



基于 Hadoop 的网络分流和流特征计算 *

刘 勇^{1,3}, 雒江涛^{1,2,3}, 邓生雄^{1,3}, 王小平^{1,3}

(1.重庆市高校通信网测试技术工程研究中心 重庆 400065;

2.重庆邮电大学电子信息与网络工程研究院 重庆 400065;

3.重庆邮电大学通信与信息工程学院 重庆 400065)

摘 要:网络流量特征计算是网络流量分析的一个重要步骤,对于海量网络流量数据,并行化计算网络流量特征是高效网络流量分析的重要方法。针对传统单机处理成本高、可扩展性差的问题,提出一种基于 MapReduce 编程模型的网络流量分析方法,并行实现网络分流和流量特征计算。通过使用 Hadoop 平台对实际数据进行分析,统计常用网络流量属性特征,实验表明,该方法分析网络流量特征的结果准确可信,且适合分析大流量数据。

关键词: MapReduce; 网络分流; 特征; 并行计算

doi: 10.3969/j.issn.1000-0801.2014.12.011

Diffluent Internet Traffic and Characteristics Computation Based on Hadoop

Liu Yong^{1,3}, Luo Jiangtao^{1,2,3}, Deng Shengxiong^{1,3}, Wang Xiaoping^{1,3}

(1.Chongqing Municipal Engineering Research Center of Institutions of Higher Education on Communication Network Testing Technology, Chongqing 400065, China; 2.Electronic Information and Networking Research Institute, Chongqing University of Posts and Telecommunications, Chongqing 400065, China; 3.School of Communication & Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: Internet traffic characteristics computation is an important step of internet traffic analysis, in the face of massive internet traffic data, parallel computing internet traffic characteristics is base to prompt the performance of internet traffic analysis. In order to solve the problems of poor expansibility and high cost that caused by the traditional stand-alone, an internet traffic characteristics analysis method based on MapReduce, which parallel processes diffluent internet traffic and characteristics computing, was proposed. By using the Hadoop platform, the actual data was analyzed and the common internet traffic characteristics were computed. Experiments show that the method is reliable to analyze the characteristic of the internet traffic and it is suitable for analyzing large traffic data.

Key words: MapReduce, diffluent internet traffic, characteristic, parallel computing

1 引言

随着互联网的发展,网络流量分析在诸多方面得到了应用,利用网络流量特征信息可统计网络负荷、检测通信

质量、预测网络流量以及分类网络流量等,网络流量分析是准确检测管理和控制网络的基础。参考文献[1]表明,基于数据流和抽样方法是流量测量中的主要方法,其中抽样方法虽减少了负荷,但误差性较大,数据流在缩减原始分

* 重庆市应用开发计划基金资助项目 (No.estc2013yykfA40006)

组数据量的同时，也保留了流量分析可控的重要信息，这些重要信息就是网络流量的流特征。

网络数据流指由源 IP 地址、目的 IP 地址、源端口号、目的端口号和协议组成的五元组相同的数据分组集合^[2]，流量特征是指数据流的数据分组大小分布、时间、特征字段等信息。流量流特征统计是网络流量流分析的基础和有效分析的前提，广泛用于流量统计、异常流量检测、流量预测和机器学习流量分类等。随着互联网的快速发展，利用传统单机散列(hash)聚合^[3]的方式进行网络级分流和特征计算时，需要占用大量 CPU、内存和硬盘等硬件资源，且可扩展性较差，单机的处理方式已慢慢不能适应网络数据的快速膨胀^[1]，为此，本文提出了一种分布式处理方法，采用 MapReduce 模型实现网络流量分流和流特征计算。

MapReduce 模型是 Hadoop^[4]的核心计算模式，是一种分布式处理海量数据的可靠方法。Lee Y 等人^[5]提出了一种处理 libpcap(packet capture library, 分组捕获函数库)文件流的方法，可直接利用 Hadoop 处理二进制 libpcap 数据文件。参考文献[6]设计了基于 Hadoop 的离线数据处理系统，但输入数据为已预处理完毕的流文本数据，缺少并行网络流量聚合处理。利用 Hadoop 平台分析数据的应用很多，然而使用 MapReduce 算法聚合网络数据流、计算流量特征的相对较少。一方面，研究主要针对上层应用的较多，忽略了数据的预处理；另一方面，MapReduce 本身的特性给网络分流带来了一定的麻烦。

本文借用散列思想将同一五元组的网络流通过 MapReduce 任务机制分配到同一数据节点处理，解决了传统散列表对高速海量网络流量分析不足的问题，弥补了分布式流量分析非一体化的缺陷，为网络流量统计、异常流量检测、流量预测和机器学习流量分类等技术提供了一种并行化流量预处理的方法。本文首先介绍待计算的流量特征和采用的数据处理框架；然后详细分析该方法的具体实

现算法；最后利用实验平台对此方法进行验证分析，总结并提出下一步工作。

2 流量特征的计算

2.1 流量属性特征的选取

在网络链路上，流量由很多不同的网络流聚合而成。参考文献[5]将数据报文分成双向 TCP(transmission control protocol, 传输控制协议)或 UDP(user data protocol, 用户数据报协议)流，将与客户端具有相同五元组信息的数据报文称为前向子流，与服务器方有相同五元组信息的报文称为后向子流。

研究中发现，通常使用流中数据分组的净荷大小、大小分布、标志位信息、持续时间分布以及数据分组间隔、时间抖动等作为网络分析的主要特征。参考文献[2]采用了流的 248 个特征对网络流量进行分类；参考文献[7]使用流中的 SYN 和 FIN 数据分组个数，预测泛洪型分布式拒绝服务攻击(DDoS)。参考文献[2]和参考文献[7~10]均对网络流量分析中较常用的流量属性特征进行了统计计算。

2.2 流量分析模型

流量分析模型的核心任务是分析网络流量，并计算表1中的流量特征，以便上层应用分析。流量分析模型的具体框架如图1所示。

模型整体是基于 Hadoop 平台部署运行的。首先，流量采集器从互联网中采集网络流量，以 libpcap 格式存储到 HDFS (Hadoop distributed file system, Hadoop 分布式文件系统)中；然后，流量分析模块使用 PcapInputFormat^[3]从 HDFS 中读取流量文件，对流量解码，获得每个数据分组的五元组、长度、时间和标识位等信息；最后，根据五元组信息将数据合并成相同的数据流，根据表1中不同流量特征属性的特点，统计计算流的特征。由于各个模块都基于 MapReduce 模型并行化实现，因此数据计算的性能瓶颈得

表 1 流量特征

序号	特征符号	特征描述
1~2	Port(src, dst)	源端口和目的端口
3~6, 7~10	PacketsLen(min, max, mean, variance)(forward, backward)	双向子流报文长度的统计特征(最小、最大、平均大小、方差)
11	Duration	流的持续时间
12	GapTimeVar	数据分组时间间隔方差
13~18	TcpFlag(syn, fin, urg, ack, psh, rst)	含 TCP 标志位的数据分组个数
19	RTT	往返时延
20	ByteSpeed	平均每秒字节数
21	PacketSpeed	平均每秒分组数

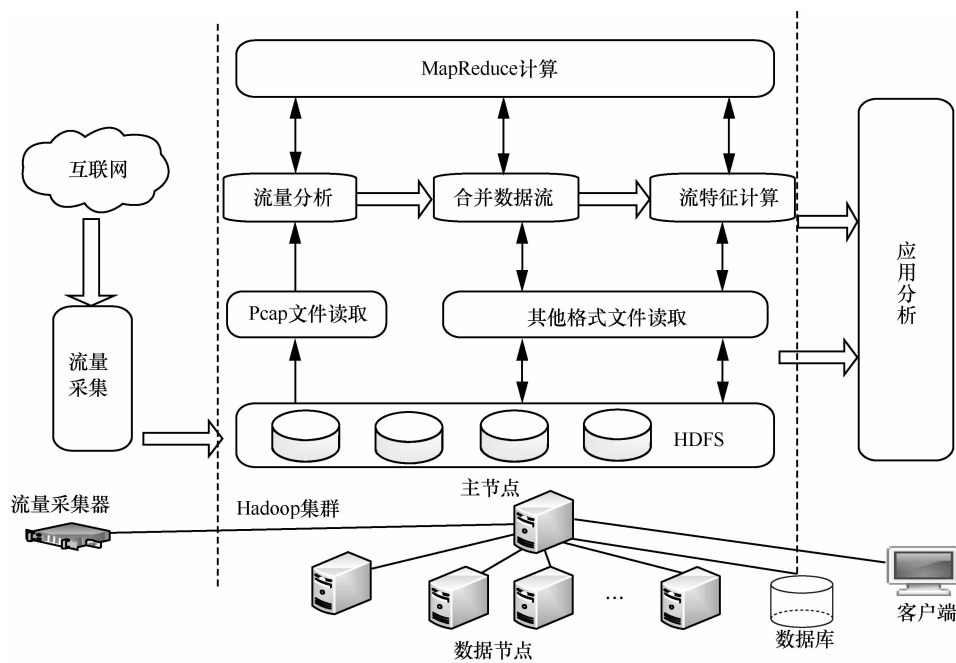


图1 流量分析模型

到了解决。

3 MapReduce 算法实现

MapReduce 是 Hadoop 的主要核心组件之一。借用函数式编程的思想,将要执行的问题拆解成 map 和 reduce 两种操作。在使用 MapReduce 分析数据时,数据流以<key, value>键值对的形式存在,键值对决定了数据的流动格式

和规则,同时键值对可作为最终的输出或下一次 MapReduce 运算的输入,增加了算法的可扩充性。

3.1 作业设置

基于 MapReduce 编程模型实现流量特征的并行计算一共设置两个作业(job),job1 主要负责数据分组的解析和流合成,job2 主要是计算流的各个属性特征。具体任务结构设计如图 2 所示。

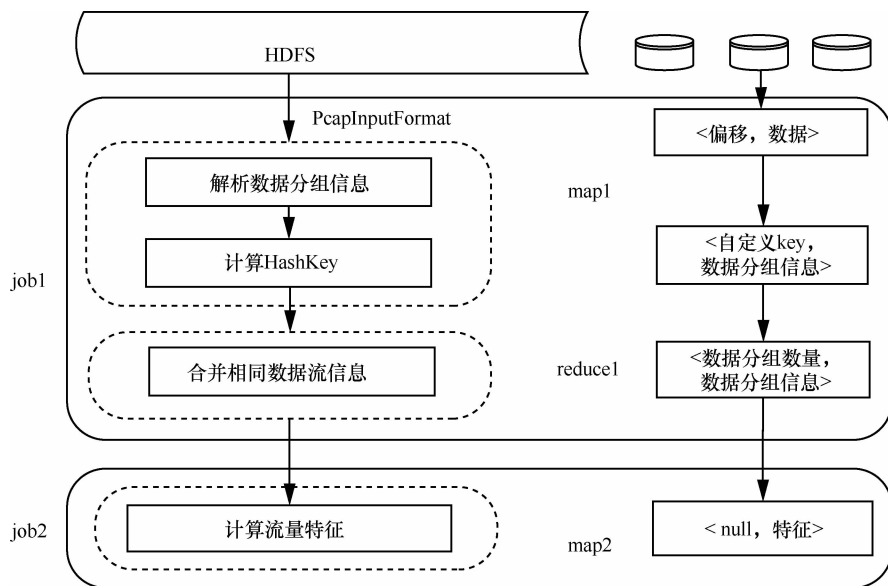


图2 任务结构

首先将需要处理的数据按照 Hadoop 默认的方式存储在 HDFS 中^[2], job1 利用 PcapInputFormat^[3]这种 Pcap 文件读取方式读取存储在 HDFS 上的 libpcap 离线数据文件,将数据分组解析为 key 和 value 键值对,传递给 map1;map1 解析数据分组,得到五元组和数据分组信息;reduce1 读取 map1 的中间结果,将具有相同五元组的数据分组信息合并。job1 的 map1 和 reduce1 操作称作数据分流过程。job2 负责调度 map2,实现流量特征的统计计算,并输出最终结果。

3.2 job1 操作

job1 操作主要完成数据分组的解析和流的合成,如图 3 所示。

map 操作主要负责解析数据分组内容,计算 HashKey 值和记录关键信息。首先,逐层读取每一个完整数据分组的分组头信息,将五元组、数据分组长度、时间戳、TCP 标志位信息作为数据分组信息(PacketInfo);然后,借用 IPSX 散列算法思想,对五元组信息求 HashKey;最后,map1 以 HashKey 和时间戳数据作为自定义类型 MyKey 的 key,以 PacketInfo 作为 value。将数据分组信息以 <MyKey, PacketInfo>输出到中间文件,等待下一步操作。

map 的数据并不是简单地写到磁盘,本文利用洗牌(shuffle)过程中的分区(partition)操作读取 MyKey 类中的 HashKey 值,并将具有相同 HashKey 的数据分组信息划分到相同区,这样能保证具有相同 HashKey 的数据流分配到同一个 reduce 中。由于在处理源数据时,分块操作可能把数据打乱,因此本文在分区操作中改写了 sort(排序)函数,将同一分区按照 MyKey 类中的时间戳的大小排序,最后将

排序的结果传递到 reduce 操作。

reduce 操作主要是将属于相同流的数据分组信息合并成同一条记录,并排除由于 IPSX 算法的不足引起的同一个 HashKey 对应不同数据流的情况。虽然 IPSX 的散列效果很好,但也会有少量散列冲突存在。这里说的散列冲突是指不同流的五元组通过 IPSX 算法得到相同的散列值。故在 reduce1 操作中,需要将产生散列冲突的数据流区分开,而并不是简单地将相同 HashKey 对应的 value 合并为同一条记录。经过 sort 函数处理后,相同 HashKey 对应的 value 信息会以迭代器的形式传送到 reduce1 操作。首先,读取第一个数据分组信息,记录该五元组信息,同时将数据分组信息写入对应的 valueBuffer 数组节点。然后,等待读取下一个数据分组信息,判断五元组是否相同。若相同,视为同一条流的信息,添加数据分组信息到相应的 valueBuffer 数组节点,并记录流数据分组个数(PacketNum);如果不同,则新建 valueBuffer 节点,缓存新的数据流,并记录第一个数据分组五元组信息,继续统计。最后,将流的信息以<PacketNum, valueBuffer>的形式依次写入输出文件,交由 map2 操作。

3.3 job2 操作

job2 操作主要是计算流的各个属性特征。job2 中的 map2 操作作为 job1 中 reduce1 的下一个操作,其输入即 reduce1 操作的中间结果。如图 4 所示,map2 操作首先读取 key,获得流的第一个数据分组信息,以便于后续处理中区分双向子流,然后读取 value 获得这个流的所有数据分组信息。具体的特征计算过程如图 4 所示。

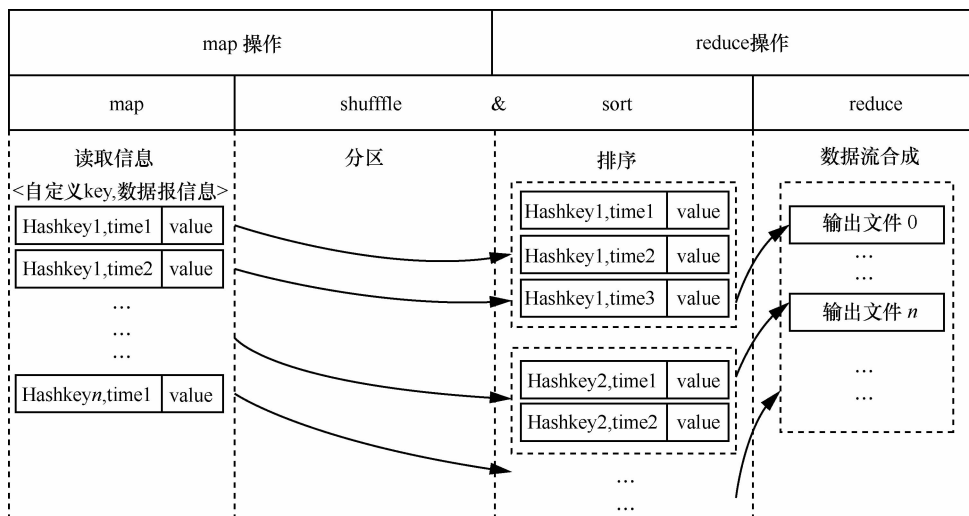


图 3 job1 设置

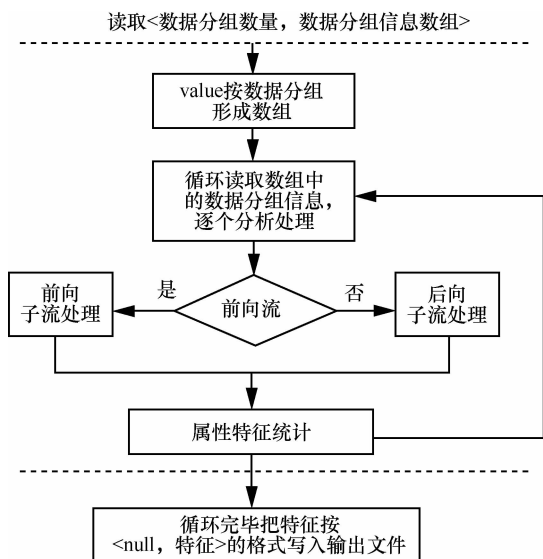


图4 map2 操作流程

map2 操作读取的 value 信息代表一个完整流的所有数据分组信息。首先, 将 value 信息按数据分组分割到 PacketInfo 数组当中。然后, 循环提取 PacketInfo 数组中每一个数据分组信息, 通过与第一个数据分组五元组信息对比, 判断是否属于前向子流。若是, 就通过前向子流模块处理; 否则, 交给后向子流模块处理。子流处理模块负责统计数据分组的长度和时间信息。循环读取完毕后, 交由属性特征统计模块处理。属性特征统计模块统计流的数据大小、含标志位的数据分组个数、持续时间、间隔时间方差和数据分组长度方差等属性特征。最后, 将所有的统计结果写入输出文件。

4 实验结果及分析

为了验证此方法的可行性, 实验搭建一个 Hadoop 集群, 系统版本采用 Hadoop1.1.2。此集群由 6 台电脑和 1 台服务器组成, 其中服务器开启两个系统版本为 CentOS-6.2 的虚拟机, 分别作为 NameNode 和 SecondNameNode, 分配 4 GB 内存、1 TB 硬盘和双核 CPU; 6 台电脑配置为 2 GB 内存、500 GB 硬盘和双核 CPU, 安装 CentOS-6.2 版本的系统, 作为 DataNode。

4.1 准确性验证

通过过滤的方式, 从单机采集 30 min 的浏览 Web 流量和迅雷下载流量作为测试数据。通过对测试数据分析, 对比特征计算结果, 以验证本方法的有效性。分析结果见表 2。

提取统计表 1 中每条数据流前向和后向数据分组在

表2 测试数据流记录

	数据大小/GB	流记录/条
Web 浏览流量	0.5	52 623
迅雷下载流量	1.8	16 987

各个长度区间出现的概率, 并将 Web 浏览和迅雷下载的流记录分别拟合为一条曲线, 分析结果对比如图 5 和图 6 所示。图 5 表示前向客户端流数据长度分布概率。可以看出, Web 浏览和迅雷下载的概率曲线基本相似, 数据分组集中分布在长度较小的范围。

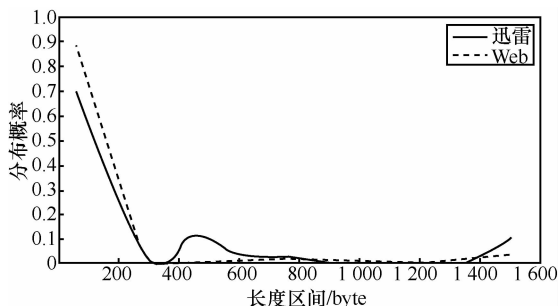


图5 前向流数据长度分布概率

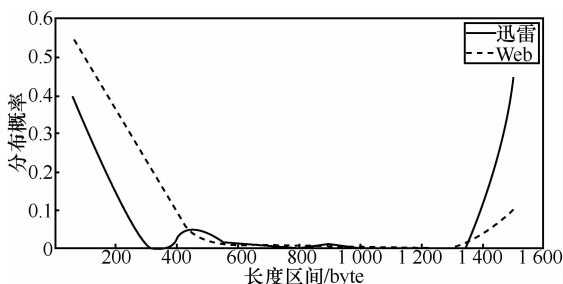


图6 后向流数据长度分布概率

图 6 表示后向服务器流数据长度分布概率。可以看出, Web 浏览和迅雷下载的概率曲线特点较为明显。Web 浏览的数据流中会有大数据分组出现, 但小数据分组出现的概率较大; 迅雷下载的数据流大数据分组和小数据分组出现概率相当。根据后向服务器数据分组长度特点, 可很好地区分 Web 浏览流量和迅雷下载流量。

由参考文献[5]可知, 不同网络应用的数据流具有不同的流量特征。本文通过对实际数据流量分析, 统计 Web 浏览和迅雷下载的 21 个流量特征, 展示了前向客户端和后向服务器流数据分组长度分布概率。Web 流量为浏览类数据, 建立网络连接多、流量小, 在数据流数量和数据分组长度特征上与迅雷下载都不同。通过以上分析验证, 本文提出的方法能有效计算网络流量特征, 对网络流量分析有重要作用。

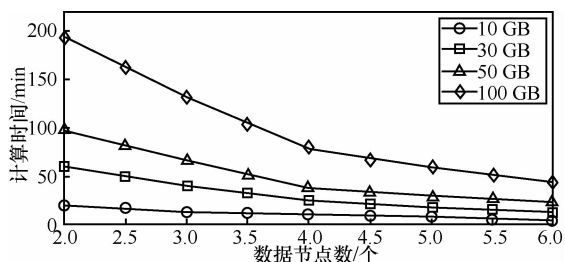


图7 测试时间对比

4.2 扩展性验证

从校园网某宿舍楼网络出口处采集数据,通过控制集群的数据节点个数和测试数据集大小验证本文方法的性能。实验采集了大小为 10 GB、30 GB、50 GB 和 100 GB 的数据集,分别使用不同数据节点的集群分析网络流量特征,计算时间对比如图 7 所示。

由图 7 可以看出,当数据集为 100 GB 时,数据节点数为 6 个的计算时间仅仅是数据节点数为 2 个的 25%左右。在节点数量不变的情况下,数据集越大,计算时间越长。此外,随着节点数的增加,数据处理时间呈非线性减少趋势,且数据量越大,本文方法的处理优势越大。因此,使用本方法进行网络流量分流和特征计算,具有很好的扩展性,可通过增加数据节点的个数提高计算能力。

5 结束语

网络流量特征计算是网络流量分析的基础,随着互联网的快速发展,网络流量暴涨,高效地计算网络流量特征显得尤为重要。本文提出的基于 MapReduce 编程模型的网络分流和流特征计算方法,有效地将并行计算和网络分析结合,解决了使用 MapReduce 模型分流网络数据和计算流量特征的问题,有利于并行化实现网络流量分析。该方法对网络流量统计、流量预测和网络安全都有重要意义。本文在实验室环境下进行模拟仿真,下一步工作是在改善本文方法运行效率的同时,在实践中对其进一步拓展和完善,实现更高的价值。

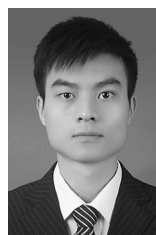
参考文献

- 1 周爱平,程光,郭晓军.高速网络流量测量方法.软件学报,2014,25(1):135~153
- 2 Li W, Moore A W. A machine learning approach for efficient traffic classification. Proceedings of the 15th International

Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, Istanbul, Turkey, 2007: 310~317

- 3 Li M, Ye J H, Li J L, *et al.* The research on network traffic management based on Hash aggregation. Journal of Jiangxi Normal University (Natural Sciences Edition), 2011, 35(2): 174~177
- 4 Hadoop. <http://hadoop.apache.org/>, 2014
- 5 Lee Y, Kang W, Lee Y. A hadoop-based packet trace processing tool. Proceedings of the 3th International Conference on Traffic Monitoring and Analysis, Vienna, Austria, 2011:51~63
- 6 Qiao Y, Lei Z, Yuan L, *et al.* Offline traffic analysis system based on Hadoop. Journal of China Universities of Posts and Telecommunications, 2013, 20(5): 97~103
- 7 杨新宇,杨树森,李娟.基于非线性预处理网络流量预测方法的泛洪型 DDoS 攻击检测算法.计算机学报,2011,34(2):395~405
- 8 何高峰,杨明,罗军舟等.Tor 匿名通信流量在线识别方法.软件学报,2013,24(3):540~556
- 9 Liu Z X, He M B, Liu S, *et al.* Research of P2P traffic comprehensive identification method. Proceedings of International Conference on Network Computing and Information Security, Guilin, China, 2011: 307~310
- 10 Thiriet M J M. Classifying application flows and intrusion detection in internet traffic. Doctoral Dissertation University of Science and Technology, 2013

[作者简介]



刘勇,男,重庆邮电大学通信与信息工程学院硕士生,主要研究方向为网络数据挖掘及流量分类。

雒江涛,男,博士,重庆邮电大学通信与信息工程学院教授、博士生导师,中国电子学会高级会员,主要研究方向为移动通信和下一代网络及测试技术与研究开发。

邓生雄,男,重庆邮电大学通信与信息工程学院硕士生,主要研究方向为网络数据挖掘及流量分类。

王小平,男,重庆邮电大学通信与信息工程学院硕士生,主要研究方向为网络数据挖掘及流量分类。

(收稿日期:2014-07-04)