基于 SIP的 VoIP流量识别方法研究*

陈 敏[1,3], 张广兴[1,2], 毕经平[1]

(1.中国科学院 计算技术研究所 下一代互联网 研究中心, 北京 100080; 2.湖南大学 计算机与通信学院, 湖南 长沙 410082; 3.中国科学院 研究生院, 北京 100049)

摘 要: 分析了已有流量识别方面的主要方法,针对基于 SIP的 VoIP流量,提出一种结合协议特征和协议流程分析的综合流量识别方法,并基于 Libpcap库实现了对应的识别工具。

关键词: 会话初始化协议; 语音互联网协议; 网络测量; 流量识别; 基于载荷分析

中图分类号: TP393 文献标志码: A 文章编号: 1001-3695(2007)04-0301-03

Research of SIP-based VoIP Traffic Identification Methodology

CHEN Min[1,3], ZHANG Guang-xing[1,2], BI Jing-ping[1]

(1. *Next Generation Network Research Center, Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100080, *China*; 2. *School of Computer & Communication, Hunan University, Changsha Hunan* 410082, *China*; 3. *Graduate School, Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract: This paper analyzed the mostly-used traffic identification methodologies, and proposed an approach based on both protocol signatures and payload-based analysis to identify SIP-based VoIP traffic. A tool is also implemented on Linux with Libpcap library.

Key words: SIP(session initial protocol); VoIP; network measurement; traffic identification; payload-based analysis

0 引言

随着 Internet带宽的增加,网络上多媒体应用越来越普遍,流媒体、VoIP、视频会议等多媒体新业务流量也越来越大。新业务的出现,极大地促进了网络的发展,但同时也改变了已有的网络流量模型,给网络管理、流量监测提出了新的挑战。对于流量识别方法的研究,尤其是对日益增长的多媒体流量的识别方法研究,有助于帮助管理员了解网络中承载的流量分布情况,进一步了解多媒体流量的增长对网络性能的影响,协助更好地对网络进行规划设计。同时,可以探索对不同业务的 QoS需求以及新的计费模式。

目前 Internet上多媒体应用主要分为如下两大类,即面向内容发布的多媒体应用(如流媒体、IPTV)和面向交互的多媒体应用(如 IP电话、视频会议)。市场上流媒体解决方案的厂家有 RealNetworks、Apple和 Microsoft,其中 RealNetworks的流媒体服务器有 HelixServer,使用该公司私有的 RDT协议; Apple公司有面向开源社区免费的 DarwinStreaming,遵循 RTSP协议标准; Microsoft有 MMS私有协议。

视频会议和 IP电话主要有 ITU制定的 H.323和 IETF的制定的 SIP[1,2](Session Initial Protocol,会话初始化协议)两大协议族。H.323初始是面向电路交换的 PSTN,它目前在小规模的 PSTN交换网络中用于处理简单的电话呼叫和 IP视频会议市场上占主要的市场份额。SIP是一个基于文本的 Internet协议,借鉴了 HTTP、SMTP等协议,在风格上遵循因特网一贯坚持的简练、开放、兼容和可扩展等原则,实现简单。因此基于 SIP的应用也越来越广泛。

1 已有的流量识别方法分析

当前 Internet中的流量依据应用的不同可以分成不同类别[3],如表 1所示。

流量识别,就是将数据包与产生该数据包的应用对应起来的过程。已有的流量识别方法,根据是否对协议载荷进行分析(即分析信息是否涉及到传输层上层信息)可分为载荷分析(Payload-based Analysis)和非载荷分析;根据识别所依据信息的不同可分为基于端口的流量识别、基于特征的流量识别、基于协议流程分析的流量识别方法。

1.1 基于端口的流量识别方法

最简单的流量识别方法是基于传输层端口的识别。IANA分配的一些周知端口(Well-known Port),如 21(FTP)、23(Telnet)、25(SMTP)、110(POP)、80(WWW)、SIP(5060)。这种方法简单,开销很小,易实现,但最大的缺点是不准确,尤其是对一些新的应用,如 P2P、多媒体应用。这些新应用为了能够穿透,防止被阻断,并不采用静态端口,而是通过动态分配。

1.2 基于特征的流量识别方法

基于特征的流量识别方法是根据不同应用表现的不同特

收稿日期: 2006-02-20; 修返日期: 2006-03-27 基金项目: 国家“863”计划资助项目(2005AA121560); 国家自然科学基金资助项目(60403031)

作者简介: 陈敏(1982-),男,安徽绩溪人,硕士研究生,主要研究方向为网络测量、流量识别(chenmin@ict.ac.cn); 张广兴(1978-),男,博士研究生,主要研究方向为网络测量与性能分析; 毕经平(1974-),女,副研究员,硕导,主要研究方向为下一代 Internet网络监控与管理。

征(Signature)来识别数据包所对应的应用。特征可以是报文中的特征字符串,也可以是应用行为特征,或者是一些统计特性。表2列出了不同P2P协议的特征字符串[4]。

表1 Internet中应用大致分类

应用分类	应用举例
批量数据传递	FTP
数据库	Postgre、SQLnet、Oracle、Ingres
交互应用	ssh、klogin、rlogin、Telnet
邮件	Imap、POP2/3、SMTP
服务	X11、DNS、ident、ldap、NTP
WWW	WWW
P2P	KaZaA、BitTorrent、Gnutella
网络攻击	网络蠕虫、病毒
游戏	反恐精英
多媒体	流媒体、VoIP、视频会议等

表2 P2P主要协议的特征字符串

P2P Protocol	String
eDonkey2000	0xe319010000
	0xc53f010000
Fasttrack	"Get/.hash"
	0x2700000002980
BitTorrent	"0x13Bit"
Gnutella	"GNUT" "GIV"
	"GND"
MP2P	GOII,MD5,SIZ0x20
Direct Connect	"$MyN" "$Dir"
	"$SR"
Ares	"GET hash:"
	"Get shal:"

以P2P的连接建立过程为例,介绍利用行为特征来识别P2P流量的应用[5]:P2P节点在加入P2P网络建立连接时,Peer之间一般会在某个时间间隔 t 内同时存在TCP和UDP流;而且,对于某个指定的Peer它在P2P网络中的标志({IP,Port}二元组)经过传播后会被其他多个Peer学习到,后者会与该{IP,Port}所标志的主机交换数据。在并发流中表现为对于某个指定的Peer存在多个{IP,Port}与其进行交互,而且与其进行交互的IP数目和Port数目基本相当。根据这种特性能够较准确地识别P2P流量。

对于特征字符串,不同协议的特征字符串不同,需要针对各个协议分析其特征字符串。对于私有协议,只能采用逆向工程(Reverse Engineering)的方法。

基于统计特性的识别方法在实时流量识别应用存在困难。根据特征分析识别方法的一个问题是扩展性差,需要大量的事前分析来确定排他特征。目前多媒体应用的特征尚不清楚。

1.3 基于协议流程分析的流量识别方法[6,7]

对于一些新业务,如多媒体应用,一般一个完整的流程会涉及到多个会话,即控制会话和动态会话。一个会话(Session)是指用户间的数据交换过程。通过控制会话建立连接、协商数据传输参数、启动和撤销传输。不同于使用固定端口或默认端口的应用,动态会话的端口、协议信息是在控制会话中动态协商的。协议流程分析方法是根据构成一次应用的多个会话之间的关联关系,从控制会话中提取动态会话信息,根据这些信息来识别该应用涉及的动态会话。

基于协议流程分析的识别方法,对控制协议的识别效率和准确率直接影响到最终的识别效果。

1.4 流量识别方法小结

流量识别技术有如下要求:①准确。需要将误报和漏报降低到一个可接受的限度。②尽早识别。识别是对新业务进行分析、控制的基础,因此要尽早识别流量所属的应用类型。最理想的识别方法是在收到该应用的第一个数据包就识别出该数据包所在流的应用类型。③可扩展。能够对高速链路上流量进行快速识别。④健壮。在网络不稳定的情况下(路由不对称、丢包、包乱序等)仍能够做到比较准确的识别。如何在这四个要求之间做到有效的权衡是流量识别方法研究要解决的问题。

基于端口的流量识别方法简单但准确性不高;基于流量特征和基于协议流程分析的识别方法在扩展性、时效性方面存在不足。

目前对流量识别的研究大多集中在对P2P流量的识别上,对多媒体识别的研究甚少。目前能够直接部署到实际链路的流量识别系统工具并不成熟。本文提出了一种结合协议特征和协议流程分析的综合流量识别方法:对控制会话,通过关键字匹配来提高识别的准确率;对于识别出的控制协议,采用协议流程分析方法,识别出动态会话。

2 基于SIP的VoIP流量识别工具实现

2.1 SIP流程

SIP是目前在流媒体中应用比较广泛的实时流媒体控制协议。Internet上大量的应用都需要使用会话的创建与管理功能,这也是IETF提出会话初始化协议的初衷。在IETF定义的网络协议体系结构中,SIP是位于传输层之上的应用层协议,通过携带可选的SDP(Session Description Protocol)载荷,SIP可以轻松地开启/关闭会话、协商会话参数、建立数据交换流以及管理会话。图1是典型的SIP应用场景。

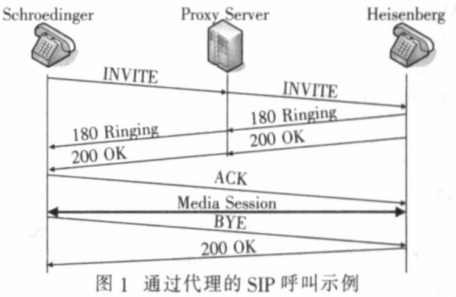

图1 通过代理的SIP呼叫示例

以下是Schroedinger通过SIP与Heisenberg建立连接的数据包片段。Schroedinger发送INVITE命令,Heisenberg对该命令进行应答。这样就建立了从〈100.101.102.103:8000〉到〈200.201.202.203:49170〉(对应于报文中粗体下画线部分)的RTP动态会话数据通道。在SIP控制会话有效期内,所有归属于流〈100.101.102.103:200.201.202.203:8000:49170:UDP〉和流〈200.201.202.203:100.101.102.103:49170:8000:UDP〉都可以被认定为是VoIP流量。

请求报文:

```
INVITE sip:wemer heisenberg@munich de SIP/2.0
…
Content Type: application/sdp
Content Length: 159
v=0
c=IN IP4 100.101.102.103
m=audio 8000 RTP/AVP 0
a=rtpmap: 0 PCMU/8000
```

应答报文:

```
SIP/2.0 200 OK
…
Content Type: application/sdp
Content Length: 159
v=0
o=heisenberg 2890844526 2890844526 IN IP4 200.201.202.203
c=IN IP4 200.201.202.203
t=0 0
m=audio 49170 RTP AVP 0
a=rtpmap: 0 PCMU/8000
```

识别工作包括数据包捕获、SIP数据包识别、动态会话信

息提取、数据流标志。

2.2　数据包的捕获

目前大部分的流量分析工具是基于 Libpcap实现的。Libpcap[8]是可以适用于多种操作系统(如 Linux、FreeBSD、Solaris等)的数据包捕获库,利用该库可以向开发人员屏蔽底层网络链路所采用的技术。

2.3　SIP会话的识别

文献[1]规定 SIP报文的语法如下:

generic-message= start-line message-header CRLF[message-body]

对于请求报文

start-Request Line=Method SP Request-URI SP SIP-Version CRLF

有如下识别规则:

(invite|register|cancel) sip[\x09 \x0d-~] * sip/[0-2] \.[0-9]

对于应答报文

start-Status Line= SIP-Version SP Status-Code SP Reason-Phrase CRLF

有如下识别规则:

sip/[0-2] \.[0-9][1-5][0-9][0-9][a-zA-Z] *

2.4　SIP的分析

在识别出 SIP报文后,下一步需要分析 SIP报文,从中提取出需要的有关动态会话的信息。提取算法如下:

(1)确定是否是 SIP的请求报文。若是,将流〈src_ip, src_port, dst_ip, dst_port, UDP〉标记为控制会话,goto(2);否则,goto(5)。

(2)确定是否是 SIP的应答报文。若是,将流〈src_ip, src_port, dst_ip, dst_port, UDP〉标记为控制会话,goto(3);否则,goto(7)。

(3)Status-Code=200? 是,goto(3);否则,goto(7)。

(4)查找头部 CSeq,确定是否是对 INVITE方法的回复。是,goto(4);否则,goto(7)。

(5)查找头部 Content-Type,是 application/sdp? 是,goto(6);否则,goto(7)。

(6)查找 SDP协议,对应属性"c=",提取 IP地址(如果是请求报文,记为 dyn_ip1;否则记为 dyn_ip2);对应属性"m="提取媒体类型和传输媒体数据所用的端口(如果是请求报文,记为 dyn_port1;否则记为 dyn_port2)。将对应于流〈dyn_ip1, dyn_port1, dyn_ip2, dyn_port2, UDP〉和〈dyn_ip2, dyn_port2, dyn_ip1, dyn_port1, UDP〉标记为动态会话,从属于(1)确定的控制会话。

(7)分析下一个数据包。

其中(1)、(2)两步根据 2.3节提出的匹配模式来识别是何种 SIP报文。

当 SIP会话接收到 BYE方法的请求报文时,表明此次多媒体会话已经结束,对应控制会话将从控制会话列表中删除,从属于该控制会话的动态会话也同时删除。

3　结束语

网络多媒体流量的识别研究对了解多媒体应用的特征、其对网络性能的影响以及为用户计费、网络与业务规划、流量工程设计均有重要的意义。本文分析了目前在流量识别方面的主要方法,提出一种结合协议特征和协议流程分析的综合流量识别方法,并基于 Libpcap库实现了一个识别基于 SIP的 VoIP流量识别工具。试验表明,该工具能够比较准确地识别出基于 SIP的多媒体应用流量。

VoIP并不是 SIP唯一的应用场景,下一步将对基于 SIP的其他应用所产生的流量识别方法作进一步研究。

参考文献:

[1] ROSENBERG J, SCHULZRINNE H, CAMARILLO G, *et al*. RFC 3261 SIP: session initiation protocol[S]. [S.l]: [s.n], 2002.

[2] HANDLEY M, JACOBSON V. RFC 2327 SDP: session description protocol[S]. [S.l]: [s.n], 1998.

[3] MOORE A W, PAPAGIANNAKI K. Toward the accurate identification of network application[C]// Passive & Active Measurement Workshop 2005 (PAM 2005). Boston: Springer Verlag GmbH, 2005: 41-54.

[4] KARAGIANNIS T, BRODIO A, FALOUTSOS M, *et al*. Transport layer identification of P2P traffic[C]// IMC'04. Taormina: [s.n.], 2004: 121-134.

[5] SEN S, SPATSCHECK O, WANG Dongmei. Accurate, scalable network identification of P2P traffic using application signatures[C]// WWW 2004. New York: [s.n], 2004: 512-521.

[6] KANG H J, KIM M S, HONG J W. Streaming media and multimedia conferencing traffic analysis using payload examination[J]. **ETRI Journal**, 2004, **26**(3): 203-217.

[7] MERWE J V, CACERES R, CHU Yanghua, *et al*. Mmdump: a tool for monitoring internet multimedia traffic[J]. **ACM Computer Communication Review**, 2000, **30**(4): 48-59.

[8] MCCANNE S, LERES C, JACOBSON V. Libpcap[EB/OL]. (2004). http://www.tcpdump.org.

(上接第 300页)

3　结束语

本文详细讨论了多媒体回铃音在 3GPP R4核心网络上,利用 H.248 Megaco作为控制协议,参照 CRBT主叫交换机方式,得到利用媒体服务器提供多媒体回铃音的实现方案,从而可以在 3G网络上快速地继续开展彩铃业务并扩展了铃音媒体。下一步将对多媒体回铃音与其他增值业务的业务特征交互、与 2G等传统网络的互连和彩铃业务的平滑演进等问题继续进行研究。个性化回铃音业务在电路域上的成功和 IP网络上可以提供视频流的能力,预示着在 3G网络建设中广泛的应用前景和商用价值。

参考文献:

[1] 中国移动通信集团公司.彩铃业务总体技术要求 v1.0.0[S].[S.l]:[s.n], 2003.

[2] 王玉龙,廖建新.基于智能网实现彩铃业务的技术研究[J].重庆邮电学院学报, 2004, **16**(4): 21-24.

[3] 甘雷.彩铃业务两种实现方式及对比分析[J].电信工程技术与标准化, 2004(83): 54-58.

[4] 赵慧玲,叶华,等.以软交换为核心的下一代网络技术[M].北京:人民邮电出版社, 2003: 47, 79.

[5] 信息产业部.基于软交换的媒体服务器技术要求[S].[S.l]:[s.n], 2004.

[6] 蔡康,李洪,朱英军,等.下一代网络(NGN)业务及运营[M].北京:人民邮电出版社, 2004: 204-205.

[7] 朱晓民,王鹏,廖建新.从智能外设到媒体服务器[J].现代电信科技, 2005(8): 55-57.

[8] 中国移动通信集团公司.彩铃总体技术要求 v2.0.0[S].[S.l]:[s.n], 2004.