning J2ME: from novice to professional", 3rd, Apress, 2005.
- [14] Masonta M. T., Oyedapo O. J. and Kurien A. M., "Mobile Client for the Next Generation Networks," in Proceedings of Broadband Communications, Information Technology & Biomedical Applications, 2008 Third International Conference on, 2008, pp.274-279.
- [15] Nokia and JCP, "JSR 180 - SIP API for Java 2 Micro Edition," in Vol.1.0.1, 2004.
- [16] IETF, "SDP: Session Description Protocol; SDP: Session Description Protocol; RFC 4566, 2006.
- [17] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; 3G security; Network Domain Security; IP network layer security (Release 7); Technical Specification 3G TS 33.210 2005.
- [18] Sher. Muhammad, Wu. Shaoke and Magedanz. Thomas, "Security Threats and Solutions for Application Server of IP Multimedia Subsystem (IMS-AS)," in Proceedings of IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation, 2006. MonAM2006, Tuebingen, Germany, September, 28-29, 2006.
- [19] Rebahi Y., Sher M. and Magedanz T., "Detecting flooding attacks against IP Multimedia Subsystem (IMS) networks," in Proceedings of the 7th ACS/IEEE Intl. Conference on Computer Systems and Applications (AICCSA 2008), Doha, Qatar, March 31 - April 4, 2008, pp.848-851.
- [20] Sher M. and Magedanz T., "Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks," in Proceedings of Information Assurance and Security, 2007, IAS 2007, Third International Symposium on, 2007, pp.171-176.
- [21] Tirado Ivan, "IP Multimedia Subsystem (IMS) signaling core security," in Proceedings of the 5th annual conference on Information security curriculum development, Kennesaw, Georgia, USA, 2008.
- [22] Chi-Yuan Chen, Han-Chieh Chao, Sy-Yen Kuo and Kai-Di Chang, "Rule-based Intrusion Detection Mechanism for IP Multimedia Subsystem," in Journal of Internet Technology, Vol.9, pp.329-336, December, 2008.
- [23] Chakraborty Shyam, Peisa Janne, Frankkila Tomas and Synnergren Per, "IMS Multimedia Telephony over Cellular Systems", Wiley, 2007.
- [24] Mogno M., Petrilli I. and Listanti M., "Vulnerability in IMS-Internet interworking: analysis and relevant solutions," in Networking Workshop 2006, 2006.
- [25] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; IMS media plane security (Release 8); Technical Report 3G TR 33.828 2005.
- [26] Yi-Bing Lin, Ming-Feng Chang, Meng-Ta Hsu and Lin-Yi Wu, "One-pass GPRS and IMS authentication procedure for UMTS," in IEEE Journal on Selected Areas in Communications, Vol.23, pp.1233-1239, 2005.
- [27] Huang C. M. and Li J. W., "One-Pass Authentication and Key Agreement Procedure in IP Multimedia Subsystem for UMTS," in Proceedings of Advanced Information Networking and Applications, 2007. AINA '07. 21st International Conference on, 2007, pp.482-489.
- [28] Chen C.Y., Wu T.Y., Huang Y.M. and Chao H.C., "An Efficient End-to-end Security Mechanism for IP Multimedia Subsystem," in Computer Communications, Vol.31, pp.4259-4268, December, 2008.



Kai-Di Chang

He received his B.S. degree in electrical engineering from National Dong Hwa University, Taiwan, R.O.C. in 2007. He received his Master's degree in institute of computer science and information engineering at National I-Lan University, Taiwan, R.O.C. He is currently pursuing his Ph.D. degree in electrical engineering at National Taiwan University of Science and Technology.. His research interests include Voice over IP, IP Multimedia Subsystem and network security.



Chi-Yuan Chen

He received his M.S. degree in electrical engineering from National Dong Hwa University in 2007. He is currently pursuing his Ph.D. degree in electrical engineering at National Dong Hwa University. His research interests include wireless networking, communication core network and network security.



Jiann-Liang Chen

He was born in Taiwan on December 15, 1963. He received the Ph.D. degree in Electrical Engineering from National Taiwan University, Taipei, Taiwan in 1989. Since August 1997, he has been with the Department of Computer Science and Information Engineering of National Dong Hwa University, where he is a professor and Vice Dean of Science and Engineering College. Prof. Chen joins the Department of Electrical Engineering, National Taiwan University of Science and Technology, as a full professor and Vice Dean of Electrical Engineering and Computer Science now. His current research interests are directed at cellular mobility management, digital home network, telematics applications, cloud computing and RFID middleware design.



Han-Chieh Chao

He is a jointly appointed Professor of the Department of Electronic Engineering and Institute of Computer Science & Information Engineering, National Ilan University, I-Lan, Taiwan. He also holds a joint professorship of the Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan. His research interests include High Speed Networks, Wireless Networks and IPv6 based Networks and Applications. He received his MS and Ph.D. degrees in Electrical Engineering from Purdue University in 1989 and 1993 respectively. Dr. Chao is also serving as an IPv6 Steering Committee member and Deputy Director of R&D division of the NICI Taiwan, Co-chair of the Technical Area for IPv6 Forum Taiwan. Dr. Chao is an IEEE senior member, IET and BCS Fellows.