第 27 卷　第 7 期
2017 年 7 月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol. 27　No. 7
July　2017

基于众核网络处理器的用户语义识别系统

杜俏俏,王　建,赵　悦,宋　乐
(西安工程大学 计算机科学学院,陕西 西安 710048)

摘　要:针对传统流量识别方法在高速网络下识别精度差、效率低、无法对应用层协议内部用户行为进行识别等问题,设计并实现了基于众核网络处理器的用户语义识别系统,并提出了软硬结合的系统实现方式。该系统以 Tilera Gx36 众核网络处理器作为硬件平台,采用基于深度语义数据包识别技术,并结合运用了改进的模式匹配方法。该方法不仅能够识别数据包的应用层协议类型,还可以对应用层协议进行深粒度行为识别,并显著减少了规则的匹配次数,有效地节省了数据包在匹配过程中消耗的时间,降低了匹配的时间复杂度和空间复杂度,进一步提高了系统的识别精度与处理能力。为验证所提出方法和所构建系统的有效性,在万兆网络带宽下进行了系统功能和性能的测试。测试实验结果表明,所构建的系统能满足对应用层协议及数据包实时、准确识别的要求。

关键词:众核网络处理器;深度语义识别;流量分类;深度包检测

中图分类号:TP311.5　　**文献标识码**:A　　**文章编号**:1673-629X(2017)07-0160-04

doi:10.3969/j.issn.1673-629X.2017.07.036

Users Semantic Identification System Based on Multi-core Network Processor

DU Qiao-qiao,WANG Jian,ZHAO Yue,SONG Le
(School of Computer and Science,Xi'an Polytechnic University,Xi'an 710048,China)

Abstract:Aiming at the problem that traditional traffic recognition method has poor accuracy and low efficiency in high-speed network and can't identify the user behavior in the application layer protocol,a DSI (Deep Semantic Inspection) system based on multi-core network processor is designed and implemented and the implementation of system combined software and hardware is put forward. With Tilera Gx36 multi-core network processor as the hardware platform,it uses the identification technology based on deep semantic packet and improved pattern matching method which not only can identify the application layer protocol but also can recognize the user behavior, thus greatly reducing the matching times of the rules and effectively saving the time during the matching process for reducing the time complexity and space complexity and further improving the system's recognition accuracy and performance. Tests on the function and performance of established system have been performed under the Gigabit network bandwidth. The experimental results show that the system can meet the real-time and accurate recognition ability of the application layer protocol.

Key words:multi-core network processor;deep semantic inspection;traffic classification;deep packet detection

1　概　述

随着互联网新的应用模式和应用需求的不断涌现,大量网络应用产生的不同协议类型的流量在给网络运营商和企业带来效益的同时,也带来了许许多多的网络规划和管理问题[1]。针对出现的问题,企业和网络运行商都希望能够详细地了解自己网络内部网络流量的分配和组成,以便针对不同地域或不同协议类型的流量采取差异化管理[2]。通过对网络数据流进行分类,统计出网络流量特征和用户行为特征,从而为企业和用户提供更好的服务质量。随着光纤通讯的发展,主干网的带宽已经普遍达到万兆,这就对系统的处理能力提出了更高的要求[3]。为了解决此问题,1996 年美国 Stanford 大学首次提出片上多处理器思想,即在一个芯片上集成多个 CPU 内核来提高性能,此结构的处理器具有性能强大、控制逻辑简单、低通讯时延等优点,已成为高性能通用处理器的发展主流[4]。目前

收稿日期:2016-09-11　　**修回日期**:2016-12-15　　**网络出版时间**:2017-06-05

基金项目:陕西省工业攻关项目(2014K05-43);陕西省教育专项科研计划(14JK1310)

作者简介:杜俏俏(1991-),女,硕士,研究方向为使用 PDA 升级基于 MSP430 系列芯片仪表的软件技术;导师:陈　亮,副教授,研究方向为计算机网络与网络分析。

网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20170605.1511.086.html

业界有多种多核产品,如 IBM 公司推出的 Power NP 系列、Inter 公司的 IXA 系列、Freescale 公司的 QorIQ 系列、CAVIUM 公司的 OCTEON 系和 Tilera 的 Tilera 系列等型号。经过对以上系列处理器的综合分析,选择 Tilera 公司的 Tilera Gx-36 众核网络处理器作为该系统的硬件平台。Tilera Gx36 是由 Tilera 公司于 2009 年推出的一款核心数量为 36 核的微处理器,采用 40 nm 工艺,由 36 个 Tile CPU 组成,相对于其他处理器,Tilera 处理器拥有数量更多、计算能力更强的 CPU,它的每个 Tile CPU 工作频率高达 1.2 GHz,并且拥有更大、更多类型的缓存空间。如每个 CPU 包含 32 KB 私有的一级指令缓存和 32 KB 私有的一级数据缓存、256 KB 私有的二级缓存和高达 26 MB 的共享缓存,CPU 之间通过 iMesh 高速网络连接,CPU 之间的访问速度达到 66 Tbps,DDR3 内存控制器的访问速率可达1 333 MT/s。此外,Tilera Gx-36 还包括 4 个双万兆以太网控制器(XAUI)。

已有的研究表明,随着 P2P 技术的不断发展,应用最为广泛的基于传输层协议端口号的协议识别技术的准确率正日益低下,并且随着网络带宽越来越高,设计和实现一种高效的深度协议识别系统可以进一步提高系统的识别深度和精度,更好地发挥系统在网络监督和网络管理中的作用[5]。为此,建立了基于 Tilera Gx36 多核网络处理器的协议识别系统结构,并重点对系统中协议特征及协议匹配技术进行研究,实现 10 Gbps 主干网下的应用层协议识别。

2　基于众核网络处理器的协议识别系统框架

设计的基于众核网络处理器的网络流量分类系统结构如图 1 所示。以 EZChip 公司的 Tilera Gx36 处理器作为并行处理平台,并结合基于应用层协议识别的方法,实现对网络数据包的深度分析。协议识别系统由基于语义的规则库、规则解析、规则模型建立、数据包捕获、结构化数据、匹配引擎等模块组成。

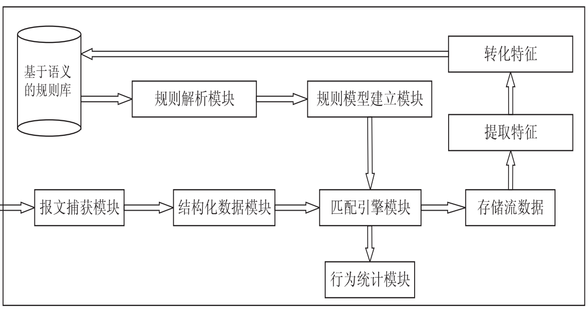

图 1　基于众核网络处理器的应用层协议识别系统

基于语义的规则库是按照一定格式存放应用层协议规则的库,它是识别应用层协议的基础;规则解析模块逐条读取规则库中的规则,然后按照规则存放的特定格式对规则进行解析,规则按照作用不同可以分为两部分,一个是用来标识数据包业务的业务字段,另一种是识别业务字段的协议识别字段。规则模型建立模块将规则解析模块根据协议域把整个规则集划分成多个协议域子集,将每一个协议域子集构建一个匹配器,根据匹配器间的关系构建一个高效的层次匹配树。

数据包捕获模块负责接收模块获取原始网络数据,并对原始网络数据依次进行 IP 碎片重组处理和 TCP 会话重组处理,得到传输层数据;结构化数据模块根据预先定义的协议规则判断应用层使用的协议类型,按照此协议类型的格式对应用层数据进行预处理,得到结构化的应用层数据。匹配引擎模块根据规则模型建立模块建立的层次匹配树对结构化后的应用层数据进行正则表达式匹配,得到匹配结果。其他模块包括用户行为模块、提取特征与转化特征模块。根据匹配引擎的结果,如果此应用层被正确识别,则将匹配结果发送到用户行为统计模块进行进一步分析或显示;如果规则库中没有此数据包对应的规则,则将数据保存并进一步提取其对应的协议特征,最终将协议特征转化为协议规则并更新规则库。

3　协议匹配模块

目前大部分网络应用都使用私有的协议类型,但其协议自身也有一定的格式,其网络应用数据包头中都含有和应用本身相关性较强的应用层特征数据,并且这种协议格式随着系统升级很少发生变化,可以采用逆向工程事先对需要识别的应用协议进行分析,找出可以唯一标识此类协议与用户行为语义的协议特征,并将此类特征作为协议特征规则库对网络数据流进行匹配[6]。另外,这些特征一般都存在于数据流的前某几个数据包中,并且绝大多数协议特征都只在一个数据包中,跨数据包的协议特征非常少[7]。

规则本身主要由业务字段和协议识别字段两部分组成。业务字段由统计输出字段自称;协议识别字段是识别应用行为的协议域和相应协议域对应的正则表达式集合。协议的具体格式如:

应用@行为@操作系统@代理|[协议 1:协议域 11,11,协议域 12,协议域 13][协议 2:协议域 21,协议域 22,协议域 23]…|[Decode1 Decode1][Decode2]…|[表达式 11,表达式 12,表达式 13][表达式 21,表达式 22,表达式 23]…

业务字段由应用@行为@操作系统@代理组成,四个字段分别代表应用名称、应用行为、应用行为操作系统和代理;协议识别字段由[协议 1:协议域 11,协议域 12,协议域 13][协议 2:协议域 21,协议域 22,协议

域 23］…｜［Decode1 Decode1］［Decode2］…｜［表达式 11,表达式 12,表达式 13］［表达式 21,表达式 22,表达式 23］…组成,分别对应匹配的协议类型、协议域和对应协议域的正则表达式。

数据包分类与协议识别模块的原理是模式匹配,根据协议对应的某种特征标识出网络数据包协议类型。协议特征用于判断一个数据包或者多个数据包是否为某一种应用层协议类型的特征数据。在协议匹配模块过程中,决定系统性能的两个重要因素就是规则的组织形式与匹配算法的性能[8]。为了提高系统的匹配速度、降低系统的使用率,在对协议特征规则进行深入分析后,提出基于层次匹配树的规则模型。并使用基于正则表达式的模式匹配算法,进一步提高系统的处理速度。

3.1　层次匹配树

目前,在一般的流量识别系统中,对于大量规则的组织方式有两种:一种是顺序匹配器,另一种是基于 DFA 的匹配器。顺序匹配器的原理如图 2 所示。

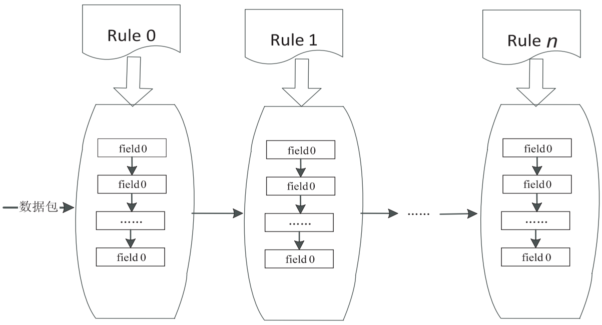

图 2　基于顺序规则的协议匹配器

对规则库中的每条规则构造一个匹配器,通过顺序匹配规则中的每个协议域完成一条规则的匹配,如果当前匹配器没有匹配到,则依次匹配下一个,直到匹配到一个匹配器或者匹配完所有的规则为止。这种方法原理简单,便于实现,但是规则的匹配直接受匹配器的数量影响,当规则较多时性能会受到限制[9-10]。

基于 DFA 的规则匹配方法,首先根据规则所在的协议域进行划分,然后再与一个协议域的规则合并到一个基于 DFA 的匹配器中,如图 3 所示。

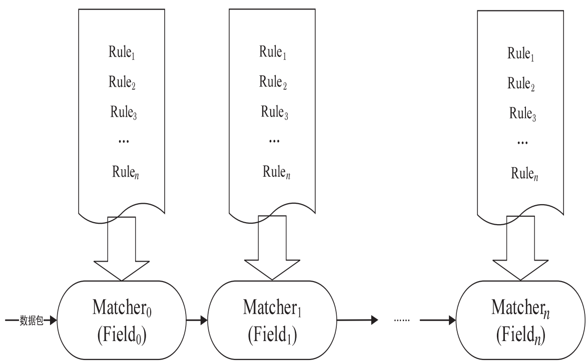

图 3　基于 DFA 规则的协议匹配器

当某一个匹配器匹配失败或者所有的匹配器都匹配完成后完成所有的匹配过程[11-12]。这种方法减少了匹配规则的次数,有效节省了匹配所消耗的时间,减少了数据包在匹配过程中消耗的时间。

3.2　协议匹配

协议匹配模块的另一个主要功能是在规则的基础上完成协议匹配,其整个匹配过程如图 4 所示。

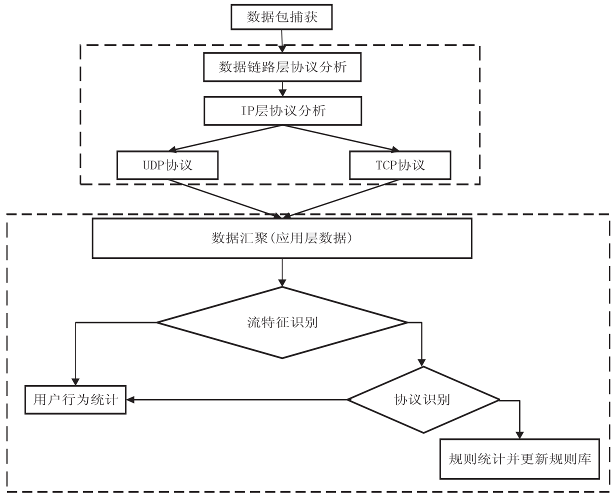

图 4　应用层协议匹配流程图

协议匹配整个过程由网络数据包捕获模块、协议分析模块和应用层协议识别模块组成。网络数据包捕获模块将经过此设备网络适配器的数据包捕获并交给协议分析模块,得到网络层和传输层的协议信息,经过对数据包五元组信息的分析,将网络层数据按照流的方式汇聚并交给应用层协议识别模块,结合根据规则组成的层次匹配树对应用层数据进行模式匹配,得到最终匹配结果。对于统计结果进行统计并发往监控端进行显示与进一步分析,对于没有规则库无法识别的数据包,将其保存并做进一步分析,并根据分析结果对规则库进行扩充[13-14]。

数据包捕获模块负责通过 mPIPE 收包并进行完整性检测,并按照设定的规则将数据包交给相应的处理器的下一个模块进行处理。mPIPE 是 Tilera Gx 系列众核处理器上一个智能数据包收发引擎,在众核处理平台上主要负责数据包捕获、包头解析、包头与负载数据缓冲区管理、负载均衡、数据包校验和计算与数据包发送等服务。其中,包头分析按照协议格式识别包头中每个字段作用并确定此数据包所属流信息;包头与负载数据缓冲区管理分配和资源,缓存包头和数据载荷;负载均衡决定此数据包送至哪个 Tile CPU 进行处理。mPIPE 提供了动态与静态两大类负载均衡模式,其中动态负载均衡模式包括动态流绑定模式和有限流绑定模式,静态负载均衡模式有轮询调度和静态流绑定模式。根据对数据包的处理方式,采用基于静态流绑定模式按流方式对数据包进行处理[15]。

协议分析模块主要对数据链路层、网络层和传输层的数据包进行处理,包括对数据包进行完整性校验、分析网络层和传输层包头,对于 IP 分片数据包进行重组,对于 TCP 数据包进行会话重组,还原出完整的传输层数据,然后将应用层数据交给应用层协议识别模块进行应用协议识别[16]。

应用层协议识别模块根据层次匹配树和协议分析模块得到的应用层数据对数据包进行模式匹配。经过协议分析模块得到应用层数据后,接下来就是根据规则识别应用层所使用的协议类型和用户行为。该方案下应用层协议识别过程为:

(1)将协议分析模块得到的流数据进行汇聚,得到要进行处理的应用层数据。

(2)按照流特征(源 IP、目的 IP、源端口、目的端口和协议类型)对数据包进行特征统计。对于可以通过端口识别的非 P2P 流量,使用基于端口映射的协议分析技术高效、快速地识别出具体应用层协议类型。对于 P2P 流量,则交给应用层协议识别模块。

(3)对 P2P 流量使用基于应用层协议规则匹配的方法对应用层协议进行识别。基于应用层协议规则匹配的方法通过对应用层数据与层次匹配树进行匹配,来确定应用层所使用的应用,采用了改进的模式匹配方法,具有较高的匹配效率。

(4)对于匹配的网络数据包,用户统计模块将识别结果发送至监控端进行展示。

(5)对于匹配引擎无法识别的网络数据包,有可能是某种较新的或者经过加密的协议类型,系统将这些数据保存并进行进一步分析,提取出对应的规则库,并对系统进行升级。

4　性能评估

为了验证基于众核网络处理器的网络流量分析系统的功能及性能,将从处理吞吐量及准确率两方面进行统计。测试环境包括一台 Tile-Gx36 众核处理平台、一台交换机和一台 PC 机,测试环境如图 5 所示。Tilera-Gx36 众核处理平台由 36 个 Tile 核组成,每个核主频为 1.2 GHz,设备使用 8 G 的 DDR3 内存,内存的访问速度为 1 333 MT/s。通过配置交换机,镜像所有流经交换机的流量到 Tile-Gx36 处理器的万兆网口上,网络数据包分类系统从网口获取数据并进行分类处理,最终将分析结果发送给远程监控端 PC 进行具体显示。

测试环境如图 5 所示,将所有经过交换机的网络流量通过路由器镜像到 Tilera Gx36 的万兆网口上,通过这种方式,可以对真实环境下的网络流量进行匹配。图 6 为在不同 CPU 数量下对数据包识别的吞吐量。

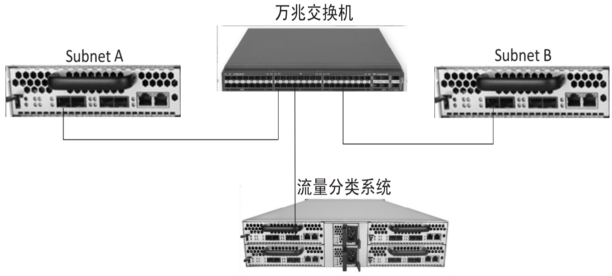

图 5　测试环境

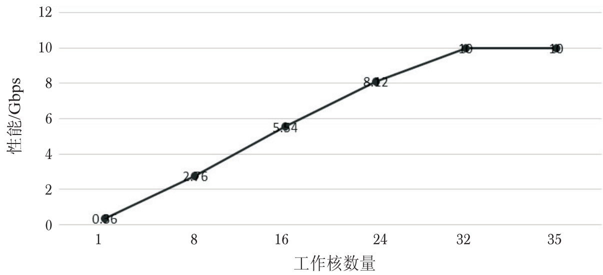

图 6　不同 CPU 数量下系统的吞吐量

实验结果表明,当 CPU 达到 32 个或以上时,可以达到 10 Gbps 的分析能力,满足了设计要求。

5　结束语

为了满足对高速网络数据流量应用层协议的深度识别,提出了基于众核网络处理器的网络流量分类系统,基于 Tilera-Gx36 众核网络处理器,采用基于改进的模式匹配方法,不仅能够识别数据包的应用层协议类型,还可以对应用层协议进行深粒度行为识别,进一步提高系统的识别精度与处理能力。其综合性能是比较理想的,最终设计并实现了流量分类系统。实验结果表明,在万兆网络流量下,该系统能够实现对数据包的识别能力,满足预期功能与性能的要求。

参考文献:

[1]　熊　刚,孟　姣,曹自刚,等. 网络流量分类研究进展与展望[J]. 集成技术,2012,1(1):32-42.

[2]　石　旺,杨英杰,唐慧林,等. 基于协议语义序列的应用层交互行为异常检测[J]. 计算机应用研究,2015,32(10):3060-3064.

[3]　牟　乔. 准确高效的应用层协议分析识别方法[J]. 计算机工程与科学,2010,32(8):39-45.

[4]　朱　宇,袁　帅. 立体化网络应用层协议识别的研究与实现[J]. 电子技术应用,2014,40(1):60-63.

[5]　Yun X,Wang Y,Zhang Y,et al. A semantics-aware approach to the automated network protocol identification[J]. IEEE/ACM Transactions on Networking,2016,24(1):583-595.

[6]　Xu Chengcheng,Chen Shuhui,Su Jinshu,et al. A survey on regular expression matching for deep packet inspection:applications,algorithms and hardware platforms[J]. IEEE Communications Surveys & Tutorials,2016,18(4):2991-3029.

(下转第 169 页)

smdb/smdb_backup_scripts/smdb_backup_incr_1. sh

5.2 BDB 库数据调度策略配置

按照 BDB 库数据调度策略,1 个月中的 1 号 GMT 6 时进行全备份,每天 GMT 6 时进行累积增量备份。

0 6 2-31 * * /space/cimiss_BEXA/storefile/ora/rman_bak_bdb/backup_scripts/bdb_backup_cum_1. sh

0 6 1 * * /space/cimiss_BEXA/storefile/ora/rman_bak_bdb/backup_scripts/bdb_backup_full_0. sh

6 结束语

安全高效的数据备份策略已成为气象数据采集、存放、发展的瓶颈,为了缓解这一矛盾,通过严格的技术选型,解析 Rman 和 TSM 技术特点,结合 CIMISS 业务需求,提出了一种基于 Rman 和 TSM 的 Oracle 数据库备份方法,并依托 CIMIS 陕西省级平台,对该方案进行了实施。运行实践表明,该方案满足了目前业务的需要,实现了数据备份的自动化管理,提高了数据备份的安全性,具有较好的可扩展性,适用于向全国其他省和区域中心推广。

参考文献:

[1] Oracledatabase backup and recovery advanced user's guide 10g release 2[EB/OL]. 2011. http://docs. oracle. com/cd/B19306_01/backup. 102/b14191/toc. htm.
[2] Freeman R G,Hart M. Oracle Database 11g RMAN 备份与恢复[M]. 北京:清华大学出版社,2011.
[3] Hart M. Oracle Database 10g RMAN 备份与恢复[M]. 北京:清华大学出版社,2008.
[4] 崔　杰,邢　薇. 用 RMAN 方法进行 ORACLE 数据库备份和恢复研究与实现[C]//黑龙江省计算机学会 2007 年学术交流年会论文集. 出版地不详:出版者不详,2007.
[5] IBM Tivoli storage manager for databases data protection for oracle and user's guide version 5 release 4 SC32-9064-03[EB/OL]. 2007. http://www-01. ibm. com/support/docview. wss? rs=0&context=SSCTKVU&dc=D400&uid=swg24018539&loc=zh_CN&cs=utf-8&lang=.
[6] IBM Tivoli storage manager for AIX administrator's guide version 5. 5 SC32-0117-01[EB/OL]. 2007. http://publib. boulder. ibm. com/tividd/td/SMAIXN/GC32-0768-01/en_US/HTML/anragd5128. htm.
[7] 张云帆. Oracle 数据库备份与恢复策略[J]. 计算机工程,2009,35(15):85-87.
[8] 王小黎,陆　明,谢　立. 新一代 Linux 启动技术的比较与测试[J]. 计算机工程与设计,2008,29(18):4828-4832.
[9] 路　川,胡欣杰,何楚林. Oracle 10g DBA 宝典[M]. 北京:电子工业出版社,2007.
[10] 袁福庆. Oracle 数据库管理与维护手册[M]. 北京:人民邮电出版社,2006:18-21.
[11] 贾代平. Oracle DBA 核心技术解析[M]. 北京:电子工业出版社,2006.
[12] 谢　东. 基于 Oracle 的数据库安全策略[J]. 现代情报,2006,26(1):119-120.
[13] 余以胜. Oracle 数据库备份解决方案的研究[J]. 计算机与数字工程,2006,34(1):118-121.
[14] 朱海青,唐　娉,王文杰. 实现 Oracle 数据库中海量数据管理的简捷方案[J]. 计算机应用研究,2005,22(2):186-188.
[15] 冯春培. ORACLE 数据库 DBA 专题技术精粹[M]. 北京:冶金工业出版社,2004.
[16] Freeman R G,Hart M. Oracle 9i RMAN 备份与恢复技术—配置和使用 Oracle 恢复管理器[M]. 北京:清华大学出版社,2004.
[17] 黄　河. Oracle 9i for Windows NT/2000 数据库系统培训教程[M]. 北京:清华大学出版社,2003:275-292.
[18] Kyte T. Expert one-on-one Oracle[M]. 北京:清华大学出版社,2002.
[19] Velpuri R,Adkoli A,Williams G. Oracle 8i backup and recovery[M]. 北京:机械工业出版社,2002.
[20] 赵元杰. Oracle 数据库实用指南[M]. 北京:电子工业出版社,2002.
[21] Smith K,Haisley S. Oracle 备份与恢复培训教程[M]. 北京:机械工业出版社,2002.

(上接第 163 页)

[7] 王　岩. 应用层协议识别技术研究[D]. 西安:西安电子科技大学,2012.
[8] 陈　亮,龚　俭,徐　选. 应用层协议识别算法综述[J]. 计算机科学,2007,34(7):73-75.
[9] 贾　堃,孙长宾,姜　凌. 基于 QQ 软件的通信原理分析[J]. 数字技术与应用,2014(4):108-109.
[10] Finsterbusch M,Richter C,Rocha E,et al. A survey of payload-based traffic classification approaches[J]. IEEE Communications Surveys & Tutorials,2014,16(2):1135-1156.
[11] 刘兴奎,邵宗有,刘新春,等. 面向深度包检测的 DFA 细粒度并行匹配方法[J]. 计算机研究与发展,2014,51(5):1061-1070.
[12] 万志涛,章　恒,张若渊. 基于多核处理器的深度包检测的实现和性能评估[J]. 电信科学,2009(S2):171-176.
[13] 林　平,余循宜,刘　芳,等. 基于流统计特性的网络流量分类算法[J]. 北京邮电大学学报,2008,31(2):15-19.
[14] 丁　晶,陈晓岚,吴　萍. 基于正则表达式的深度包检测算法[J]. 计算机应用,2007,27(9):2184-2186.
[15] Lee S H,Park J S,Yoon S H,et al. High performance payload signature-based Internet traffic classification system[C]//17th Asia-Pacific network operations and management symposium. [s. l.]:IEEE,2015:491-494.
[16] Park J W,Kim M S. Performance improvement of the statistic signature based traffic identification system[J]. KIPS Transactions Partc,2011,18C(4):243-250.