doi:10.3969/j.issn.1001-893x.2014.05.023
引用格式:王小平,王建勇,杨坝.采用云计算技术的网络流量检测[J].电讯技术,2014,54(5):650-655.[WANG Xiao-ping,WANG Jian-yong,YANG Xun. Network Traffic Detection with Cloud Computing[J]. Telecommunication Engineering,2014,54(5):650-655.]

采用云计算技术的网络流量检测*

王小平**,王建勇,杨 坝
(重庆城市管理职业学院,重庆 401331)

摘 要:为了实现对现网大数据网络流量的实时、有效检测,提出了一种基于云计算的网络流量检测方案。该方案充分利用 Hadoop 平台 Map/Reduce 编程模型在海量数据处理方面的优势,采用分层化的设计思想,克服了传统检测方案在海量数据应用环境中效率低下、可扩展性与安全性不足的缺点。重庆移动 DPI 平台应用表明,该方案较为有效,流量检测效果良好,在大数据处理时效率较普通分布式处理有明显提高。

关键词:网络流量检测;云计算;大数据;深度包检测
中图分类号:TP393 **文献标志码**:A **文章编号**:1001-893X(2014)05-0650-06

Network Traffic Detection with Cloud Computing

WANG Xiao-ping, WANG Jian-yong, YANG Xun
(Chongqing City Management College, Chongqing 401331, China)

Abstract: In order to detect the network traffic in real time and effectively, a traffic detection scheme based on cloud computing is proposed. The scheme makes full use of the advantages of Hadoop platform's Map/Reduce programming model and adopts the thought of hierarchical design to avoid the inefficiency, the defects of scalability and security of traditional detection schemes in big data application environment. The application of the proposed scheme in DPI platform of Chongqing Mobile Communication Company has proved its effictiveness. The detection result is satisfying and the data processing speed has been improved obviously compared with the common distributed processing.

Key words: network traffic detection; cloud computing; big data; deep packet inspection

1 引 言

随着互联网技术的快速发展,互联网已步入大数据时代,网络流量指数级增长的趋势使网络运营面临各种巨大挑战。首先,网络应用的日益多样化与越来越多的 P2P 业务占据了大量带宽,因此需要寻找一种对其进行有效检测与管理的方法,以保证移动互联网业务的正常运行。与此同时,网络攻击手段和异常流量不断升级,运营商存在对其进行有效识别和禁止的需求[1]。另外,从信息安全的角度,复杂多变的国内外局势也要求对互联网流量加强监控。

目前,网络流量分析方法主要包括基于传输层端口、基于特征内容及基于流量特征统计。其中基于流量统计特征匹配技术已被证明更加有效[2-3],该技术的分析程序多集中在高性能的服务器上运行,数据的收集主要采用 NetfFlow 或类似工具。但随着数据中心的不断涌现,数据处理量已达到 PB 或者更高,传统的单服务器处理模式由于存在扩展性差等因素已无法满足海量数据存储和实时处理要求。网络流量检测急需扩展性更好且能充分发挥计

* 收稿日期:2014-04-16;修回日期:2014-05-19 Received date:2014-04-16;Revised date:2014-05-19
** 通讯作者:workmail73@126.com **Corresponding author**: workmail73@126.com

算和存储资源能力的并行分析方案。

为此,本文提出一种基于 Hadoop 的网络流量检测系统框架,并在此基础上设计实现了一种流量分析检测方案。通过对流量处理层的详细设计,对流量数据的存储读取接口(I/O 接口)、流量检测的 Map/Reduce 编程以及协议解码三大关键技术的设计与实现,验证了该方案能充分利用 Hadoop 平台存储与高速运算的优势,以并行方式对网络流量实时大数据进行高效检测与处理。

2　基于 Hadoop 的云计算技术

Hadoop 是一个分布式系统基础架构,用户可以在不了解分布式底层细节的情况下,开发分布式程序,主要通过集群应用、网格技术或分布式文件系统等功能,充分利用集群的高速运算和存储优势。Hadoop 的核心架构[4]包括分布式文件系统 HDFS(Hadoop Distributed File System)和海量数据并行计算编程模型 Map/Reduce。

2.1　HDFS

HDFS 由大量服务器集群组成,采用 Master/Slave[5]架构,即由一台中心服务器作为 Namenode(元数据节点),负责执行文件、目录的命名空间操作,如打开、关闭、重命名文件和目录,同时决定数据块(block)到数据节点(Datanode)的映射[6-7];Datanode 是系统真正存储数据的地方,由多台服务器组成。为保证系统安全,用另一台服务器作为辅助节点,负责不断地将 Namenode 中的编辑日志 edit log 应用到 fsimage(二进制文件,记录 HDFS 中所有文件和目录的元数据信息)中,减少下次 Namenode 的启动时间,同时也保证了系统的安全性。

2.2　Map/Reduce

Map/Reduce 是 Google 提出的分布式并行计算编程模型,用于大规模数据的并行处理[8]。Map/Reduce 将大规模数据处理作业拆分成若干个可独立运行的 Map 任务,分配到不同的机器上去执行,生成某种格式的中间文件,再由若干个 Reduce 任务合并这些中间文件获得最后的输出文件[9-10]。

3　流量检测方案设计

流量检测指利用各种流量检测技术对网络流量进行处理,得到流量中部分内容、分布情况等信息,为网络运营商网络优化提供数据支撑。它是网络运营管理的有利工具。本文提出的流量检测方案主要是针对移动现网业务流量识别,并实时统计各个业务的流量占用情况。为了后文描述方便,现将有关字段介绍如表 1 所示。

表 1　相关字段信息

Table 1 Fields information

字段	描述	类型	大小
Wiredlen	Pcap 包头	理论包长	4B
Caplen	Pcap 包头	实际包长	4B
TimeStamp	时间戳	UNIX	32
u Time	间隔时间	UNIX	32

3.1　流量检测系统框架设计

流量检测系统采用分层化设计思想,共分为网络层、采集层、云处理层和应用层 4 层,如图 1 所示。

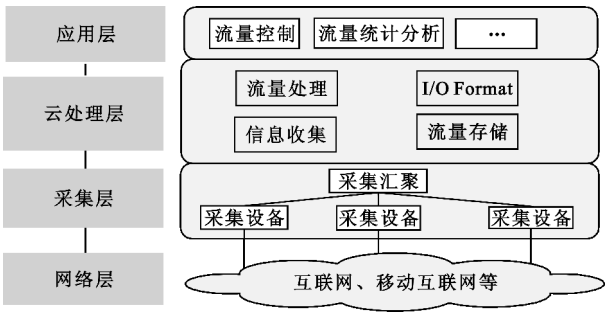


图 1　流量检测系统框架

Fig. 1 Traffic detection system structure

下面将详细介绍流量检测系统每层的功能。

(1)网络层

网络层指的是各种类型的互联网络,可以是移动互联网、计算机网络或者其他类型的需要进行流量检测的私有网络。

(2)采集层

采集层主要负责从各种类型的网络中采集流量数据。由于网络的组网方式和速率各异,网络层需要能够适应各种类型网络流量的采集。流量采集一般采取旁路采集的方式,以保证不影响网络的正常运行。

(3)云处理层

云处理层主要负责网络流量的检测处理,是流量检测的关键所在。云处理层又分为 HDFS 和 MR(Map/Reduce)两个子层。HDFS 子层完成流量数据的分布式存储,为 MR 子层处理打下基础。MR 子层完成流量的分布式处理,需要对数据进行的处理包括协议解码、TCP/IP 重组和流量识别等。由于 HDFS 子层在存储数据时数据分割不规则,可能导

致某个任务处理的数据包不完整,所以设计了 I/O Format 层,专门进行 Pcap 格式数据的读取转换。

(4)应用层

应用层的功能是根据云处理层结果进行相应的上层处理。如:根据业务识别结果与需求,对不同的业务流量进行流量控制或对业务流量进行统计分析等。

3.2 云处理层详细设计

如何对云处理层进行子模块划分,是本方案设计中的关键。根据系统框架,云处理层的功能是接收流量数据并进行处理。为此首先将云处理层分为流量收集、存储和检测处理 3 个子功能模块,以达到模块间低耦合、同时互相协作完成流量检测目的。其次,将流量检测处理过程分为读取 Pcap 格式数据、流量检测。最后,由于 Hadoop 平台的 HDFS 存储可能会导致 Pcap 格式的数据包在包中间切断状况,为实现快速高效读取 Pcap 数据需设计一个 I/O 接口,以完成该功能。同时,由于流量检测采用 DPI 技术,而 DPI 技术需要特征库的支持且特征库需要定期更新,所以,需将特征库与流量检测分析分开。

综上,云处理层主要包括 HDFS 存储、IO 接口、协议检测分析、流量收集和业务特征五部分。因此,提出如图 2 所示的 Hadoop 平台网络流量处理方案。

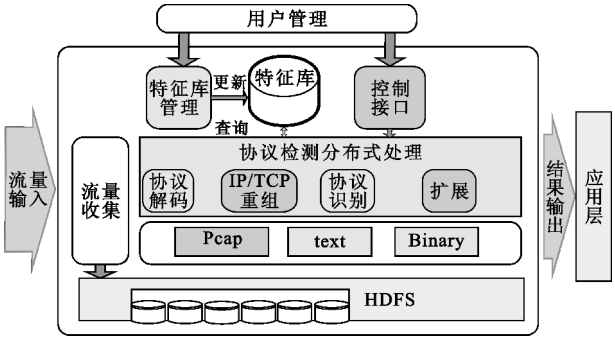


图 2 云处理层详细设计图

Fig. 2 Detail design of cloud processing layer

流量收集主要是负责接收采集层采集到的流量数据,并按一定格式存入 HDFS 文件系统中。本方案拟采用 HDFS 系统自带的文件装载功能进行处理,block 块的大小可根据不同的性能需求进行不同的优化设置。HDFS 存储是 Hadoop 平台的重要组成部分,其主要存储网络流量,并为流量的分布式处理提供支撑。

由于 Hadoop 对文本文件的读取效率高于对二进制文件的读取,然而重庆移动 DPI 平台主要针对的是 Pcap 格式的流量数据。因此,需依据设计 IO 接口实现 Pcap 格式文件到文本文件格式的转换,以提高流量数据的读取效率,具体方法将在后文介绍。特征库部分是为流量识别提供支撑,本文采用深度包检测(Deep Packet Inspection,DPI)技术进行业务流量识别,由于业务特征随时在改变,需要定期对特征库进行更新。协议分布式处理也是 Hadoop 平台的重要部分之一,主要包括协议解码、IP/TCP 重组、协议识别和其他扩展功能,所有功能均采用 Map/Reduce 分布式算法进行实现。

4 流量检测方案的实现

4.1 IO 接口实现

当 MapReduce 任务开始对存储在 HDFS 中的流量数据进行处理时,需要调用 IO 接口完成对 HDFS 中的数据进行读取,正确找到 Pcap 格式数据的包头。IO 接口的实现方法如下:

(1)假设每个 map 任务对应的 block 块中数据为正常的 Pcap 格式数据,即认为 block 块开始的 16 字节为一个 Pcap 格式数据的包头。同时跳过第一个包头中 len 长度的字节数,找到第一个包的包头位置;

(2)按 Pcap 格式读取步骤一中假设的两个 Pcap 格式包头中的时间字段、长度字段、wiredlen 和 caplen 字段,并判断各字段是否满足条件;

(3)若步骤 2 中读取的字段不满足条件,则证明步骤 1 中假设无效,跳过 block 中的一个字节,继续继续步骤 2,直至满足条件为止。

以上方法需要满足的条件:

(1)TimeStamp1, TimeStamp2 ∈时间值;

(2)wiredlen-caplen < 最大包长度;

(3)TimeStamp2-TimeStamp1 < uTime。

按如上方法查找到 map 任务对应 block 块中 Pcap 数据包的开始位置,然后从此位置开始读取 Pcap 数据包,进行供 map 任务处理。

4.2 Map/Reduce 编程模型的实现

利用 Hadoop 的 Map/Reduce 编程模型可以对海量数据进行高效并行处理,从而大大提高流量检测的速率和效率。基于 Hadoop 的流量检测处理分为 Map(映射)和 Reduce(简化)两个阶段。每个流量处理功能当作一次 Map/Reduce 任务,如协议解码、IP/TCP 重组和流量识别等。一次任务将流量数据集切分为多个独立的数据块,并为每个数据块建

立一个 Map,各个 Map 独立并行地处理对应的数据块。Map 阶段产生输出作为 Reduce 阶段的输入,Reduce 在 Map 的基础上对中间结果进行归并处理,并生成输出。Map 和 Reduce 的个数可根据 Map 和 Reduce 阶段的任务复杂度进行合理分配,两者没有关联性。

下面以流量识别任务为例,结合 Map/Reduce 编程模型,实现网络流量检测中最为关键的流量识别,其整体框架如图 3 所示。

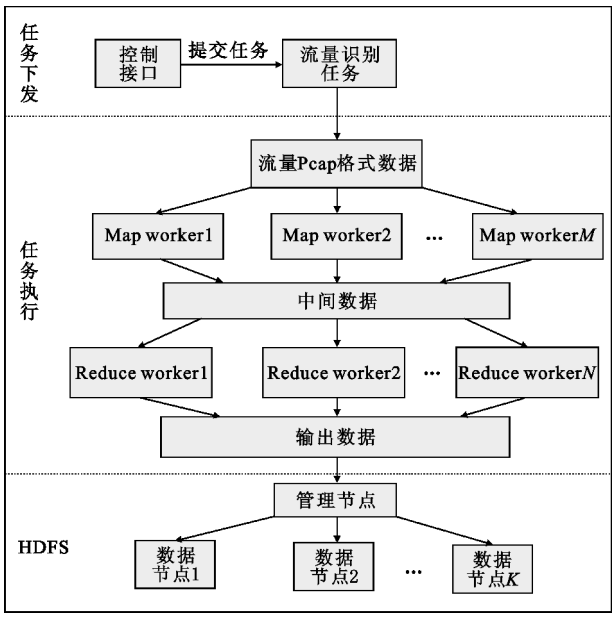


图 3　流量识别 Map/Reduce 模型

Fig. 3 Map/Reduce module of traffic identification

流量识别的具体实现流程如下:

(1)通过云平台向外提供的控制接口,提交任务;

(2) Hadoop 平台启动一个任务管理器 JobTrack, JobTracker 首先读取待处理的流量 Pcap 格式数据,并将 Pcap 数据分成大小相等的 *M* 份,同时在 HDFS 中做好备份,最后 JobTracker 创建多个 JobWorker,并合理给每个 JobWorker 分配任务;

(3)每个 JobWorker 通过调用 IO 接口,读取步骤 2 中被分割好的 Pcap 数据作为输入,并生成输入<KEY, VALUE>键值对,输入键值对 KEY 要能唯一标识一个数据包,本文选取每个数据包包头距 block 块的字节数作为 KEY。输入 VLAUE 就是数据包。Map 任务通过调用 Map( )函数来进行流量处理操作,不同的任务间的区别在于 Map( )函数的实现不一样。Map 子经过处理后生成中间<KEY,VALUE>键值对,供 Reduce 子任务处理;

(4) Reduce 子任务获取 Map 子任务输出的中间兼职对,进行归并处理,此过程也是调用 Reduce( )函数实现。以流量识别为例,Map 子任务输出的中间键值对中,KEY 值与 Map 子任务输入键值对 KEY 值相同,用于标识每个数据包;VALUE 值为数据包对应的业务类别;

(5)当所有 Map 和 Reduce 子任务执行完之后,JobTracker 将 Reduce 的输出结果保存到 HDFS 中,供上层应用使用。

4.3　Map/Reduce 函数实现

Map/Reduce 编程模型主要描述的是任务的分解过程及其输入、中间输出键值对和最终输出结果的选取。Map/Reduce 模型中真正的处理部分是在 Map( )和 Reduce( )函数中实现,本文以协议解码为例,详细介绍其实现过程。

协议解码的分布式处理时,Map( )函数完成数据包按协议格式解析,Reduce( )函数完成解码结果的统计和保存。协议解码的流程如图 4 所示。

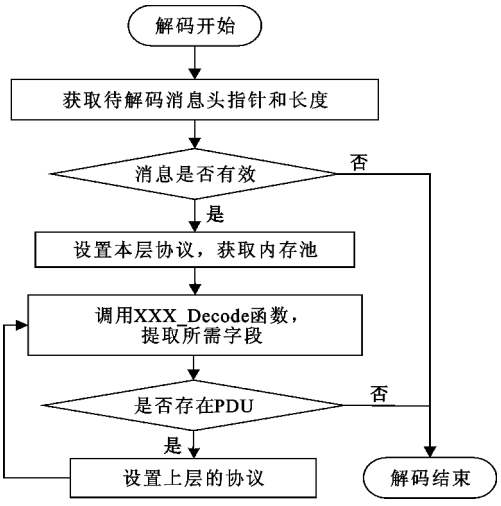


图 4　协议解码流程图

Fig. 4 Flow chart of protocol decoding

协议解码步骤如下:

(1)调用解码接口后,解码开始;

(2)获取需要解码的数据包的相关信息,包括数据包在内存中的首地址和数据包的长度;

(3)判断数据包是否有效,主要判断依据是数据包协议所携带的长度字段与实际数据包的长度进行比较,若不等,则数据包无效,解码结束;若相等,进入步骤 4;

(4)数据包有效,进行相应的初始化操作,如获取本层协议信息,并申请解码结果表;

(5)根据步骤 4 获取到的数据包协议,调用相应的协议解码函数,得到解码结果并将本次解码所

能获取到的解码结果字段填入结果表;

(6)判断数据包是否包含上层 PDU 信息,若包含,则转到步骤 5 继续对上层 PDU 进行解码;若无,则解码结束。

5 方案测试与结果分析

5.1 测试环境

以重庆某高校校园网实时数据为本方案测试对象,搭建如图 5 所示的测试系统。系统组件与参数配置说明如下:

(1)系统由 5 台 PC 机(每台配置:4GB 内存,1TB 硬盘,酷睿双核 CPU)、2 台 PC 机(每台配置:2 GB 内存,500 GB 硬盘、酷睿双核 CPU)、1 台千兆交换机和若干网线构成;

(2)在 5 台配置相同的 PC 上,每台用虚拟机软件构造出 4 个配置相同虚拟机,网络方式选择桥接模式,虚拟机 IP 配置如下:物理机 192. 168. 1. 3 上的 4 个虚拟机 IP 分别为 192. 168. 1. 31-34,依次类推,所有机器通过千兆交换机构成一个高速局域网;

(3)在 22 个机器(20 个虚拟机和两台物理机)上装 Linux 64 位操作系统,并搭建 Hadoop 平台。由其中两台配置相同的物理机分别当作 Namenode 和 SecondaryNamenode,20 个虚拟机作 Datanode。

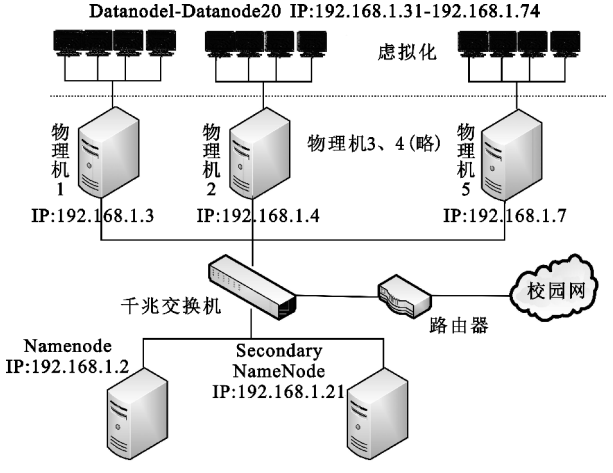


图 5 系统集成示意图

Fig. 5 Illustration of system integration

启动 Hadoop 平台,通过 SSH 登陆到管理节点(IP:192. 168. 1. 2)上,进入 hadoop 的 bin 目录,执行./start-all. sh 命令,就可以启动 Hadoop 集群。登陆 Hadoop 的 DFS(Distributed File System)管理界面查看,启动成功后的 HDFS 集群总容量为7. 61 TB,活动节点有 20 个,非活动节点 0 个,如图 6 所示。

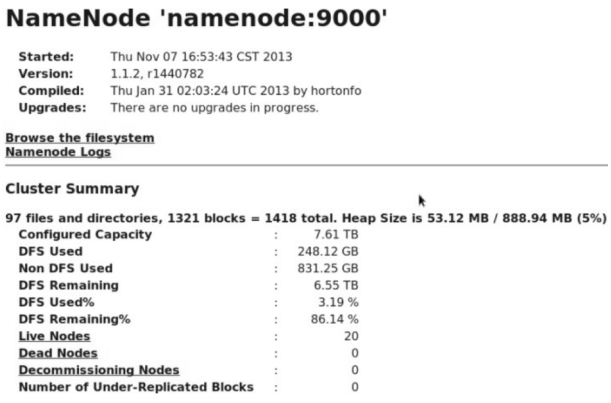


图 6 HDFS 管理界面

Fig. 6 Management interface of HDFS

在一定的 Hadoop 平台参数配置下,硬件配置越高,节点个数越多,数据会被分割成更小的块进行存储,对小数据量而言,由于数据处理调度会占据大部分时间,所以处理时间会增加;对于大数据,调度时间的影响相对较小,由于节点数增加,处理时间会显著缩短。

5.2 结果分析与性能对比

利用检测系统对从校园网抓取的 4. 3 GB 流量进行检测处理,识别出业务类别及其对应的流量信息,如图 7 所示。

ClassID	ClassName	Total_Bytes	Up_Bytes	Down_Bytes
4	浏览下载	759079	164991	594088
9	音乐	618254	122980	495274
10	视频	572072	110553	461519
8	游戏	452274	96750	355524
11	P2P业务	462379	117046	345333
2	微博	230652	49063	181589
0	未识别	232243	55685	176558
7	邮箱	235038	59469	175569
1	即时通信	284230	111284	172946
3	VoIP	251679	78776	172903
5	阅读	238263	78346	159917
6	支付	192511	49321	143190
12	应用商店	116444	25757	90687
13	其他业务	301	129	172

图 7 业务流量识别与统计结果

Fig. 7 Traffic identification and statistic results

从图 7 可以看到,被检测的流量中,浏览下载类业务总流量最大,占据整个流量的 16%,其次为音乐类和视频类,分别占据总流量的 13% 和 12%,这基本符合该特定区域业务流量特性和人们对业务喜爱程度。通过该统计方案,我们能在保证资源最小开销的状态下完成移动互联网业务的流量识别与检测,数据展示结果已通过重庆移动相关部门审核。

利用基于 Hadoop 的测试系统和基于单台服务

器的流量检测系统同时处理移动数据业务部门采集的相同大小的流量数据,对比两者处理完相同数据需要的时间,结果如表 2 所示。

表 2　流量处理耗时对比

Table 2 Time consumption of traffic processing

数据大小/GB	基于 Hadoop 系统耗时 t_1/s	单机多线程耗时 t_2/s	加速比 (t_2/t_1)
0.3	1 156	489	0.423
1.0	2 682	1 655	0.617
20.0	27 356	49 925	1.825
40.0	49 241	235 126	4.775
100.0	103 406	1 105 617	10.692

从表 2 可以看出,在小数据量情况下,基于 Hadoop 的耗时比单机多线程对流量的处理耗时更大,加速比为 0.423。但随着处理数据量的增大,基于 Hadoop 的系统耗时相对单机多线程耗时的加速比逐渐提高,尤其当数据量为 100 GB 时,加速比可达到 10.692,实时处理效率较为显著,表明了基于 Hadoop 平台的流量检测系统与普通分布式处理在大数据处理上具有优势。经重庆移动数据处理中心产品部实际测试,结果表明当被处理数据大于 200 GB 时性能会更加明显。

6　结束语

本文设计并实现了一种基于 Hadoop 平台的流量检测方案,并基于校园网现网实时数据完成了方案的测试验证,成功实现了对网络流量的检测分析。目前该方案已在重庆移动数据处理中心成功上线运行,经实际运用该方案可对现网大数据进行有效地流量检测,且数据处理速度较普通分布式处理有明显提高。应用本文成果进一步分析,还可对具体业务的人口偏好度进行统计,为运营商增值业务的统计需求提供数据支撑。未来研究方向可通过对 Hadoop 参数进一步调优,利用该方案进行流量的深度识别与详细统计。

参考文献:

[1] 王元卓, 靳小龙, 程学旗. 网络大数据的现状与展望[J]. 计算机学报, 2013,36(6):1125-1137.
WANG Yuan-zhuo,JIN Xiao-long,CHEN Xue-qi. Network Big Data: Present and Future[J]. Chinese Journal of Computers,2013,36 (6):1125-1137. (in Chinese)

[2] 吴建军. 网络舆情的云计算监测模式分析与实现[J]. 电讯技术,2013,53(4):486-488.
WU Jian-jun. Analysis and implementation of network public opinion monitoring based on cloud computing[J]. Telecommunication Engineering, 2013,53(4):486-488. (in Chinese)

[3] 李乔,郑啸. 云计算研究现状综述[J]. 计算机科学,2011,38(4): 32-37.
LI Qiao, ZHENG Xiao. Summary of Research on Cloud Computing[J]. Computer Science, 2011,38 (4): 32-37. (in Chinese)

[4] 刘琨,李爱菊,董龙江. 基于 Hadoop 的云存储的研究及实现[J]. 微计算机信息,2011,27(7):220-221.
LIU Kun,LI Ai-ju,DONG Long-ju. Research and Implementaiton of Cloud Storage Based on Hadoop[J]. Microcomputer Information,2011,27(7):220-221. (in Chinese)

[5] Lee Yeonhee,Kang Wonchul,Lee Yonngseok. A Hadoop-Based Packet Trace Processing Tool[C]// Proceedings of Third International Workshop on Traffic Monitoring and Analysis:Austria: IEEE,2011:51-63.

[6] White T. Hadoop:The Definitive Guide [M]. 3rd ed. New York:O'Reil-ly Media,2012:1-47.

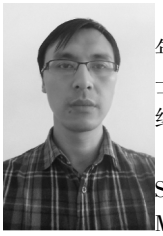
[7] 罗军舟,金嘉辉,宋爱波,等. 云计算:体系架构与关键技术[J]. 通信学报,2011,32(7): 3-7.
LUO Jun-zhou,JIN Jia-hui,SONG Ai-bo,et al. Cloud Computing: Architecture and Key Technology[J]. Journal on Communications,2011,32 (7):3-7. (in Chinese)

[8] 徐雅斌,李艳平,刘曦子. 一种基于云计算的 P2P 流量识别系统模型的研究[J]. 电信科学,2012,28(10):58-63.
XU Ya-bin,LI Yan-ping,LIU Xi-zi. Research of P2P Traffic Identification System Module Based on Cloud Computing[J]. Telecommunications Science,2012,28(10): 58-63. (in Chinese)

[9] 陶彩霞,谢晓军,陈康,等. 给予云计算的移动互联网大数据用户行为分析引擎设计[J]. 电信科学,2013,29(3):27-31.
TAO Cai-xia, XIE Xiao-jun, CHEN Kang,et al. Design of Mobile Internet Big Data User Behavior Analysis Engine Based on Cloud Computing[J]. Telecommunications Science,2013, 29(3): 27-31. (in Chinese)

[10] 宋均,祝林. 基于云计算的海量数据处理平台设计与实现[J]. 电讯技术,2013,52(4): 566-570.
SONG Jun, ZHU Lin. Mass data processing platform design and implementation based on cloud computing[J]. Telecommunication Engineering, 2013,53 (4): 566-570. (in Chinese)

作者简介:



王小平(1973-),男,四川阆中人,2007 年于重庆邮电大学获通信与信息系统专业硕士学位,现为副教授,主要研究方向为宽带网络、无线通信、嵌入式系统等。

WANG Xiao-ping was born in Langzhong, Sichuan Province, in 1973. He received the M. S. degree from Chongqing University of Posts and Telecommunications in 2007. He is now an associate professor. His research concerns wideband network, wireless communication and embedded system.

Email:workmail73@126.com