# 一种高速网络流识别处理系统的设计与实现

路　琪[1],高　翔[2],许　晓[3],陈　朝[4]

(1.空军预警学院,湖北 武汉 430000;2.63870 部队,陕西 渭南 714200;3.国防科技大学,湖南 长沙 410072;
4.95865 部队,北京 100162)

**摘　要**:随着骨干网络传输速率不断提高,对高速网络信号分析处理系统的需求十分迫切。骨干网络高速率、大带宽的特点给整个网络空间的管理带来了许多困难。采用五元组定义的网络流作为研究对象,通过理论分析,设计和实现了高速网络流识别处理系统硬件平台,实现网络信号在流层面的分析识别,并根据分析结果执行不同的处理策略,从而为网络流的分类处理提供了依据。

**关键词**:高速信号;网络流;流识别

**中图分类号**:TN915　　**文献标识码**:A　　DOI:10.19358/j.issn.2096-5133.2020.02.009

**引用格式**:路琪,高翔,许晓,等.一种高速网络流识别处理系统的设计与实现[J].信息技术与网络安全,2020,39(2):45-52.

# Design and implementation of a high-speed network flow recognition and processing system

Lu Qi[1],Gao Xiang[2],Xu Xiao[3],Chen Zhao[4]

(1.Air Force Early Warning Academy,Wuhan 430000,China;2.No.63870 Troops of PLA,Weinan 714200,China;
3.National University of Defense Technology,Changsha 410072,China;4.No.95865 Troops of PLA,Beijing 100162, China)

**Abstract**:At present,the backbone network transmission rate continues to increase,and the demands for high-speed network signal processing system are quite urgent.The backbone network has brought many difficulties to the entire network space management due to its high-speed and large bandwidth features.This paper takes the network flow defined by five-tuple as the research object,and through the theoretical analysis,shows the design and implementation of the hardware platform of high-speed network flow recognition and processing system.This system can achieve the recognition of network content in flow-level.And according to the result of recognition,different strategies are employed in order to achieve network flow classification.

**Key words**: high-speed signal;network flow;flow recognition



## 0　引言

从1969年到2019年,经过半个世纪的飞速发展,出现了网络购物、网上外卖、旅行预订、互联网理财、网络支付、网络直播、网约车、在线教育等新型互联网应用服务,互联网已经成为人类社会不可或缺的一部分。根据中国互联网络信息中心(CNNIC)于2019年8月发布的《第44次中国互联网发展状况统计报告》,截止到2019年6月,我国网民规模达8.54亿[1]。在2019年1至6月,移动互联网接入流量消费达553.9亿GB,同比增长107.3%,而随着2019年6月6日我国5G(第五代移动通信技术)商用牌照的正式发放,这一数据未来还会继续高速增长。

但是,互联网所具有的开放性特点使得任何符合互联网网络规范的设备都被允许接入互联网,这就给网络安全与网络管理带来了前所未有的挑战。根据国家计算机网络应急技术处理协调中心(CNCERT/CC)于2019年7月发布的《2018中国互联网网络安全报告》,2018年CNCERT/CC全年捕获计算机恶意程序样本数量超过1亿个,涉及计算机恶意程序家族51万余个,较2017年增加8 132个,尽管近三年来增长速度有所放缓,但仍保持高速增长趋势;此外,包括木马病毒、僵尸网络等网络安全问题频频发生,给网络环境的安全与和谐造成

了极大的威胁[2]。本文介绍了一种高速网络流识别系统的设计与实现,通过该系统能够完成对高速网络流的深度识别并为流分类提供依据,从而缓解后端设备处理压力、提高处理效率,为网络状态的监测和管理提供了保障。

## 1 流的定义

从广义上说,数据传输从比特级到语义层面都属于网络内容识别技术研究的范畴。图 1 所示的分层模型将网络内容识别问题分解为七个不同层面的问题,从而实现网络内容识别系统从比特级到语义信息层面的分析处理[3]。而高速网络流分类针对的目标粒度从小到大主要为包级(packet-level)、流级(flow-level)、会话级(session-level)。

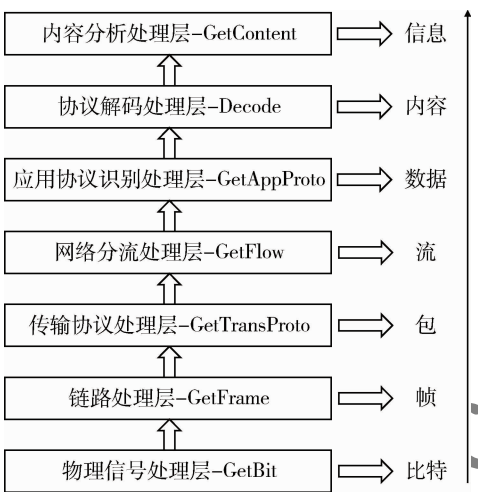


图 1 广义高速骨干网内容分析识别系统分层结构模型

包级分类主要是基于网络数据包所具有的一些特征,只考虑单一数据包,并对其进行分类;流级分类基于五元组进行分类,除了关注单一数据包特征之外,还要关注包与包之间的关系,即进一步考虑流级的指纹特征、统计特征或者行为特征等;会话级分类基于三元组进行分类,主要适用于一些简单网络服务环境的流量粗分类[4-7]。其中研究最多的是流级分类。

网络流(flow)通常是指在一段特定时间范围内两个通信节点之间具有相同五元组特征的一系列数据包的集合。这种利用五元组定义的流虽然不是十分完整,但大多数情况下是具有一定的准确性的。其形式化定义如下:

网络流定义为一对通信节点 A(假设为通信发起方)和 B(假设为通信接收方)通过特定的应用协议在特定场景下生成的流,通常用一个五元组来表示:flow = {sa,da,sp,dp,pro},分别对应节点 A 的 IP 地址(源 IP 地址)、节点 B 的 IP 地址(目的 IP 地址)、节点 A 的端口号(源端口号)、节点 B 的端口号(目的端口号)以及 A 和 B 通信所使用的应用协议。设流 flow 相关的所有 IP 包 $P_f = P_{fa} \rightarrow \cup P_{fb} \rightarrow$,其中 $P_{fa} = \{P_{a1}, P_{a2}, \cdots, P_{am}\}$ 是 A 发送给 B 的网络数据包;$P_{fb} = \{P_{b1}, P_{b2}, \cdots, P_{bn}\}$ 是 B 发送给 A 的网络数据包。

在骨干网或核心网中,大多会采用分布式非对称路由设计,对于某一个网络节点,发送的数据包与接收的数据包会经过不同的网络链路,从而导致在某一个观察点只能看到单方向的数据包。随着骨干网扁平化的发展趋势,应用于高速骨干网络的流分类设备往往只针对单向流进行设计,而对于双向流不做过多的考虑。

基于以上对流定义的阐述,相同网络流应具备三个要素[8]:

(1)方向性。出于对网络可靠性的需要,骨干网一般会采用分布式非对称路由,由此引出了单向流问题,即同一个网络流的输出方向数据包和输入方向数据包会经由不同的网络链路,从而导致在观察点只能看到单个方向的数据包,这些单个方向的数据包称为单向流(Uni-directional flow),与之对应的完整网络流称之为双向流(Bi-directional flow),即网络流的输出与输入经过同一链路。

(2)端点特性。流的端点特性主要关注的是数据包的起始端点和终结端点以及使用的协议类型。因此,根据端点特性定义一组流通常包括源 IP 地址、目的 IP 地址、源端口、目的端口和协议类型 5 个元素,即五元组。

(3)超时约束。对于某一条流来说,起始时间定义为属于该流的第一个数据包到达时间。超时约束就是判断在一个规定的时间内没有属于该流的数据包通过,即认为该数据流已经终结。

## 2 高速网络流识别处理系统设计

根据模块化设计的原则,通过对高速网络信号处理技术的深入分析,高速网络流识别处理平台应该包括:高速网络信号收发模块、系统核心处理模块、高速网络流缓存模块、高速网络流内容匹配模块、数据管理模块及相关辅助模块,能够满足高速信号的处理以及反馈设备信息等,系统的整体架构

如图 2 所示。

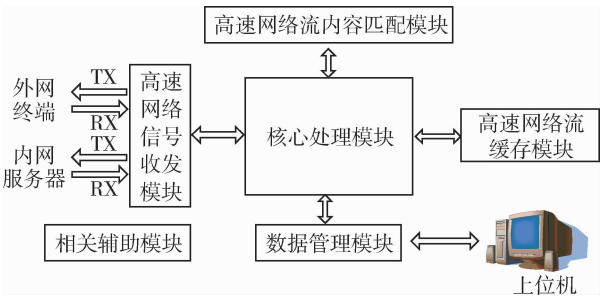


图 2　高速网络流识别处理平台总体架构

## 2.1　高速网络信号收发模块

该模块将骨干网络的高速光纤信号转换为电信号,并发送给核心处理模块进行物理层、数据链路层的处理,以恢复出数据包。该模块能够接收后端设备的反馈数据并发送至骨干网络中。其过程与接入过程相逆。信号接入和发送的过程中,在满足高速处理需求的前提下,要尽可能保证低丢包率和低误码率。

随着光纤通信技术的发展,以 100 Gb/s DP-QPSK 规格的信号来说,其收发要完成调制解调、数模转换等一系列处理[9],处理过程难度相对较大,目前满足此类超高速率的处理设备需进行定制;即使对于100 Gb/s WDM 信号的处理,除了所需的 QSFP 模块以外,还需搭配专用的变速箱(Gearbox)芯片,处理难度也相应增加。

对于单光纤 10 Gb/s 的处理技术相对比较成熟,模块集成度高、成本低、使用简单。在业界实现多格式光信号接收一般采用一体化模块,主要包括 XFP(10 Gigabit Small Factor Pluggable)和 SFP +(Small Form-factor Pluggable)两种:XFP 模块通常工作在 850 nm、1 410 nm 或 1 550 nm 的近红外波长下,主要应用包括 10 Gb/s Ethernet、10 Gb/s 光纤通信、OC-192 和 STM-64 的同步光网络(SONET/SDH)、10 Gb/s的光传送网(Optical Transport Network,OTN);SFP 是一种支持热插拔的紧凑型光模块收发器,调试使用时更加方便,主要用于数据通信领域,由于 SFP 尺寸较小,在大多数应用领域已经取代了千兆接口转换器(GBIC),故 SFP 也被称为小型化的 GBIC(Mini-GBIC)。

SFP + 是 SFP 的升级版,即增强型 SFP,支持数据速率高达 16 Gb/s。SFP + 可支持 8 Gb/s 光纤通信、10 Gb/s Ethernet 以及 10 Gb/s OTN 等标准。SFP + 相对于 XFP 在空间利用率和集成度上具有明显的优势。其次,采用简单电源供电,SFP + 的工作稳定性也更高,故障率较低,功耗更低。故系统平台设计采用 SFP + 实现高速信号光电转换,利用核心处理器件 FPGA 中高速收发器(Transceiver)完成对信号的物理层和数据链路层的处理。

## 2.2　系统核心处理模块

系统核心处理模块主要负责系统整体的控制、各个模块工作状态配置以及数据处理和调度。完成的主要任务包括各功能模块的配置、信号部分物理层和数据链路层处理、信息交互以及各模块之间的协调管理和控制。

在设计时主要有以下考虑:首先,要考虑接入速率,高速网络流识别系统所处理的对象来自骨干网络,其高速率大容量的特点要求系统至少能够完成单链路 10 Gb/s 信号的接入;其次,在系统的开发过程中要便于升级、更新,从而便于未来对系统功能进行优化。目前主流的网络信号处理系统通常有四种方案:一是通用处理器的应用方案;二是基于专用集成电路的应用方案;三是基于网络处理器的应用方案;四是基于现场可编程门阵列的应用方案。表 1 列出了四种处理器件的对比[10-11]。

表 1　四种常用核心处理器件对比

| 对比方面 | GPP | ASIC | NP | FPGA |
|---|---|---|---|---|
| 开发周期 | 短 | 长 | 较短 | 短 |
| 开发环境 | 较丰富 | 单一 | 较丰富 | 丰富 |
| 灵活性 | 一般 | 差 | 较好 | 非常好 |
| 处理速度 | 慢 | 较快 | 快 | 快 |
| 可扩展性 | 好 | 较差 | 一般 | 好 |
| 逻辑处理能力 | 一般 | 一般 | 差 | 好 |

本文设计的高速网络流识别处理平台采用 Stratix V GX 系列 5SGXA7K2F40 芯片,该型号 FPGA 具有 62.2 万个逻辑元素和 93.9 万个寄存器,36 个支持 14.1 Gb/s 速率的高速收发器和超过 800 个通用输入输出口即 GPIO,全局可支持 6 个频率达 1 066 MHz的高速缓存 DDR3 接口。而且 FPGA 支持高速嵌入式硬核、软核设计,支持多种网络传输格式的解调,如集成有 10GbE、Interlaken 芯片间互联协议编码器等。因此,基于查找表结构的 FPGA 将作为高速网络信号分析处理平台的处理核心。

### 2.3 高速网络流缓存模块

该模块提供大量的缓存空间,主要完成数据的缓存和流级信息的识别。

处理平台设计用于满足四路光纤信号,同时平台应满足最高速率达 40 Gb/s 的数据量压力测试。显然短时间内如此大量的数据是无法在核心器件模块中完成存储的,从而更难以完成数据流的识别。因此,在系统平台中设计缓存模块是有必要的,以确保大量数据访问时系统的稳定性。网络流的完整性对于流识别分析十分重要。在网络中,无法在单个数据包中完成大量数据的传输,往往通过多个数据包进行分组传输。对于流识别分析处理系统,如果单单只关注单个数据包,会丢失很多重要信息。此时,通过对数据的高速缓存和信息重组以获得完整流级信息显得十分重要。目前技术领域中可实现高速缓存的方案主要包括 Flash、Cache、DDRAM 等。考虑到所需的传输速率和内存带宽以及目前 DDR4 和 DDR5 主要用于显存,选取 DDR3 作为高速网络流缓存模块的核心器件。DDR3 为了提高系统性能增加了点对点连接(point-to-point,P2P),这也是 DDR3 与 DDR4 的关键区别。在 DDR3 系统中,一个内存控制器只与一个内存通道打交道,从而大大地减轻了地址/命令/控制与数据总线的负载。Altera DDR3 SDRAM 高性能控制器为 DDR3 提供了简化的接口。

为满足最高达 40 Gb/s 的接入速率,数据每秒的储量至少为 40 Gb/8 = 5 GB。一般情况下,64 位宽 DDR3 模组已经普遍成为主流,根据 JEDEC 标准 DDR3 最低等级等效传输频率也为 800 MHz,如表 2 所示。

表 2 某厂商几种 DDR3 模组速率

| 工业标准 | 时钟频率/MHz | 等效频率/(MT/s) |
|---|---|---|
| PC3-14900 | 933 | 1 866 |
| PC3-12800 | 800 | 1 600 |
| PC3-10600 | 667 | 1 333 |
| PC3-8500 | 533 | 1 066 |
| PC3-6400 | 400 | 800 |

由于在时钟的上下沿均进行采样,等效频率(MT/s)表示单位时间内的传输次数,就是内存工作频率的 2 倍。事实上,硬件系统本身在执行速率上不会达到非常高,结合 FPGA 输入输出结构规范,在频率不超过 533 MHz 的情况下,考虑一般 DDR3 工作中的地址输入、命令控制以及非常重要的自刷新过程,可以假设效率不超过 50%,因此一个最高频率为 800 MHz 的 4 GB DIMM 模组在 533 MHz 频率下的带宽为 533M × 64 × 2 × 50% = 34.112 Gb/s,显然一个模组是不满足性能要求的。如果使用 2 个模组,那么 34.112 Gb/s × 2 = 68.224 Gb/s > 40 Gb/s,且总量 8 GB > 5 GB。

由此可以得出结论,识别处理平台采用 2 个工作频率达到 533 MHz、单片容量是 4 GB 的 DDR3 内存模组是完全满足系统设计要求的。并且考虑物理尺寸最终采用了直插插槽的标准 VLP MINI-UDIMM,总容量为 8 GB。

### 2.4 高速网络流内容匹配模块

该模块核心功能是完成规则匹配工作,通过比对选出满足条件的数据,为数据分流提供依据。此外还提供一定的存储空间供匹配规则的存储使用。

网络链路速率的快速增长和分类匹配规则的增多,给高速网络内容匹配模块设计带来了挑战。以本文设计的流识别设备为例,当骨干网络链路速率达到 40 Gb/s、数据报文长度为 40 B 时,每个数据报文的处理时间应小于 8 ns,如此短的处理时间在 FPGA 内部利用软件算法实现难度较大。为了满足上述处理需要,寻求硬件解决方案是可行的。内容可寻址寄存器(Content Addressable Memory,CAM)是一种专用于高速搜索功能的计算机存储器,其搜索功能的实现主要有三种操作:写操作、读操作、查找操作。读、写操作与一般存储器相同;查找操作过程中,输入要搜索的数据,并将其与存储数据表中的数据进行比较,并返回匹配数据的地址[12]。

高速网络流识别处理平台内容匹配模块的核心器件选用 Netlogic 公司 NL3300 系列(型号为 NL3360DFVH-266H)。NL3300 可配置数据表中每一条规则的位宽为 72 bit、144 bit、288 bit 或 576 bit,以 IPv4 五元组匹配为例,五元组数据长度为 13 B(104 bit),故需配置 TCAM 的数据表每一条规则的位宽为 144 bit。根据以太网与 POS 信号的帧结构可知,POS 信号的开销包括分界符、帧头以及 CRC 共 9 B;以太网信号的开销包括帧间隙、前导码、定界符、目的 MAC、源 MAC、协议类型以及 CRC 共 38 B。

由于 POS 信号开销较小、承载能力较强，此时考虑到极端情况，每路传输速率为 10 Gb/s 的 POS 信号，由于 IP 网络包长平均为 200 B，故可知此时系统每秒接收数据包为 4 × 10G ÷（200 + 9）÷ 8 = 23.9M 个，TCAM 需要满足在五元组 104 bit 位宽基础上的处理带宽为：144 bit × 23.9 M/s = 3.44 Gb/s。数据总线宽度为 72 bit，当 TCAM 的工作频率为 266 MHz 时，TCAM 实际的匹配带宽为：72 bit × 2 × 266 MHz = 37.5 Gb/s，远远大于所需的 3.44 Gb/s，显然所选 TCAM 可以满足设计要求。

### 2.5 数据管理模块及相关辅助模块

数据管理模块主要包括一个 RJ45 千兆网口及相应的 PHY 芯片（用于与上位机进行通信）和一片 Flash 闪存芯片（用于在系统掉电后存储匹配规则）。数据管理模块与上位机之间采用千兆以太网进行通信。由于 FPGA 强大的处理能力，平台与 PC 之间的通信可以采用 SFP 来完成，FPGA 的高速通道也是完全够用的。然而，由于所设计的电路板在硬件空间上还存有余量，在不影响信号走线的前提下，采用 RJ45 接口加外置物理层芯片的方案减少了硬件成本。

时钟模块为上文中所设计的各个模块芯片提供相应的工作时钟。由于所使用的芯片功能不同、规格不同，各个模块对时钟的频率与精度要求也不同。不同频率时钟信号的获得是通过锁相环倍频与分频的功能来实现的。对于精度要求不高的时钟，如数据管理模块中使用的 SPI 接口工作时钟，可通过外置晶振直接产生时钟信号，调用 FPGA 内置 PLL IP core 便可得到所需时钟，实现上简单易行，操作灵活。而对于高精度时钟信号，主要是通过高精度芯片来产生的。时钟芯片的本质就是锁相环，设计使用 Si5326 型号时钟芯片，通过配置芯片寄存器，可产生的时钟频率范围为 2 kHz ~ 935 MHz。系统设计采用了 6 片时钟芯片，分别为 4 个 SFP、TCAM、PCI-express 接口提供高精度时钟。在对时钟芯片中各个寄存器功能了解的前提下，寄存器配置流程与 TCAM 寄存器配置相同。

根据所选器件的工作要求，本系统中涉及的电源网络主要有 0.85 V、1.0 V、1.5 V、2.5 V、3.3 V 等，通过改变电源芯片的外挂配置电阻即可完成不同电源的配置。

## 3 系统功能测试与结果分析

系统测试主要针对高速网络信号的接入与处理，具体包括信号的收发、缓存、数据包关键字提取与匹配。利用 Altera 配套的 FPGA 专用调试软件 Quarters Ⅱ 13.1 和超高速集成电路硬件描述语言（Very-High-Speed Integrated Circuit Hardware Description Language，VHDL）编写相应功能代码对各模块信号进行实时捕获并进行分析，对基本功能的测试验证系统平台的合理性和可行性。

### 3.1 信号接入与数据包提取测试

系统通过 SFP + 接入 10 Gb/s 以太网信号，完成光电转换，通过 FPGA 高速网络信号收发模块，在 156.25 MHz 工作时钟下，将通过光电转换的输入信号进行串并转换成 64 位宽的并行数据。通过 Quarters Ⅱ 内置的调试工具 SignalTap 对关键信号进行触发式采集，结果如图 3 所示。其中 ETH_RX_SOP 表示以太网数据包的包头信息；ETH_RX_EOP 表示以太网数据包的包尾信息；ETH_RX_VALID 表示以太网数据包有效载荷；ETH_RX_DATA 则表示数据包载荷信息，包括符合以太网传输标准的数据包包头信息。

根据以太网信号帧格式，可知数据包相关信息所在位置，结果如图 4 所示。

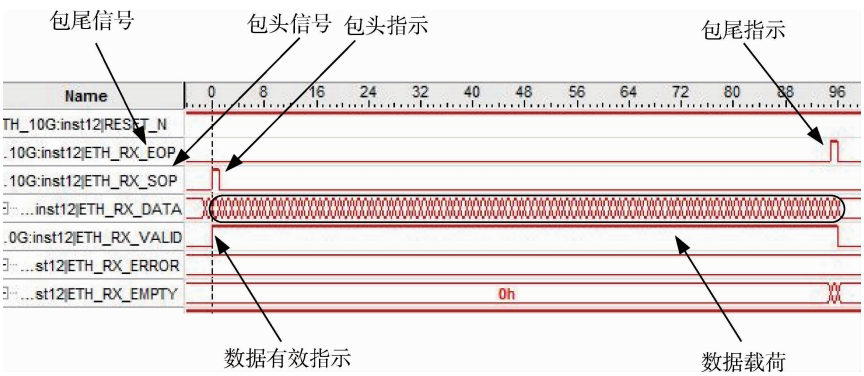


图 3 数据包的捕获

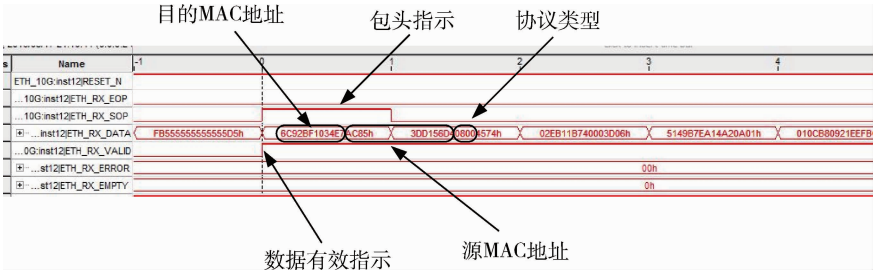


图 4　数据包 MAC 地址

### 3.2　关键词提取与匹配测试

本系统已应用于珠海某公司食品安全追溯系统,服务于食品生产企业、消费者以及政府监管部门。根据该公司对数据包处理的特殊要求,在对网络信息内容进行匹配时,不仅要识别出数据流中包含的五元组信息,还要识别出深层的信息,如用户查询的食品类型、食品的生产时间。只有在五元组信息、食品类型、生产时间等信息都符合规则的情况下才完成对一个数据包的匹配识别。

在完成数据包提取之后,根据食品安全追溯系统的要求,需要对数据包中五元组以及生产日期、类型信息进行提取。根据 IP 包格式规定,可在直接特定位置提取到五元组信息。而根据数据包类型的不同,生产日期、类型信息的位置是不同的,这就需要依靠搜索关键字来完成。搜索关键字采用了基于 TCAM 的线性搜索算法,在数据量不是很大的情况下,该算法具有原理简单、易于实现的特点。本系统处理的数据包主要来源于用户手机端上传,根据用户所使用查询设备的不同,数据包主要有两种:一种来源于 iOS 设备用户,一种来源于 Android 设备用户。以 iOS 用户数据包为例,选取“ataDeal/”为提取关键字,数据包格式如图 5 所示。根据是否搜索到关键字与关键字的位置,可提取出待匹配数据。

通过搜索关键字,可以从数据包中得到生产日期、类型信息。SignalTap 捕获信号如图 6 所示。

### 3.3　数据管理单元测试

为满足对匹配规则的在线更新,本系统还设计了专用的上位机,大大增加了对系统状态的监测效率。上位机主要完成以下两个功能:

(1)配置功能。根据目前对系统所处理数据量的预测,共预留有黑名单、白名单各 1 000 条,食品类型 32 种,食品生产时间可任选。

(2)监测功能。能够实时查看此系统对数据的识别情况,并对流经系统的数据进行简单分析。

图 7 所示为数据管理上位机软件整体界面。图 8 所示为上位机实时显示界面。

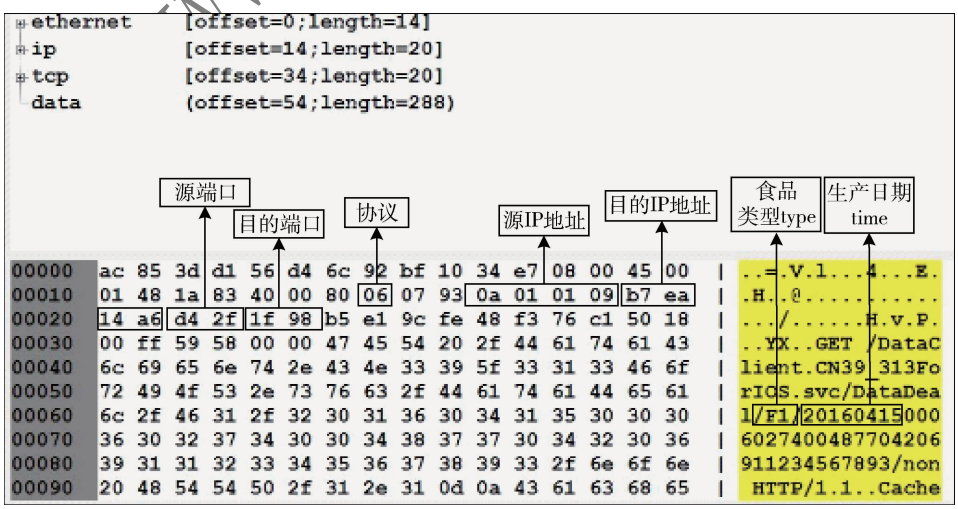


图 5　数据包格式

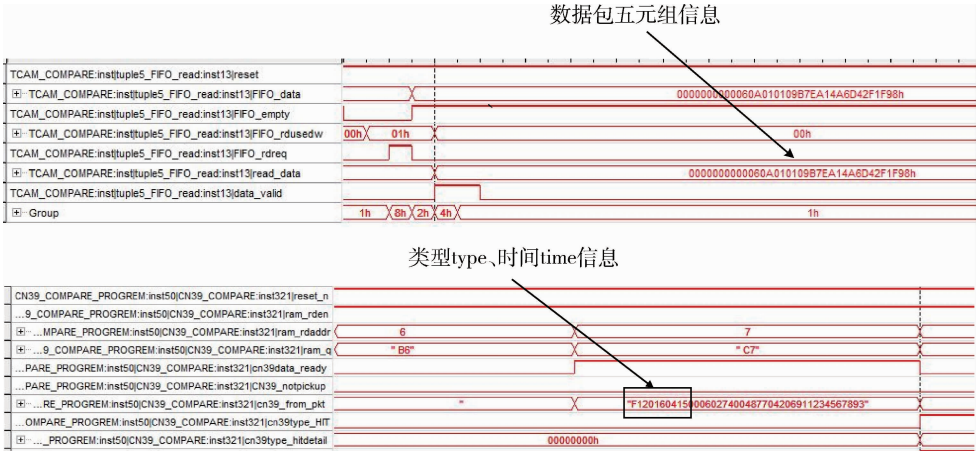


图 6　关键词提取

图 7　数据管理软件整体界面

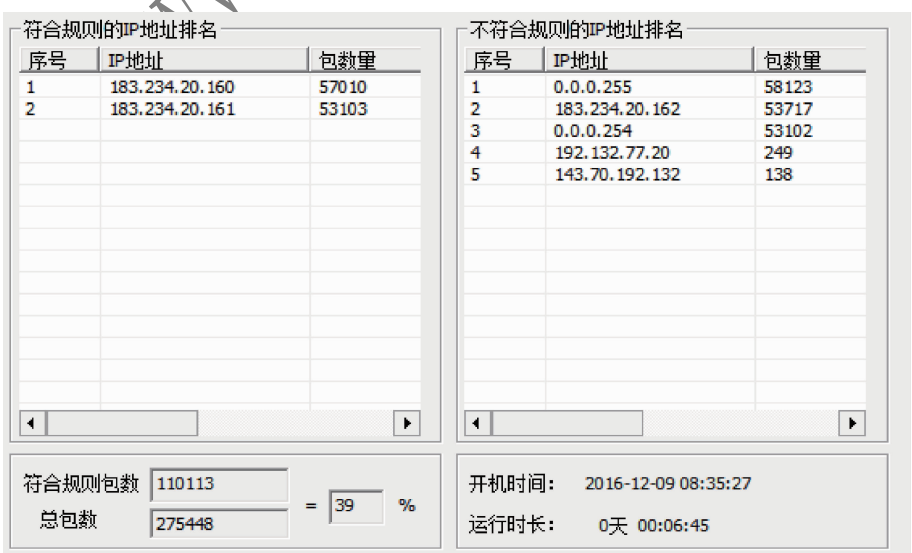


图 8　数据包分类结果显示

### 3.4 测试结果分析

通过上述对系统平台的测试结果显示,此系统在应用于某食品安全追溯系统时,能够完成信号接入、数据包提取、关键字匹配等功能。虽然在此应用中对于数据包的处理结果只有两种:允许通过和丢弃,"分类"功能显示不是十分充分,但是如果将此系统应用于其他应用背景,平台后端接入多个处理设备,增加平台输出通道数量,那么此平台的"分类"功能可进一步增强。

## 4 结束语

目前,骨干网络传输速率不断提高,对高速网络信号处理系统的需求十分迫切,骨干光网络高速率大带宽给整个网络空间的管理带来了许多问题。高速网络流识别处理技术作为网络空间测控领域关键技术之一,对其进行研究是十分有必要的,也极富有挑战性。本文从高速网络流识别分析处理的需求出发,设计了用于高速网络流识别分析处理的系统平台,基于所设计的系统平台,研究了高速网络内容识别技术的关键问题,最后对系统性能进行了测试,并对测试结果进行了分析。

本文设计的高速网络流识别处理平台还具有一定的局限性,主要体现在系统平台的多业务能力承载不足以及高速网络内容识别算法性能还不够高效。随着未来骨干网络传输速率的提升、业务格式的增多,对网络空间数据监测技术、对高速骨干网络流识别分析处理技术的研究将会取得更大的突破。

## 参考文献


[1] CNNIC. 第 44 次中国互联网络发展状况统计报告[EB/OL]. (2019-08-××)[2019-11-01]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201908/P020190830356787490958.pdf.

[2] CNCERT/CC. 2018 年中国互联网网络安全报告[EB/OL]. (2019-07-××)[2019-11-01]. http://www.cert.org.cn/publish/main/upload/File/2018annual.pdf.

[3] 李丹丹. 基于网络流行为的网络流分类技术研究[D]. 哈尔滨:哈尔滨理工大学,2015.

[4] 夏海平. 高速网络信号接入与分流技术研究[D]. 长沙:国防科学技术大学,2015.

[5] 鲁佳琪. 多规格信号接入与高速网络流检测技术研究[D]. 长沙:国防科学技术大学,2016.

[6] 刘康. 网络流分类中的特征选择研究[D]. 扬州:扬州大学,2013.

[7] SINGH S, BABOESCU F, VARGHESE G, et al. Packet classification using multidimensional cutting[J]. ACM Sigcomm Computer Communication Review,2003,33(4):213-224.

[8] 刘德胜. 高速网络内容分析识别系统关键技术研究[D]. 长沙:国防科学技术大学,2016.

[9] 肖昌成,黄芝平,逄鑫,等. 100 Gb/s OTN 信号接入技术研究[J]. 光通信技术,2018,42(3):14-16.

[10] MCCANNE S, JACOBSON V. The BSD packet filter: a new architecture for user-level packet capture[C]. Proceedings of the USENIX Winter 1993 Conference. USENIX Association,1999:259-269.

[11] 李昀晖. 基于网络处理器的流分类系统研究与设计[D]. 北京:北京交通大学,2008.

[12] 朱晴. 基于 FPGA 大流量数据识别与分流系统的设计与实现[D]. 南京:南京航空航天大学,2011.


(收稿日期:2019-11-19)


**作者简介:**

路琪(1994 - ),男,硕士研究生,助教,主要研究方向:高速网络信号处理技术、信息对抗技术、深度包检测(DPI)与深度流检测(DFI)算法。

高翔(1993 - ),男,硕士研究生,助理工程师,主要研究方向:信息对抗技术。

许晓(1993 - ),男,硕士研究生,助理工程师,主要研究方向:导航制导与控制技术。

# 版权声明