# 基于 DPI 技术的网络电视监控系统设计

王跃红，余文
北京邮电大学计算机科学与技术学院，北京（100876）
E-mail：yuehong7@126.com , yuwen@tsinghua.org.cn

**摘　要：**随着网络电视与 P2P 技术的完美融合，网络电视的用户群日益壮大，人们在享受网络电视带来的流畅、高清、精彩的视频体验的同时，也会给宽带网络造成巨大的压力，导致网络拥塞。本文简单介绍 DPI 技术和 P2P 流量控制技术，剖析网络电视的通信机制，并采用 DPI 技术分析协议特征，最后给出一种网络电视监控系统--IPTV Detection System 的设计方案，该监控系统旨在检测并控制网络电视流量，释放网络带宽，缓解网络压力。

**关键词：**DPI；P2P；IPTV；协议分析
**中图分类号：**TP393

## 1. 引 言

网络电视以宽带网络为载体，以个人 PC 为终端，是互联网络技术与电视技术结合的新型媒体传播形式。目前流行的网络电视多数基于 P2P 的流媒体播放技术，利用 P2P 网络的优势，结合组播技术，直接连接到其他多个用户节点，一边下载一边播放，实现流畅、高质的在线视频。

根据 eMarketer 的统计资料[a)][1] ，到 2012 年，全球网络电视用户将达到六千一百万,随着网络电视技术的日趋成熟和市场的日益壮大，网络带宽承受着越来越大的压力，据德国互联网管理与分析公司 ipoque 的数据[2]显示，不同地区的 P2P 应用占据了 43%-70%的互联网流量，被视为“宽带杀手”，如何疏导并控制 P2P 应用，释放网络带宽已迫在眉睫。

## 2. 相关技术简介

### 2.1 DPI 技术

现在流行的 P2P 软件采用动态端口，常规的端口识别方法已不能准确地识别 P2P 应用，所以 DPI（Deep Packet Inspection）即深层数据包检测技术便应运而生。DPI 通过分析应用层负载数据，提取负载所包含的协议特征值，这些特征值存储在 Key Lib 中组成特征库，对网络上实时传输的数据流，采用模式匹配算法，符合 Key Lib 中协议特征的数据流即视为 P2P 某种应用。DPI 技术具有如下的优点和缺点[3]：

优点：DPI 技术扫描应用层数据，对协议特征进行精确模式匹配，因此误判率低，准确率高，且可以根据载荷特征准确划分 P2P 应用。此外，DPI 技术可以处理数据包丢失、重组等，能适应复杂的 P2P 应用。

缺点：DPI 技术通过分析报文的明文特征来识别协议，因此，对加密协议的分析就显得无能为力。随着 P2P 应用的不断发展，其协议特征也会随之改变，这就要求定期更新特征库，在特征库升级前可能无法检测新的 P2P 应用，具有一定的滞后性。另外，DPI 识别技术需要对报文进行解析还原和特征匹配，计算和存储开销较大。

### 2.2 P2P 流量控制技术

#### 2.2.1 直路串接流量控制模式

直路串接流控模式通常以透明模式采用二层透传或三层互联的方式串联在链路中，通过

丢弃需要限制的 P2P 数据包，可以方便的对不同类型的流量实施灵活的控制策略。直路串接流量控制的工作方式如图 1 所示[4]：

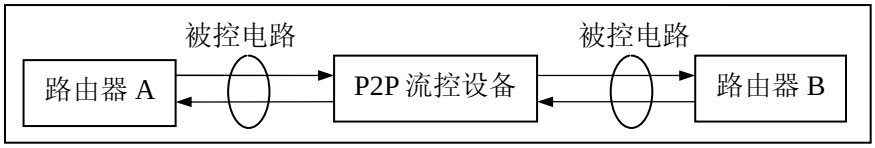


图 1 直路串接干扰电路

### 2.2.2 旁路干扰控制模式

旁路干扰控制模式采用数据包伪装技术，将干扰报文发到正在通信的 TCP、UDP 连接中，切断连接或降低数据传输速率，以达到流量控制的目的。旁路干扰控制方法分为 TCP 干扰和 UDP 干扰。TCP 干扰方式伪造并发送 RST/FIN 报文，拆除 TCP 连接。UDP 干扰方式伪造并发送 P2P 应用层特殊控制命令，截断 UDP 连接或降低 UDP 传输速率。旁路干扰流量控制的工作方式如图 2 所示[4]：

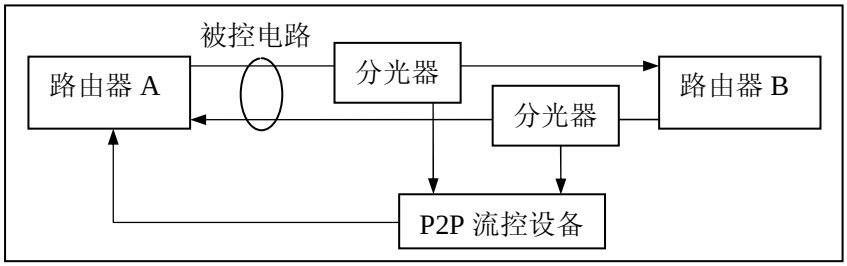


图 2 旁路干扰电路

## 3. 协议分析

### 3.1 网络电视通信机制

(1) 获取频道列表和广告信息

网络电视启动后，就会向服务器发起连接请求，获取节目的频道信息和广告信息。

以 PPLive 为例，客户端启动后，首先发出若干 DNS 请求，查询 PPLive 各服务器 IP 信息，如图 3 所示。获取服务器 IP 后，客户端向这些服务器发起 TCP 连接，请求频道列表和广告等信息。

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 4 | 0.365997 | 10.0.0.99 | 202.96.134.133 | DNS | Standard query A time.windows.com |
| 5 | 0.411226 | 202.96.134.133 | 10.0.0.99 | DNS | Standard query response CNAME time.microsoft.akadns.net A 207.46.197.32 |
| 6 | 0.422803 | 10.0.0.99 | 202.96.134.133 | DNS | Standard query A h.g1d.net |
| 8 | 0.467048 | 202.96.134.133 | 10.0.0.99 | DNS | Standard query response CNAME s.g1d.net.fastwebcdn.com A 124.225.112.204 A 61.15 |

图 3 PPLive 客户端发起 DNS 请求服务器信息

(2) 获取 Peer 信息

收看节目时，客户端向服务器提交节目信息，服务器返回拥有该节目资源的 Peer 信息。

(3) 与其他用户节点通信，传输数据

客户端获取 Peer 信息后，就会向这些 Peer 发起连接请求，将节目码发送给对方，对端会返回该节目的分块信息，双方开始数据传输。

### 3.2 协议特征分析

协议特征分为 UDP 特征和 TCP 特征，同时 UDP 和 TCP 特征又有上行下行之分。这里以 PPLive UDP 上行特征为例，采集多条 PPLive 数据样本，发现如下特征：

(1) 负载长度：68 字节；负载起始位置：2100

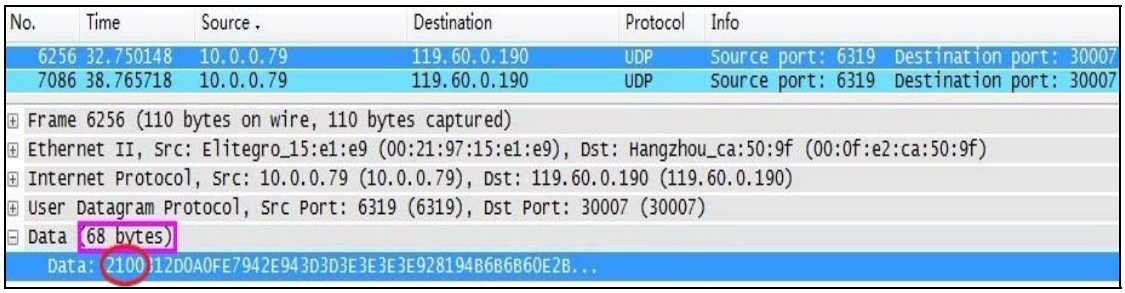


图 4 PPLive 协议 UDP 上行特征（1）

(2) 负载头部 8 字节处：0006000000；负载尾部 38 字节处：06000000；负载尾部 13 字节处：0001

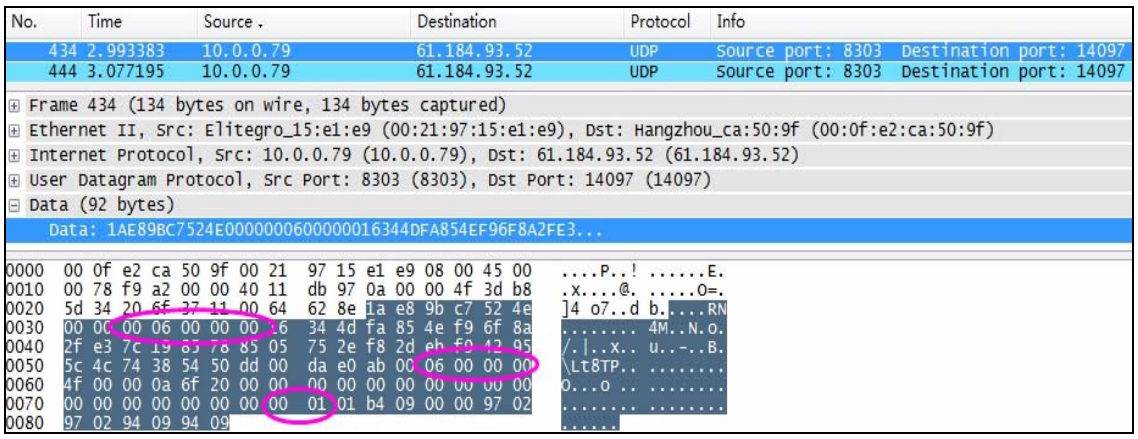


图 5 PPLive 协议 UDP 上行特征（2）

## 4. 网络监控系统的设计

### 4.1 模块设计

系统由 Data Collection , Protocol Detection 和 Strategy Management 三个模块组成。如图 6 所示：

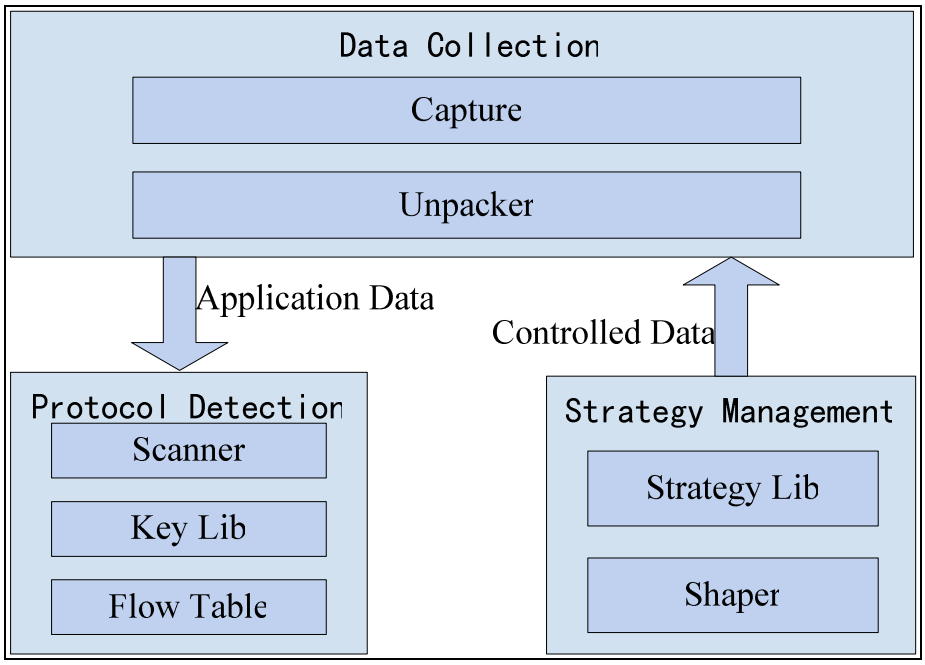


图 6 IPTVDS 系统架构图

#### 4.1.1Data Collection

该模块的功能是实时捕获网络数据流，并逐层剥离数据流头部信息，得到应用层数据。Data Collection 包含 Capture 和 Unpacketer 两个子模块。

Capture 采用 WinPcap 函数实现现网报文的实时捕获。[5]WinPcap 基于 Win32 平台提供一套标准的抓包接口，包括一个内核级网络数据包过滤器 NPF，低级动态链接库 packet.dll 和高级动态链接库 Wpcap.dll。WinPcap 通过NDIS（Network Driver Interface Specification）与网卡设备驱动交互,占用的系统资源较少,且与 Unix 下的 LibPcap 兼容。

Unpacketer 逐层剥离 Capture 模块捕获的以太帧，得到用户数据。根据网络七层协议，应用程序传送数据自上而下通过每一层时，都会对数据进行封装。Unpacketer 根据每层首部的固定长度和确切含义，解析捕获的以太帧。

#### 4.1.2 Protocol Detection

Protocol Detection 的主要功能是扫描 Unpacketer 解码的应用数据，与 Key Lib 的特征进行模式匹配，从而判断所获流量是否属于某网络电视协议。该模块由 Key Lib，Flow Table 和 Scanner 三个子模块组成。

Key Lib 是一个 XML 文件，用于存放各种协议的特征 Key。如前面分析的 PPLive，在提取完特征后，按照 Key Lib 约定的格式，将 PPLive 的特征写进 Key Lib。

Flow Table 用来存储已识别流量的五元组信息。如果后续数据流的源三元组或目的三元组信息与 Flow Table 中相同，则可以直接判定该流的识别结果，无需模式匹配 Key Lib，这样可以提升系统性能。Flow Table 需定时刷新。

Scanner 扫描 Unpacketer 解码的应用层数据报文，采用多模匹配算法，扫描 Key Lib 的特征记录，从而判断出该数据流的协议类型。

#### 4.1.3 Strategy Management

Strategy Management 的核心功能是对已识别出的网络电视流量进行干扰和控制。该模块

主要由 Strategy Lib 和 Shaper 两个子模块组成。

Strategy Lib 用于管理各种 IPTV 协议的控制方案，配置是否对某种协议进行控制，并设置上下行的带宽。

Shaper 采用旁路干扰控制模式，根据用户设置的控制方案，构造干扰报文并发送给网络电视的服务器和 Peer 用户，以限制 P2P 流量。构造干扰报文的思路主要有两种，一是伪造服务器发送错误的请求资源或 Peer 列表，二是在 Peer 两端伪造文件传输完毕。

## 4.2 系统流程

IPTVDS 工作流程（见图 7）如下：

(1) 系统启动后，Capture 实时捕获网卡上流经的数据流，并将捕获到的数据流传给 Unpacketer；

(2) Unpacketer 根据七层网络协议规范，逐层解析 Capture 传入的以太帧，剥离各层头部信息，得到的用户数据传递给 Scanner；

(3) Scanner 查询 Flow Table，若命中 Flow Table 的五元组信息，则直接显示识别结果；否则，模式匹配 Key Lib 中存储的各网络电视协议特征。

(4) 如果用户在 Strategy Lib 中配置了某种网络电视协议的控流选项，则 Shaper 根据配置，调用该协议的控制程序，向网络电视的服务器或 Peer 用户发送控制报文，以限制流量。

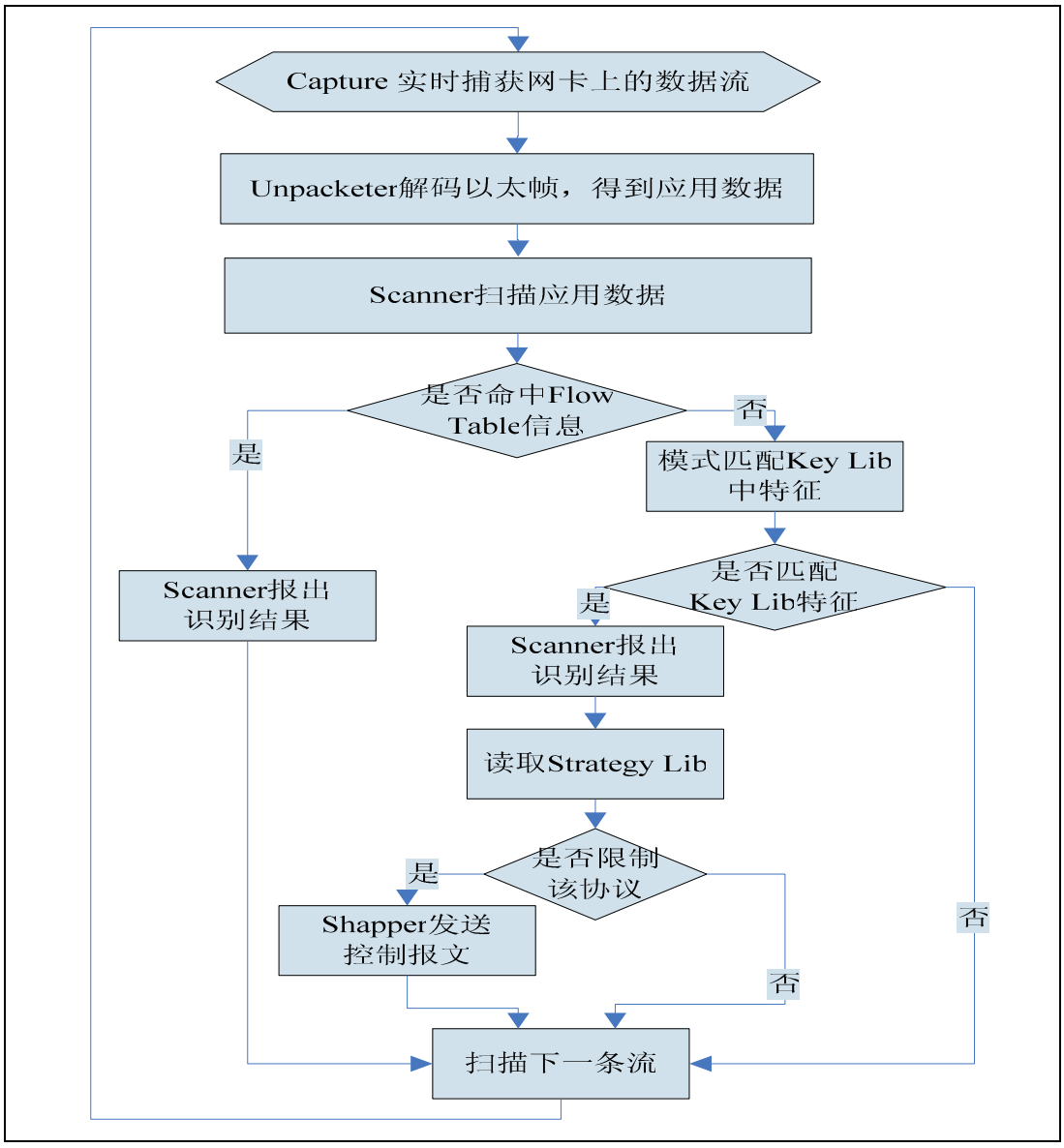


图 7 IPTVDS 系统流程图

## 5. 结束语

IPTVDS 采用 DPI 技术分析网络电视协议，随着网络电视的不断升级，协议的特征也会随之更新，为保证识别的精准度，需定期更新 Key Lib。为了减少重复劳动，提高协议分析的高效性和识别的准确性，可以开发一套特征自动化提取工具，这将是后续工作的主要研究方向。

### 参考文献

[1] eMarketer. Broadband Services: VoIP and IPTV Trends [EB/OL]. http://www.emarketer.com/Reports/All/Emarketer_2000393.aspx. 2008.
[2] Ipoque.Internet Study 2008/2009 [EB/OL]. http://www.ipoque.com/resources/internet-studies/internet-study-2008_2009. 2009.
[3] 刘强. P2P 流量监控技术研究与实现 [D]. 北京：北京邮电大学密码学专业，2007.
[4] 李芸. 流量识别与管控技术应用研究 [J]. 信息通信技术，2008，第五期：18-24.
[5] 张玮. 议分析的网络流量监测系统研究与开发 [D]. 湖南长沙：中南大学通信与信息系统专业，2008.

# The Design of IPTV Detection System Based on DPI

Wang Yuehong, Yu Wen
Computer Science and Technology School, Beijing University of Posts and Telecommunications, Beijing (100876), China

**Abstract**

Along with the integration of IPTV and P2P technique, the market of IPTV has presented prosperity and more and more people enjoy the experience of watching IPTV. While People watch the smooth and splendid video on internet, the broadband is suffering from huge pressure. This paper introduces DPI technology and P2P flow control technique firstly .Then, I analyze the correspondence mechanism and parse the characteristic of IPTV protocol. Finally, IPTV Detection System is designed for the purpose of examining and detecting IPTVs. IPTV Detection System will release network band width and alleviate pressure on the network.

**Keywords:** DPI; P2P; IPTV; Protocol Parsing