

文章编号: 1001-9081(2012)07-1816-04

doi: 10.3724/SP.J.1087.2012.01816

基于多粒度的自适应 UDP 流检测

李 宁*, 殷 宏, 许继恒, 王建民, 陈红跃

(解放军理工大学 工程兵工程学院, 南京 210007)

(* 通信作者电子邮箱 liningmayi@163.com)

摘要: 针对用户数据报协议(UDP)流检测研究不足, 其准确率和效率不高等问题, 提出一种基于多粒度的自适应 UDP 流检测方法。通过分析 UDP 流的特征, 设计两种不同粒度的动态超时策略, 对短流使用“细粒度”方法, 对长流采用多粒度结合的方法。与其他超时策略比较, 其准确率与固定超时相近, 内存约占其他方法的 75%。结果证实了方法适用于 UDP 流检测。

关键词: 用户数据报协议流; 流检测; 多粒度; 自适应方法

中图分类号: TP393.07 **文献标志码:**A

Adaptive UDP flow detection based on multi-granularity

LI Ning*, YIN Hong, XU Ji-heng, WANG Jian-min, CHEN Hong-yue

(Engineering Institute of Engineer Corps, PLA University of Science and Technology, Nanjing Jiangsu 210007, China)

Abstract: Concerning the lack of research on User Datagram Protocol (UDP) flow detection, and its low accuracy and efficiency, an adaptive UDP flow detection based on multi-granularity was proposed. Two different dynamic timeout strategies based on different granularity were designed by analyzing the characteristics of UDP flow. Compared with other timeout strategies, the accuracy of the proposed method was similar to the fixed timeout strategy, and the memory usage was only about 75% of the others. The experimental results show that the proposed method is suitable to the UDP flow detection.

Key words: User Datagram Protocol (UDP) flow; flow detection; multi-granularity; adaptive method

0 引言

互联网出现的 40 多年间, 网络行为模式日益复杂, 传统的基于文字和图片的网络服务已经不能满足人们的需求, 越来越多的音/视频、在线游戏等内容生动、互动性强的网络应用开始成为网络的主体, 导致网络流量剧增。Cisco 2011 可视网络索引(Visual Networking Index, VNI)年度报告预测, 2015 年全球互联网总流量将达到目前的 4 倍, 约 966 EB, 仅 2014 年一年的增长就会超过 2010 年全球 IP 流量的总和^[1]。因此, 对网络流量的分析变得更加重要。

传输层网络流量由传输控制协议(Transmission Control Protocol, TCP)和用户数据报协议(User Datagram Protocol, UDP)两种协议承载。TCP 是面向连接的可靠的传输协议; UDP 是无连接的传输协议。TCP 一直占据网络流量较大比重, 但随着新型网络服务的发展 UDP 流量也在迅猛增加。音/视频通信、网络电视、在线游戏等应用, 要求用较少的资源支持较多用户的实时应用, 冗余性较强, 对个别数据包丢失不敏感, UDP 是一个很好的选择。Mena 等^[2]研究发现 60% 到 80% 的音频数据流都是通过 UDP 进行传输, 控制命令的传输使用 TCP 协议。近年的研究发现, VoIP、非 Web 的聊天系统(如 ICQ 和 AM)以及大量的第一人称视角的网络游戏^[3-5]绝大多数使用 UDP 进行网络传输。可见, UDP 作为一种重要的底层传输协议正被越来越多的使用。

网络流量的分析按照测量粒度可分为: 比特级(Bit-level,

关注流量的数据特征)、分组级(Packet-level, 关注 IP 分组的特征)和流级(Flow-level, 关注流的特征)^[6]。目前, 基于流的网络流量分析已成为发展的趋势。传统流量分析主要关注 TCP 协议, 针对 UDP 研究很少。但随着 UDP 流量的不断增加, UDP 流量分析变得非常重要。UDP 流检测作为 UDP 基于流的流量分析基础, 成为首要解决的问题。因此, 本文将提出一种基于多粒度的自适应 UDP 流检测(adaptive UDP flow detection based on multi-granularity, MGAD)方法, 保证 UDP 流检测的效率和准确率。

1 流检测研究现状

1.1 流的定义和分类

流的定义最早可以追溯到 1992 年由 Patridge^[7]提出的: 流是主机向网络请求服务使用的一种数据结构; 随着对流的关注, 人们根据需求定义了各种流, 如 CAID^[8], NetFlow^[9]。其中使用最广泛的是 Cisco 的 NetFlow V5 对流的定义: 流是一个单一方向的在源和目的端之间的一系列数据包(端点是由 IP、端口以及传输层协议来定义的); 还有一种定义是按照流的获取方式来定义, 即 Olivier 等^[10]提出的: 一系列时间间隔没有超过超时值的数据包作为一个流。

流按协议栈层次分可以分为四种: 数据链路层流、网络层流、传输层流以及应用层流。同时, 各层次的流又可以按具体协议来划分, 如传输层流可以分为 TCP 流和 UDP 流, 应用层流的分类就更多了, 如超文本传送协议(Hypertext Transport

收稿日期: 2012-01-13; 修回日期: 2012-03-02。 基金项目: 国家自然科学基金资助项目(70971137)。

作者简介: 李宁(1986-), 男, 山东诸城人, 硕士研究生, 主要研究方向: 军事仿真、军用数据及知识工程; 殷宏(1967-), 男, 安徽黄山人, 副教授, 博士, 主要研究方向: 军事仿真、虚拟现实; 许继恒(1976-), 男, 陕西咸阳人, 副教授, 博士, 主要研究方向: 军事仿真、虚拟现实; 王建民(1985-), 男, 河北邯郸人, 硕士研究生, 主要研究方向: 军事仿真、虚拟现实; 陈红跃(1986-), 男, 河南许昌人, 硕士研究生, 主要研究方向: 联合作战演练系统分析。

Protocol, HTTP) 流、文件传输协议 (File Transfer Protocol, FTP) 流、实时传输协议 (Real-time Transport Protocol, RTP) 流等。目前, 研究的主要集中在传输层流和应用层流, 应用层流主要用来分析具体的网络应用, 需要传输层流来支持, 通过传输层维持流状态。本文针对传输层流进行分析, 包括 TCP 流和 UDP 流。

1.2 流检测的定义和方法

所谓流检测, 是指在从网络大量数据包中检测出各种有规律的流数据。

目前, 流的检测主要有两种方法。1) 标识识别。以 TCP 流为例, TCP 是面向连接的协议, 以三次握手作为连接的开始, 四次握手作为连接的结束。则可以根据握手的标志信息来识别流的开始和结束, 如果交互数据包中含有同步 (Synchronize, SYN) 标志, 则认为是新流的开始, 当数据包中出现结束 (Finish, FIN) 或者重置连接 (Reset the connection, RST) 标志时, 则认为是流结束的标志。2) 超时时间。TCP 流检测当发现不了流标志时也需要用超时来判断, 是两种方法的结合。UDP 是无连接协议, 也没有流标志可以使用, 当每一个数据包到来, 如果没有 UDP 流与该包对应, 则认为是 UDP 流的开始, 对于 UDP 流的结束则只能通过超时来判断。

基于超时的流检测方法有很多种, 目前的研究主要集中在设计合理的超时策略以提供及时准确、资源占用少的流检测。最早的方法是在 1994 年由 Claffy^[11-12] 提出的基于固定超时策略 (Fixed timeout strategy, FIX) 的流检测, 其通过实验证明了这种方法的正确性和优点, 目前已成为各种流检测方法的标准。但是它没有区分流的不同类型, 即短流和长流, 固定超时策略需将超时值设为较大值才能准确地检测出流, 使得一些已经结束的流在内存中保存很长时间, 对于系统资源是很大的浪费。超时值设置过小, 会把一些长流错误的截断为多个流, 造成识别结果的不准确。

固定超时的不足引发了对自适应流检测 (即动态超时的流检测) 的研究。2001 年 Ryu 等^[13] 提出了一种基于测量的二进制指数超时 (Measurement-based Binary Exponential Timeout, MBET) 策略, 其根据一定时间段内的数据包的吞吐量来动态改变 (保持或减小) 超时值, 一定程度上减少了对资源的浪费。但是有一个缺点: 一旦超时值减小, 就不会增加, 这使得将长流截断成多个短流的几率大大增加。

Wang 等^[14] 中提出一种可能性保证的适应超时策略 (Probability-Guaranteed Adaptive Timeout algorithm, PGAT), 针对不同应用类型的流, 分析其速度规律, 然后通过一系列参数值来精细控制流的超时, 如流产生的比例和流的完整率等。该策略需要对流的类型作分析和判断, 主要适用于对长流的检测, 对短流没有作相关优化, 而且策略在实现方面比较复杂, 其所需的时间复杂度有待深入分析。

周明中等^[15] 提出一种动态超时策略 (Dynamical Timeout Strategy, DToS), 是包标记和 MBET 结合的策略, 对 TCP 根据数据包标记信息和超时来检测 TCP 流, 对 UDP 则通过 MBET 超时策略来判断 UDP 流, 并通过综合分析网络使用状况, 根据流的长度设置不同的超时初始值, 并能为突发流量报警。该方法同样存在 MBET 的一些不足。

2010 年, Cai 等^[16] 提出了基于支持向量机 (Support Vector Machine, SVM) 的动态超时检测方法, 使用最大时间间隔作为超时值, 利用 SVM 分类。但这种方法需要提前训练, 对训练样本要求较高, 其对结果影响较大。

以上方法大多是基于 TCP 流和 UDP 流共同设计的, 并且存在各种不足, 如造成资源浪费, 检测结果不准确等问题。随着新型网络应用的不断出现, TCP “绝对优势” 的地位会被 UDP 撼动, UDP 会成为影响网络流量的一个重要因素。而 UDP 无连接的特征也使得难以使用当前 TCP 检测的方法和技术。因此, UDP 流检测作为 UDP 流量分析的第一步, 正成为流量分析要解决的热点问题。

2 基于多粒度的自适应 UDP 流检测模型

一般基于流的流量分析主要包括三部分: 流产生部分、流存储部分和流量分析部分。流产生部分主要作用在检测点, 通过流量镜像获取数据包, 检测出流信息; 流存储部分将检测到的流收集和存储; 流量分析部分就是流量分析的过程, 根据获得的包到达的频率以及流的数量来进行流量分析。可见, 流检测作为流量分析的基础, 是不可缺少的一部分。

2.1 UDP 流分析

在进行 UDP 流分析之前, 先按照流的检测方法给出本文关于流的定义。

定义 1 流是指在源和目的端点之间一段连续的时间内受标志或超时影响的一系列数据包的集合。

这里的流是双向的, 端点之间所有的交互数据包都看作是流的一部分。

对北京教育网主节点的流量进行 24 h 的统计, 传输速率约为 100 Mbps, 其中 UDP 流量约占 25%。对 UDP 时间间隔分布和流数量分布进行了分析。

UDP 时间间隔分布 使用固定超时策略对 UDP 时间间隔分布进行分析, 设置固定超时值为 120 s。结果如表 1 在所有的 481 745 291 个时间间隔中只有 0.86% 的时间间隔大于 30 s, 并且大多数的时间间隔分布在 0 s 到 10 s 之间, 其中 1 s 内的时间间隔约占 84.77%, 1 s ~ 10 s 约占 12.17%。可见, UDP 流时间间隔绝大部分都很小。

表 1 时间间隔分布

时间间隔/s	数量	时间间隔/s	数量
≤10	466 991 855	(30, 60]	4 149 184
(10, 30]	10 584 107	>60	20 145

UDP 流分布 本文按每个流中包的数目对流进行划分, 分为四种类型, 统计结果如表 2 所示, 可见网络中存在大量的单包或者双包流, 可能是 DNS 查询或者心跳包等, 包数量小于 8 的流约占总流的 91.5%, 其长流数量很少。以 8 个包作为界限, 8 包以上的流字节约为 242 989.3 MB, 占总字节长度的 90.6%。

表 2 UDP 流分布

流类型	数量	流类型	数量
1 ~ 2	51 199 558	9 ~ 12	1 983 499
3 ~ 8	15 691 724	>12	3 171 704

Fang 等^[17] 对骨干网流量数据进行了分析, 发现在 AS 之间占总数 9% 的流承载了 90% 的流量, 满足重尾数分布。UDP 流同样满足这一规律。

2.2 自适应 UDP 超时策略

UDP 动态超时策略一般使用固定时间段 T 内的流量信息作为超时值改变的依据, 通过固定时间段内其网络参数的变化, 动态修改超时值, 一定程度上达到了动态的效果。但存在

三方面问题:首先, T 需要一个特定的时钟监测, 实现较繁琐;其次, T 内第一个和最后一个数据包的到达时间与 T 的边界有一定的时间间隔, 会造成一定误差;再次, 使用固定时间段的动态超时测量对流量变化不敏感, 遇到流量突增时, 反应速度较慢, 不够准确及时。

与其他动态超时检测方法不同, 本文提出了两种超时调节方法。分别从“微观”和“宏观”两种不同粒度调节超时值, 二者相互补充, 既有“细粒度”实时的动态超时又有“粗粒度”时间段内的动态超时, 形成了准确、及时的超时策略, 节省了资源。

1) “细粒度”方法。

每次包到达之后, 将时间间隔 T_i 与超时值 T_o 对比。 T_i 为每个包到来时的时间间隔, T_o 为使用“粗粒度”方法获得的超时值。设 $K(0 < K < 1)$ 为超时变化阈值, $P = T_i/T_o$, 则:

$$T'_o = \begin{cases} T_o * (1 + P - K), & P > K \\ T_o, & P \leq K \end{cases}$$

可以看出, 当 T_i 与 T_o 接近时, T'_o 会适当增加, 越接近, 增加的值越大;当 T_i 小于 T_o 时, 返回到原 T_o , 即使 T_o 已经通过微观方法改变。“微观”方法能更实时改变 T_o 值, 避免突发间隔变化造成的流截断情况。

2) “粗粒度”方法。

“宏观”方法上的时间段与前面固定时间段不同, 按照最近 N 个数据包的信息来分析超时的变化, 其时间段是动态的, 与包到达的速率有关。其优势是不需要单独的时钟检测时间段 T 是否到达, 处理更加简单。这里有两个定义, 如下。

1) 包速率:

$$pkt_per_s = N / (t_s - t_e)$$

2) 流速率:

$$byte_per_s = \sum_{i=0}^{i < N} B_i / (t_s - t_e)$$

则平均时间间隔 i 可表示为:

$$i = 1 / pkt_per_s$$

包速率和流速率分别表示 N 个数据包时间段内平均每秒到达的包数目和比特值, t_s, t_e 分别为本阶段第一个包和最后一个包到达的时间, B_i 为包的大小。

UDP 流具有流的共同特征:流时间间隔越大, 吞吐量越小, 越平稳;反之, 则易发生突发状况。因此, 本文将时间间隔以及流吞吐量作为标准, 同时考虑时间间隔的波动情况, 提出“粗粒度”的方法。

平均时间间隔 I 和流吞吐量(即流速率) P 按照流量分为 k 个等级, 分别为 $\{i_1, i_2, \dots, i_k\}$ 和 $\{p_1, p_2, \dots, p_k\}$ 。对于 I 为每一个等级按升序与集合 $A = \{a_1, a_2, \dots, a_k\}$ 建立降序的一一映射;流吞吐量则按升序与集合 $B = \{b_k, b_{k-1}, \dots, b_1\}$ 建立升序一一映射。集合 A, B 中的元素作为超时参数。当时间间隔为 i_x , 流吞吐量 p_y , 则超时参数 μ 可表示为:

$$\mu = a_x \cdot b_y$$

例如: 时间间隔 $\{<10 \text{ s}, 10 \sim 30 \text{ s}, >30 \text{ s}\}$ 对应参数 $\{3, 2, 1\}$, 吞吐量 $\{<10 \text{ Bps}, 10 \sim 30 \text{ Bps}, >30 \text{ Bps}\}$ 对应参数 $\{1, 2, 3\}$ 。当时间间隔为 $10 \sim 30 \text{ s}$, 吞吐量 $<10 \text{ Bps}$ 时, 则 μ 为 6。超时参数能反映流的平稳程度, 越小表示流越平稳。

时间间隔的波动情况, 可以由 w 和 v 两个参数表示, 分别代表超时值 T_o 与平均时间间隔以及超时值与最大时间间隔的比值。表示如下:

$$w = T_o / \bar{T}$$

$$v = T_o / T_m$$

“粗粒度”的方法根据 w 表示如下(T_b 为流的最大超时阈值)。

1) 当 $1 < w < 2$ 时, 则 $T_o = \min\{\mu \cdot T_m, T_b\}$ 。

2) 当 $2 \leq w < 4$ 时, 若 $1 < v < 2$, 则 $T_o = \min\{\mu \cdot T_m, T_b\}$; 否则, T_o 保持不变。

3) 当 $w \geq 4$ 时, 则 $T_o = \min\{\max\left\{\frac{T_o \cdot \mu}{2 \cdot a_1 \cdot b_k}, 2 \cdot T_m\right\}, T_b\}$ 。

2.3 基于多粒度的自适应 UDP 流检测方法

前面提出了“细粒度”和“粗粒度”两种超时策略, 由 UDP 流的分析可知, UDP 流中短流占据了大部分, 数据包时间间隔一般分布在 $0 \sim 30 \text{ s}$ 。可以将流分为短流和长流两类分别分析, 根据短流和长流的不同特征, 使用不同的自适应超时策略, 能更准确且更节省资源。

首先, 设置初始值。短流: 包含数据包数目 $\leq N_f$, 初始超时值 T_s ; 长流: 初始超时值 T_l , 设置平均时间间隔 I 和流吞吐量 P 以及对应的参数集合 A, B ; 设置“粗粒度”超时处理包的数目 N_f 。

其次, 当一个数据包到达, 包总数和临时包数目均加 1, 同时统计流量等信息, 然后:

1) 检查包总数目是否等于 $N_f + 1$, 是则将初始时间值设置为 T_l (长流)。

2) 检查临时包数目是否等于 N_f , 是则计算 pkt_per_s 和 $byte_per_s$, 按照“粗粒度”策略计算 T_o , 再按“细粒度”策略计算超时值, 临时包数目置 0; 否则, 则按照按“细粒度”策略计算超时值。

3) 若包总数目 $\leq N_f$, 先执行 2), 然后利用“细粒度”策略计算超时值(短流)。

4) 若包总数目 $> N_f + 1$, 则执行 2), 计算超时值。

最后, 当时间内没有数据包到达, 则认为该流超时, 结束该流, 将其信息保存。

本文方法相对于固定超时, 在资源利用方面, 每个流只是增加了超时值 T_o 、临时包个数 N_f 、包速率 pkt_per_s 、平均流速率 $byte_per_s$ 以及最大时间间隔 T_m 等 5 个变量的存储; 相对于动态超时节省出的资源, 基本可以忽略。

在时间复杂度方面, 对于超时值的判断, 与固定超时相同。在包处理过程中, 由于要计算临时包个数、速率等变量, 由固定超时的 $O(n)$ 变为 $O(c \cdot n)$, 其中 c 为常量。可见, 基于多粒度的自适应 UDP 流检测方法(MGAD)的时间消耗基本接近固定超时方法。

3 实验结果

MGAD 的正确性及优越性需要实验进行验证, 本文进行了一系列实验, 并与固定超时策略以及基于测量的二进制指数超时策略进行对比。

使用一个 40 GB 约一小时的离线数据包来测试, 经统计 UDP 数据包约占数据包总量的 36%, 而流量占总流量的 26%。

根据前面时间间隔分布和流分布的分析, 设置静态超时值为 32 s, 并且与 FIX、MBET 进行了对比。固定超时的固定超时值设置为 64 s; MBET 的参数设置: T_o 设置为 8 s, S 设置成 3 个等级, 集合 R 由 $\{64, 32, 16\}$ 组成; MGAD 参数设置: 长短流的分界 N_f 设为 8, 短流的初始超时值 T_s 为 16 s, 最大超时

值 32 s, 长流初始超时值 32 s, 最大超时值 64 s, 粗粒度方法中 $I = \{ < 10 \text{ s}, 10 \sim 30 \text{ s}, > 30 \text{ s} \}$, $P = \{ < 10 \text{ Bps}, 10 \sim 50 \text{ Bps}, > 50 \text{ Bps} \}$, 其参数集合 $A = \{3, 2, 1\}$, $B = \{1, 2, 3\}$, 处理包数目 N 为 8。

从表 3 可以看出, MBET 长流数目明显多于其他两者, 比固定超时策略多大约 17%, 说明 MBET 不太适合处理 UDP 流, 主要原因是 UDP 流不稳定的, 包传输过程中乱序和丢包较严重。当超时值到达最小超时值时, 超时值不能根据实际情况增加, 对突发状况(如一定时间内丢包较严重造成的时间间隔变大)的处理不利, 易造成长流被截断成多个长流或者短流。MGAD 与固定超时的流在各方面均非常接近, 长流仅多出约 1.3%, 说明 MGAD 方法在 UDP 流检测的准确性是可以保证的。

表 3 UDP 流数目

流类型	FIX	MBET	MGAD
长流	78 290	91 482	79 326
短流	1964 794	1998 016	1980 423
总数	2043 084	2089 498	2059 749

三种策略的内存使用情况如图 1 所示, 横坐标代表时间轴, 单位为 40 s(即每 40 s 测量一次数据), 纵坐标为每时刻上占用的内存大小。从图中可以清晰地看出, 固定超时策略(FIX)占用内存最多; MBET 与固定超时相差不多, 但波动较大, 一定程度上也反映了其处理 UDP 流不够稳定; MGAD 内存占用最少, 约占固定超时的 75%, 且比较平稳。

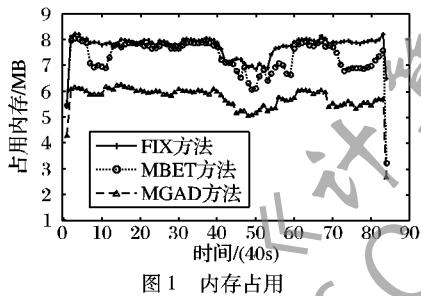


图 1 内存占用

图 2 表示 MGAD 策略的实时流的分布的情况, 横坐标含义与图 1 相同, 纵坐标代表每时刻流的数目。可以看出, 短流实时数目占流实时总数的绝大多数, 流数目波动较严重, 且影响实时总流的波动情况, 而长流的实时数目占的比例很少, 且相对稳定。

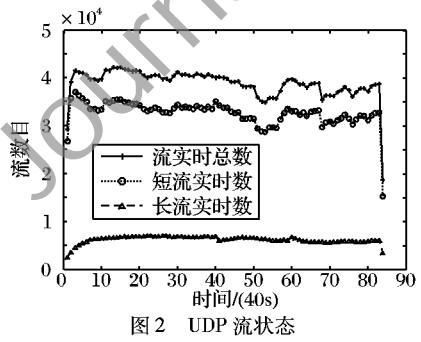


图 2 UDP 流状态

4 结语

UDP 流检测作为 UDP 流量分析的第一步也是必需的一步, 已经越来越受到人们的关注, 但目前的方法一般都基于 TCP 协议。本文提出的基于多粒度的自适应 UDP 流检测方法将“细粒度”和“粗粒度”两种不同粒度的方法结合, 分别从宏观和微观上动态调节 UDP 超时时间, 并根据流长度的不同

使用不同的粒度, 满足自适应的性质。UDP 流量分析逐渐成为流量分析研究的重点, UDP 流量的检测成为首要解决的难题, 本文方法在准确性和资源利用方面都具有很大的优势, 对于 UDP 流分析有很大的作用和意义。后续可以使用该方法研究具体的 UDP 应用层协议特征, 或者利用统计学或者人工智能的方法研究 UDP 流量特征, 以更好地分析和管理 UDP 流量。

参考文献:

- [1] CISCO. Cisco visual networking index: forecast and methodology 2010 – 2015 [EB/OL]. [2011 – 12 – 28]. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf.
- [2] MENA A, HEIDEMANN J. An empirical study of real audio traffic [C]// INFOCOM 2000: Proceedings of the 9th Annual Joint Conference of the IEEE Computer and Communications Societies. Piscataway: IEEE, 2000: 101 – 110.
- [3] BONFIGLIO D, MELLIA M, MEO M, et al. Tracking down skype traffic [C]// INFOCOM 2008: Proceedings of the 27th Conference on Computer Communications. Piscataway: IEEE, 2008: 261 – 265.
- [4] DEWES C, WICHMANN A, FELDMANN A. An analysis of Internet chat systems [C]// SIGCOMM 2003: Proceedings of the 3rd Conference on Internet Measurement. New York: ACM, 2003: 51 – 64.
- [5] FENG WU-CHANG, CHANG F, FENG WU-CHI, et al. A traffic characterization of popular online games [J]. IEEE/ACM Transactions on Networking, 2005, 13(3): 488 – 499.
- [6] 苗娟迎, 马力. 网络流量分析方法综述[J]. 西安邮电学院学报, 2010, 15(4): 20 – 23.
- [7] PATRIDGE C. RFC 1363, A proposed flow specification [S]. Lenexa, KS: IETF, 1992: 1 – 19.
- [8] CAIDA. Preliminary measurement specifications for Internet routers [EB/OL]. [2011 – 12 – 28]. <http://www.caida.org/tools/measurement/measurement-spec/>.
- [9] CISCO. NetFlow services and applications white paper [EB/OL]. [2011 – 12 – 28]. http://mauigateway.com/~surfer/library/netflow_wp.pdf.
- [10] OLIVIER P, BENAMEUR N. Flow level IP traffic characterization [C]// Proceedings of the 17th International Teletraffic Congress. Salvador da Bahia, Brazil: Elsevier Science, 2001: 25 – 36.
- [11] CLAFFY K C. Internet traffic characterization [D]. SanDiego: University of California, 1994.
- [12] CLAFFY K C, BRAUN W H, POLYZOS G C. A parameterizable methodology for Internet traffic flow profiling [J]. IEEE Journal on Selected Areas in Communications, 1995, 13(8): 1481 – 1494.
- [13] RYU B, CHENEY D, BRAUN W H. Internet flow characterization: adaptive timeout strategy and statistical modeling [C]// Proceedings of Passive and Active Measurement Workshop 2001. Berlin: Springer, 2001: 45 – 57.
- [14] WANG JUN-FENG, LI LEI, SUN FU-CHUN, et al. A probability-guaranteed adaptive timeout algorithm for high-speed network flow detection [J]. Computer Networks, 2005, 48(2): 215 – 233.
- [15] 周明中, 龚俭, 丁伟. 高速网络中基于流速测度的动态超时策略 [J]. 软件学报, 2005, 16(5): 562 – 568.
- [16] CAI JING, ZHANG ZHI-BIN, ZHANG PENG, et al. An adaptive timeout strategy for UDP flows using SVMs [C]// Proceedings of Parallel and Distributed Computing, Applications and Technologies. Piscataway: IEEE, 2010: 118 – 127.
- [17] FAN G WEN-JIA, PETERSON L. Inter-AS traffic patterns and their implications [C]// Proceedings of IEEE Global Telecommunications Conference. Piscataway: IEEE, 1999: 1859 – 1868.