

# IMS路由相关问题及安全分析

## Routing in IMS and Related Security Issues

中图分类号: TP393 文献标识码: A 文章编号: 1009-6868 (2009) 06-0023-05

**摘要:** IMS采用会话启动协议(SIP)作为主要信令协议,运行于IP网络之上,是下一代融合网络核心的可选方案之一。IMS中和路由相关的描述主要包括: SIP消息中与路由有关的消息头描述、用户注册路由描述、用户会话发起路由描述,用以解决注册路由和会话路由等。在IMS的部署结构和路由的过程中,接口受到的安全威胁最大,需要设备商和运营商之间根据实际情况达成共识,来提高网络的健壮性和安全性;由于普遍采用简单易实现的递归查询方式,从而导致一级服务器查询量大,需要减少查询开销。

**关键词:** IP多媒体子系统;路由;互通;安全

**Abstract:** IP Multimedia Subsystem (IMS) is one of the important solutions for next generation Fixed and Mobile Convergence (FMC) networks. Based on IP network, it uses Session Initiation Protocol (SIP) as the major signaling mechanism. In IMS, such routing-related descriptions as the routing-related SIP message header, user registration routing and user session initiation routing are used for fulfill registration and session routing. In the IMS deployment structure and its routing mechanism, interfaces are most vulnerable to attacks; therefore, it is necessary for equipment vendors and operators to, based on actual situations, reach a consensus for improving network robustness and security. Another security issue is heavy query overhead of the first-level server, which is caused by the widely applied easy-to-implement recursive query.

**Key words:** IP multimedia subsystem; routing; connectivity; security

### 1 IP多媒体子系统

在3G网络中存在着电路交换域和分组交换域。从电信技术的发展趋势来看,分组交换技术是发展方向,其效率更高,并有逐渐取代电路交换技术的可能。

尽管理论上说通过分组域可以使3G用户使用所有的业务,通过这种方式使得数据传输更快,而且大大增加了因特网接入的可用带宽。但依然存在3个方面的问题:服务质量

(QoS), 计费 (Charging) 和业务整合 (IDS)。

由于消费兴趣不断推陈出新,运营商不得不考虑提高自身提供丰富个性化业务的能力,而不是在某项具体业务上过多投资。因此,高效的新业务开发成为实现个性化通信消费产品的系统集成项目的关键要素。

IMS(IP多媒体子系统)选取会话启动协议(SIP)<sup>[1]</sup>作为主要的信令协议来完成呼叫的建立、更改和终止对媒体会话或会议的功能。以上所述的这些问题都是IMS系统加以解决的目标,体现IMS网络相比于传统网络来说所具有的优势。IMS在不断的完善,

方桂彬/FANG Guibin<sup>1</sup>

李洋/LI Yang<sup>2</sup>

张云飞/ZHANG Yunfei<sup>2</sup>

(1. 北京邮电大学 计算机学院 智能通信软件与多媒体北京市重点实验室,北京 100876;

2. 中国移动通信研究院,北京 100053)

(1. Beijing Key Lab of Intelligent Telecommunication Software and Multimedia, School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;

2. China Mobile Research Institute, Beijing 100053, China)

事实证明IMS基础架构作为下一代融合网络的核心是一个非常好的可选方案。

### 2 IMS基础架构

IMS网络的基础架构主要分为3层:用户接入层、会话控制层和应用层。图1说明了一个典型的IMS架构,图中没有列出IMS网络中的所有实体,只是列出了3个层次的主要功能实体。

#### (1)用户接入层

IMS最初的设计思想是与具体的接入方式无关,本层接入主要包括:各类SIP终端接入、有线接入、无线接入、互联互通网关(如通用分组无线业务(GPRS)接入时的服务GPRS支持节点(SGSN)和网关GPRS服务节点(GGSN)),还包括POT话机通过综合接入设备(IAD)、接入网关(AG)和用户小交换机(PBX)接入等设备。

#### (2)会话控制层

会话控制层完成基本会话控制,实现用户注册、SIP会话路由控制、和应用服务器交互触发应用业务的会话、维护管理用户数据。

控制层主要包括呼叫会话控制

**基金项目:** 国家重点基础研究发展规划 (“973” 计划) 课题 (2007CB307101、2007CB307106)

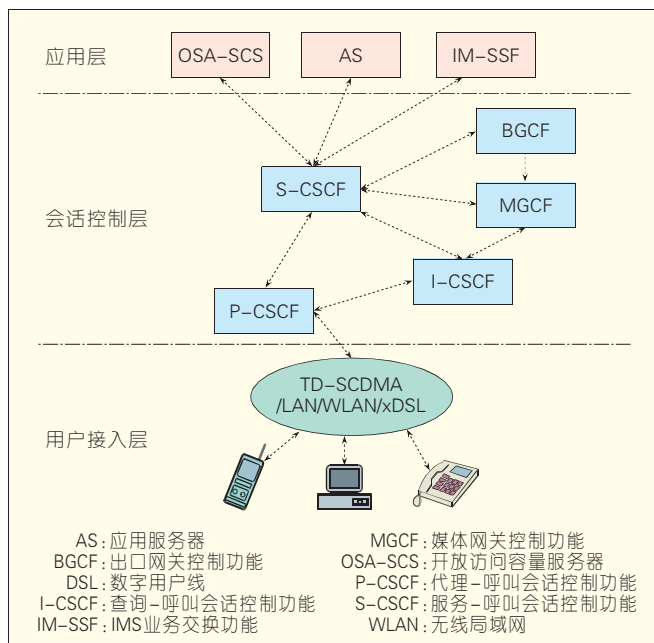


图1  
IMS结构层面对应的网络架构图

功能(CSCF)、出口网关控制功能(BGCF)、媒体网关控制功能(MGCF)等功能实体。其中,BGCF是IMS网络到电路域(CS)的出口,而MGCF是IMS网络和CS域互通的纽带,完成这两个域之间控制信令和媒体的转换。CSCF包括代理-呼叫会话控制功能(P-CSCF)、查询-呼叫会话控制功能(I-CSCF)、服务-呼叫会话控制功能(S-CSCF),它们可以在物理上合设在一起也可以分设。P-CSCF是用户设备(UE)接入IMS系统的入口,终端和P-CSCF之间的接口称为Gm接口。S-CSCF在IMS核心网中处于核心控制地位,负责UE的注册鉴权和会话控制,执行针对主/被叫端IMS用户的基本会话路由功能,并根据用户签约的IMS触发规则,在条件满足时进行到应用服务器(AS)的增值业务路由触发与业务控制交互。I-CSCF在IMS核心网中起到关口节点的作用,提供本域用户服务节点分配(确定哪个S-CSCF为用户提供服务)、路由查询和不同IMS域间拓朴隐藏等功能。

### (3)应用层

应用层主要包括3种不同类型的服务器,分别为SIP AS、开放访问容量服务器(OSA-SCS)和IP多媒体业务交

换功能(IM-SSF)。它们向用户提供业务逻辑,既可以传统的基本电话业务,如呼叫前转等业务,还可以提供基于SIP的许多新业务,又像第三方

表1 与路由有关的消息头

消息头	功能	设置
Via	对请求消息进行路由转发。	在请求的路由转发过程中,每个途经的SIP实体都来设置,将其地址写入Via消息头。
Route	对请求消息进行路由转发。	初始请求:由发起请求的UE来设置,它填入P-CSCF(出站代理)地址和Service-Route消息头的条目。初始请求:由CSCF来设置,它们从请求URI中的公共用户标识(通过查询DNS和HSS)或者收到的Path消息头中发现下一跳。后续请求:由发起请求的UE来设置,它根据初始请求传递过程中由Record-Route消息头所采集的条目放入Route消息头。
Record-Route	为一个会话中的后续请求记录Route消息头中的条目。	由CSCF来设置,如果它们希望收到对话中的后续请求,就将其地址放入Record-Route消息头。
Service-Route	指示初始请求的Route消息头条目,初始请求由UE发往用户的S-CSCF(用户发起)。	由S-CSCF来设置,它在对REGISTER请求的200 OK响应中返回本消息头。
Path	收集Route消息头条目,用于从S-CSCF向用户P-CSCF发出初始请求(用户终结)。	由P-CSCF来设置,它将自己的地址放入REGISTER消息的Path消息头中,并将其发往S-CSCF。

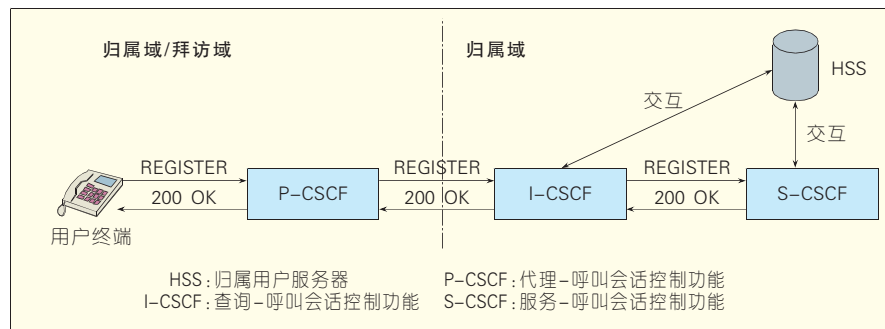


图2 IMS用户位于归属域发起的注册

提供API接口,便于拓展新业务。

## 3 IMS路由相关问题

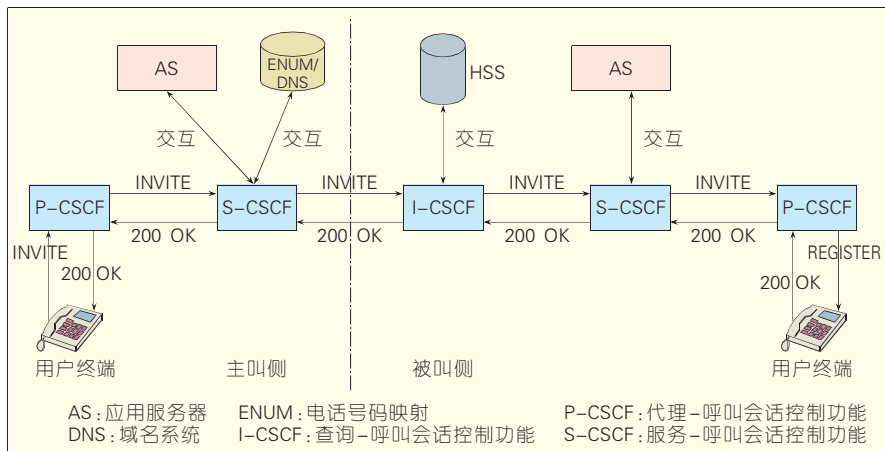
为了描述上的方便,不妨构造一个IMS用户注册和会话场景。我们可以设定Tom想要与Bob通话,在这个成功会话建立之前,先要保证Tom和Bob已都在IMS网络中成功注册。

### 3.1 SIP消息中与路由有关的消息头描述

在IMS用户注册或发起会话的过程中,SIP消息中与路由有关的头域主要包括:Via、Route、Record-Route、Services-Route和Path。这些头域的相关描述如表1所示<sup>[2]</sup>。

### 3.2 用户注册路由描述

Tom要想与Bob成功进行会话,前提就是他们都要在IMS网络上成功注册。注册过程如图2所示,在Tom向IMS网络发起注册的过程中,Tom的



▲图3 IMS用户之间互通的会话路由过程

UE首先会生成一个REGISTER请求,发往Tom运营商的归属域。相关信息将从Tom的通用用户标志模块(USIM)中的IP多媒体服务标志模块(ISIM)应用中获得。不论在归属域,还是在拜访域,这里存在一个P-CSCF发现的过程。在第三代伙伴计划(3GPP)中,对P-CSCF发现定义了两种机制:动态主机配置协议(DHCP)<sup>[3]</sup>域名系统(DNS)过程<sup>[4]</sup>和GPRS过程。另外也可以在UE中配置P-CSCF名字或者P-CSCF的IP地址来获得P-CSCF的地址。

该请求发送到归属域或者是拜访域的P-CSCF,一般而言,P-CSCF需要通过执行RFC 3263<sup>[5]</sup>中定义的DNS流程来定位登录归属网络的接入点,即归属网络的I-CSCF的SIP URI。P-CSCF把该注册请求发送给该I-CSCF,如果没有事先指定S-CSCF,I-CSCF通过和归属用户服务器(HSS)进行交互为用户选择一个S-CSCF,I-CSCF不保留任何与注册相关的状态。然后,S-CSCF通过和HSS交互和其他的一系列动作完成用户的注册,期间一些认证鉴权之类的动作和路由无关在此不做描述。

在注册过程中,UE可以从S-CSCF返回的200 OK中的Service-Route消息头中获知通往S-CSCF的直接路由。此后,当Tom的UE需要发出初始请求时,就不再需要联络I-CSCF了。同样,S-CSCF从P-CSCF插入的Path消息头

中得知P-CSCF的地址,以后所有发往Tom的初始化请求都必须首先经过P-CSCF才能达到UE。

### 3.3 用户会话发起路由描述

技术和网络的发展都不是一蹴而就的,同样的,IMS网络的部署也不可能一步到位。所以我们就面临着IMS网络和其他网络互通的问题。对于其他网络,我们选取IMS网络和CS域的互通来举例说明。主要在两个方面进行介绍。

#### (1)IMS用户和IMS用户间的互通

IMS中最复杂的问题之一就是请求消息的路由,尤其是初始请求的路由,简要路由过程如图3所示,因为用户漫游场景和非漫游场景类似,所以我们在此不再做区分描述。在我们的描述场景中Tom发送初始INVITE请求给Bob。其结果就是建立了一个SIP对话,并通过它发送若干后续的请求,例如ACK、PRACK、UPDATE和BYE。

Tom的UE发送INVITE请求主要提供的信息如下:(a)INVITE请求的最终目的地,即Bob的公共用户标志之一的SIP URI;(b)P-CSCF的地址,即Tom的UE注册是通过P-CSCF发现过程中获得的,它是呼叫路由的第一跳;(c)S-CSCF的地址,即Tom的UE注册是通过Service-Route消息头获得的。P-CSCF的地址和S-CSCF的地址都存在于初始INVITE消息中的Route头域

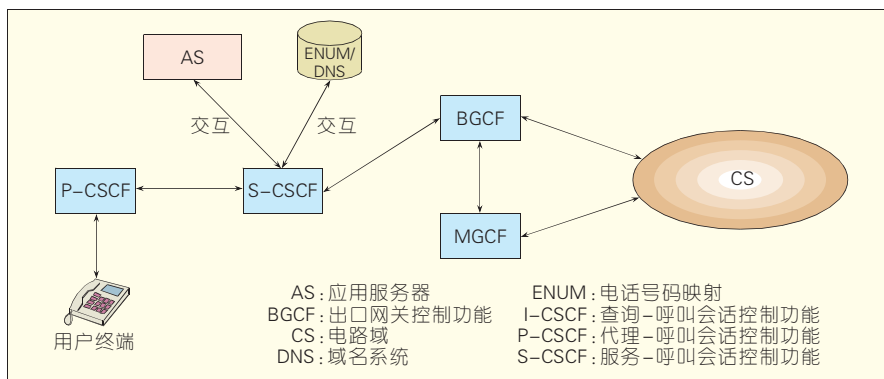
中。当该条INVITE请求到达S-CSCF后,S-CSCF根据用户终端注册时在HSS中下载的初始过滤标准(iFC)触发规则,串行触发一系列的AS来获得一系列的业。

发端归属网络的S-CSCF是第一个注意目的地的节点。S-CSCF为了要找到被叫用户归属网络的入口点,要查询电话号码映射/域名系统(ENUM/DNS)服务器。这个查询主要分为两个步骤<sup>[6]</sup>:(a)查询ENUM服务器,找到和被叫TEL URI所对应的SIP URI;(b)根据上一步得到的SIP URI里的域名,通过进行DNS查询找到被叫归属域的I-CSCF的IP地址。之后把这条INVITE请求发送给该I-CSCF。I-CSCF根据Request URI所说明的被叫用户,通过查询HSS,得到被叫用户注册时为被叫用户分配的S-CSCF,并把这条INVITE消息发送给它。

被叫归属域的S-CSCF根据被叫注册时下载的iFC,同样触发一系列的AS来获得所定制的业务。然后,S-CSCF继续处理INVITE请求并向下载发送,并要经过一系列的代理服务器,最后把INVITE请求发送给终端。这一系列代理服务器一定会包含一个P-CSCF,因为这是在用户终端注册是S-CSCF通过Path头得知的,也可能会包含I-CSCF,这主要和网络的拓扑隐藏有关。最后由被叫的UE对这条INVITE消息进行处理。

我们要注意的,在这个过程中,从主叫到被叫所经过的CSCF,在它们把INVITE消息发往下一跳之前都会把自己的地址加入到Record-Route中,只有被叫归属域的I-CSCF有一些特别<sup>[7]</sup>,根据运营商的策略,如果运营商不想把S-CSCF暴露给一个外部网络产生的SIP信令,I-CSCF就会把它自己的SIP URI加入到Record-Route头中。否则,I-CSCF不会把它自己加入到Record-Route头中,在INVITE消息处理完成后,后续SIP请求及其应答就不会再经过I-CSCF,如PRACK、UPDATE和ACK





▲图4 IMS用户拨打CS用户

等。终端根据收到的Record-Route,将其倒序反转,作为会话请求的路由根据。这样一来,主叫和被叫都获知了后续路由的过程。后续消息的请求及响应都是根据以上的路由发现和与路由相关的头域在实现自己的路由的,我们就不再分别描述了。

#### (2)IMS用户和CS用户之间的互通

其实,当一个IMS用户发起会话时,他不必关心被叫用户是一个IMS用户还是一个其他类型的用户。基于IMS终端在注册时学习到的路由,来自主叫用户的会话请求总能够到达为主叫服务的S-CSCF。

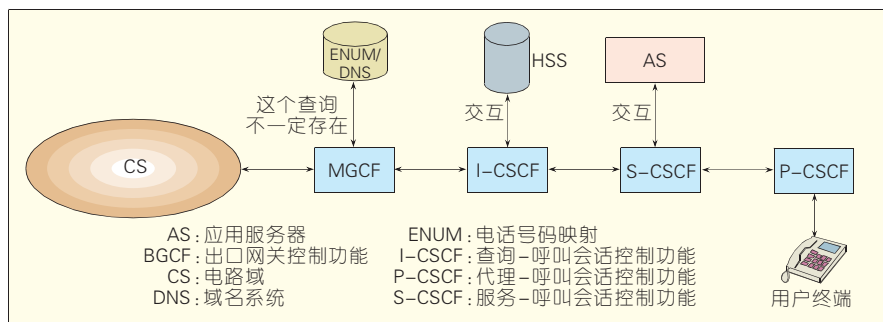
我们以Tom拨打一个CS用户为例,如图4所示。Tom发出的INVITE消息到达他归属域的S-CSCF所进行的一系列动作与IMS用户和IMS用户之间互通中描述的相同,不过不同点就在于S-CSCF在进行ENUM/DNS查询时找不到被叫用户的信息,即无法找到被叫的TEL URI和SIP URI的对应关系。这时,IMS网络就会尝试将会话请求路由到CS域。为了进入CS网络,S-CSCF就会把会话请求路由到与其位于同一网络的BGCF。所选择的BGCF有两条路由原则<sup>[8]</sup>: (a)BGCF选择同一网络中的MGCF,并把会话请求路由到CS域去;(b)BGCF选择不同IMS网络中的另一个BGCF,并由所选择的BGCF把请求路由到与其在同一网络中的MGCF,并进一步路由到CS域去。

在这里,MGCF是SIP信令的终结

点,它将把SIP协议转换为ISUP/BICC信令并控制IMS-MGW。如果CS网络的SS7由IP承载,在信令控制层面,MGCF可直接与CS域互通,而在用户媒体层面,IMS-MGW与MGW直接互通。如果CS网络的SS7由TDM承载,对于信令控制层,MGCF还需要通过SGW实现信令的适配,再与传统的交换机互通。

反之,如果是一个CS用户拨打一个IMS用户,如图5所示。该CS用户拨打Tom的E.164号码,这个会话请求向其他会话请求一样在CS域得到处理,在进行路由分析后,该请求将被送到IMS用户的归属网络中的MGCF。在收到CS域发过来的ISUP/BICC信令后,MGCF把它们转换为SIP信令,并与IMS-MGW交互,以创建一条用户平面的连接。之后MGCF会向I-CSCF发送一条INVITE消息,之后的过程与IMS用户和IMS用户之间互通时被叫侧的描述一样。

我们要注意的是MGCF是怎么选



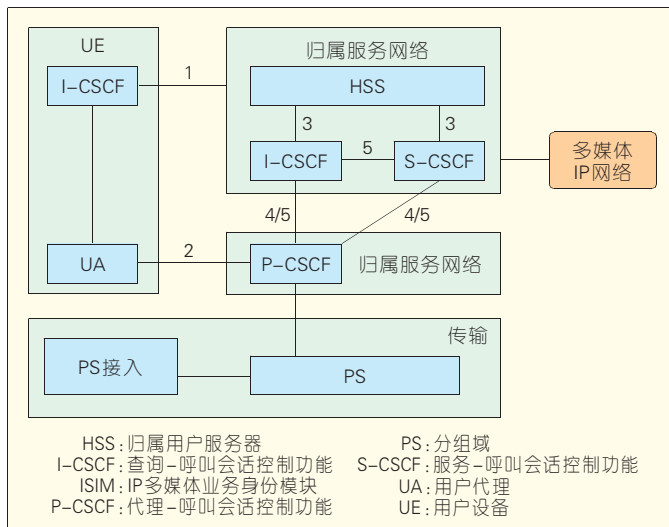
▲图5 CS用户拨打IMS用户

择I-CSCF来进行消息发送的。在3GPP规范24.229中定义MGCF即可以以TEL URI的格式路由,也可以以SIP URI的格式路由。如果是前者,我们可以把要发送到的I-CSCF地址事先配置在MGCF中;而如果是后者的话,MGCF就应该有ENUM/DNS查询的能力,把请求中的E.164号码转换为与之对应的SIP URI,并根据得到的SIP URI的域名查询DNS以获得将要发往的I-CSCF的地址。

## 4 路由过程中存在的安全问题分析

因为IMS网络是覆盖于IP网络之上的一个网络,所以它不可避免的继承了一些原有IP网络上的威胁,如病毒攻击等。但是由于IMS网络的服务质量(QoS)机制,认证鉴权机制,并且IMS网络一般部署在运营商的私有网络中,所以对原有VoIP网络中的一些威胁,如拒绝服务(DoS)、电话窃听、话费欺骗、假冒用户以及篡改SIP消息等有一定的防护作用。以上提到的这些都是业界广泛知道的一些威胁,本文在此不再做过多的介绍。我们所关心的是,当IMS网络商业部署之后,由于它的部署架构和路由机制所导致的一些弱点和威胁,我们将在下文主要通过两个方面来介绍。

(1)当IMS网络真正的商业部署之后,IMS网络一般都会存在于运营商为其所建的专有网络中,这就对IMS网络起到了一定的保护作用。在信令平面,P-CSCF是IMS终端和IMS网络之间的第一个连接点,它和终端之间的

图6  
IMS安全架构

接口称为Gm接口。在3GPP的规范中所定义的5个安全联盟<sup>[9-12]</sup>中,如图6所示,只有Gm接口处的安全联盟是暴露给外部网络的,所以这个接口受到的安全威胁也将会最大,所以要解决这个接口处的安全问题就变得非常关键。

IMS最初的设计是假定IPv6和IP安全协议(IPSec)都会在网络中得到运用,这也是IMS网络和传统的VoIP环境相比较会更安全的地方。但是,IPv6在现实中还没有完全普及,我们运用的还主要是IPv4,而且IPSec的建立是基于用户认证的基础之上,由于目前终端和IMS网络之间实际运用的认证算法为超文本传输协议(HTTP) Digest网络对终端的单向认证,而不是采用3GPP AKA双向认证等原因,设备商对于Gm接口的安全联盟做的不是非常完善,所以带来了用户终端外部网络和IMS私有运营网络之间的一些安全问题,这就需要设备商和运营商之间根据实际情况达成一种共识,来提高网络的健壮性和安全性。

(2) 在目前的IMS网络中,ENUM/DNS服务器普遍地采用简单易实现的递归查询方式。全国分为两级架构,负责省内路由的成为二级ENUM/DNS服务器,负责省间路由的成为一级ENUM/DNS服务器。在进行省间呼叫的时候,如A省的用户拨打

B省的用户,每次查询都要经过一级ENUM/DNS服务器,给一级ENUM/DNS服务器造成了不小的查询负担,即时有缓存技术的存在,但不能防止恶意用户通过不停拨打不同的电话号码,而致使缓存中存放的条目不停的换入换出,从而导致大量查询一级服务器,花费较大的查询开销,而且这种现象的发生极有可能造成严重的后果,例如有可能会使ENUM/DNS服务器的性能降低,甚至出现DoS。

## 5 结束语

IMS网络相比于传统的网络来说具有无可比拟的优越性。IMS的基础架构为下一代网络(NGN)的部署提供了一种强有力的框架机制。本文主要介绍了IMS网络中的一些路由过程和机制,针对这些路由情况IETF也试图通过扩充SIP能力集来满足IMS的路由需求。同时,我们也根据IMS网络的部署架构和路由机制提出了一些安全问题。IMS网络也在不断的进行完善中,我们相信IMS在将来一定会得到广泛的应用。

## 6 参考文献

- [1] ROSENBERG J, SCHULZRINNE H, CAMANILLO G. SIP: session initiation protocol [R]. IETF RFC3261. 2002.
- [2] POIKSELKA M, MAYER G, KHARTABIL H, et al. IMS: IP多媒体概念和服务[M]. 2版. 望玉梅, 董文宇, 周胜, 译. 北京: 机械工业出版社, 2007.

- [3] DROMS R, BOUND J, VOLZ B, et al. Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [R]. IETF RFC 3315. 2003.
- [4] MOCKAPETRIS P. Domain names—concepts and facilities[R]. IETF RFC 1034. 1987.
- [5] ROSENBERG J, SCHULZRINNE H. Session Initiation Protocol(SIP): Locating SIP servers [R]. IETF RFC 3263.2002.
- [6] FALTSTROM P. E.164 number and DNS[R]. IETF RFC 2916.2000.
- [7] CAMARILLO G, GARCIA-MARTIN M A. 3G IP多媒体子系统IMS——融合移动网与因特网[M]. 张同须, 等译. 北京: 人民邮电出版社, 2006.
- [8] 3GPP TS 24.229-790. IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol(SDP), stage 3(Release 7)[S]. 2007.
- [9] 3GPP TS 33.203. Access security for IP-based services(Release 8)[S]. 2008.
- [10] 3GPP TS 33.210. Network domain security; IP network layer security(Release 5)[S]. 2002.
- [11] 3GPP TR 33.978. Security aspects of early IP Multimedia Subsystem(IMS) (Release 7) [S]. 2007.
- [12] 3GPP TS 29.328. IP Multimedia (IM) subsystem Sh interface; Signaling flows and message contents (Release 5)[S]. 2005.

收稿日期: 2009-07-30

## 作者简介



方桂彬, 北京邮电大学计算机学院智能通信软件与多媒体北京市重点实验室在读硕士生, 主要研究方向为计算机网络、VoIP、IMS网络安全。



李洋, 中国科学院计算技术研究所博士毕业。中国移动通信研究院研究员、项目经理, 主要研究领域为网络安全、IMS安全、SIP协议安全分析及分布式计算等。已经发表学术论文30余篇。目前为 IEEE Communications Letters、Elsevier Computers & Security等著名学术期刊

的特约审稿人。



张云飞, 北京交通大学博士毕业。中国移动通信研究院研究员、项目经理, 负责分布式业务网络DSN的研发和标准化工作, 研究领域为网络架构、分布式计算与P2P、移动互联网、未来核心网演进、云计算等。已经发表学术论文20余篇。在IETF发起建立P2P流媒体协议PPSP, 并担任BOF主席, 在ITU担任SG13 DSN研究课题Editor, 目前为Computer Communications等著名学术期刊的特约审稿人。