

Investigation on the Use of the UDP Protocol by some Application Software

WANG Jingqun^{1,2}, YANG Wang^{1,2}, DING Wei^{1,2}

1. Department of Compute Science and Engineering, Southeast University, Nanjing 210096, China

2. Jiangsu Provincial Key Laboratory of Computer Network Technology, Southeast University, Nanjing, 210096, China

1.E-mail: jqwang@njnet.edu.cn, 2.E-mail:wyang@njnet.edu.cn, 3.E-mail:wding@njnet.edu.cn

Abstract—Along with the continuous development of network technology, the audio / video, download services, instant messaging and other applications in the Internet have become the mainstream. Meanwhile, UDP business data in the Network traffic is keeping sharp increase in recent years. In order to investigate the reasons for the dramatic increase, we select a popular instant messaging software, video player software, download software for packet capture analysis in this paper. Then we conduct a initial discussion on which software applications caused the dramatic increase of the UDP traffic after analyzing the message through the packet capture software——ethereal.

Keywords- UDP; ethereal; instant messaging; IPTV; downloading software

部分应用软件使用 UDP 协议调查

王敬群^{1,2}, 杨望^{1,2}, 丁伟^{1,2}

1. 东南大学 计算机科学与工程学院, 江苏 南京, 210096

2. 江苏省计算机网络技术重点实验室, 江苏 南京, 210096

1.E-mail:jqwang@njnet.edu.cn, 2.E-mail:wyang@njnet.edu.cn, 3.E-mail:wding@njnet.edu.cn

【摘要】随着网络技术的不断发展, 互联网中的音/视频、下载、即时通讯等应用逐渐成为主体。与此同时, 网络流量中的 UDP 业务数据在近年来剧增。为了对网络流量中 UDP 数据流量剧增的原因进行调查, 本文选取了常用的即时通讯软件、视频播放软件和下载软件来进行抓包分析, 通过抓包软件 ethereal 对报文进行分析, 来初步探讨哪些软件应用引起了 UDP 流量的剧增。

【关键字】UDP ; ethereal; 即时通讯; 网络电视; 下载软件

1 引言

随着网络技术与应用的快速发展, 互联网正在逐步从提供单一数据传输, 变成了一个能提供音频、视频、数据等多种业务的实体。文献[1]中提到 P2P 和在线视频服务流量已经超过了网页浏览、电子邮件这些传统的网络服务, 且正在占用越来越多的网络带宽。

与此同时, 网络流量中 UDP 业务数据在近年来剧增。在 CAIDA2009 年的一篇报告中, 2003 年, UDP 无论在包数、字节数还是流数上, 只占网络流量的 20% 以下。从 2006 年开始, UDP 流量在逐年增加, 到 2009 年初, UDP 在流级别上已经占有了巨大优势, 是 TCP 的 2.6~3 倍^[1]。

自 2000 年以来, 以具体应用为背景的网络测量研究主要集中在音/视频、即时聊天、P2P、在线游戏等新的网络服务上, 这些测量结果显示 UDP 正在逐渐成为新兴网络服务进行数据传输的主要选择, 其重要性正在逐渐赶上或者超过 TCP。文献[1]中提到 Mena 等

人发现 60%——80% 的音频数据流都是通过 UDP 进行传输, 而 TCP 只用于进行控制命令的传输。Dewes 等指出某些聊天系统如 ICQ 普遍使用 UDP。在发展迅速的 P2P 应用方面, UDP 通信也占有相当的比率。Karagiannis 等人指出目前主流 P2P 协议一般都可以使用 TCP 或者 UDP 进行数据传输。

UDP 协议是一种无连接协议, 其具有以下几个特性^[2]:

(1) UDP 是一个无连接协议, 传输数据之前源端和终端不建立连接, 当它想传送时就简单地去抓取来自应用程序的数据, 并尽可能快地把它扔到网络上。

(2) 由于传输数据不建立连接, 因此也就不需要维护连接状态, 包括收发状态等, 因此一台服务器可同时向多个客户机传输相同的消息。

(3) UDP 使用尽最大努力交付, 即不保证可靠交付, 因此主机不需要维持复杂的链接状态表。

为了对网络中 UDP 数据流量剧增的原因进行调查, 本文选取了常用的即时通讯软件、视频播放软件

和下载软件进行抓包分析,通过抓包软件对报文进行分析,探讨哪些软件应用引起了 UDP 流量的剧增。实验环境为 CENRET 江苏省网内的东南大学校园网。

2 抓包软件和抓包方式

抓包过程中所用的工具是 **ethereal**。该软件是 Gerald Combs 为了跟踪网络问题并更好的研究网络而开发的一种工具。它是一款网络协议分析软件,可以捕获网络上的数据包,并尽可能详细的显示,ethereal 主要有以下特点[3]:

- l Windows 和 Unix 都可以使用。
- l 可以在网络接口上实时的抓包。
- l 可以显示数据包非常详细的协议信息。
- l 可以打开和保存捕获的数据包。
- l 能够以多种标准过滤数据包,能够以多种标准查找数据包。
- l 彩色显示数据包。不同的协议或情况,颜色不同。
- l 能够创建多种统计信息。

在抓包过程中只对本机 IP 所相关的报文进行抓取,且只开启了某一特定应用软件,从而保证抓取到的报文主要是与某个软件相关。具体过程如下:

(1) 连上 Internet,启动 ethereal 抓包软件,不启动特定应用软件,观察 ethereal 中不同协议的流量情况。

(2) 在确保抓包前没有其他软件的干扰流量情况下,启动特定应用软件。

(3) 每次抓包完毕后,关闭特定应用软件,断开网络连接 30s,再重新开始抓包。

3 抓包结果分析

一般来说,网络应用服务在选择传输层协议时有两大选择:TCP 或 UDP。TCP 是一种面向连接的、具备可靠传输特性的协议;UDP 是一种面向无连接的传输协议。曾占据网络中绝大部分流量的 TCP 目前仍然是网络流量的较大组成部分,但 UDP 流量伴随着新型网络服务的发展而迅猛增加。由于音/视频通信、在线游戏等服务数据冗余性较强,对个别数据包的丢失不敏感,但是都具有较强的实时性要求,而且希望占用尽量少的管理资源从而可以支持更多的同时在线用户,目前这些新兴的网络服务越来越多地选择 UDP 作为其底层的传输协议,故本文选择常见的即时通讯软件、网络电视播放软件和下载软件来进行抓包分析。

3.1 即时通讯软件

即时通讯(Instant Messenger)软件由于具有速度

快、效率高、费用低等特点而受到互联网用户的喜爱。即时通信软件的出现改变了人们的生活方式,使得人们的通信更加方便快捷。随着上网人数的增长,即时通信使整个互连网变成了一个虚拟的社会。

表 1 所示为北青网提供的 2010 年 1 月份即时通讯软件日均覆盖人数排名^[4]。

Table 1. Some popular instant messaging software

表 1. 常用即时通讯软件

排名	软件	日均覆盖人数(万人)	日均网民到达率
1	腾讯 QQ	14449	76.1%
2	飞信	2091	11%
4	MSN	1749	9.2%

故本文选取了常见的即时通信软件——飞信(Fetion),腾讯 QQ,MSN,来抓包分析。图 1,图 2 和图 3 分别是 Fetion,腾讯 QQ,MSN 的一次抓包结果。

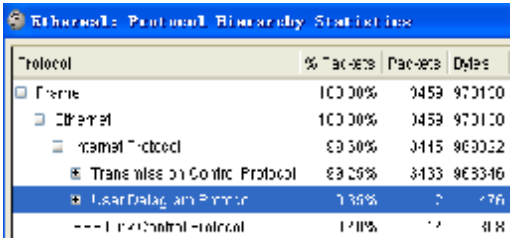


Figure 1. The result of a packet capture of Fetion

图 1. Fetion 的一次抓包结果

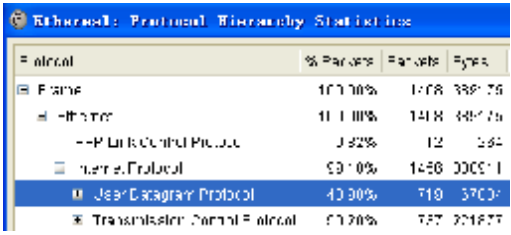


Figure 2. The result of a packet capture of Tencent QQ

图 2. 腾讯 QQ 的一次抓包结果

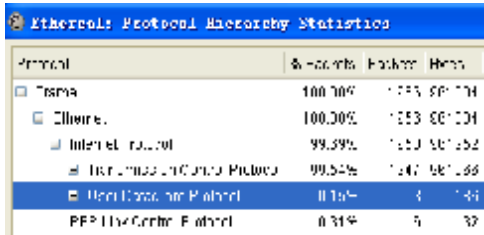


Figure 3. The result of a packet capture of MSN

图 3. MSN 的一次抓包结果

通过多次抓包实验，结合 ethereal 统计情况，得出三种软件的多次实验后的结果，见表 2。

其中抓包时间，报文总数，UDP 报文数，所占比率，都是多次实验的平均结果。

Table 2. The packet capture result of three types of Instant Messaging software

表 2. 三种即时通讯软件抓包结果

软件名	抓包时间（s）	报文总数	UDP 报文数	所占比率
Fetion	371.0	3574	4	0.13%
QQ	307.4	1092.8	389.8	41.02%
MSN	164.7	1156	7.8	0.94%

该类软件所产生的总流量假定为 x ，日均网民达到率可假定为软件的使用比率 R_1 ，软件的 UDP 协议平均所占比率为 R_2 ，记 $A(i) = R_1(i) \cdot x \cdot R_2(i)$ ；假设 Fetion，QQ，MSN 分别用数字 1，2，3 编号代表。

则在即时通讯应用中，UDP 所占比率大致为

$$R = \frac{\sum_{j=1}^3 A(j)}{x} \tag{1}$$

代入各项数据可计算得 $R=31.3\%$

从表 2 和公式(1)计算结果可以看出，Fetion 和 MSN 并不是使用 UDP 协议进行传输，其中 99%的通信协议是 HTTP 协议和 TCP 协议。QQ 的通讯协议中 UDP 所占比率相对较多，接近 50%，但腾讯 QQ 的网络用户量很大，所以这对于网络中的 UDP 流量的影响是很大的。总体而言，即时通讯软件对网络中 UDP 流量影响较大。

3.2 网络电视播放软件

常见的网络电视播放软件有很多，表 3 显示的是中关村在线提供的截止到 2010-8-4 网络电视软件排行榜^[5]。

Table 3. The ranking of IPTV software

表 3. 网络电视软件排名

排名	软件	历史下载总量	所占比率
2	PPStream	115990441	31.12%
3	PPLive	232229569	62.30%
7	QQLive	20176422	5.42%

13	土豆	1563	≈ 0
14	优酷	1297	≈ 0
19	迅雷看看	4311033	1.16%

因此本次抓包过程中对以下软件：PPStream, PPLive, QQLive, 优酷，土豆，迅雷看看进行了抓包分析。

通过多次抓包实验，结合 ethereal 统计情况，得出这六种软件的多次实验后的结果，见表 4。

其中抓包时间，报文总数，UDP 报文数，所占比率，都是多次实验的平均结果。

Table 4. The packet capture result of some popular IPTV software

表 4. 常见网络电视播放软件抓包结果

软件名	抓包时间（s）	报文总数	UDP 报文数	所占比率
PPStream	339	83250.7	81914	98.61%
PPLive	289	64294	44366	70.83%
QQLive	285.3	86331.7	74866	87.36%
土豆	305.3	129223.7	0	0
优酷	331	91070.7	3203	2.74%
迅雷看看	315.3	58363.7	34607	58.51%

PPStream: 通过对抓包过程观察，软件启动后，UDP 与 TCP 约各占 50%，随后 TCP 所占比率逐渐增多，UDP 逐渐减少（约 30s 后，所占比率低于 1%）。在点击播放某个节目后，UDP 快速增多，约 15s 后占绝对多比率（大于 95%，接近 100%）。这其中包含使用 UDP 封装的 eDonkey, SSDP 应用层协议和没有应用层的 UDP 协议，图 4 为其中的一次抓包结果。

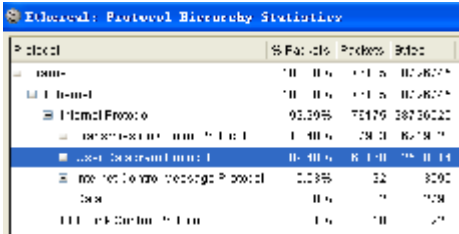


Figure 4. The result of a packet capture of PPStream

图 4. PPStream 的一次抓包结果

PPLive: PPLive 是基于 P2P 技术的网络电视平台。从抓包分析可知，PPLive 可以同时兼容 TCP 和 UDP

方式，但以 UDP 传输方式为主。软件启动后，UDP 所占比率略低于 50%，选中某个节目正式开始播放时，TCP 所占比率急剧下降，UDP 逐渐增多，最终所占比率大于 70%，其中包含使用 UDP 封装的 STUN，WCCP，NBNS，QICQ 应用层协议和没有应用层的 UDP 协议，图 5 为其中的一次抓包结果。

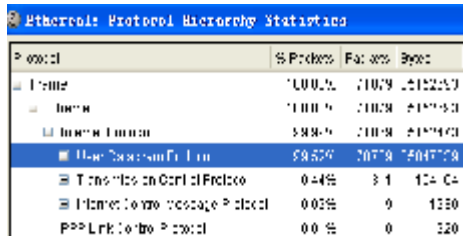


Figure 5. The result of a packet capture of PPLive
图 5. PPLive 的一次抓包结果

QQLive: QQLive 是一款由腾讯开发的网络电视软件。对抓包结果分析可知，QQLive 可以同时兼容 TCP 和 UDP 方式，但以 UDP 协议为主。软件启动后，UDP 较少（低于 5%），正式播放后，UDP 逐渐增多，最终所占比率大于 80%，其中包含使用 UDP 封装的 QICQ，STUN 应用层协议和没有应用层的 UDP 协议。图 6 为其中的一次抓包结果。

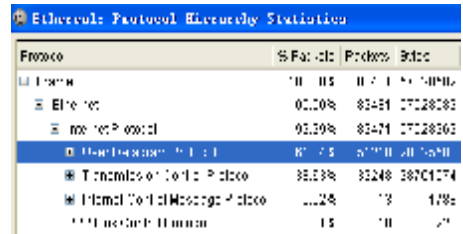


Figure 6. The result of a packet capture of QQLive
图 6. QQLive 的一次抓包结果

优酷网(YOUKU): 抓包分析后结果显示，UDP 协议所占比率很少（低于 5%）。图 7 为其中的一次抓包结果。

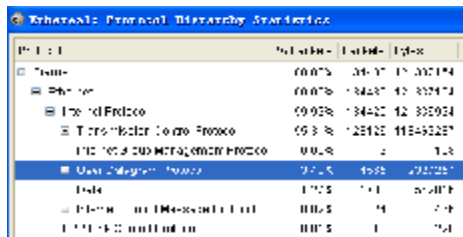


Figure 7. The result of a packet capture of YOUKU
图 7. 优酷网的一次抓包结果

土豆网(TuDou): 抓包分析可知，UDP 所占比率为 0，多次抓包都没有发现 UDP 报文。图 8 为其中的一次抓包结果。

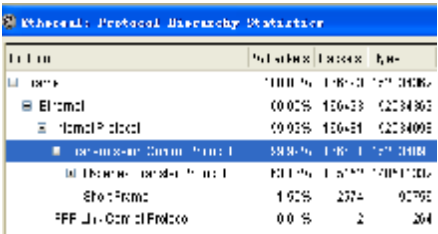


Figure 8. The result of a packet capture of TuDou
图 8. 土豆网的一次抓包结果

迅雷看看(XunLeiKankan): 迅雷公司出品的一款在线播放插件，采用 P2P 点对点传输技术。通过抓包分析可知，软件启动后，UDP 很少（低于 5%），正式播放某个节目后，UDP 逐渐增多，并占据绝对主流（大于 60%）。其中包含使用 UDP 封装的 DNS，ICQ，QICQ 协议和没有应用层的 UDP 协议。图 9 为其中的一次抓包结果。

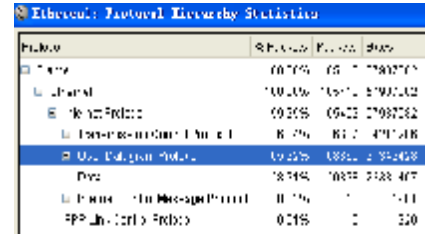


Figure 9. The result of a packet capture of XunLeiKankan
图 9. 迅雷看看的一次抓包结果

假定该类软件所产生的总流量为 x ，网络电视软件所占比率为软件的使用比率 R_1 ，软件的 UDP 协议所占比率为 R_2 ，记 $A(i) = R_1(i) \cdot x \cdot R_2(i)$ ；假设 PPStream，PPLive，QQLive，土豆，优酷，迅雷看看分别用 1，2，3，4，5，6 编号代表。

则在网络电视应用中，UDP 所占比率大致为

$$R = \frac{\sum_{j=1}^6 A(j)}{x} \quad (2)$$

代入各项数据可计算得 $R=80.2\%$

从抓包结果和 (2) 式运算结果可看出，PPStream，PPLive，QQLive 主要应用的是 UDP 协议进行电视节目播放。而优酷网和土豆网则主要是基于 TCP 协议传输。网络电视播放类软件的应用对于互联网中的 UDP

流量影响很大。

3.3 下载工具软件

下载工具软件几乎是每天必须要用到的。表 5 是天空软件站提供的常用下载工具软件^[6]:

Table 5. Some popular downloading softwares

表 5. 常用下载软件

软件	人气	所占比率
迅雷	152860330	78.58%
电骡 eMule	23595073	12.13%
比特彗星 BitComet	18059165	9.28%
uTorrent	116050	0.01%

因此选取了常见的迅雷，电驴，比特彗星和 uTorrent 来进行了抓包分析。结合 ethereal 统计结果，得出这四种软件的多次实验后的平均报文总数，平均 UDP 报文数以及所占比率，见表 6。

Table 6. The packet capture result of some downloading softwares

表 6. 常用下载工具抓包结果

软件名	抓包时间 (s)	报文总数	UDP 报文数	所占 比率
迅雷	287	127535.3	60264.3	46.79%
eMule	198.3	134636.7	2972.3	2.82%
BitComet	358.7	52747.3	5909	12.52%
uTorrent	262.7	66533.3	1063	1.60%

迅雷(Thunder): 在软件启动后，UDP 所占比率低于 50%，在正式开始下载时，UDP 逐渐增多，最终所占比率大于 50%。通过查看报文，其主要使用 UDP 封装的 MGCP，MSMMS，QICQ，eDonkey 应用层协议。图 10 为其中的一次抓包结果。

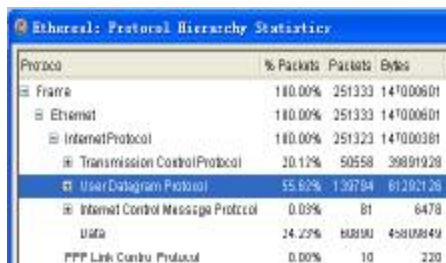


Figure 10. The result of a packet capture of Thunder

图 10. 迅雷的一次抓包结果

电骡(eMule): 在软件启动后，UDP 逐渐增多，所占比率大于 90%，正式下载后，UDP 逐渐减少，最终所占比率小于 5%。通过查看报文，其主要使用 UDP 封装的 eDonkey, HSRP, QUAKE 应用层协议和没有应用层的 UDP 协议。图 11 为其中的一次抓包结果。

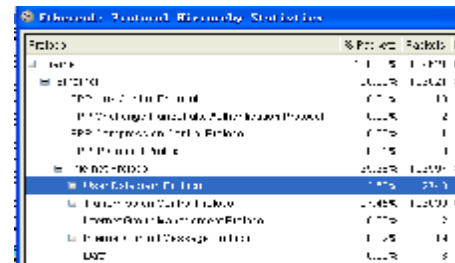


Figure 11. The result of a packet capture of eMule

图 11. 电骡的一次抓包结果

uTorrent: uTorrent 是一个免费 BitTorrent 软件。在软件启动后，UDP 逐渐增多，所占比率大于 90%，正式下载后，UDP 逐渐减少，最终所占比率小于 5%，图 12 为其中的一次抓包结果。

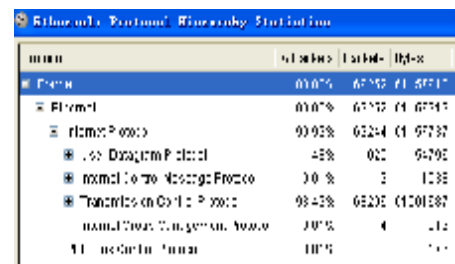


Figure 12. The result of a packet capture of uTorrent

图 12. uTorrent 的一次抓包结果

比特彗星(BitComet): 在软件启动后，UDP 逐渐增多，所占比率大于 90%，正式下载后，UDP 逐渐减少，最终所占比率低于 10%。图 13 为其中一次抓包结果。

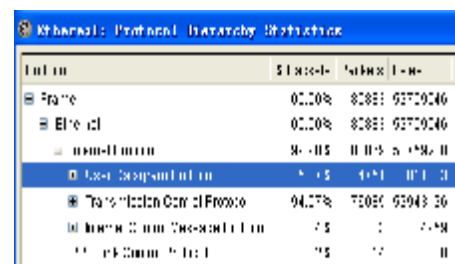


Figure 13. The result of a packet capture of BitComet

图 13. BitComet 的一次抓包结果

假定该类软件所产生的总流量为 x ，下载软件人气比率假定为软件的使用比率 R_1 ，软件的 UDP 协议所占比率为 R_2 ，记 $A(i) = R_1(i) \cdot x \cdot R_2(i)$ ；设迅雷，eMule，BitComet，uTorrent 分别用 1, 2, 3, 4 编号代表。

则在下载软件应用中，UDP 所占比率大致为

$$R = \frac{\sum_{j=1}^4 A(j)}{x} \quad (3)$$

代入各项数据可计算得 $R=38.3\%$

从抓包结果和(3)式运算结果可以看出，迅雷主要使用 UDP 协议进行传输，其他的下载软件如电骡，uTorrent，BitComet 使用 UDP 协议较少（低于 5%）。下载工具软件对于互联网中的 UDP 流量也是有很大影响的。

4 总结

通过对三种应用类型的软件的通讯报文抓包分析和数据处理，可以得出以下结论：

(1) 证实了网络中 UDP 流量占很大比率。

(2) 部分软件使用了特殊的应用层协议，这些应用层协议在传输层使用 UDP 进行传输，如 ICQ、QICQ、eDonkey 等应用层协议。

(3) 部分即时通讯软件，如 QQ；网络电视播放软件，如 PPStream，PPLive，QQLive，迅雷看看；下载软件，如迅雷等对互联网中的 UDP 流量影响巨大。

其原因一方面在于这些软件应用主要使用了 UDP 协议（通讯中 UDP 协议所占比率接近甚至超过 50%），另一方面由于这些软件应用有巨大的用户群。大量的用户群以及 UDP 协议的大量使用导致了网络中的 UDP 流量的剧增。

当然，本文中所列出的软件是有限的，还存在其他的软件应用对 UDP 流量有很大影响。但本文中所列出的实验结果对于研究互联网中 UDP 流量变化具有一定的参考作用。

References (参考文献)

- [1] 张艺瀚等，TCP 与 UDP 网络流量对比分析研究[J]，计算机应用研究，2010，27(6)，P2193.
- [2] 百度百科 http://baike.baidu.com/view/21943.htm?fr=ala0_1_1.
- [3] 李代玲，基于网络测量的 ppstream 网络电视系统研究[D]，北京：北京交通大学，2008
- [4] 2010 年 1 月即时通讯软件日均覆盖人数排名，<http://bjyouth.ynet.com/article.jsp?oid=66316023>
- [5] 本周网络电视排行

http://xiazai.zol.com.cn/download_order/sub_345.html

- [6] http://www.skycn.com/sort/sort2011200_down_times_DESC_1.html