网络流量实时监控分析系统的设计与实现

于　娟, 袁春蕾
(南京晓庄学院 数学与信息技术学院, 江苏 南京 211171)

摘　要 :网络流量监控分析是网络管理与网络安全的重要组成部分。文章介绍了一种基于深度报文检测技术的网络流量实时采集分析系统RT-TMA, 同时给出了其设计框架和关键技术实现方法。测试结果表明, 该系统运行稳定、准确, 可以达到预期效果。

关键词 :深度报文检测 ;流量监控 ;流量分析
中图分类号 :TP393　　文献标识码 :A　　文章编号 :2095-1302(2013)02-0071-03

Design and implementation of real-time network traffic monitoring and analysis system

YU Juan, YUAN Chun-lei
(School of Mathematics and Information Technology, Nanjing Xiaozhuang University, Nanjing 211171, China)

Abstract: Network traffic monitoring and analysis is an essential part of network management and network security. A real-time network traffic monitoring and analysis system based on deep packet inspection (DPI), named as RT-TMA, was developed and its framework and the implementation method of key techniques are given in this paper. The experiment results show that the system has stability and accuracy and achieves the desired results.

Keywords: deep packet inspection; traffic monitor; traffic analysis

0 引 言

随着计算机网络的快速发展和普及, 各类网络应用层出不穷。当前, 计算机网络的规模越来越大, 业务也越来越复杂, 系统对网络的可靠性、可用性及网络服务质量的要求也越来越高。网络流量监控分析 [1] 可以在很少甚至完全不影响现有网络的情况下, 对计算机网络的运行状况进行全面的监控分析, 是实现网络管理和网络安全防护的重要组成部分。高效合理地运行网络流量实时监控分析系统, 可以在最短时间内发现安全威胁, 并在第一时间进行分析, 确定攻击源。结合基于流量的网络管理系统 [2] 和入侵检测系统 [3] 等, 可以及时地发出威胁预警, 以便快速采取措施, 及时化解网络攻击, 确保网络的运行效率和安全。

网络流量监控分析的基础是协议识别技术, 目前的主要方法有常用端口识别、深度报文检测 (Deep Packet Inspection, DPI)、深度流检测 (Deep Flow Inspection, DFI)[4-7] 以及这几种方法的混合。常用端口识别技术是根据协议通信五元组中的端口号来识别应用的, 如常用的 HTTP 协议一般采用 80 端口, 以协议所用的端口号为 80 来识别 HTTP 协议。当前, 由于采用自定义端口、随机端口甚至加密隧道等应用日益增多, 采用常用端口识别已经很难满足需要。深度报文检测是根据各类应用的连接数、单个 IP 地址的连接模式、上下行流量的比例关系、数据包发生频率等数据流的行为特征, 来对流量的应用类型进行区分的技术 [4], 可以较好地识别出应用的类型 (如是否 P2P 应用等), 但无法对具体的应用进行详细的分析, 只能实现应用类型的初步归类。DPI 技术是一种基于特征字的识别技术, 可根据不同协议的特征 (包括协议所使用的端口、协议报文负荷 (payload) 中的特定字符串或特定的二进制数据等) 来检测和识别出具体的应用协议。DPI 具有检测准确率高、原理相对简单、实现速度快等多个优点, 因而具有较为广泛的应用。本文介绍的网络流量实时监控分析系统 (以下简称 RT-TMA, Real-Time network Traffic Monitor and Analysis system) 就是采用 DPI 技术来实现协议识别的。

基于 DPI 的网络流量实时监控分析系统在网络管理与网络安全防护中起着非常重要的作用, 而目前的网络流量实时监控

收稿日期 :2012-11-08
基金项目 :2012年江苏省大学生实践创新训练计划项目 (2012JSSPITP2042)

分析大都针对运行商的核心骨干网络，价格昂贵。此外，作为高校使用的网络流量监控分析系统，还需具备足够的可扩展接口，以便在完成网络管理与安全防护的同时，提供学生认知实习、开放性实验以及科研支撑。为此，本文提出了一种基于 DPI 的网络流量实时监控分析系统 RT-TMA。该系统具有高可扩展性、实现简单、接口丰富等特性，可较好地满足高等院校，特别是高校实验教学中心对网络流量实时监控分析系统的需要。

1 RT-TMA 的系统模型

RT-TMA 是一种被设计用于高等院校校园网、实验室网络及中小型企业的网络流量实时监控分析系统。与其他网络流量监控系统不同的是，RT-TMA 还提供有丰富的二次开发接口，为网络流量监控分析相关开发人员及科研人员提供理论验证和算法研究的实验平台。

RT-TMA 由高性能报文收发引擎 (Packet I/O Engine)、DPI 引擎、规则库、RT-TMA 用户界面以及可能的扩展库等几个部分构成，其体系结构如图 1 所示。

图 1 中的高性能报文收发引擎主要完成网络流量的采集以及可能的控制报文发送，可选的技术包括 netmap[8]、PF_RING[9] 和零拷贝网卡驱动等。通过对这些技术的具体实现接口进行封装，可使之对外提供规范的 libpcap 或 winpcap 接口，在确保对外接口函数不变的情况下，使 RT-TMA 可使用或测试多种不同的高性能报文收发引擎。

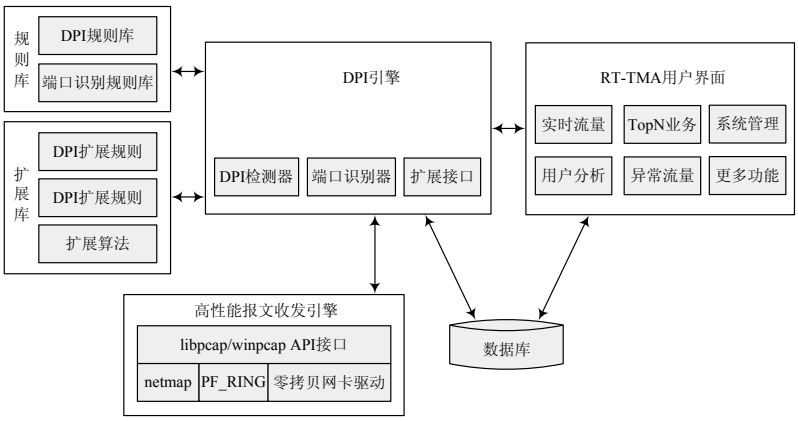

图 1 RT-TMA 体系结构图

规则库主要包括具体协议的 DPI 特征字及其检测算法的实现，同时包括传统规范网络应用的端口表，以用于配合 DPI 引擎完成对具体协议的识别。

DPI 引擎是 RT-TMA 的核心，可在 DPI 规则库、数据库 (配置信息等)、可选的扩展库以及用户操作等基础上，完成对网络流量的协议识别、统计、分析等功能。

RT-TMA 用户界面作为人机交互界面，主要提供用户操作和管理 DPI 引擎、显示各类信息等。

2 RT-TMA 的关键实现

RT-TMA 主要针对高等院校、实验教学中心和中小企业的网络进行流量监控分析，此外，RT-TMA 还可作为科研平台和实验平台来使用，因此，在 RT-TMA 的实现中，采用先实现全部功能再进行性能优化、先实现基本功能再进行二次扩展的思路。

2.1 基于 winpcap 的报文收发实现

考虑到 RT-TMA 对现有流量采集技术的兼容性，在高性能报文收发引擎的实现中，确保对上层提供统一的 libpcap/winpcap 接口函数，底层所用技术则根据硬件平台、网卡驱动、操作系统等各种因素决定。考虑到 Windows 操作系统的限制，RT-TMA 当前的报文收发引擎采用了 winpcap 来实现。后续根据需要，也可改用零拷贝网卡驱动或其他 NDIS 技术来实现。

winpcap 是 libpcap 的 Windows 版本，具有跟 libpcap 一样的接口函数。Winpcap 由一个核心的包过滤驱动程序、一个底层动态链接库 packet.dll 和一个高层的独立于系统的函数库构成，可提供一整套标准的报文收发接口，同时具有良好的性能。利用 winpcap 来实现流量采集的步骤及函数调用如下：

(1) 打开指定网卡。winpcap 提供了一个 pcap_open_live(const char *device, int snaplen, int promisc, int to_ms, char *ebuf) 函数来打开指定的网卡进行监控，其中第 3 个参数指定是否设置为混杂模式，第 1 个参数用于指定要监控的网卡。在具体实现时，程序从配置文件中读入要监控的网卡，或者直接由用户通过 RT-TMA 用户界面来指定要监控的网卡。winpcap 还提供了 pcap_findalldevs() 这个函数来获取所有可用的网卡列表，用户可通过用户界面来选择要监控的列表。

(2) 设置过滤规则。根据用户对网络流量监控分析的侧重点不同，可以设置只采集 IP 报文或者全部报文。根据配置文件或用户操作，可通过调用 pcap_compile(pcap_t *p, struct bpf_program *fp, char *str, int optimize, bpf_u_int32 netmask) 和 pcap_setfilter(pcap_t *p, struct bpf_program *fp) 两个函数来实现。

(3) 处理采集的数据包。winpcap 提供了集中处理采集到的报文的方式来适应不同的需要，这里 RT-TMA 选择了使用阻塞的多线程方式来实现。在正确完成第 (1) 步和第 (2) 步的工作后，可通过循环调用 pcap_next_ex 获得报文，然后调用具体的数据包处理函数进行分析处理。

2.2 DPI 引擎的实现

OpenDPI[10] 是一个源自商业 PACE 的 DPI 开源库，支持

IPv6 并能识别近 120 种协议，还可以根据网络协议对数据包进行分类统计，包括协议数据包的数量、大小、协议类型等信息，得到了业界广泛的认同。更为重要的是，OpenDPI 使用 LGPL 开源协议，允许开发者自行修改代码并用于商业应用。

RT-TMA 的 DPI 引擎采用的是在 OpenDPI 基础上开发的 xDPI 引擎。相比 OpenDPI, xDPI 主要包括如下几个方面的改进：一是支持的协议更加丰厚；二是支持更多的统计属性；三是可提供扩展接口，为深度流检测及其他算法提供基础；四是性能得到进一步优化。xDPI 的基本流程如下：

(1) 数据结构初始化。完成对基本数据结构的初始化，包括时间戳、调用信息输出函数等。

(2) 设置要检测的协议。设置要检测的协议，这里指设置检测全部支持的协议，代码为：

```
// enable all protocols
XDPI_BITMASK_SET_ALL(all);
xdpi_set_protocol_detection_bitmask2(m_xdpi_struct, &all);
```

(3) 设置调用协议规则库时的初始条件和函数入口地址。

```
m_xdpi_struct =xdpi_init_detection_module(m_ndetection_tick_resolution, debug_printf);
if (m_xdpi_struct == NULL)
{
 OutputDebugString(“ ERROR: global structure initialization failed\n ” );
return FALSE;
}
```

(4) 将所有待分析协议分类划分。可以先根据协议的类型 (只处理 IPv4 报文，并且不处理碎片报文) 进行初步的划分，将不支持的报文类型都设置成 Unknown；然后按照 TCP/IP 分层协议的层次，依次将报文由下至上进行处理，解析出源地址、目的地址、源端口、目的端口和报文负载等信息，并根据源地址、目的地址、源端口、目的端口的信息归并到对应的数据流 (flow)；再将 TCP 报文和 UDP 报文等分别调用对应的处理函数进行协议识别。

(5) 协议识别。根据协议报文的负载和端口信息进行详细的分析，判断报文的具体协议。

(6) 报文统计。对原始报文数量、原始流量大小、IP 报文数量、IP 报文大小等数据进行详细统计。

3 运行测试

为了测试 RT-TMA，本文选取对千兆网络接入的实验教学示范中心的出口网络进行监控分析。RT-TMA 的网络部署如图 2 所示。

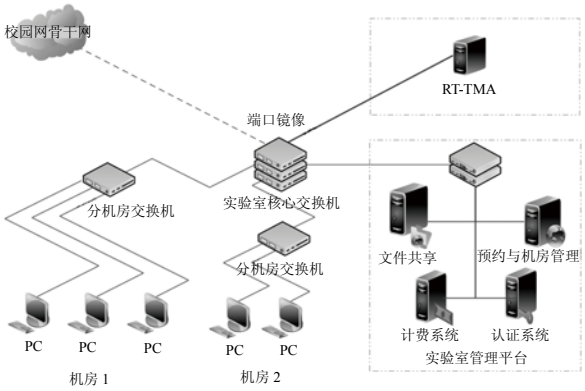

图 2 RT-TMA 在实验室的部署测试网络拓扑图

通过对实验室核心交换机 D-LINK DGS-1210-24 进行配置，可将上行端口的流量通过端口镜像的方式发送到 RT-TMA，再由 RT-TMA 进行实验室网络的流量实时监控分析。

4 结 语

本文介绍了一个名为 RT-TMA 的网络流量实时监控分析系统的设计方案和关键技术实现方法，并给出了系统的运行测试结果。该方法对于网络流量监控分析系统的开发、DPI 算法研究等，都具有较高的参考价值。本文介绍的 RT-TMA 目前可识别的协议还有限，DPI 规则及检测器的性能和算法还有较大的进一步优化空间。此外，混合 DFI 及其他协议识别技术来进一步提升系统的协议识别准确率和性能还需要进一步的研究和测试。这些都是需要在下一步工作中进行研究和测试的内容。

参 考 文 献

[1] 杨厚云，王遵刚，龚汉明 . 校园网数据流量监控设计与实现 [J]. 北京信息科技大学学报：自然科学版，2009，24(4)：97-91，96.
[2] 王文蔚 . 协议分析及其在网络管理中的应用 [J]. 信息技术与信息化，2009(2)：31-33.
[3] 周杨 . 协议分析技术在入侵检测系统中的应用 [J]. 计算机系统应用，2011，20(6)：161-164.
[4] 聂瑞华，黄伟强，吴仕毅，等 . 基于 DPI 技术的校园网络带宽管理 [J]. 计算机技术与发展，2009，19(4)：250-253.
[5] 叶文晨，汪敏，陈云寰，等 . 一种联合 DPI 和 DFI 的网络流量检测方法 [J]. 计算机工程，2011，37(10)：102-104，107.
[6] Liao M Y, Luo M Y, Yang C S, et al. Design and evaluation of deep packet inspection system: A case study[J]. Networks, IET. 2012, 1(1): 2-9.
[7] 孙广路，郎非，杨明明 . 基于混合方法的流量测量系统 (英文)[J]. 电机与控制学报，2011，15(6)：91-96.
[8] RIZZO L, CARBONE M, CATALLI G. Transparent acceleration of software packet forwarding using netmap [C]// 2012 Proceedings of 2012 IEEE INFOCOM. Orlando: IEEE, 2012: 2471-2479.
[9] Jie H, Yu-Jie H, Jia-Yu C, et al. An efficient tcp flow reassembling algorithm based on PF_RING [C]// 2009 International Conference on Apperceiving Computing and Intelligence Analysis. Chengdu: IEEE, 2009: 246-249.
[10] 魏永，周云峰，郭利超 .OpenDPI 报文识别分析 [J]. 计算机工程，2011(S1)：106-108.