基于深度包检测的防火墙系统设计

路 琪 黄芝平 鲁佳琪

(国防科技大学机电工程与自动化学院 长沙 410073)

摘 要 随着互联网的飞速发展,防火墙作为网络安全防护的重要手段已经成为了人们研究的重点。为了能够高效地过滤无关数据报文、抵御恶意攻击、保障网络的安全稳定运行,在研究深度包检测技术的基础上,提出了一种基于现场可编程门阵列、三态内容可寻址寄存器架构而实现的硬件防火墙系统。测试表明,该系统能够满足实际要求。

关键词 深度包检测,硬件防火墙,现场可编程门阵列,三态内容可寻址寄存器

中图法分类号 TP393,TP302 **文献标识码** A

System Design of Firewall Based on Deep Packet Inspection

LU Qi HUANG Zhi-ping LU Jia-qi

(College of Mechatronics Engineering and Automation, National University of Defense Technology, Changsha 410073, China)

Abstract With the rapid development of the Internet, as an important means of network security, firewall has become the focus of research. In order to effectively filter the irrelevant data packets, resist the malicious attacks, and ensure the safe and stable operation of the network, on the basis of researching on the deep packet inspection (DPI) technology, a firewall system based on field programmable gate array (FPGA) and ternary content addressable memory (TCAM) was presented. The test results show that the designed firewall system based on deep packet inspection technology can meet the actual requirements.

Keywords DPI, Hardware firewall, Field programmable gate array, Ternary content addressable memory

1 引言

随着互联网技术的高速发展及网络环境的日益复杂,为了保障网络的安全运行和用户数据资料的安全,防火墙技术应运而生并得到了飞速的发展。防火墙技术主要包括3种:包过滤防火墙、状态检测防火墙和深度包检测防火墙[1]。

包过滤防火墙没有状态的概念,属于第一代防火墙,工作在网络层。通过五元组(源IP地址,目的IP地址,源端口,目的端口,协议号)的匹配对数据包进行过滤,管理员能够允许或者禁止其通过。但是,此类防火墙的最大缺陷在于无法感知上层的信息,易被欺骗,从而遭到黑客攻击。因此,包过滤防火墙的安全性较差。为了提高防火墙的安全性能,状态检测防火墙技术应运而生。

状态检测防火墙采用了状态检测包过滤技术,是对传统包过滤的一种功能扩展。它同样工作在网络层,依据五元组信息对数据包进行处理,不同之处在于状态检测防火墙能够通过感知会话信息来做出决策。处理数据包时,状态检测防火墙会先保存数据包中的会话信息并判断其是否被允许。由于数据包在传输过程中会被网络设备(如路由器)分解成为更小的数据帧,状态检测防火墙设备会先将这些小的IP数据帧按顺序重组为完整的数据包后再进行决策。但是,在设计状态检测防火墙时,无法对遭受攻击的应用程序进行防护,使得应用程序受到极大的威胁。在此背景下,深度包检测防火墙技术应运而生。

深度包检测防火墙基于深度包检测技术(Deep Packet Inspection,DPI),在包过滤技术、状态检测技术的基础上能够对TCP或UDP数据包内容进行深入的分析,从而能够抵御复杂网络中应用程序受到的攻击,提高了防火墙的性能和内部网络的安全稳定。

文献[2]提出了一种深度包检测引擎的FPGA硬件实现方法,平台采用了FPGA+MCU+TCAM的设计架构,整体功能较完整。但是,此平台处理能力有限,接入速率较低,架构相对复杂。文献[5]提出了基于FPGA+TCAM架构的网络分流系统,精简了硬件结构,提高了平台接入速率和处理能力,但是对数据的分流处理仅仅局限于五元组匹配,处理深度明显不足。为了兼顾处理能力和处理深度,并满足高接入速率和深度处理的实际需求,本文设计了基于深度包检测技术的网络硬件防火墙系统。

2 深度包检测技术

深度包检测技术是一种直接面向数据分组中特定字符字段且能完成负载内容提取、匹配、分析并按照既定数据库策略识别等一系列操作的深度解析技术。检测的信息包括数据分组标识信息(如IP包头地址协议信息等),以及内容负载信息(如文本语音等内容);技术的硬件实现方式可以是基于FPGA或网络处理器等底层处理核心的硬件加速设备,也可以是基于现行Windows、Linux或Unix等操作系统的高级层软件系统,如开源分布式SNORT入侵检测系统。

深度包检测技术的实现过程的一般参考模型如图1所示。ISO/OSI模型与TCP/IP模型在层级定义上有所区别。

路 琪(1994-),男,硕士生,主要研究方向为网电空间测控,E-mail:qq466729206@icloud.com(通信作者);**黄芝平**(1965-),男,博士,教授,博士生导师,主要研究方向为网电空间测控;**鲁佳琪**(1990-),男,硕士,主要研究方向为网电空间测控。

深度包检测是传统普通报文检测在横向与纵向上的扩展。传统的普通报文检测技术(或者被称为状态检测技术)的检测对象主要针对前三层,习惯上更关注“五元组”的信息。深度包检测技术在实现上已有多种算法,但是归结起来可以概括为两种具体方法:字符串模式匹配和基于正则表达式。由于字符串模式匹配的方法简单可行,且目前匹配所需的信息数据库规模不大,因此本系统采用 TCAM 硬件匹配算法。

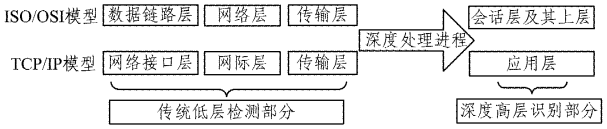

图 1　深度包检测的一般参考模型

3　防火墙系统的硬件平台设计

鉴于骨干网传输速率的大幅度提升,需要既满足目前的网络状况又面向未来发展的更高效的互联技术,高速网络信号深度处理平台是一种可扩展、高密度、易构建的体系结构。可扩展性可以实现总体系统平台的快速升级,及时适应现实物理条件的变化,从而保证即使在高载荷效率的情况下也能在一定期间内保持深度处理功效。基于系统的高密度,可以实现单机设备对大量信息的采集、分析与处理,其体积更小,重量更轻,可以满足接入处理过程的透明性、便捷性、易构建性等要求。在满足当前实际链路需求的前提下,突出系统的实用性、可靠性、可维护性和低成本。

本文设计了基于深度包检测技术的网络防火墙系统用于某食品安全的追溯。对数据包进行处理时不仅要过滤满足相应五元组条件的数据包,还要过滤满足相应应用层信息(如食品类型 type、生产时间 time)的数据包。

图 2 所示为食品安全追溯系统的整体布局。硬件防火墙的设计采用 FPGA+TCAM 架构,现场可编程门阵列(Field Programmable Gate Array,FPGA)具有强大的并行处理能力,算法在底层硬件上实现,开发时间短,在网络信号处理方面具有明显的优势;三态内容可寻址寄存器(Ternary Content Addressable Memory,TCAM)具有并行全相联结构,在一个周期内即可获得匹配结果,相比于内容可寻址寄存器(Content Addressable Memory,CAM),TCAM 的每一个匹配位不仅可以存储为“0”或“1”,还可存储为“X”,从而进行模糊匹配,使得匹配范围更加广泛。

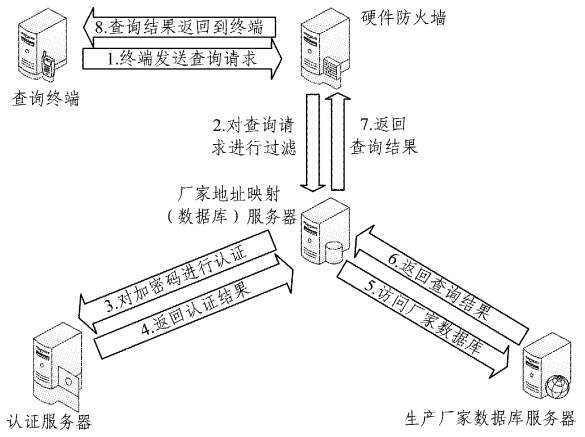

图 2　某食品安全追溯系统

由信号处理的基本流程可知,系统的功能应该包括信号的采集与获取、信号的处理、信号的存储等,并且由于食品安全追溯系统的用户量庞大,设计的防火墙应能满足高速、大容量网络信号的接入和处理需求。基于上述功能和要求,将此防火墙硬件系统分为 5 个模块:高速网络信号接入单元、核心处理单元、数据缓存单元、硬件匹配单元、在线管理单元。图 3 给出了防火墙系统方案的整体设计方案。

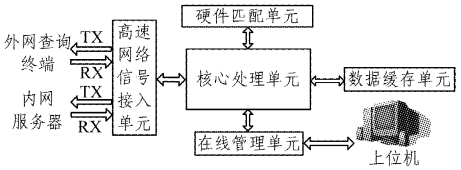

图 3　防火墙系统的整体方案

3.1　高速网络信号接入单元

接入模块接收外网通道的光信号,将其转换为电信号并同步解扰后还原成原始帧数据。该模块为保证线速处理的要求,其输出速率必须达到 Gbps 量级且尽可能地限制丢包率。

光网络接收模块作为系统分析处理信号的来源,其兼容性、稳定性、误码率等会对处理结果产生重大影响。当前光纤骨干网络的单波主流传输速率为 10Gbps,设计的系统平台应能满足 10Gbps 及以下速率网络信号的接入。硬件网络防火墙系统主要针对 10Gbps 信号的接入,因此在光电转换领域中,实现 10Gbps 速率的接收的主要方式有高端口密度和低成本,一种基于 SFP+技术,另一种基于 XFP 技术。SFP+技术的前身即 SFP 技术主要应用在 1G 和 4G 速率领域,随着时代的进步,满足更高速率的 SFP+技术应运而生。相比而言,SFP+在接口定义上类似于 SFP 接口定义;在物理特性上,SFP+没有做任何修改。在性能上,SFP+光模块及接插件能够支持的最大速率已经突破 10Gbps。SFP+具有比 SFP 更严格的电磁屏蔽要求,标准规定它必须具备更好的屏蔽效果。考虑到 SFP+可以保证 10Gbps 的通信容量且满足前向和后向兼容性,能实现硬件模块低成本且高密度集成,目前它被认为是 10G 传输光收发器的理想解决方案。因此,系统光模块采用标准 SFP+接收模块,不仅能顺利接收高速信号,而且还适应未来新协议技术。系统设计采用了 4 路集成化接口来收发多种业务的网络数据,接入速率高达 40Gbps。

3.2　核心处理单元

核心处理单元是整个系统的主控部分,与高速缓存模块和硬件匹配单元进行数据信息交互,连接智能管理模块并监控系统的执行过程。它完成了深度处理解析工作,包括原始帧数据接入后的 IP 包提取、高速流缓存、关键信息匹配操作、依据规则负载均衡转发输出、监控信息收集以及其他重要系统性功能。

根据高速网络信号深度处理系统的功能需求,选择处理核心时必须首先满足速率为 10Gbps 的数字信号接入要求;其次,对于高速信号同步、解扰、IP 包提取等技术,逻辑运算能力成为制约性能效果的主要因素;再者,面对网络日新月异的发展,处理网络信息的技术也在深入和提高,这就要求处理核心在软件层面上支持易修改、可以任意编程等特性。

在目前的网络应用中,主流处理核心通常采用 3 种方案:1)基于 ASIC 专用集成电路的应用方案;2)基于 NP 网络处理器的应用方案;3)基于 FPGA 现场可编程门阵列的应用方案。结合这 3 种方式,表 1 对包含通用处理器(GPP)在内的 4 种处理器件进行了对比。

表 1 4 种常用处理器件的对比

对比方面	网络处理器	通用处理器	FPGA	专用集成电路
开发周期	较短	短	短	长
开发环境	较丰富	较丰富	丰富	单一
灵活性	较好	一般	非常好	差
处理速度	快	慢	快	较快
可扩展性	一般	好	好	较差
逻辑处理能力	差	一般	好	一般

专用集成电路(Application Specific Integrated Circuit,ASIC)是一种具有特定功能的专用定制集成电路,例如设计用于数字录音机的芯片就是 ASIC。ASIC 具有芯片面积利用率高、功耗低、处理速度快以及使用成本低廉的优点,但是其本身设计过程的周期长、工作量大、错误率高,这是因为其内部硬件被优化固定后,灵活性大大降低。

网络处理器(Network Processor,NP)是一种可编程器件,专门针对高速网络应用处理而设计。仅从设计目的来看,NP 在硬件上已经针对多种网络应用做出了特殊的优化,其在牺牲一定通用性的情况下获得了可编程能力,灵活性大大提高,从而可以快速适应网络协议应用的变化。NP 网络处理器成功的关键在于它具有一个能在面对高速网络流的情况时保持高级应用层面的处理能力的架构。

从广义上来讲,现场可编程门阵列(Field Programmable Gate Array,FPGA)也是 ASIC 系列中的一种特殊集成芯片。它也是一种基于 LUT 查找表技术,在 PLD 可编程逻辑器件的基础上应用静态随机存取存储器即 SRAM 进行可编程的集成电路。作为一种半定制电路,相较于 ASIC 固定电路,其灵活性、扩展性以及可重复编程等特性赋予了 FPGA 非常广阔的应用前景,目前在通信、网络、航天、计算等诸多领域已经得到大量应用。实际上,FPGA 还有设计周期短、测试验证方便、厂商提高全面的开发环境、编程形式多样等优势。

从表 1 可知,FPGA 是基于 SRAM 查找表的逻辑结构,因此在逻辑解析方面,尤其是针对网络高速信号(诸如与或、异或操作等逻辑运算)时拥有天然的优势,并且针对论文研究的高速光网络信号,以 Altera 公司产品 Stratix 系列为代表的 FPGA 已经集成了超高性能、面向高超速应用的高速收发模块,即高速 Transceiver,其全双工收发速率在 5SGX 和 5SGT 系列中已经分别达到 14.1Gbps 和 28.05Gbps,完全满足高速数字信号 4 路 10Gbps 的接入要求。

3.3 数据缓存单元

数据的完整性对匹配功能精确性的影响非常大,在高速光纤骨干网络中,数据以分组形式传输,有的数据包也被分解为数据帧后再传输。因此,为了对分组数据进行重组,保证其数据完整性,需要对数据进行缓存。从系统的稳定性考虑,接入 4 路 10Gbps 信号时最高接入速率达到了 40Gbps,故对高速数据缓存 1s 的容量至少需要 40Gb/8=5GB,带宽也至少需要 40Gbps。

目前常用的缓存技术方案有高速 Cache、Flash、DDR、固态硬盘 SSD 等。双倍速率同步动态随机存储器系列(Double SDRAM,DDR)在速度、容量和体积等方面优势明显,因此深度包检测防火墙系统采用 DDR3 作为 IP 包缓存结构。一般情况下 DDR3 的位宽为 64bit,采用双倍读写工作模式,单片容量为 4GB,结合 FPGA 输入输出结构规范,在频率不超过 533MHz 的情况下,可满足最高带宽需求为 533MHz×64×2=68.224Gbps>40Gbps;设计使用两片 DDR3 作为缓存单元,总量达到了 8GB>5GB。理论上,此设计满足接入速率为 40Gbps 网络信号的缓存需求。

3.4 硬件匹配单元

在完成数据包恢复和解析之后,将五元组信息送入硬件匹配单元进行匹配操作。在匹配单元的核心器件 TCAM 中存储了匹配数据库,只需将要匹配的数据送入匹配单元中即可。匹配单元会自动搜索匹配表项,返回最优匹配结果至核心处理单元 FPGA 中。核心处理单元 FPGA 根据匹配结果来决定此数据包是通过、丢弃还是进一步解析。由于 TCAM 中的匹配规则数据会在断电之后丢失,并且为了不占用核心处理单元 FPGA 过多的存储资源,在系统设计中加入了一片 FLASH 模块,从而使系统在上电后无需操作即可直接进行工作,简化了配置工作。

高速网络深度处理平台选用 Netlogic 公司的 TCAM 作为关健字匹配搜索模块。假设主要针对 IPv4/IPv6 五元组匹配,以 144bit 为信息提取位宽,考虑到极端情况,即 10Gbps 信息中有 15M 个包,那么 8 路 POS 信号利用网络搜索引擎时进行五元组匹配需要的带宽为 144×8×15M=17.28Gbps。系统所使用的 TCAM 传输总线接口采用并行双路搜索的工作方式,位宽达到 80bit,最高工作频率可到 300MHz,其匹配带宽实际为 2×80×300MHz=48Gbps,因此在要求系统可扩展性、运行稳定性和可靠性的基础上,采用冗余设计的理论计算值远远超过目标需求。

4 防火墙系统的软件设计

外网的数据通过高速网络信号接入单元进入此硬件平台。首先,在核心处理单元进行数据包的解析,提取五元组信息。将获取的五元组信息送入硬件匹配单元进行匹配,根据硬件匹配单元的反馈来得知此数据包是否命中匹配数据库中的信息,从而决定此数据包是否需要进一步解析。然后,对于不需要进一步解析的数据包,直接令其通过或将其丢弃;对于需进一步解析的数据包,在核心处理单元中对其进行深度解析,以获取包内食品类型 type 和生产时间 time 信息。可令食品类型 type 和生产时间 time 均满足限定条件的包通过核心处理单元并进入内网,否则丢弃。数据处理流程如图 4 所示。

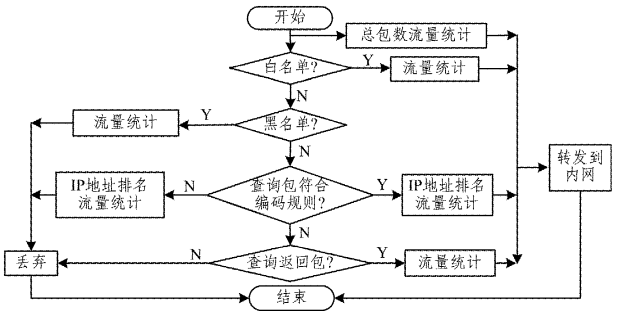

图 4 数据处理流程

此外,数据缓存单元满足了处理高速、大容量数据的需求;在线管理单元包含配套的上位机,可以在线对匹配数据库、食品类型 type、生产时间 time 等匹配条件进行更新和回读,大大增强了硬件系统的人机交互能力。

由于互联网用户量庞大,对新出现的威胁进行及时的化解是一个功能完善的网络防火墙必备的能力。本系统设计了

配套使用的上位机程序,能够对匹配规则进行更新,大大增强了系统使用的灵活性和扩展性。图 5 所示为上位机界面。

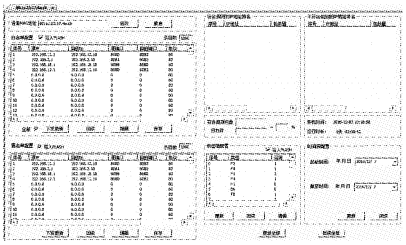

图 5　上位机界面

5　系统平台测试

系统测试主要从网络信号的接入处理、数据包解析、上位机测试 3 个方面开展。基于 Altera 公司专用开发环境 QuartusII 软件,采用 VHDL 作为基本硬件描述语言,并使用QuartusII集成的内建调试工具 SignalTap 对数据进行实时分析,以验证硬件防火墙系统的可行性。

5.1　测试信号的产生

测试信号源所用的软件测试仪可任意设定包内数据。设定的数据包内容如图 6 所示。数据包中包含五元组信息、类型 type 信息、时间 time 信息。

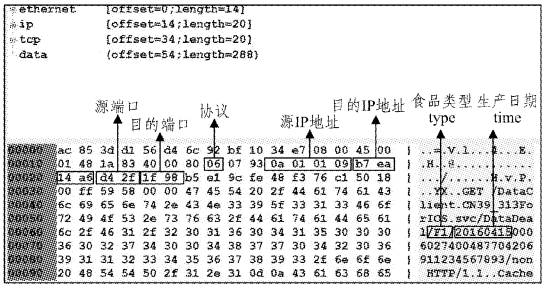

图 6　数据包格式

5.2　网络信号接入测试

调用 FPGA 内部高速网络信号的 PHY(physics) IP core 以及 MAC IP core,在对 IP core 进行配置之后,便可以完成接入信号处理并直接得到数据包。利用 SignalTap II 捕捉包头,结果如图 7 所示。

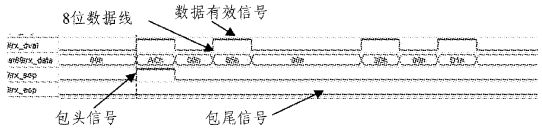

图 7　数据包的捕获

5.3　数据包的解析测试

在数据包的解析过程中主要对包结构进行分解,得到五元组信息、类型 type 信息、时间 time 信息。利用 SignalTap II 观察解析结果,如图 8 所示。

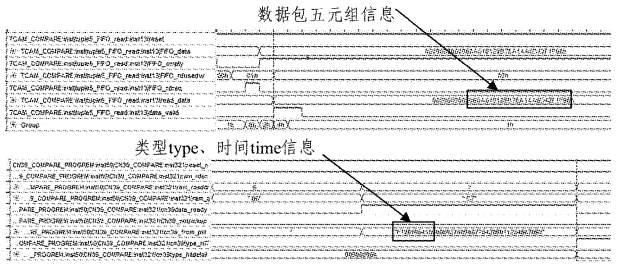

图 8　数据包相关信息的提取

5.4　上位机测试

上位机的功能主要有两个:1)在线配置黑名单、白名单、类型 type、时间 time;2)对匹配结果进行显示,上位机会显示出满足匹配要求和不满足匹配要求的数据包数,测试结果如图 9 所示。由此可见,此防火墙系统的功能基本得以实现。

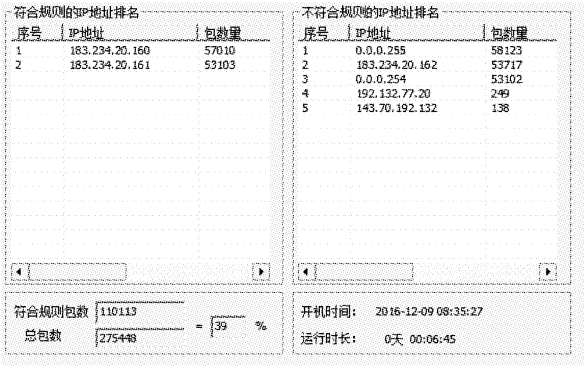

图 9　上位机实时显示界面

结束语　本文设计了一种基于深度包检测技术的硬件防火墙系统平台,其采用了 FPGA+TCAM 架构。该系统通过深度处理,能够实现对数据包的筛选和过滤。相对于文献[2,5]中设计的系统,本次设计结合了二者的优点,优化了硬件结构,提高了系统接入速率和数据包的处理深度。从测试结果来看,此系统能够实现高速信号的接入,不仅能利用传统的五元组匹配方式完成对数据包的过滤,还能够利用数据包的内部信息对其进行深度筛选,达到了设计的基本要求。未来将进一步对该系统的软硬件进行优化,使其适应更加复杂的网络环境。

参 考 文 献

[1]　陈宁,李忠. 一种防火墙新技术——深度包检测技术[J]. 重庆科技学院学报(自然科学版),2007,9(3):69-79.

[2]　陈世文,黄万伟,曹建业. 一种深度包检测引擎的 FPGA 硬件实现[J]. 测控技术,2014,33(6):100-109.

[3]　汪立东,钱丽萍. 网络流量分类方法与实践[M]. 北京:人民邮电出版社,2013.

[4]　王建东,祝超,谢应科,等. 基于 FPGA 的万兆流量并行实时处理系统研究[J]. 计算机研究与发展,2009,46(2):177-185.

[5]　鲁佳琪,黄芝平,刘纯武,等. 基于 FPGA+TCAM 架构的网络分流系统的设计与实现[J]. 微型机与应用,2016,35(15):65-71.

[6]　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.

[7]　ZHAN Y R. Deep Packet Inspection Based on Many-Core Platform[J]. Journal of Computer and Communications,2015,3(5):1-6.

[8]　CHU W C C,CHAO H C,YANG S J H,et al. Cost Analysis of Deep Packet Inspection in PCC Architecture[M]. IOSPress:2015.

[9]　SHARMA J,SINGH M. CUDA based Rabin-Karp Pattern Matching for Deep Packet Inspectionona Multicore GPU[J]. International Journal of Computer Network and Information Security (IJCNIS),2015,7(10):70-77.