

國立交通大學

資訊工程學系

碩士論文

W-CSCF 之一段式認證機制設計

The design of W-CSCF with one Pass Authentication Mechanism



指導教授：張明峰 教授

研究生：邱文凱

中華民國九十三年六月

W-CSCF 之一段式認證機制設計

The design of W-CSCF with One Pass Authentication Mechanism

研究生：邱文凱

Student: Wen-Kai Chiu

指導教授：張明峰教授

Advisors: Prof. Ming-Feng Chang



A Thesis Submitted to
Department of Computer Science and Information Engineering
College of Electrical Engineering and Computer Science
National Chiao Tung University
in Partial Fulfillment of the Requirements
for the Degree of Master
in
Computer Science and Information Engineering
June 2004
Hsinchu, Taiwan, Republic of China

中華民國九十三年六月

W-CSCF 之一段式認證機制設計

學生：邱文凱

指導教授：張明峰 博士

國立交通大學資訊工程學系（研究所）碩士班

中文摘要

全球行動電信系統(Universal Mobile Telecommunication System, UMTS) 透過網際網路通訊協定多媒體子系統(IP Multimedia Subsystem, IMS) 來達成支援多媒體服務。而在網際網路通訊協定多媒體子系統中，是由呼叫通話控制功能(Call Session Control Function, CSCF) 來提供多媒體服務。WGSN 整合了 SGSN 和 GGSN 的功能，並且在分封數據網路和無線網路結點之間扮演閘道的角色。除此之外，WGSN 提供了連接到 GPRS 網路的存取機制。

於本論文中，我們提出無線區域網路之呼叫通話控制功能(WLAN-based CSCF, W-CSCF)這個元件，使得在 WGSN 網路上的無線用戶端可以取得 IMS 的服務。W-CSCF 整合了 Interrogating CSCF (I-CSCF) 和 Serving CSCF (S-CSCF)的功能，並且負責提供服務控制和通話控制的功能。當使用者欲取得 IMS 服務之前，必需在 GPRS 和 IMS 兩個網路上通過認證機制。針對無線用戶端透過 WGSN 存取 IMS 服務，我們提出了一段式認證機制 (One-Pass Authentication mechanism)。一段式認證機制也是需要執行 GPRS 的認證機制，但是簡化了 IMS 的認證機制。

The design of W-CSCF with One Pass Authentication Mechanism

Student: Wen-Kai Chiu

Advisor: Dr. Ming-Feng Chang

Department of Computer Science and Information Engineering
National Chiao Tung University

Abstract

Universal Mobile Telecommunications System (UMTS) supports multimedia services through IP Multimedia Subsystem (IMS). In IMS, multimedia services are set up and controlled by the Call Session Control Function (CSCF). The WLAN-based GPRS Support Node (WGSN) integrates both Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) functionalities and acts as a gateway between the Packet Data Network (PDN) and the WLAN node. Besides, the WGSN node provides an access mechanism to a GRPS network.

In this thesis, we propose a new component, *WLAN-based Call Session Control Function* (W-CSCF), to enable WLAN users in a WGSN network to access the IMS services. The W-CSCF node integrates both the I-CSCF and S-CSCF functionalities of the IMS and is responsible for the service control and call control. For UMTS, authentication procedure is performed at both the GPRS and the IMS networks before an MS can access the IMS services. We present a *One-Pass Authentication mechanism* for WLAN users to access the IMS services through a WGSN. One-Pass Authentication performs the GPRS authentication but simplifies the IMS authentication.

誌謝

感謝我的指導老師，張明峰教授，兩年來細心及費心的指導。方能順利完成此篇論文。於受業間，老師的耐心指正和灌輸我正確的人生方向，亦是讓我受益良多。在撰寫論文期間，感謝孟達學長的指導和相互研究。感謝弘鑫學長在實驗量測上的意見提供。感謝芳森學長和則嘉學長平日的叮嚀和照顧。感謝逸聖和毓麒這兩位同儕的彼此砥礪和互相扶持，一起走過這研究所的兩年生活。也要感謝 IC 實驗室的學弟們，榮泰、其範、瑋晟和建彰的支持和鼓勵。在此也要感謝我六年來的好室友，育旻及宏儒的鼓勵和關心。另外，由衷的感謝我的摯愛，宜蓁，從大學到研究所無怨無悔默默的支持我，是我心靈上最大的支柱。最後要感謝父母的全力栽培，讓我無後顧之慮的可以全力在學業上衝刺。養育之恩，謹記在心。

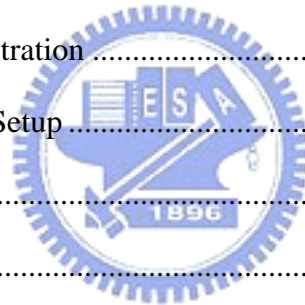
最後，原將此篇論文獻給我所愛的家人與好友。



Tables of Contents

中文摘要	i
Abstract.....	ii
誌謝	iii
Tables of Contents	iv
List of Figures.....	vi
List of Tables	viii
Chapter 1 Introduction.....	1
1.1 IMS	2
1.2 SIP	3
1.3 P-CSCF.....	5
1.4 I-CSCF.....	6
1.5 S-CSCF.....	7
1.6 HSS.....	9
1.7 P-CSCF discovery	10
1.8 WGSN	12
1.9 Motivation and Overview of this thesis.....	13
Chapter 2 WLAN-based CSCF	14
2.1 Overview	14
2.2 Architecture of W-CSCF	15
2.2.1 I-CSCF module Feature.....	16
2.2.2 S-CSCF module Feature.....	17
2.2.3 Subscriber Information Database	18
2.3 Application Server	20
2.3.1 AS acts as SIP Proxy mode.....	22

2.3.2 AS acts as B2BUA mode	25
2.4 Summary	28
Chapter 3 Authentication Procedure	29
3.1 Overview	29
3.2 Two-Pass Authentication.....	30
3.2.1 Composition of the GPRS authentication.....	30
3.2.2 Two-Pass Authentication procedure Message Flow	34
3.3 One-Pass Authentication	41
3.4 Comparison.....	43
Chapter 4 Performance Measurement	45
4.1 The Platform and Measurement Tools.....	45
4.2 Measurement of Registration	46
4.3 Measurement of Call Setup	48
Chapter 5 Conclusion	52
Chapter 6 Reference	53



List of Figures

Figure 1-1: Architecture of the IP Multimedia Subsystem.....	2
Figure 1-2: S-CSCF Service Control Model	7
Figure 1-3: P-CSCF and I-CSCF locations for MS.....	8
Figure 1-4: HSS Structure and Interface	10
Figure 1-5: P-CSCF discovery using DHCP and DNS	11
Figure 1-6: P-CSCF discovery using PDP context activation.....	11
Figure 1-7: Architecture of the WGSN network	12
Figure 2-1: Architecture of the WGSN with the W-CSCF network.....	14
Figure 2-2: Architecture of W-CSCF.....	15
Figure 2-3: IMS Registration.....	16
Figure 2-4: W-CSCF Triggering Architecture.....	19
Figure 2-5: Call Filtering Service architecture.....	23
Figure 2-6: Message flow of the AS supporting Call Filtering Service	24
Figure 2-7: Call Forwarding Service architecture	25
Figure 2-8: Message flow of the AS supporting Call Forwarding Service	26
Figure 3-1: Distribution of authentication data from HSS to SGSN.....	31
Figure 3-2: Generation of Authentication Vector	32
Figure 3-3: Authentication and Key Agreement.....	33
Figure 3-4: User authentication function in the USIM.....	34
Figure 3-5: Message Flow for 3GPP GPRS Authentication.....	36
Figure 3-6: Message Flow for 3GPP IMS Authentication.....	37
Figure 3-7: Illegal IMS Registration	40
Figure 3-8: One-Pass Authentication procedure.....	41
Figure 4-1: Measure Environment.....	46

Figure 4-2: Performance of the W-CSCF (Registration).....48

Figure 4-3: Performance of the W-CSCF (no AS involved) 50

Figure 4-4: Performance of the W-CSCF (AS involved) 51



List of Tables

Table 1-1: SIP Request	4
Table 1-2: SIP Response	5
Table 2-1: Classification of Service Point Trigger	19
Table 2-2: Operation modes of Application Server	21
Table 3-1: Identical Steps in GPRS and IMS Authentications	39
Table 4-1: Measurement Results for Registration	47
Table 4-2: Measure Results for Call Setup (Normal)	49
Table 4-3: Measure Results for Call Setup (with AS involved)	51



Chapter 1 Introduction

Mobile communication has become a very important technology in recent years. The first generation radio access network for mobile communication is based on analog technology. The 2nd generation is based on digital technology such as Global System for Mobile Communications (GSM), Personal Handy Phone System (PHS) and Personal Access Communications System (PACS) [1]. Recently, the 2.5G technology, such as General Packet Radio Service (GPRS) [2], with mobile data service has become more attractive to both operators and subscribers. In the next generation mobile network, 3G and B3G, the Core Network (CN) will be an all-IP architecture using the Internet Protocol (IP). In the all-IP architecture, IP Multimedia Subsystem (IMS) [3] uses Session Initiation Protocol (SIP) [4] for signaling control and call control. Besides, IMS provides Call State Control Function (CSCF) [3] for IP telecommunication services, real-time interactive games and multimedia services. The service of IMS may become more flexible than those of the Intelligent Network (IN). The advantages of IP networks include lower equipment cost, lower bandwidth requirements for transporting voices and the widespread availability of IP. AS a result, IP multimedia services can be easily deployed in heterogeneous networks, such as wired network and wireless network.

1.1 IMS

CSCF: Call Session Control Function
 HSS: Home Subscriber Server
 MRF: Multimedia Resource Function
 AS: Application Server
 SGSN: Serving GPRS Support Node
 GGSN: Gateway GPRS Support Node

MGCF: Media Gateway Control Function
 BGCF: Breakout Gateway Control Function
 SCP: Service Control Point
 T-SGW: Transport Signaling Gateway
 R-SGW: Roaming Signaling Gateway

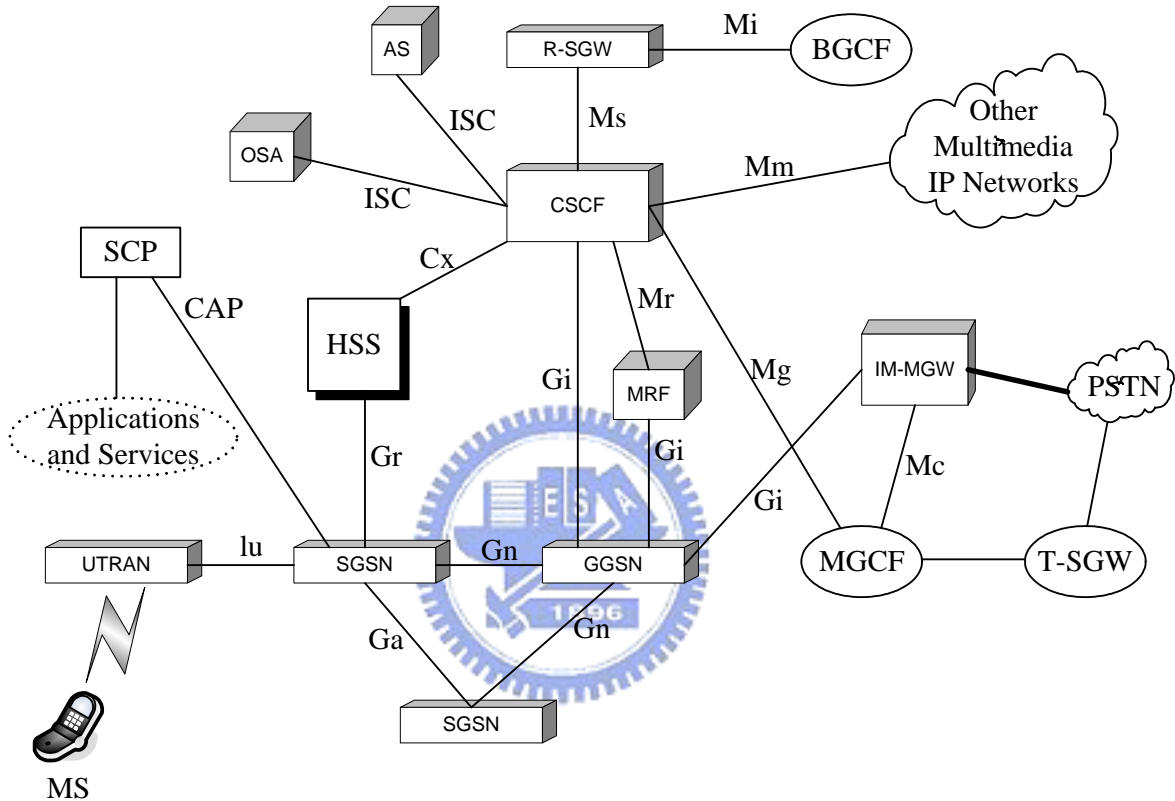


Figure 1-1: Architecture of the IP Multimedia Subsystem

The IP Multimedia Subsystem (IMS) comprises all CN elements for provision of multimedia services. Figure 1-1 shows the architecture of the IP Multimedia Subsystem.

The IMS services are not only the evolution of the circuit switch services but also a level of services, mobile terminals, and user expectation. The IMS enables PLMN (Public Land Mobile Network) operators to offer their subscribers multimedia services based on and built

on Internet protocol, applications and services. In order to provide IMS services, vendors must supply new entities; the new function entities provided by the IMS are Call State Control Function (CSCF) [3, 7], Home Subscriber Server (HSS) [3, 7] and Application Server (AS) [5].

The CSCF is responsible for session control. It manages SIP sessions and collaborates with other network elements for session control, service control and resource allocation. The CSCF may be combined on the same platform with other logical entities that perform signaling functions (as showed in Figure 1-1). A CSCF in IMS network can perform as three different roles, such as Proxy-CSCF, Interrogating-CSCF and Serving-CSCF. The detailed description of the three types of CSCFs will be discussed in following sections.



1.2 SIP

Session Initial Protocol (SIP) is an application-layer control protocol that can establish, modify and teardown multimedia sessions such as Internet telephony calls. SIP can also be used to invite new participants to already existing sessions for multicast conferences. Internet Engineering Task Force (IETF) SIP working group is responsible for SIP standardization. SIP can also be used in conjunction with several other IETF protocols, such as Session Description Protocol (SDP) [6], to handle the setup, modification and teardown of multimedia sessions. The 3rd Generation Partnership Project (3GPP) also uses SIP in the

IMS network that offers voice and multimedia service for 3G mobile devices. SIP is also one of call control protocols in 3G networks and it is used for signaling establishment in the IMS network. It can support sessions via multicast or single uni-cast, a mesh of uni-cast sessions, or a combination of these choices.

Table 1-1: SIP Request

Method	Functionality
REGISTER	Log in and register with a SIP server
INVITE	Initiate a session
ACK	Confirm that the final response has been received
CANCEL	Terminate a pending request
BYE	Terminate a session
OPTIONS	Query a server about its capabilities

SIP defines five types of network entities: (1) User Agent Client, (2) User Agent Server, (3) Registrar, (4) Redirect Server, and (5) Proxy Server. More detailed information can be found in [4]. There are also six methods and six classes of response, as listed in Table 1-1 and Table 1-2. SIP extensions, documented in RFCs, define additional methods. For example, SUBSCRIBE message is a new SIP method which is not mentioned in [4].

Table 1-2: SIP Response

Response	Functionality
1XX	Provisional: received, continuing to process the request
2XX	Success: the action was successfully received, understood, and accepted
3XX	Redirection: further action needs to be taken in order to complete the request
4XX	Client Error: the request contains bad syntax or cannot be fulfilled at this server
5XX	Server Error: the server failed to fulfill an apparently valid request
6XX	Global Failure: the request cannot be fulfilled at any server

A SIP server can be stateless or stateful. The stateless implementation provides good scalability and the server need not remember anything about the call. SIP uses the format and syntax of HTTP. The SIP message is opaque (it can be any syntax); it can be described with the Multipurpose Internet Mail extension (MIME), or the Extensible Markup Language (XML). SIP identifies a user with a Uniform Resource Identifier (URI), which can be placed in web pages, e-mail message or printed literature, to provide the user the ability to initiate and maintain a communication session.

1.3 P-CSCF

The Proxy-CSCF (P-CSCF) is an entry point for a UE to the IMS network. The P-CSCF can be discovered by a UE using two methods: (1) DHCP/DNS procedure discovery (2) PDP context activation [3] (see section 1.7).

The P-CSCF provides the following functionalities:

- ✓ Forward SIP REGISTER messages received from a UE to an I-CSCF determined by the home domain name of the UE.
- ✓ Forward SIP messages received from the UE to the S-CSCF whose name the P-CSCF has received as a result of the registration procedure.
- ✓ Forward the SIP request or response to the UE.
- ✓ Maintain a security association between itself and each UE.
- ✓ Should perform SIP message compression/decompression.

1.4 I-CSCF



The Interrogating-CSCF (I-CSCF) is an IMS entity that provides a contact point within an operator's network. It allows subscribers of the home network and roaming subscribers to register. The I-CSCF behaves as a firewall forwarding SIP messages toward the home network and is responsible for selecting an S-CSCF for the MS. There may be multiple I-CSCFs within an operator's network.

The I-CSCF provides the following functionalities:

- ✓ Assigning an S-CSCF to a user performing SIP registration procedure.
- ✓ Route a SIP request received from a UE towards the S-CSCF of the UE.
- ✓ Obtain the address of the S-CSCF from HSS.

- ✓ Forward SIP request and response to the S-CSCF

1.5 S-CSCF

The S-CSCF provides session control for subscribers accessing services within the IMS network. Within a network, different S-CSCFs may have different functionalities and provide different services. The S-CSCF has responsibility for interacting with network databases such as the HSS for mobility and the AAA (Authentication, Authorization and Accounting) Servers for security. As part of the SIP Registration process, a user will be allocated an S-CSCF that will reside in the subscriber's home network and be responsible for all aspects of session control. Furthermore, the S-CSCF also interacts with the application servers to obtain value added services. Figure 1-2 shows the Service Control Model of the S-CSCF [5].

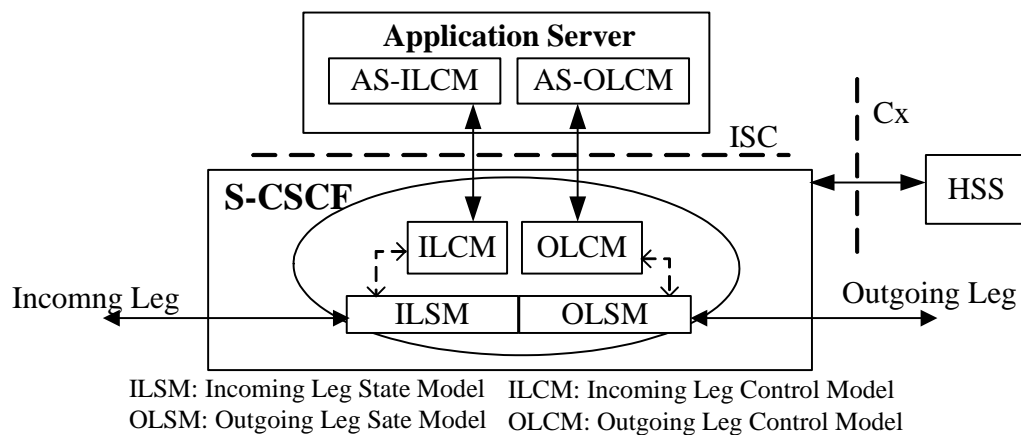


Figure 1-2: S-CSCF Service Control Model

The S-CSCF provides the following functionalities:

- ✓ May behave as a SIP Registrar [4], i.e. it accepts registration requests and makes its information available through the HSS.
- ✓ Session control for the registered UE's session.
- ✓ Finds out I-CSCF in case of roaming subscriber or if destination subscriber is the customer of the different operator network and forwards SIP requests or responses to the I-CSCF
- ✓ Modify the SIP request for routing an incoming session to Circuit Switch (CS) domain according to HSS and service control interactions.

The CSCF may be distributed in both the visited and the home networks to support home network call control of a session. Figure 1-3 shows the possible CSCF locations.

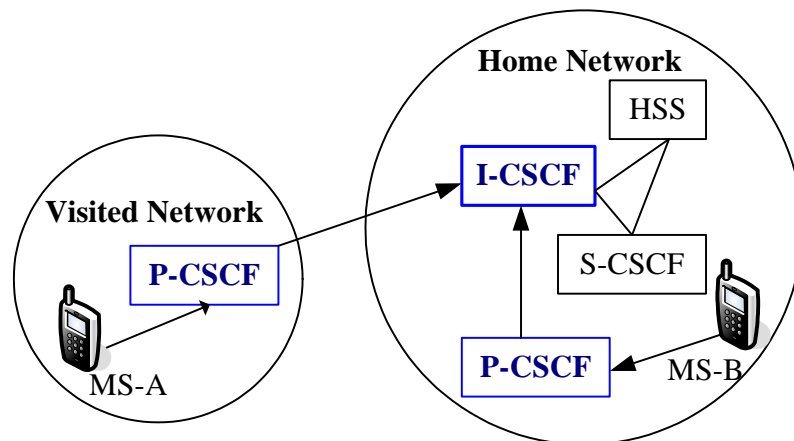


Figure 1-3: P-CSCF and I-CSCF locations for MS

1.6 HSS

Home Subscriber Server (HSS) includes many database functions that are required in 3G networks. These functions provided by Home Location Register (HLR), DNS server, AAA server and location server. Figure 1-4 shows the structure and interface of HSS [7]. HSS also contains related subscription information to support S-CSCF handling calls/sessions. A home network may contain one or several HSSs that may depend on the number of mobile subscribers, on the capacity of the equipment and on the organization of the network.

The HSS is responsible for holding the following user related information: (1) User Identification, Numbering and addressing information. (2) User Security information (i.e., Network access control information for authentication and authorization) (3) User Location information (i.e., the HSS supports the user registration, and stores location information, etc) (4) User profile information, detailed description in [7].

The HSS provides the following functionalities:

- ✓ IP multimedia functionality to provide support to control functions of the IMS such as the CSCF. It is needed to enable subscriber access to the IMS services.
- ✓ The subset of the HLR functionality required by the PS Domain.
- ✓ The subset of the HLR functionality required by the CS Domain, if it is desired to

enable subscriber access to the CS Domain or to support roaming to legacy GSM/UMTS CS Domain networks.

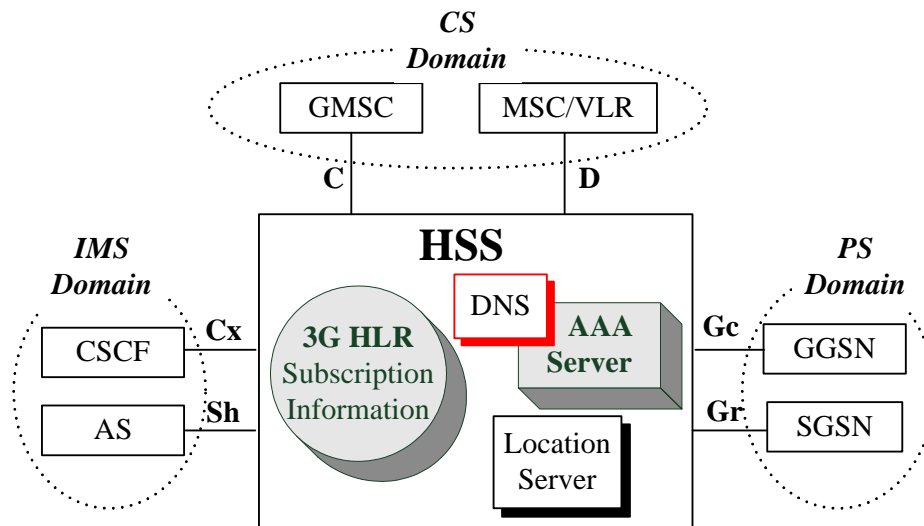


Figure 1-4: HSS Structure and Interface

1.7 P-CSCF discovery

In this section, we illustrate two methods for P-CSCF discovery: (1) DHCP/DNS procedure (2) PDP Context Activation. We first illustrate DHCP/DNS procedure. The GGSN acts a DHCP Relay Agent to relay DHCP messages between UE and the DHCP server (see Figure 1-5):

1. Establish PDP context bear.
2. UE requests a DHCP server and request the domain name of the P-CSCF and IP addresses of DNS server.
3. UE performs a DNS query to retrieve a list of P-CSCF(s) IP addresses.

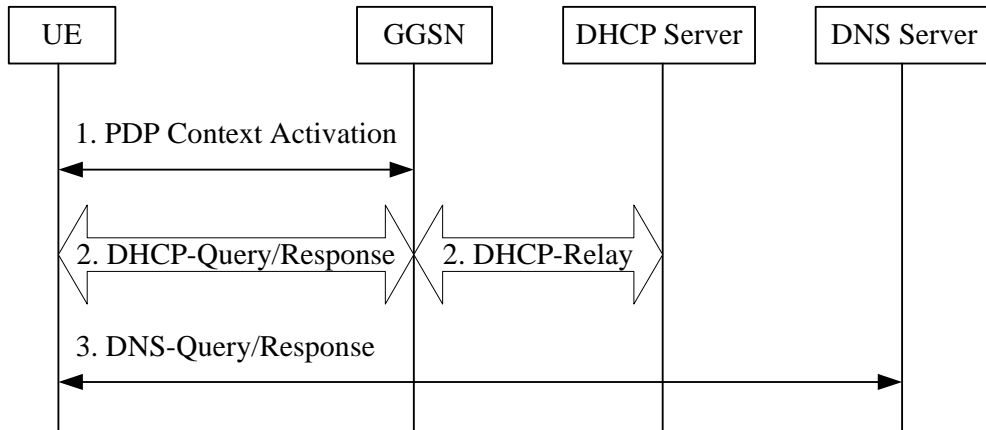


Figure 1-5: P-CSCF discovery using DHCP and DNS

The second discovery method is PDP Context activation. During PDP Context Activation signalling (see Figure 1-6):

1. UE indicates the request of P-CSCF IP address in PDP context request. The indication is forwarded to the GGSN by SGSN.
2. GGSN gets IP-CSCF IP address (internal configure, implement choice).
3. P-CSCF IP address in response message is forwarded to UE.

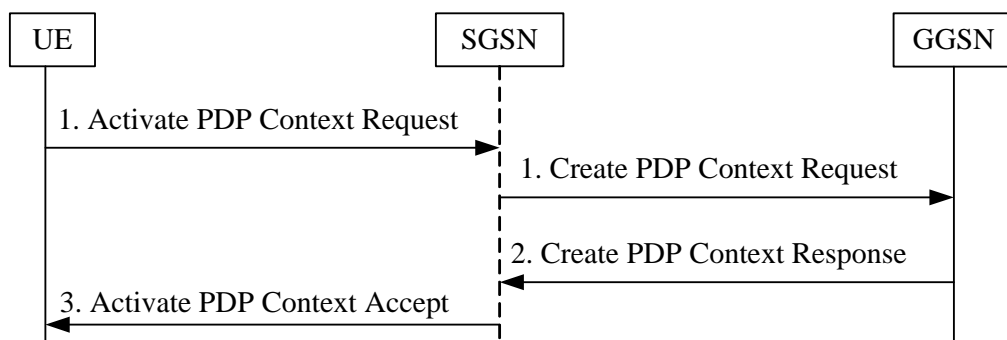


Figure 1-6: P-CSCF discovery using PDP context activation

1.8 WGSN

The WGSN project develops a solution for integrating 3G and WLAN services. The WLAN-based GPRS Support Node (WGSN) [9] located in the WLAN network enables the WLAN technique as an access technology to the 3G network. The WGSN integrates both SGSN and GGSN functionalities. That is, WGSN can communicate with Home Location Registrar (HLR) and external Packet Data Network (PDN). Figure 1-7 shows the architecture of the WGSN network. The WGSN utilizes the standard UMTS access control for users to access WLAN services. The WGSN reuses the existing UMTS Subscriber Identity Module (SIM) card and the subscriber data records in the HLR. Therefore, the WGSN customers do not need a separate WLAN access procedure. The WGSN also utilizes the existing UMTS authentication mechanism.

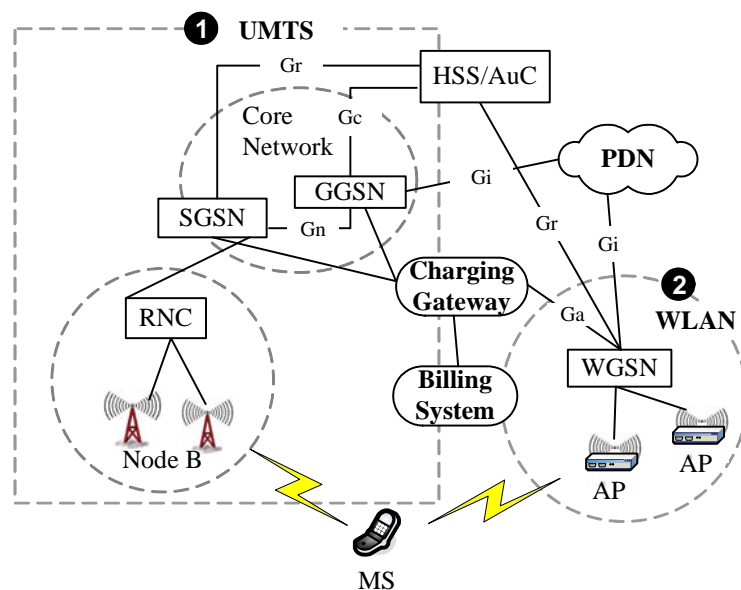


Figure 1-7: Architecture of the WGSN network

1.9 Motivation and Overview of this thesis

Recently, WLAN equipments and environments have been widely deployed and become more widespread. 3G-WLAN dual mode handsets or Personal Data Assistant (PDA) equipped with both WLAN network Interface Card and 3G module are also becoming attractive to the customers. Users can choose the access network based on bandwidth requirements, cost, and network availability.

We design a WLAN-based CSCF (W-CSCF) node in the IMS network for WLAN users in a WGSN network to access the IMS services. When mobile station (MS) roams to a WGSN network, it performs GPRS attach procedure which triggers UMTS authentication through the WGSN to the HSS. Therefore, MS can access the IMS network through W-CSCF. In Chapter 2, we present the architecture of W-CSCF in detail and show the interworking of the W-CSCF and the Application Server (AS). Chapter 3 describes the One-Pass Authentication mechanism for the W-CSCF and explains the advantages of this procedure. In chapter 4, we measure the performance of W-CSCF. Finally, we conclude this thesis in Chapter 5.

Chapter 2 WLAN-based CSCF

2.1 Overview

Universal Mobile Telecommunication System (UMTS) proposed by 3GPP is a 3G mobile telecommunication technology evolved from GPRS. UMTS supports voice and multimedia services through the Packet Switched Core Network based on the IP technology. The IMS network (as described in section 1.1) defined by 3GPP is to support multimedia services such as voice telephony, multimedia messaging services, video mail, real-time interactive games, and multimedia conferences. In IMS network, the multimedia services are provided through P-CSCF, I-CSCF and S-CSCF (as described in section 1.3, 1.4 and 1.5).

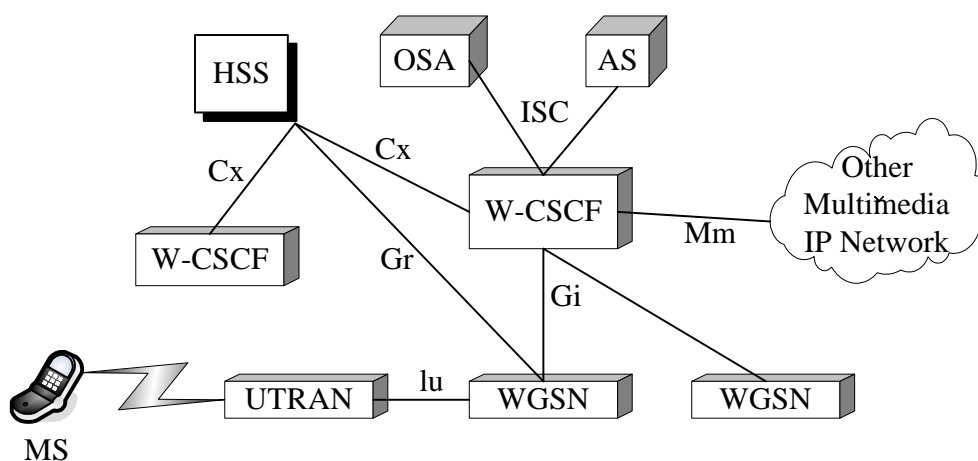


Figure 2-1: Architecture of the WGSN with the W-CSCF network

Now, we will illustrate the WLAN-based CSCF (W-CSCF) node in the IMS network to support WLAN users in a WGSN network to access IMS services. Figure 2-1 shows the system architecture. Users in WLAN network first connect to the WGSN node (like an access point) so that they can easily access the IMS services provided by the W-CSCF in the home domain. The WGSN behaves like as a P-CSCF in the traditional IMS network. The W-CSCF combines the functionalities of both I-CSCF and S-CSCF and is responsible for call control and service control. Furthermore, W-CSCF must also deal with the security issue, so we will propose an authentication mechanism in Chapter 3 to satisfy the security feature.

2.2 Architecture of W-CSCF

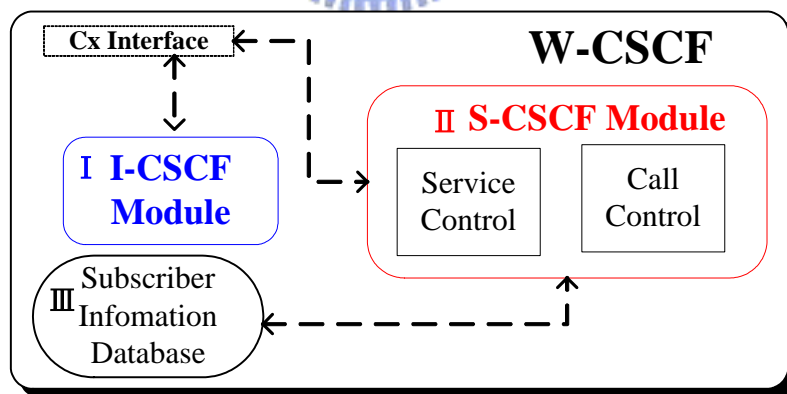


Figure 2-2: Architecture of W-CSCF

In this section, we introduce architecture and functionalities of the W-CSCF and give two scenarios of cooperation with the Application Server (AS) in section 2.3.1 and 2.3.2.

Figure 2-2 shows the architecture of the W-CSCF which has three modules: (1) S-CSCF module, (2) I-CSCF module and (3) Subscriber Information database. Obviously, the W-CSCF has capabilities of both I-CSCF and S-CSCF so that W-CSCF is responsible for call filtering (as a firewall), service control and call control. The W-CSCF communicates with the HSS via Cx Interface [10, 11] and communicates with the AS via ISC (IP multimedia Subsystem Service Control) Interface [5]. The Cx Interface is based on the Diameter protocol [12] and the ISC Interface is based on the SIP protocol.

2.2.1 I-CSCF module Feature

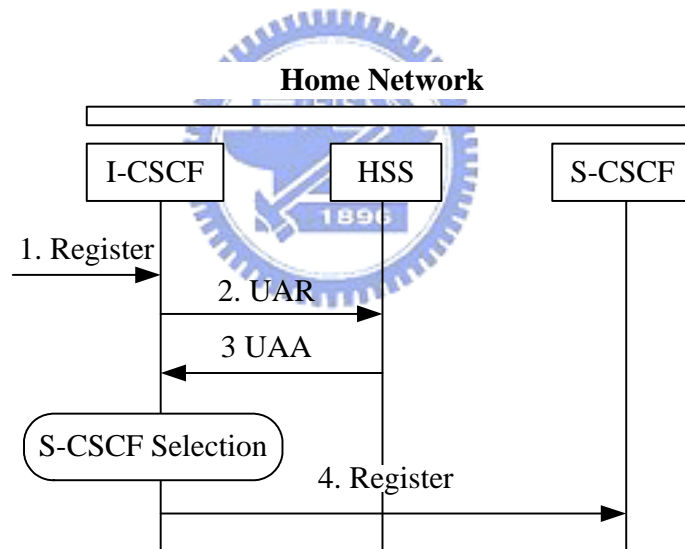
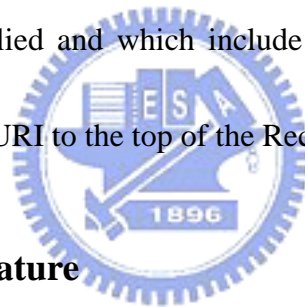


Figure 2-3: IMS Registration

In this section, we illustrate the I-CSCF module feature of the W-CSCF. In Figure 2-3, we can find that when I-CSCF receives a SIP Register request, the I-CSCF starts the registration status query procedure to the HSS via Cx Interface [3] to select an appropriate S-CSCF for MS. In the W-CSCF, the query status procedure can be omitted, because

W-CSCF itself can play the role of serving MS to provide multimedia services. In a word, Cx *User Authorization Request* (UAR) and *User Authorization Answer* (UAA) [11] in figure 2-3 can be skipped. Messages exchanged between I-CSCF and S-CSCF can be skipped so that traffic flow for registration can be reduced through the W-CSCF. The I-CSCF module communicates with the S-CSCF module through function call defined by ourselves. Upon receiving an incoming SIP Register request for network hiding has to be applied and which includes a Path header, the W-CSCF shall add the routable SIP URI of itself to the top of the Path header. Upon receiving an incoming initial request for which network hiding has to be applied and which include Record-Route header, the W-CSCF shall add its own routable SIP URI to the top of the Record-Route header.




2.2.2 S-CSCF module Feature

The W-CSCF performs the session control for subscribers accessing multimedia services within the IMS network. In essence, the W-CSCF is a SIP server which is responsible for interacting with the HSS for mobility and security purposes. After SIP Registration procedure is completed, a subscriber is assigned to a specific W-CSCF that resides in the home network of the subscriber and be responsible for all aspects of session control. The procedures executed by W-CSCF contain Mobile Originating (MO) procedure and Mobile Terminating (MT) procedure. In MO procedure, the W-CSCF receiving request will check the originating initial filer criteria with the highest priority in the downloaded

user profile (detailed described in section 2.2.3). If checking matches, the W-CSCF forwards the request to the specified AS and then check the next following filter criteria with lower priority. If no more of the initial filter criteria apply, the W-CSCF forwards the request downstream based on the route decision. In MT procedure, the W-CSCF also examines the terminating initial filter criteria of user profile by priority and forwards the request to the specified AS. If the Request-URI change when visiting an AS terminates the checking of user profile and route the request based on the changed value of the Request-URI.

2.2.3 Subscriber Information Database



Information in User Profile is the principal criterion to provide multimedia services to subscribers. A subscriber can establish the own profile on the database (i.e., the HSS) that will handle calls based on criteria (such as caller identity, location and time) set up in the profile. For example, an outgoing call would be forwarded to user's SIP phone on duty, to the cell phone on a business trip, and to voice mail when user does not want to be disturbed. We will introduce the feature of the Subscriber Information database of the W-CSCF.

Upon IMS Registration, the W-CSCF uses *Cx Server Assignment Request* (SAR) and *Server Assignment Answer* (SAA) messages [11] to communicate with the HSS and to download the user profile in W-CSCF local database. The user profile retrieved from the HSS contains the user subscription information and the W-CSCF can handle the service

control functions based on it, therefore subscribers can get added value services via the AS.

Information in the *Filter Criteria* (FC) [10] contains the relevant *Service Point Trigger* (SPT)

[10] for a particular application, address of the AS to be reached, priority number of the FC

and the default handling procedure to apply when W-CSCF can not reach the AS.

Table 2-1: Classification of Service Point Trigger

1.	SIP Method
2.	SIP Header
3.	Request URI
4.	Direction of the Request
5.	Session of Description

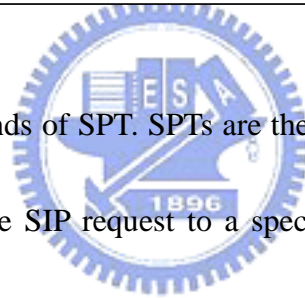


Table 2-1 lists the five kinds of SPT. SPTs are the points in the SIP signaling that may cause the W-CSCF to send the SIP request to a specific AS if SPT matched. Figure 2-4

shows the W-CSCF triggering architecture. First, the W-CSCF downloads the user profile after the IMS registration. When the W-CSCF receives a request, it executes the FC

handling procedure; if SPT matches, forwards the request to the specific AS.

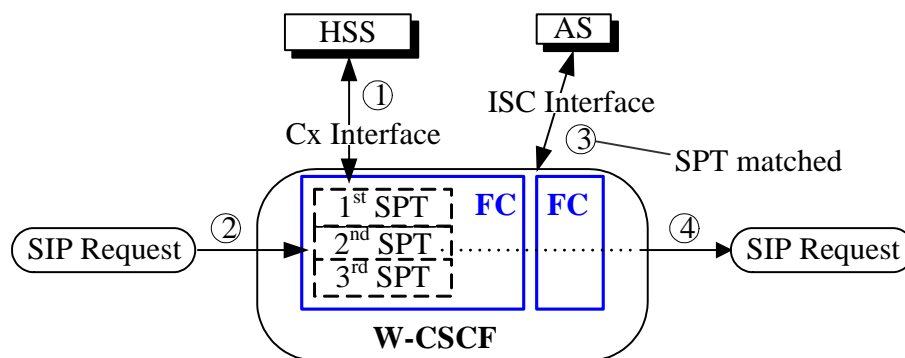


Figure 2-4: W-CSCF Triggering Architecture

In order to allow the W-CSCF to handle the different FCs in the right sequence, each FC has a unique priority number for the W-CSCF to check. Upon reception of SIP requests, the W-CSCF would handle these FCs based on the following steps:

Step 1: Make the list of FC by priority number in decreasing order. (lower priority number means higher priority)

Step 2: Parse the received request to find out all SPTs included in it.

Step 3: Check whether the SPTs in the FC with the highest priority are matched by the SPTs in the received request.

Step 3.1: If it does not match, check the FC with the next highest priority and repeat step 3.

Step 3.2: If it matches the W-CSCF shall forward the request via the ISC interface to the AS indicated in the current matched FC. The AS may modify the request and may send it back to the W-CSCF also via the ISC interface.

Step 4: If the request is received from the AS, repeat step 2, 3.

After the last FC in the list made in the step 1 has been checked, route the request based on the normal SIP routing behavior.

2.3 Application Server

In the IMS network, subscribers not only can use telephony services but also can

access multimedia services. Application Server (AS) plays the important role to support the IMS network to provide such attractive services. The ISC Interface can be used by the AS to control IP multimedia session via the W-CSCF. Those multimedia services can be provided by using combination of the five modes of AS operation [5]. Table 2-2 shows those five modes of AS.

Table 2-2: Operation modes of Application Server

	Operation Mode
1	Terminating UA
2	Originating UA
3	SIP Proxy
4	Third Party Call Control
5	No Involved

In Terminating UA mode, the W-CSCF is like a proxy, forwards the requests to the AS.

The AS may be a Redirect Server to provide redirect services. In Originating UA mode, the AS acts as a UA generating a SIP request and sending to the W-CSCF. In SIP Proxy mode, the AS can add, remove and modify the header content in the receiving request. But SIP dialog is still the same after request is sent back to the W-CSCF. In Third Party Call Control mode, the AS receives the incoming SIP request then generates a new SIP request for different SIP dialog and sends to the W-CSCF. In this mode, the AS behaves as a Back-to-Back User Agent (B2BUA) [4] for the multiple SIP dialogs. In fifth mode, the AS is never involved in the SIP session signalling, the incoming SIP request is proxied by the

W-CSCF to the destination.

We have implemented two operation modes of the AS, one is Terminating UA mode and the other is Third Party Call control mode. By the way, we can demonstrate the functionalities of the W-CSCF can work correctly with the AS. We provide two scenarios in section 2.3.1 and section 2.3.2 to show the cooperation of the W-CSCF with the AS.

2.3.1 AS acts as SIP Proxy mode

We have illustrated the AS with five operation modes and we shall give an example to show the AS with *SIP Proxy mode* interworking with the W-CSCF. Figure 2-3 shows the architecture of the AS providing *Call Filtering* service to the user (i.e., Bob). The AS in Figure 2-5 acts as *SIP Proxy mode* and provides subscribers Call Filtering service so that a Bob can establish his calling list. Callers in this list can have permission to initialize a call with him or does not have permission to communicate with him. Bob has already subscribed the Call Filtering service to this AS and he does not allow Alice to communicate with him maybe he does not want Alice to bother him.

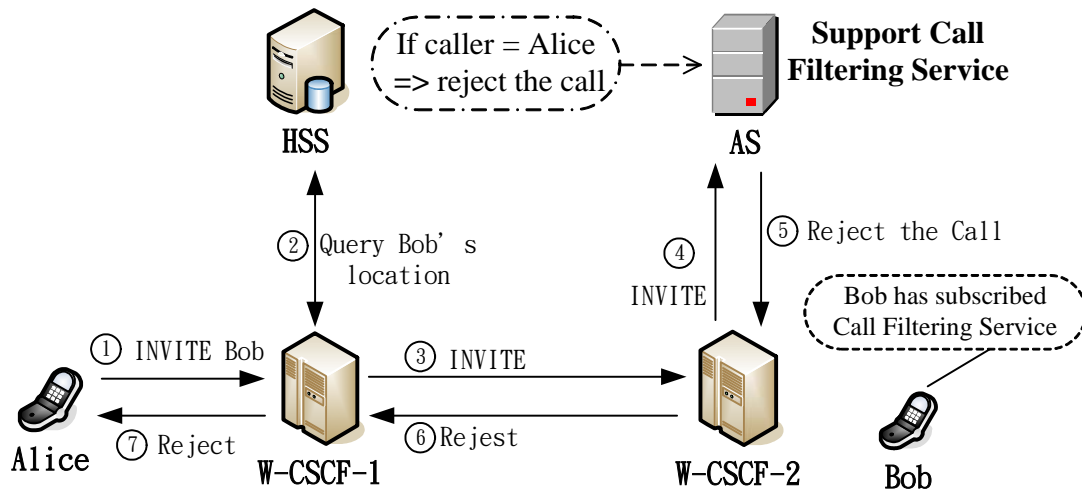


Figure 2-5: Call Filtering Service architecture

Figure 2-6 shows the message flow of the AS supporting Call Filtering Service. We assume that MS-1 and MS-2 have executed IMS Registration with corresponding W-CSCF-1 and W-CSCF-2 and MS-2 subscribed the Call filtering Service to the AS. We give a detailed description in the following steps:

Step 1: MS-1 determines the complete set of codecs that it is capable of supporting for this session. It builds a SDP containing media type, port number, transport protocol, and media format. After all preparation is done, MS-1 sends SIP INVITE to the W-CSCF-1.

Step 2: Upon reception of the INVITE message, the W-CSCF sends *Cx Location Information Request (LIR)* [10] to the HSS to query which the W-CSCF serves MS-2.

Step 3: The HSS send *Cx Location Information Answer (LIA)* to the W-CSCF-1. The LIA contains the address of the W-CSCF-2 which is serving the MS-2.

Step 4: Receiving the INVITE message, the W-CSCF-2 will check MS-2's user profile

which has downloaded upon IMS Registration. Based on the procedure for FC examination described in section 2.2.3, the W-CSCF-2 finds that the request triggers the service point in MS-2's user profile.

Step 5: The W-CSCF-2 sends the INVITE message to the AS specified in the triggered FC. The AS bases on the filtering rules to check whether the MS-1 can setup a call with the MS-2.

Step 6: The AS finds the MS-2 does not allow MS-1 to setup a call with him, so rejects the request and sends the *SIP 403 Forbidden* response to the W-CSCF-2.

Step 7: The W-CSCF-2 forwards the response to the W-CSCF-1.

Step 8: The W-CSCF-1 sends the response to the MS-1.

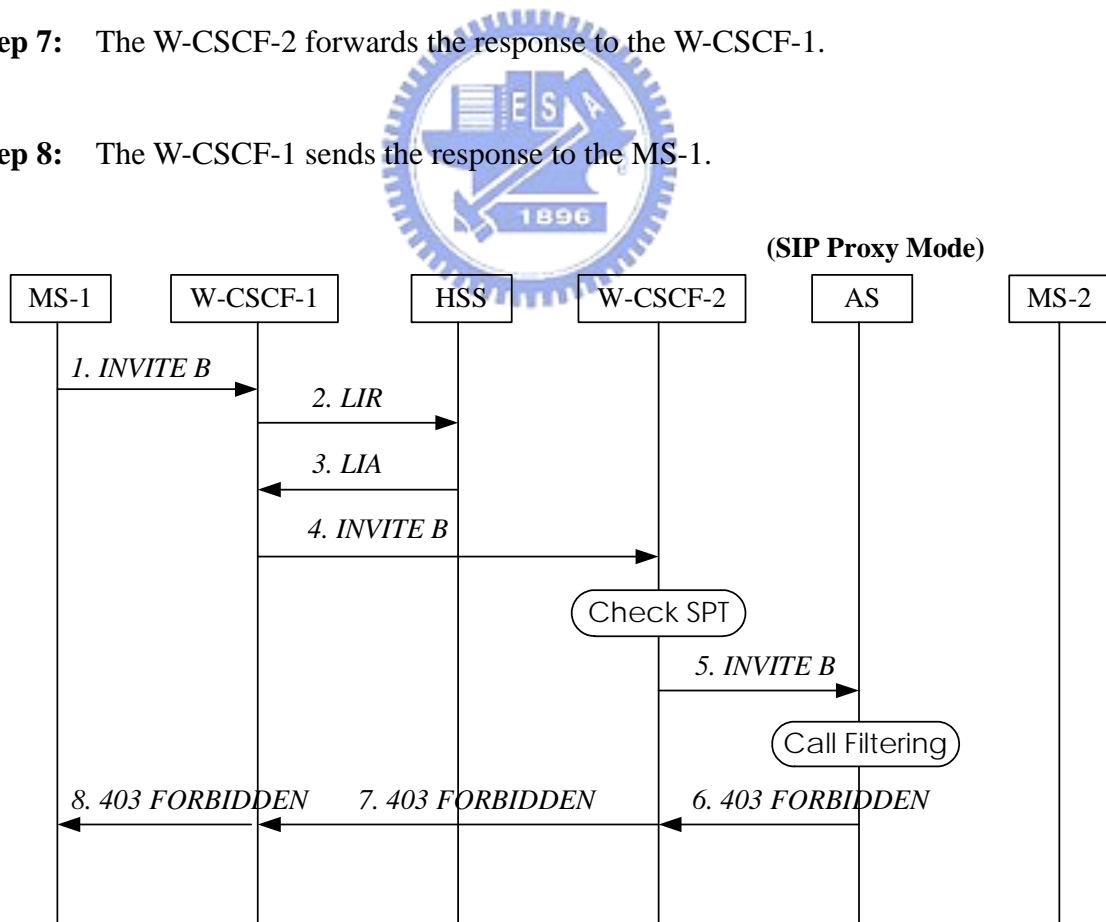


Figure 2-6: Message flow of the AS supporting Call Filtering Service

2.3.2 AS acts as B2BUA mode

In this section, we will give an example to show the B2BUA operation mode of the AS. Figure 2-7 shows the AS supporting the *Call Forwarding Service* with B2BUA operation mode. Alice wants to call Jay but Jay subscribes the Call Forwarding Service to the AS so that Alice finally makes a call with Bob. In this example, the AS behaves as a B2BUA mode such that the AS received the request and processes it as a User Agent Server (UAS). To correctly handle this request, the AS acts as a User Agent Client (UAC) and generates a new request to W-CSCF-2. The AS will maintains dialog state and must participate in all request sent on the dialogs it has established.

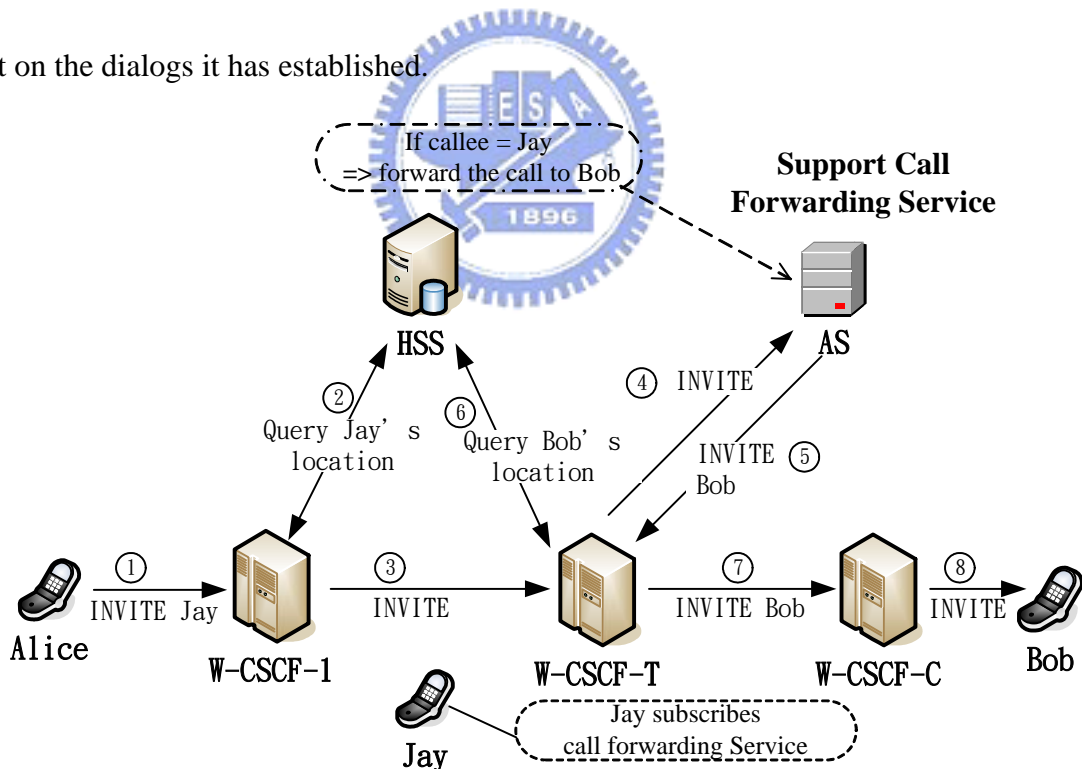


Figure 2-7: Call Forwarding Service architecture

Figure 2-8 shows the message flow of the AS supporting Call Forwarding Service. We assume that MS-1, MS-C and MS-T have executed IMS Registration with corresponding

W-CSCF-1, W-CSCF-C and W-CSCF-T and MS-T has subscribed the Call Forwarding Service to the AS. If anyone makes a call to MS-T then the call will be forwarded to the MS-C (current location of the user). We give a detailed description in the following steps:

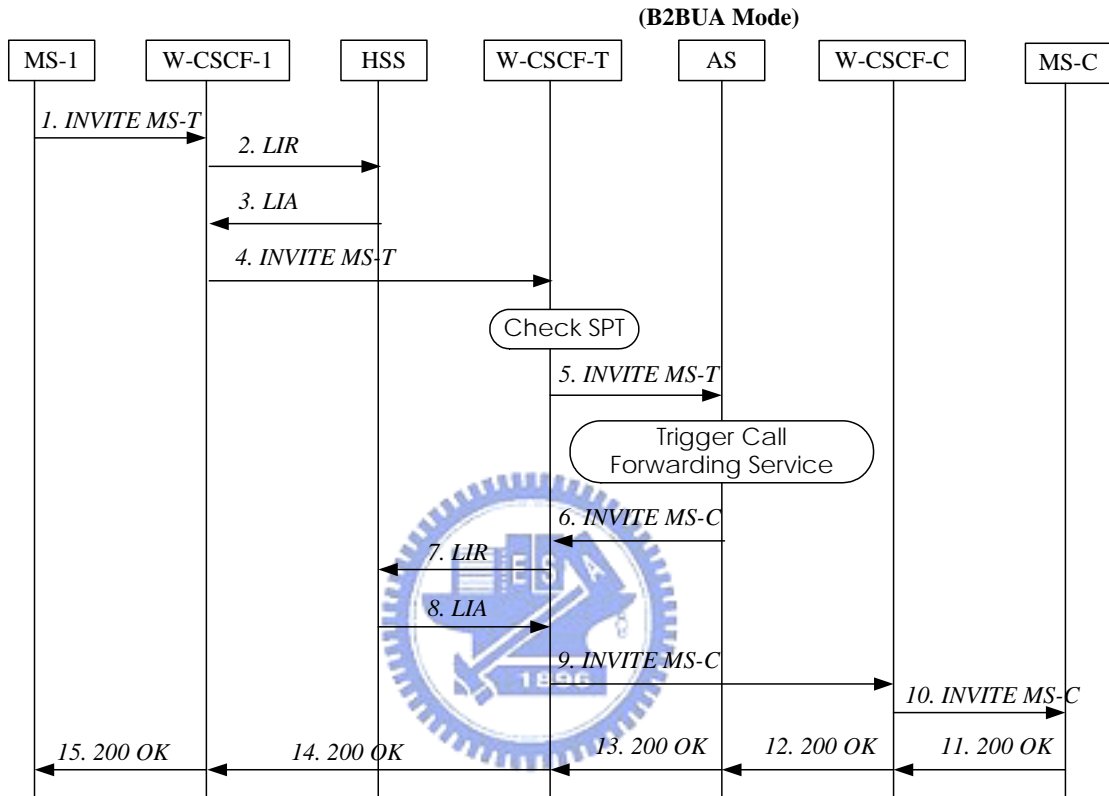


Figure 2-8: Message flow of the AS supporting Call Forwarding Service

Step 1: MS-1 determines the complete set of codecs that it is capable of supporting for this session. It builds a SDP containing media type, port number, transport protocol, and media format. After all preparation is done, MS-1 sends SIP INVITE to the W-CSCF-1.

Step 2: Upon reception of the INVITE message, the W-CSCF-1 sends *Cx LIR* to the HSS to query which the W-CSCF serves MS-2 (i.e. W-CSCF-T).

Step 3: The HSS send *Cx LIA* message to the W-CSCF-1. The LIA contains the address of the W-CSCF-T which is serving the MS-2

Step 4: Receiving the INVITE message, the W-CSCF-T will do FC check described in section 2.2.3 and the W-CSCF-T finds the request triggers the service point in the user profile.

Step 5: The W-CSCF-T sends the INVITE message to the AS specified in the triggered FC. The AS bases on the call forwarding rules to check to where the call is forwarded.

Step 6: After the AS checking, the AS generates a new INVITE message to make a call to MS-C where the callee currently located.

Step 7: Upon reception of the INVITE message, the W-CSCF-T sends *Cx LIR* to the HSS to query which the W-CSCF serves MS-C (i.e., W-CSCF-C).

Step 8: The HSS send *Cx LIA* message to the W-CSCF-T. The LIA contains the address of the W-CSCF-C which is serving the MS-C

Step 9: Sends the INVITE message to the W-CSCF-C which serves the MS-C now.

Step 10: Sends the INVITE message to MS-C.

Step 11-15: The *200 OK* response is routed in the reverse path of INVITE request.

2.4 Summary

We illustrate the architecture and functionalities of the W-CSCF and give two scenarios of cooperation with the AS. The W-CSCF is the first contact point for WLAN users in a WGSN network to access the IMS network. The W-CSCF combines the functionalities of both I-CSCF and the S-CSCF and can reduce messages exchange between the I-CSCF and the S-CSCF. It also can skip Cx UAR/UAA messages when doing IMS registration. The W-CSCF downloads user's subscription information and service profiles from the HSS. The W-CSCF uses the user profile to control the session flow and decides whether SIP messages shall be forwarded to the specific AS to provide multimedia services.



Chapter 3 Authentication Procedure

3.1 Overview

Network security and authentication have always been the essential issue for all kinds of telecommunication networks to assure network reliability and stability. The authentication function should include both *user authentication feature* and *network authentication feature*. User authentication is a process through which a serving network entity, such as SGSN or W-CSCF, should be able to verify the identity of the user. The network authentication is a process through which a user is able to verify whether the serving network is authorized by the user to provide services. In this chapter, we propose a *One-Pass Authentication* mechanism [13] which is performed at the GPRS level, but can authenticate an IMS user without explicitly performing the IMS-level authentication. In our proposed method, we need to modify a software module of the WGSN that implements a *SIP Application Level Gateway* (SIP ALG) [14]. A SIP ALG can add, remove and modify the format of incoming SIP messages. We first describe the 3GPP *Two-Pass Authentication* procedure and its message flow. Then we would simplify the Two-Pass procedure steps to a One-Pass Authentication procedure. Last, we will give a brief comparison of the One-Pass and the 3GPP Two-Pass Authentication procedures.

3.2 Two-Pass Authentication

When an MS wants to access the IMS services, it must perform the authentication procedures at both the GPRS and the IMS network in advance. Without doing IMS authentication, a mobile user passes the GPRS authentication can easily fake being another IMS user to illegally access IMS services. When an MS invokes the WGSN network access, like a GPRS handset to send an attach request to the SGSN, the MS also sends an attach request to the WGSN. This message will trigger the GPRS authentication [2]. The GPRS authentication procedure in UMTS achieves mutual authentication between an MS and the network. The authenticating parties are the HSS in the user's home domain network and the Universal Subscriber Identity Module (USIM) in the MS. The GPRS authentication consists of two procedures that will be illustrated in section 3.2.1 [8].

3.2.1 Composition of the GPRS authentication

The GPRS authentication procedure has two major functions to achieve the mutual authentication. One is *Distribution of Authentication Vector (AV)* and the other is *Authentication and Key Agreement*. The purpose of this first function is to provide a SGSN with an array of fresh authentication vectors from HSS to perform the GPRS authentication procedure. The mechanism is illustrated in Figure 3-1.

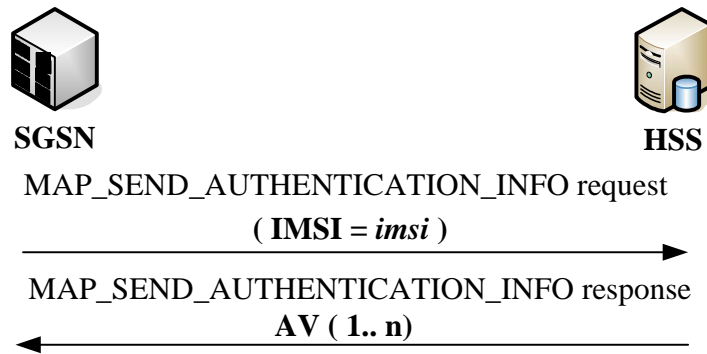


Figure 3-1: Distribution of authentication data from HSS to SGSN

The behavior of the WGSN node is like as an SGSN in Figure 3-1; it retrieves the AVs from the HSS and is responsible to authenticate the MS. The WGSN invokes this procedure by sending a MAP_SEND_AUTHENTICATION_INFO request message to the HSS. The request shall include the parameter *International Mobile Subscriber Identity* (IMSI) of the MS. Upon receiving the request from the WGSN, the HSS may have computed the needed AVs in advance or may compute them on demand. The HSS sends a MAP_SEND_AUTHENTICATION_INFO response message back to the WGSN that contains an ordered array of AV (1...n). The AVs are ordered based on a sequence number.

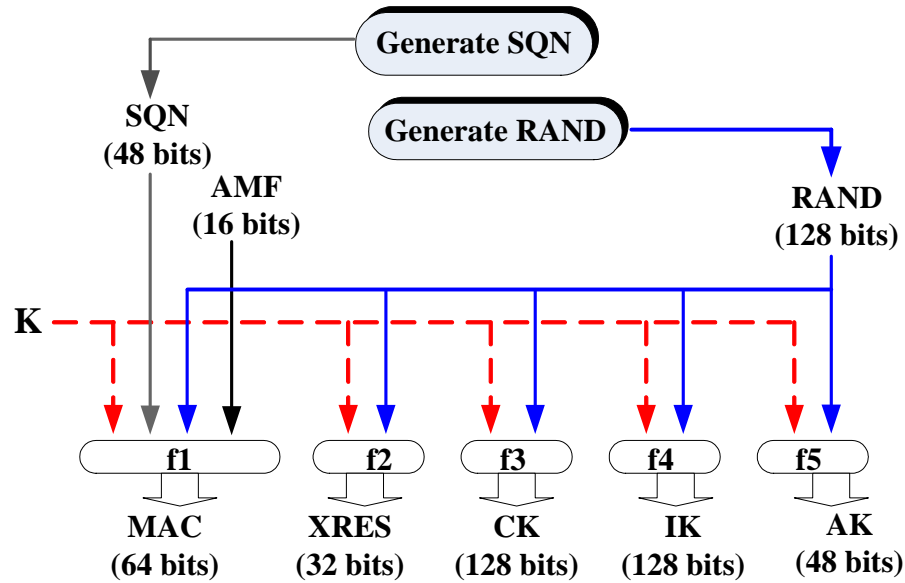


Figure 3-2: Generation of Authentication Vector

Figure 3-2 shows the generation of an authentication vector AV in the HSS. In Figure 3-2, f1 and f2 are message authentication functions and f3, f4 and f5 are key generation functions. The SQN exposes the identity and location of the user, the AK (Anonymity Key) may be used to conceal it. Note that each AV consists of a random number *RAND*, an expected response *XRES*, a cipher key *CK*, an integrity key *IK* and an authentication token *AUTN*. The *AUTN* consists of a sequence number *SQN*, an anonymity key *AK*, an authentication and key management field *AMF* and message authentication code *MAC*. The detail description about generation of AV can be found in [8].

$$\begin{aligned}
 AUTN &:= SQN \oplus AK \parallel AMF \parallel MAC \\
 AV &:= RAND \parallel XRES \parallel CK \parallel IK \parallel AUTN
 \end{aligned}$$

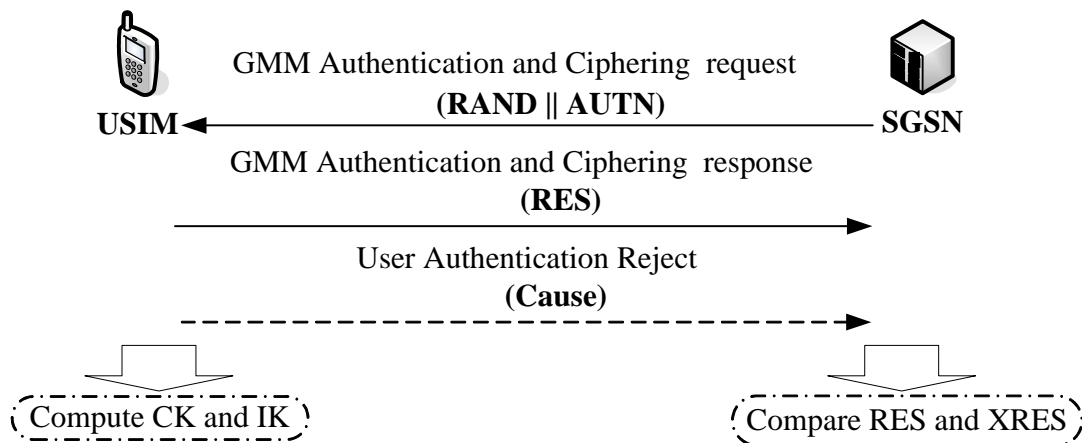


Figure 3-3: Authentication and Key Agreement

The purpose of second function is to authenticate the user and establish a new pair of cipher and integrity keys between the SGSN and the USIM. The mechanism is illustrated in Figure 3-3. During the authentication, the USIM verifies the freshness of the authentication vector that is used. This procedure achieves mutual authentication between an MS and the network by showing knowledge of a pre-shared secret key K that is only available in the USIM of the MS and the HSS. The key is never exposed in the network. The MS uses the AUTN to authenticate the network and the SGSN use $RES/XRES$ pair to authenticate the MS (where the RES is generated by the MS). The SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the SGSN database. Selection of AV is based on first-in / first-out basis (FIFO). The MS also computes two keys CK and IK using the received $RAND$ and the pre-shared key K stored in the USIM. On the network side, the SGSN passes the CK and IK to the UTRAN in the authentication procedure. During data transmission, CK and IK are used for ciphering and

integrity between the MS and the UTRAN. The WGSN node also executes the same procedures processed by the SGSN in Figure 3-3 to achieve the mutual authentication.

Figure 3-4 shows the user authentication function in the USIM. Upon receipt of the authentication request which contains RAND and AUTN, the USIM first computes the AK by function f5 and retrieves the sequence number SQN. Afterward, the USIM computes XMAC and compares with MAC to authenticate the network. The detailed description about user authentication function in the USIM can be found in [8].

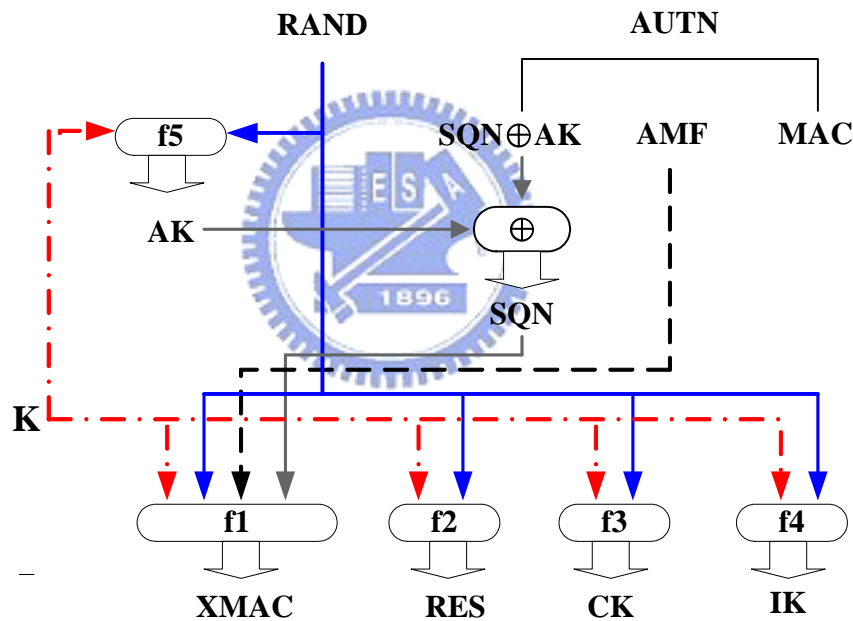


Figure 3-4: User authentication function in the USIM

3.2.2 Two-Pass Authentication procedure Message Flow

The message flows of the GPRS and IMS authentication procedures are illustrated in Figures 3-5 and Figure 3-6, respectively. We can clearly observe that many steps in Figure 3-5 and Figure 3-6 are identical. Between the SGSN and the HSS, the GPRS authentication

procedure is implemented by *Signaling System Number 7 (SS7) Mobile Application Part (MAP)* [1], which consists of the following steps:

Step 1: Consider an MS with the IMSI value *imsi*. To access the GPRS services, the MS sends a *GMM Attach Request* (with the parameter $IMSI = imsi$) to the SGSN.

Step 2: If the WGSN has the AVs of the MS, then Steps D.2 and D.3 are skipped.

Otherwise, the WGSN must obtain the AVs from the HSS. That is, the SGSN invokes the AV distribution procedure (illustrated in Figure 3.2.1) by sending a *MAP_SEND_AUTHENTICATION_INFO* Request message to the HSS (with the parameter $IMSI = imsi$).

Step 3: The HSS uses parameter $IMSI = imsi$ to retrieve the record of the MS, and generates an ordered array of AVs (based on the pre-shared secret key **K** in the MS record). The generated AVs are sent to the SGSN through *MAP_SEND_AUTHENTICATION_INFO* Response message.

Step 4: The SGSN selects the next unused AV in the ordered AV array and sends the parameters *RAND* and *AUTN* (form the selected AV) to the MS through a *GMM Authentication and Ciphering Request* message.

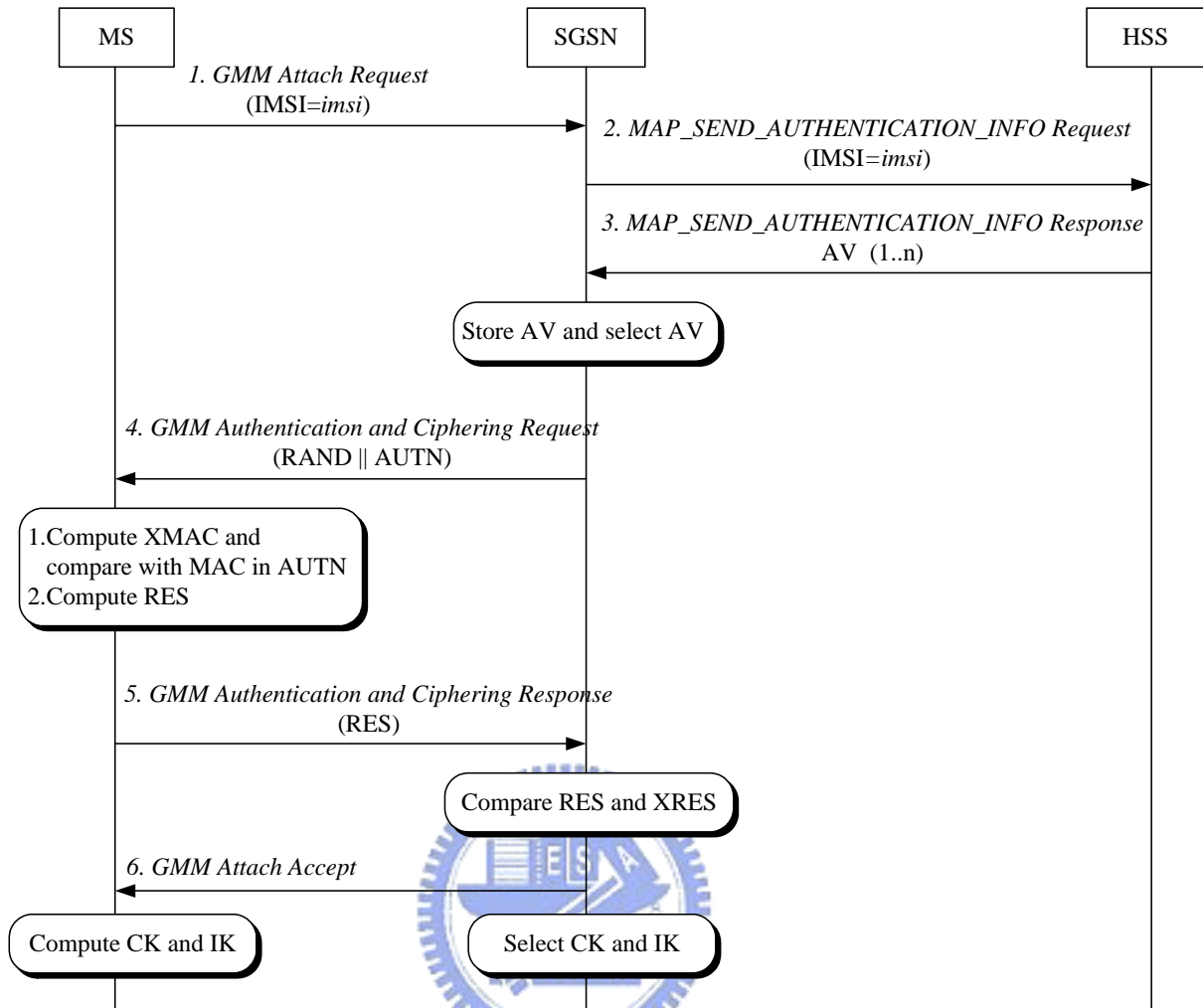


Figure 3-5: Message Flow for 3GPP GPRS Authentication

Step 5: The MS computes XMAC and compare the MAC in *AUTN*. If equal, the MS produces a response *RES* that is sent back to the SGSN through a GMM Authentication and Ciphering Response message. The SGSN compares the received *RES* with the *XRES*. If they match, then the authentication and key agreement exchange is successfully completed.

Step 6: The SGSN sends a GMM Attach Accept message to the MS, and the attach procedure is completed.

After GPRS authentication, the MS performs PDP context activation to obtain access to the GPRS network. The PDP context specifies the application-layer packet data protocol and the routing information used for the communication session. After PDP context activation, the MS can retrieve the IMS services after performing the registration procedure illustrated in Figure 3-6. This procedure is implemented by SIP and Diameter protocols and consists of the following steps:

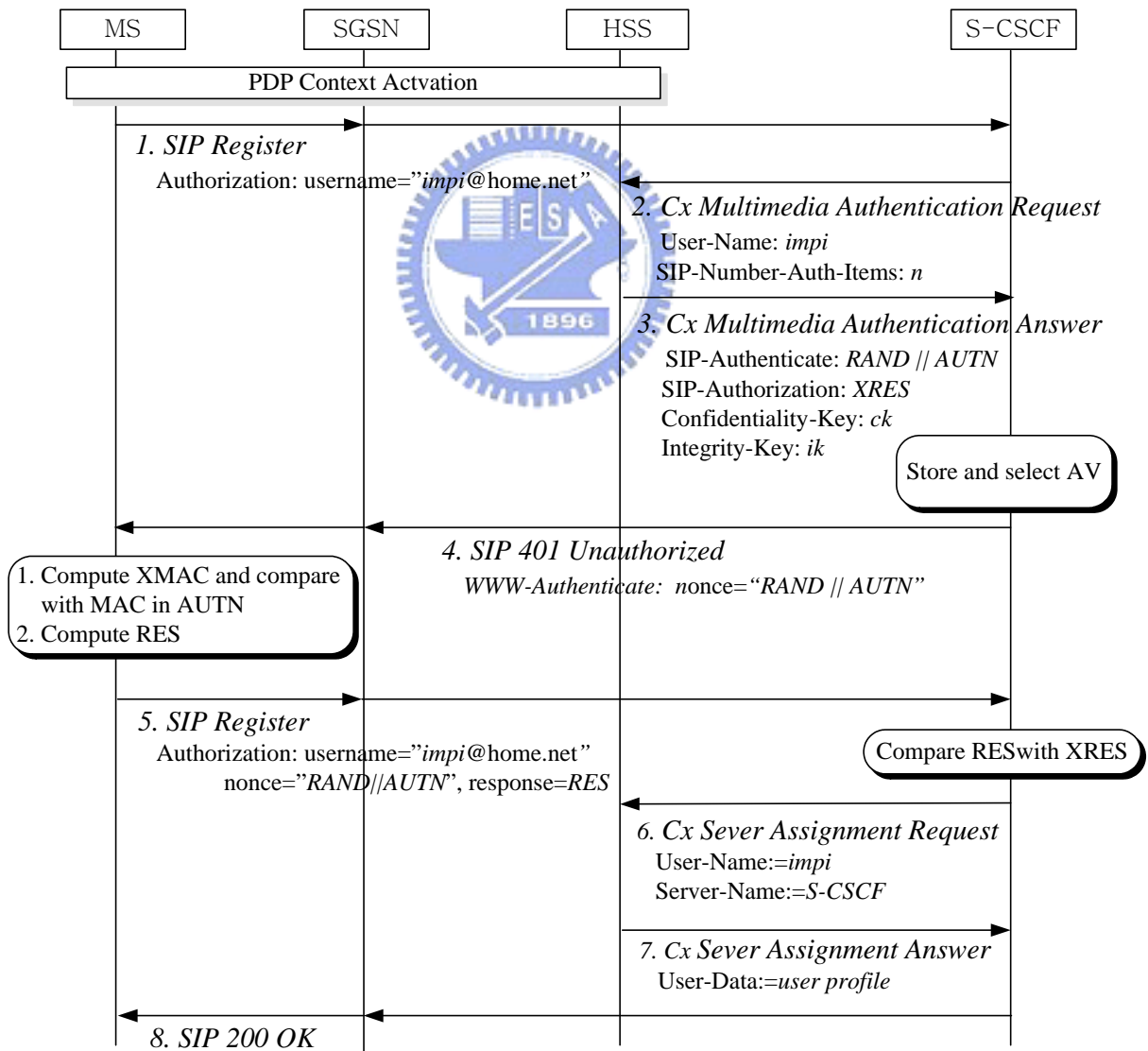


Figure 3-6: Message Flow for 3GPP IMS Authentication

Step 1: The MS sends a *SIP Register* message with the *IP Multimedia Private Identity* (IMPI) = *impi* in the *Authorization Header* to S-CSCF through the SGSN.

Step 2: Assume that the S-CSCF does not have the AVs for the MS. The S-CSCF invokes the authentication vector distribution procedure by sending a *Cx Multimedia Authentication Request* (MAR) [10] with IMPI parameter of the MS to the HSS. If the S-CSCF already has the AV array, this step and next step are skipped.

Step 3: The HSS uses parameter IMPI = *impi* to retrieve the record of the MS, and generate an ordered array of AVs. The HSS sends the array to the S-CSCF through a *Cx Multimedia Authentication Answer* (MAA) [10].

Step 4: The S-CSCF selects the next unused authentication vector from the ordered AV array and sends the parameter *RAND* and *AUTN* (form the selected authentication vector) in the *WWW-Authenticate Header* to the MS through a *401 Unauthorized* response message.

Step 5: The MS computes XMAC and compare with MAC in *AUTN* to authenticate the network. If equal; it produces a response *RES* otherwise, it rejects the request. The MS sends this response back to the S-CSCF through a *SIP Register* message in the *Authorization Header*. The S-CSCF compares the received *RES* with the *XRES*. If they are equal, then the authentication and key agreement exchange is successfully completed.

Step 6: The S-CSCF sends a *Cx Serve Assignment Request* (SAR) to the HSS.

Step 7: Upon receipt of SAR from the S-CSCF, the HSS stores the S-CSCF name and replies a *Cx Server Assignment Answer* (SAA) to the S-CSCF. The user profile of the MS is also carried in the SAA message.

Step 8: The S-CSCF sends a *200 OK* response to the MS through the SGSN, and the IMS registration procedure is completed.

Although GPRS authentication is implemented by SS7 MAP and IMS authentication is implemented by SIP and Diameter (Cx Interface), many steps of these two authentication procedures are duplicated (see Table 3-1). If WALN users want access the IMS network via WGSN, they also perform the above GPRS and IMS authentication (in Figure 3-5 and 3-6). Unfortunately, these redundant steps are required. That is, after GPRS authentication, it is necessary to authenticate the MS again at the IMS level. Without IMS authentication, an IMS user may pretend to be another IMS user.

Table 3-1: Identical Steps in GPRS and IMS Authentications

Step	GPRS authentication (SS7 MAP)	IMS authentication (SIP/Cx)
	2: MAP_SEND_AUTHENTICATION_INFO	2: Multimedia Authentication Request
	3: MAP_SEND_AUTHENTICATION_INFO Parameter: AV[1..n]	3: Multimedia Authentication Answer Parameter: AV[1..n]
	4: User Authentication Request Parameter: RAND AUTN	4: 401 Unauthorized Parameter: RAND AUTH
	5: User Authentication Response Parameter: RES	5: Register Parameter: RES
	6: GMM Attach Accept	8: 200 OK

Consider the example in Figure 3-7. There are two MSs. MS-A has the IMSI value $imsi-A$ and the IMPI value $impi-A$. MS-B has the IMSI value $imsi-B$ and the IMPI value $impi-B$. Suppose that MS-B is a legal GPRS user and has passed the GPRS authentication (by using $imsi-B$) to obtain GPRS network access. If no IMS authentication is required, MS-B may perform IMS registration by sending the W-CSCF a *SIP Register* request that includes the MS-A's IMPI value $impi-A$ as a parameter. The W-CSCF will consider this IMS registration as a legal action activated by MS-A. Therefore, MS-B can illegally access the IMS services of MS-A. The above example shows that IMS-level authentication is required to prevent illegal access to the IMS services. In section 3.3, we describe a *One-Pass Authentication* procedure for both GPRS and IMS authentications. Our approach reduces the number of times for accessing the HSS and reduces duplicate steps in Two-Pass Authentication procedure.

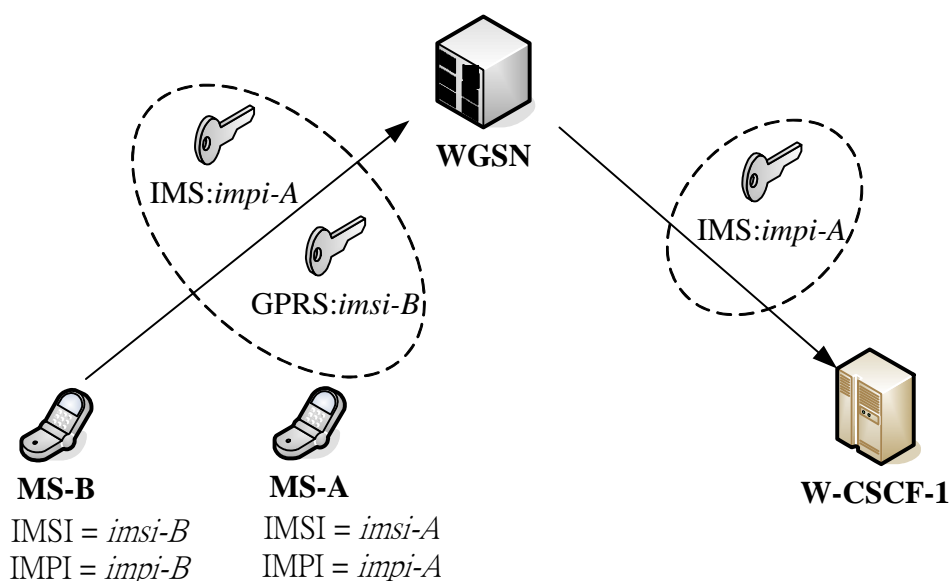


Figure 3-7: Illegal IMS Registration

3.3 One-Pass Authentication

In Table 3-1, we can observe many steps both in the GPRS authentication and the IMS authentication. There are too many times to access the HSS. In other words, Two-Pass Authentication proposed in [14] is duplicate and inefficient for WLAN users to access the IMS network. So we propose a mechanism called *One-Pass Authentication* procedure to authenticate a user more efficient and also guarantee security issue.

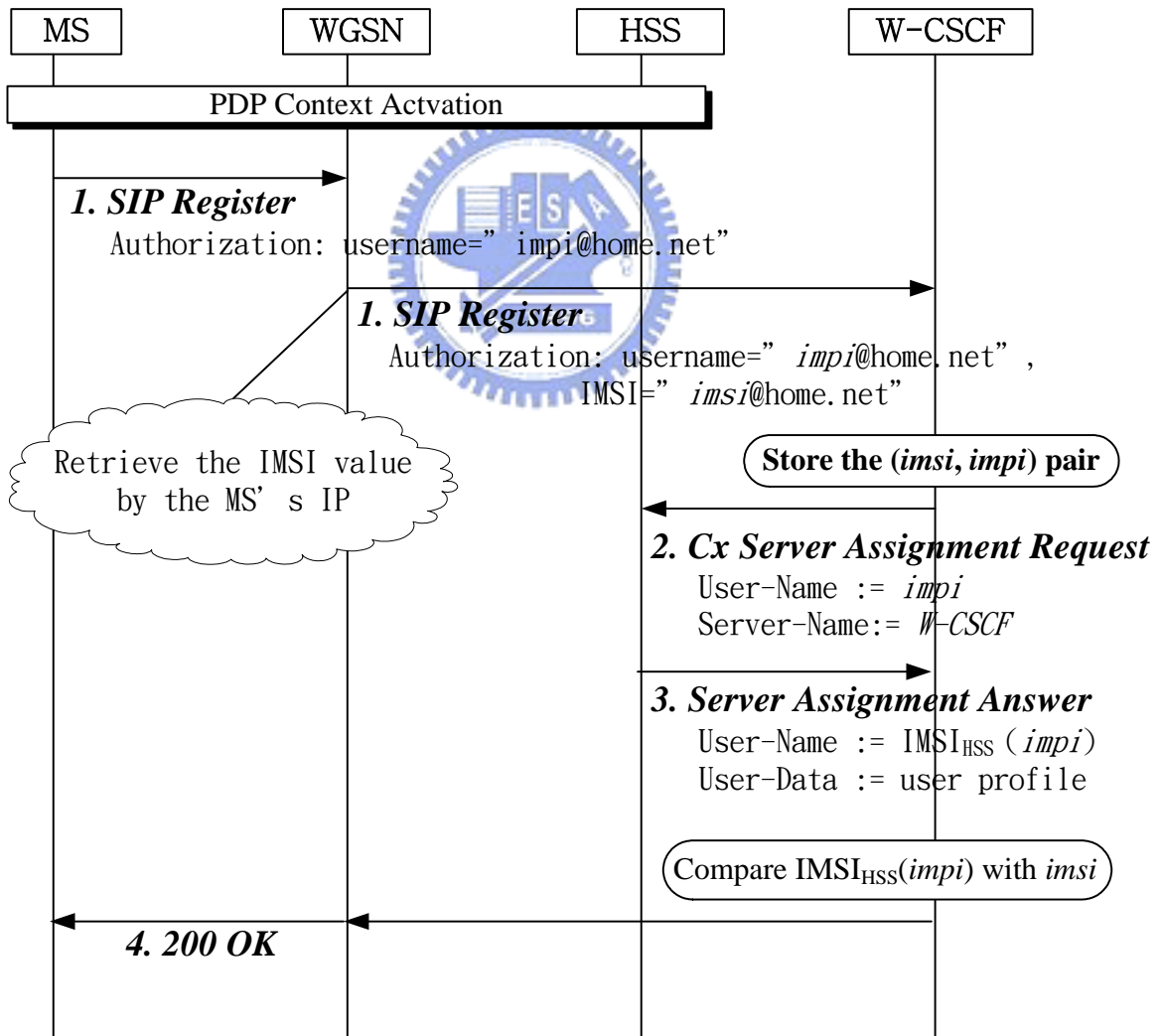
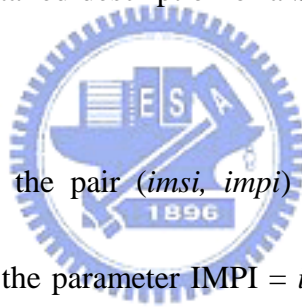


Figure 3-8: One-Pass Authentication procedure

After WLAN user performs GPRS authentication (Steps 1 – 6 in Figure 3-5) through WGSN, the MS can perform PDP context activation to obtain GPRS access. Then the MS registers to the IMS network through **Steps 1 – 5** in Figure 3-8:

Step 1: The MS sends a *SIP Register* message to the WGSN with the parameter $IMPI = impi$ in the *Authorization Header*. Note that after PDP context activation, the WGSN can identify the IMSI of MS that transmits the GPRS packets [2]. The SIP ALG in the WGSN adds the IMSI value (i.e. *imsi*) of the MS in the *Authorization Header* and sends it to the W-CSCF. The detailed description of a SIP ALG implementation can be found in [15].



Step 2: The W-CSCF stores the pair $(imsi, impi)$ in the MS record, and sends a *SAR* message to the HSS with the parameter $IMPI = impi$. We note that if the W-CSCF has stored the $(imsi, impi)$ pair before, then **Steps 2** and **3** are skipped.

Step 3: The HSS uses the received $IMPI$ value *impi* as an index to retrieve the *IMSI value* and the *user profile* of the MS. We denote $IMSI_{HSS}(impi)$ as the *IMSI value* retrieved from the HSS. The HSS stores the W-CSCF name and sends a *SAA* (contains the parameters $IMSI_{HSS}(impi)$ and user profile) to the W-CSCF. We modify the *SAA* message so that it can carry the parameters $IMSI_{HSS}(impi)$.

Step 4: The W-CSCF checks whether the value *imsi* and $IMSI_{HSS}(impi)$ are the same. If so, the W-CSCF sends a *200 OK* response to the WGSN and the authentication is considered

successful. If $IMSI_{HSS} (impi) \neq imsi$, then it implies that the registration is illegal (i.e., the scenario illustrated in Figure 3-7 occurred). Suppose that $IMSI_{HSS} (impi) = imsi$. The WGSN sends a *200 OK* response to the MS, and the IMS registration procedure is successfully completed.

Step 5: If it triggers the FC (as described in section 2.2.3), sends the SIP Register message to the specified AS.

3.4 Comparison

Table 3-2 Comparison of One-Pass and Two-Pass Authentication Procedure

One-Pass Procedure	Two-Pass Procedure
1: Register Parameters: <i>impi</i> and <i>imsi</i>	1: Register Parameter: <i>impi</i>
-	2: MAR Parameter: <i>impi</i>
-	3: MAA Parameter: <i>AV[1..n]</i>
-	4: 401 Unauthorized Parameter: <i>RAND AUTH</i>
-	5: Register Parameter: <i>RES</i>
2: <i>SAR</i>	6: <i>SAR</i>
3: <i>SAA</i>	7: <i>SAA</i>
4: 200 OK	8: 200 OK

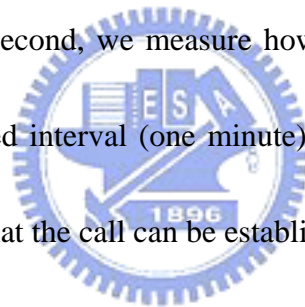
Table 3-2 shows the comparison of the One-Pass and the Two-Pass Authentication procedures for WLAN users doing Registration at IMS level. We can clearly find One-Pass Authentication can save two Cx messages (MAR and MAA) and two SIP messages (Register

Request and 401 Unauthorized Response). In addition, it reduces the number of times to access the HSS. Another significant advantage of the One-Pass Authentication procedure is that it consumes much less AVs than the Two-Pass Authentication procedure. Although Cx message SAR/ SAA appear both in One-Path and Two-Path Authentication procedure, they are not all the same. The Cx SAR message for One-Pass Authentication procedure must carry the parameter IMPI (*impi*) of the MS. The Cx SAA message for One-Pass Authentication procedure must carry the parameter IMSI retrieved from the HSS according to parameter $IMPI = impi$. To sum up, One-Pass Authentication procedure only performs the GPRS authentication. At the IMS registration, the One-Pass Authentication procedure performs several simple operations and one comparison to verify whether a user is legal.



Chapter 4 Performance Measurement

In this chapter, we want to measure the capability and performance of the W-CSCF. We extremely esteem the capability and performance of the W-CSCF as important factor for QoS (Quality of Service). At first, we measure how many subscribers that can register to the W-CSCF in a fixed interval. If we can calculate the number of SIP Registration procedures that the W-CSCF can process per minute then we could decide how many the W-CSCF are required for the whole home network deployment. The measurement can reduce the cost of deploying the IMS network. Second, we measure how many calls that can be established through the W-CSCF in a fixed interval (one minute). The measurement divides into two parts; one is normal scenario that the call can be established successfully and the other is the call is rejected through the AS.



4.1 The Platform and Measurement Tools

The platform of the W-CSCF is based on Red Hat Linux and the functionalities provided by the W-CSCF are described in Chapter 2. The platform of the HSS is also based on Red Hat Linux and functionalities provided by the HSS are described in section 1.6. The Cx Interface between the HSS and W-CSCF is implemented by Computer & Communication Research Laboratories of the Industrial Technology Research Institute.

The Sim-UA (User Agent) is implemented on Microsoft Visual C++ and can be executed on Windows XP. The Sim-UA behaves as multiple User Agent Clients (UAC) that simultaneously register to the IMS network. The Sim-UA also can behave as User Agent Server (UAS) to receive SIP messages. We use Ethereal Tool, which is a network protocol analyzer and packet sniffer, to monitor the packets through the W-CSCF. So we can calculate the number of SIP Registration procedures completed in one minute. The related information about Ethereal Tool can be obtained on <http://www.ethereal.com>.

Figure 4-1 shows our measurement environment.

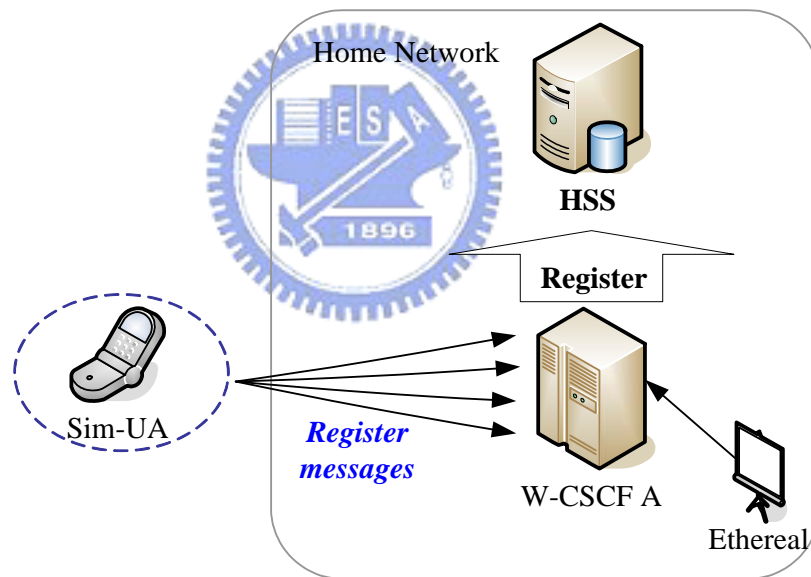


Figure 4-1: Measure Environment

4.2 Measurement of Registration

We use Sim-UA to simulate lots of subscribers that can simultaneously register to the W-CSCF in the home network. We use different arrival rate of SIP Register to measurement

the capability of the W-CSCF. By Ethereal Tool, we can observe how many SIP Registration procedures that the W-CSCF can handle in one minute.

Table 4-1 shows the result of our measurement. Figure 4-2 plots the corresponding data in Table 4-1. We send each Register message sequentially with the same delay (i.e., uniform distribution), so the lower arrival rate means the higher delay between two Register messages. We can find that if SIP Register sent with lower arrival rate, the W-CSCF can almost handle every Register message correctly in one minute. If arrival rate becomes higher, the W-CSCF may not handle all incoming messages and omit some messages. In order to obtain the maximum capability of the W-CSCF, we adjust the arrival rate to measure the number of SIP Registers handled by the W-CSCF. We repeat 10 times measurement for each arrival rate.

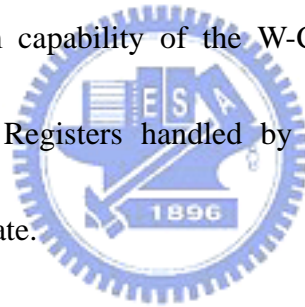


Table 4-1: Measurement Results for Registration

Arrival Rate (msgs/min)	Received Responses	Percentage (%)	Arrival Rate (msgs/min)	Received Responses	Percentage (%)
100	100.0	100	700	692.6	98.94
200	200.0	100	800	791.9	98.98
300	300.0	100	900	864.5	96.05
400	400.0	100	1000	531.3	53.13
500	498.4	99.68	1100	496.0	45.09
600	593.3	98.88	1200	369.3	30.77

From Figure 4-2, we can suppose the value of 900 messages/min (arrival rate of SIP Register message), stands for the system performance threshold for each W-CSCF. If arrival rate exceeds the threshold, the performance of the W-CSCF becomes worse. The system performance will be supported and guaranteed while arrival rate of SIP Register message is less than the threshold.

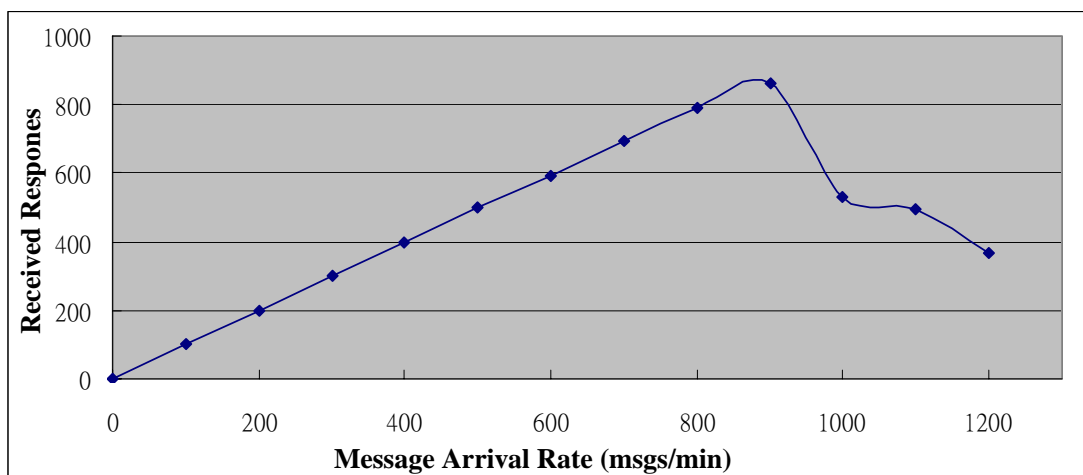


Figure 4-2: Performance of the W-CSCF (Registration)

4.3 Measurement of Call Setup

We use Sim-UA (behaves as UAC) to simulate that many users can simultaneously send SIP INVITE messages to the other Sim-UA (behaves as UAS) through W-CSCF in the home network. We use different arrival rate of SIP INVITE messages to measurement the max number of INVITE messages which the W-CSCF can handle. First part, the Sim-UA (behaves as UAC) can correctly setup calls with the other Sim-UA (behaves as UAS). We assume the W-CSCF#2 does not check Service Point Trigger (SPT) of callee.

By Ethereal Tool, we can observe how many calls that the W-CSCF can handle in one minute. Table 4-2 shows the result of our measurement. Figure 4-3 plots the corresponding data in Table 4-2. We also send each SIP INVITE message sequentially with the same delay (i.e., uniform distribution) and repeat 10 times for each arrival rate. From Table 4-2, we can suppose the value of 900 messages/min (arrival rate of SIP INVITE message), stands for the system performance threshold for the W-CSCF when the AS is not involved. From Figure 4-3, we clearly find that arrival rate exceeds the threshold, the number of calls that the W-CSCF can handle drops rapidly. In our measurement, we assume that the Sim-UA will not send 180 (Ringing) Response.

Table 4-2: Measure Results for Call Setup (Normal)

Arrival Rate (msgs/min)	Received Responses	Percentage (%)	Arrival Rate (msgs/min)	Received Responses	Percentage (%)
100	100.0	100	700	690.7	98.67
200	200.0	100	800	783.2	97.90
300	300.0	100	900	780.3	86.70
400	399.1	99.77	1000	528.7	52.87
500	496.1	99.22	1100	441.6	39.49
600	592.9	98.81	1200	365.3	30.44

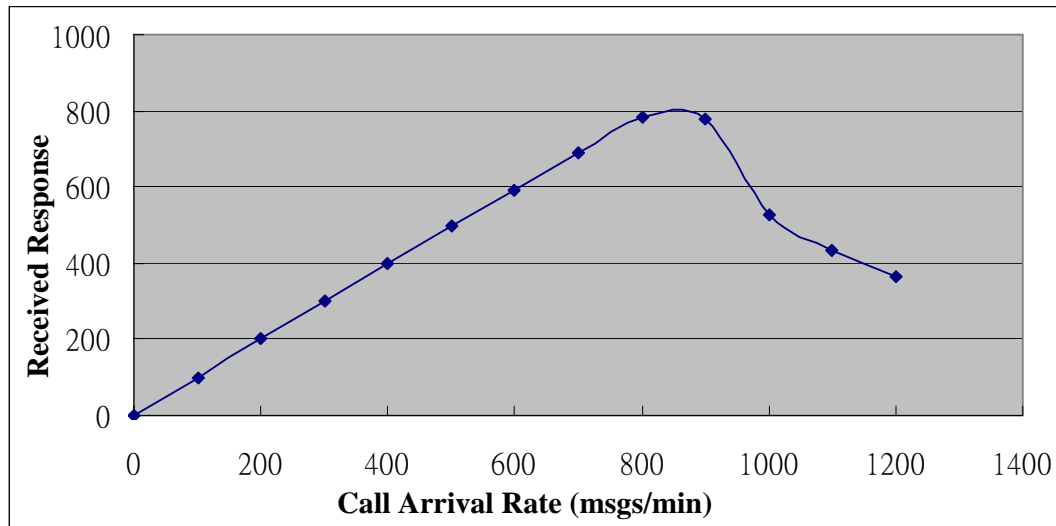


Figure 4-3: Performance of the W-CSCF (no AS involved)

Second part, the AS is involved and the AS generates the 403 Forbidden response to the callee's W-CSCF (as described in section 2.3.1). Table 4-3 shows the result of our measurement. Figure 4-5 plots the corresponding data in Table 4-3. We assume the W-CSCF#1 and W-CSCF#2 is the same machine which must handle both the MO procedure and MT procedure. In this part, the W-CSCF would check the SPT of callee. The W-CSCF must query the callee's location (by Cx Messages) and must check SPT of the callee, hence the time of setting up a call is longer than the time of normal scenario.

We also send each SIP INVITE message sequentially with the same delay (i.e., uniform distribution) and repeat 10 times measurement for each arrival rate. From Table 4-3, we can suppose the value of 900 messages/min stands for the system performance threshold for the W-CSCF when the AS is involved. From Figure 4-5, we can clearly find that arrival rate exceeds the threshold, the number of calls that the W-CSCF can handle drops rapidly.

Table 4-3: Measure Results for Call Setup (with AS involved)

Arrival Rate (msgs/min)	Received Responses	Percentage (%)	Arrival Rate (msgs/min)	Received Responses	Percentage (%)
100	100.0	100	700	690.4	98.62
200	200.0	100	800	780.5	97.56
300	300.0	100	900	781.6	86.84
400	398.7	99.67	1000	522.6	52.26
500	498	99.60	1100	420.5	38.22
600	592.4	98.73	1200	359.3	29.94

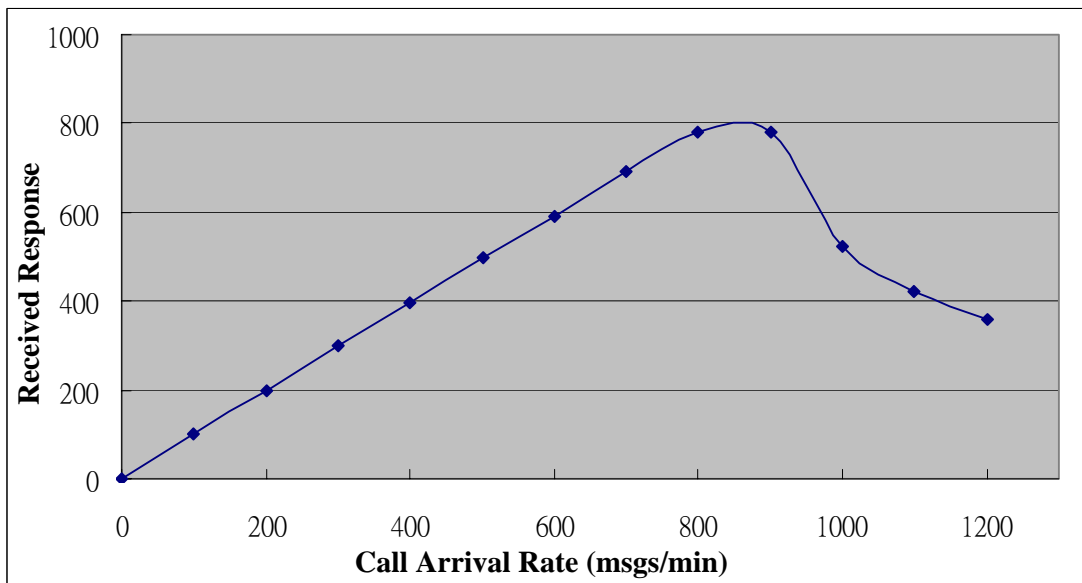


Figure 4-4: Performance of the W-CSCF (AS involved)

Chapter 5 Conclusion

Recently, more and more telecommunication operators have started to deploy WLAN as the access network to the Internet. Mobile Network operators can provide subscribers both GPRS access and WLAN access to the Internet. In this thesis, we present W-CSCF, for the IMS network, to enable WLAN users to access the IMS services. In addition, we also propose an efficient IMS registration procedure without explicitly performing redundant authentication steps. As specified by 3GPP, after a mobile user has obtained GPRS network access through GPRS authentication, another authentication procedure must be executed again during IMS registration before it can retrieve the IMS services. For One-Pass Authentication procedure, a user only needs to perform the GPRS authentication. At the IMS registration, a user performs simple operations (described in Figure 3-8) to verify if a user is legal. Compared with the 8-step two-pass authentication, the 4-step one-pass authentication saves four SIP message exchanged among the MS, the WGSN, the W-CSCF, and the HSS. Finally, we perform experiments to estimate the capability of the W-CSCF to ensure the system performance.

Chapter 6 Reference

- [1] Lin, Y.-B., and Chlamtac, I. *Wireless and Mobile Network Architectures*. John Wiley & Sons, 2001
- [2] 3GPP. Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service Description; Stage 2. 3GPP TS 23.060 V4.1.0 (2001-06), 2001
- [3] 3GPP. Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2. 3GPP TS 23.228 V6.2.0 (2003-06), 2003
- [4] M. Handley et al., SIP: Session Initiation Protocol, RFC 3261, June 2002
- [5] 3GPP. Technical Specification Group Core Network; IP Multimedia (IM) session handling; IM call model; Stage 2; 3GPP TS 23.218 V5.5.0 (2003-06), 2003
- [6] M. Handley and V. Jacobson, SDP: Session Description Protocol, RFC 2327, IETF, April 1998
- [7] 3GPP. Technical Specification Group Services and System Aspects; Network architecture; 3GPP TS 23.002 V6.1.0 (2003-03), 2003
- [8] 3GPP. Technical Specification Group Services and System Aspects; 3G Security; Security Architecture; 3GPP TS 33.102 V5.1.0 (2002-12), 2002
- [9] Feng, V. W.-S., Wu, L.-Y., Lin, Y.-B., and Chen, W.E. WGSN: WLAN-based GPRS Environment Support Node with Push Mechanism. Accepted and to appear in *The Computer Journal*, 2004
- [10] 3GPP. Technical Specification Group Core Network; IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signaling flows and message contents; 3GPP TS 29.228 V5.4.0 (2003-06), 2003
- [11] 3GPP. Technical Specification Group Core Network; Cx and Dm Interfaces Based on the Diameter Protocol; Protocol Details. 3GPP TS 29.229 V5.3.0 (2003-06), 2003

[12] P. Calhoun et al., Diameter Base Protocol, RFC 3588, September 2003

[13] Yi-Bing, Ming-Feng, Meng-Ta Hsu, and Lin-Yi Wu. One-Pass GPRS and IMS Authentication Procedure for UMTS, January 2004

[14] 3GPP. Technical Specification Group Services and System Aspects; 3G Security; Access Security for IP-based Services; 3GPP TS 33.203 V5.5.0 (2003-03), 2003

[15] Chen, W.E., Wu, Q., Pang, A.-C., and Lin, Y.-B Design of SIP Application Level Gateway for UMTS. Accepted and to appear in Design and Analysis of Wireless Network edited by Pan, Y., and Xiao, Y. Nova Science Publishers, 2004

