基于 Winpcap 的数据包捕获和协议分析系统的设计与实现

李延会 岳彩祥 徐金艳 李亚斐 长春工业大学研究生院 130012

摘 要

介绍了 winpcap 的结构组成和 Winpcap 的包捕获操作的重要部件。在 visual c++ 环境下采用多线程技术实现数据包捕获的方法；并根据 TCP/IP 协议簇对捕获到的数据包进行分析，并给出有效实验结果。

关键词

Winpcap；包捕获；多线程；协议分析

Abstract

introduced the structure of the Winpcap and a package of Winpcap operation to capture the important parts. In the visual c + + environment, multi-threading technology to capture packets. And in accordance with the TCP / IP protocol on the cluster to capture packets for analysis, and gives effective results.

Key words

Winpcap；capture packets；multi-threading；Protocol Analysis

1、Winpcap 概述

1.1 Winpcap 简介

Winpcap（windows packet capture）是由意大利人 Fulvio Risso 和 Loris Degioanni 提出并实现的[1]。它是一个 Windows 平台下捕包和网络分析的体系架构。它具有访问底层的能力，提供了捕获原始数据包，按照一定规则过滤数据包，以及发送原是数据包的功能. WinPcap 为用户级的数据包提供了 Windows 下的一个平台。WinPcap 是 BPF 模型和 Libpcap 函数库在 Windows 平台下网络数据包捕获和网络状态分析的一种体系结构，这个体系结构是由一个核心的包过滤驱动程序，一个底层的动态连接库 Packet.dll 和一个高层的独立于系统的函数库 Libpcap 组成。底层的包捕获驱动程序实际为一个协议网络驱动程序，通过对 NDIS 中函数的调用为 Win95、Win98、WinNT 和 Win2000 提供一类似于 UNIX 系统下 Berkeley Packet Filter 的捕获和发送原始数据包的能力。Packet.dll 是对这个 BPF 驱动程序进行访问的 API 接口，同时它有一套符合 Libpcap 接口（UNIX 下的捕获函数库）的函数库。WinPcap 的主要结构图如图 1 。

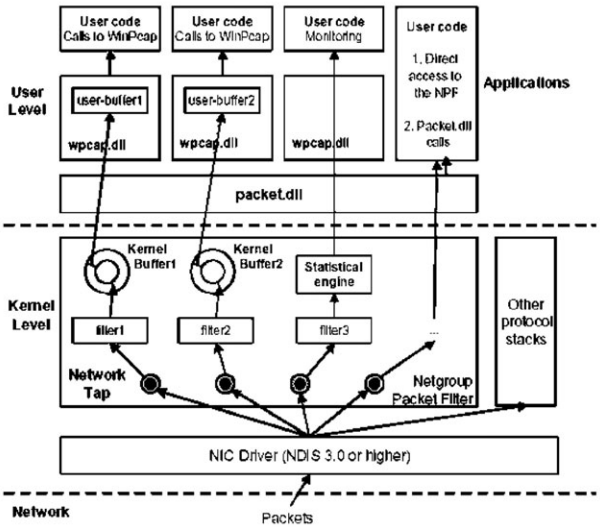

图1 WinPcap结构图

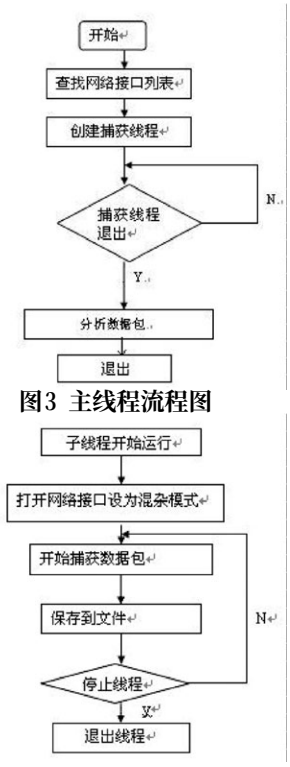

图3 主线程流程图

图4 子线程流程图

1.2 winpcap 构成

WinPcap 主要有三个模块构成[2,3]：第一个模块 NPF(Netgroup Packet Filter)，是一个虚拟设备驱动程序文件。它的功能是过滤数据包，并把这些数据包原封不动地传给用户态模块，这个过程中包括了一些操作系统特有的代码。第二个模块 packet.dll 为 win32 平台提供了一个公共的接口。不同版本的 Windows 系统都有自己的内核模块和用户层模块。Packet.dll 用于解决这些不同。调用 Packet.dll 的程序可以运行在不同版本的 Windows 平台上，而无需重新编译。第三个模块 Wpcap.dll 是不依赖于操作系统的。它提供了更加高层、抽象的函数。

packet.dll 和 Wpcap.dll：packet.dll 直接映射了内核的调用。 Wpcap.dll 提供了更加友好、功能更加强大的函数调用。WinPcap 的优势提供了一套标准的抓包接口，与 libpcap 兼容，可使得原来许多 UNIX 平台下的网络分析工具快速移植过来便于开发各种网络分析工具，充分考虑了各种性能和效率的优化，包括对于 NPF 内核层次上的过滤器支持，支持内核态的统计模式，提供了发送数据包的能力。图2显示了 Winpcap 的不同组件。

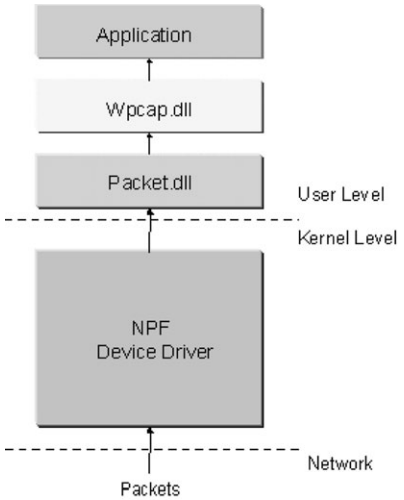

图2 WinPcap主要结构图

2、网络数据包捕获的原理及软件的实现

2．1 数据包捕获原理

以太网（Ethernet）具有共享介质的特征，当网络适配器设置为监听模式（混杂模式，Promiscuous）时，由于采用以太网广播信道争用的方式，使得监听系统与正常通信的网络能够并联连接，并可以捕获任何一个在同一冲突域上传输的数据包。IEEE802.3 标准的以太网采用的是持续 CSMA 的方式，正是由于以太网采用这种广播信道争用的方式，使得各个站点可以获得其他站点发送的数据。运用这一原理使信息捕获系统能够拦截的我们所要的信息，这是捕获数据包的物理基础[4]。

以太网是一种总线型的网络，总线的特点是：当一台计算机发送数据时，总线上所有计算机都能检测到这个数据[5]。以太网从逻辑上来看是由一条总线和多个连接在总线上的站点所组成各个站点采用上面提到的 CSMA/CD 协议进行信道的争用和共享。每个站点（这里特指计算机通过的接口卡）网卡来实现这种功能。网卡主要的工作是完成对于总线当前状态的探测，确定是否进行数据的传送，判断每个物理数据帧目的地是否为本站地址，如果不匹配，则说明不是发送到本站的而将它丢弃。如果是的话，接收该数据帧，进行物理数据帧的 CRC 校验，然后将数据帧提交给 LLC 子层。

2.2 Winpcap 编程模式

Winpcap 提供了数据包的捕获功能，在不同的应用中需要设计不同的协议分析模块。针对不同的协议，设计相应的协议分析功能，是基于 Winpcap 应用的关键所在[6]。在基于 Winpcap 的应用程序中，有基本的编程模式。使用 Winpcap 捕获和分析网络数据包的基本流程如图 5 所示。

2．3 数据包捕获的实现

捕获过程按先后顺序具体步骤如下：

1）．寻找系统中可用的接口列表。

2）．选择接口并将其设为混杂模式准备捕捉。

3）．将捕捉到的数据包保存到文件以便读取和分析。

4）．读取保存在文件中的数据包并进行分析。

5）．关闭接口。

本软件建立在 Winpcap 架构的第三层模块 Winpcap.Dll 之上。使用 Visual C++6.0 开发平台利用多线程技术实现。主线程负责寻找和选择网络接口、设置分析过滤器、分析捕获数据包。子线程负责打开选择的接口并将其设为混杂模式、捕获数据包并将其保存到文件中。其流程图见图 3，图 4。

3、软件运行及实验结果

运行该软件应确保本地机器上安装了 Winpcap 驱动，可从其官网下载。软件运行效果如图 6 所示。

4、结束语

本文实现的这个系统可以监听局域网内流经所有主机的数据包，并分析了每个包的协议、源 / 目的 Mac 地址、源 / 目的 IP 地址、数据包长度和包内的数据既可以管理和维护网络健康运行还可以检测网络入侵，甚至可以学习网络协议知识。

本系统也有一些不足和需要改进的地方：

（1）跨平台运行兼容性需要改进。本系统只能运行在 Windows NT,Windows 2000,Windows Xp 并且机器上必须安装 Winpcap 才能运行。

（2）只能在局域网内捕获数据包，无法跨路由进行监测。

虽然基于 Winpcap 的网络数据协议分析软件在应用中还有许多局限性，但是仍然作为一种代表性的技术，对于今后发展更高层的网络安全应用提供了前提和基础通过对这方面的研究，可以理解网络各层通讯协议的机理。

参考文献

[1] 胡晓元，史浩山 .Winpcap包捕获系统的分析及其应用 [J].计算机工程.2005，96 － 98

[2] The Winpcap Team. The Winpap manual and tutorial for Winpcap 4.0 [EB/OL]. Http://www.Winpcap.org/docs/docs_40/html/main.html, 2006-05-30.

[3]陈辉，陶洋．基于Winpcap实现对ARP欺骗的检测和恢复[J].计算机应用.2004 24（10）：67 － 68，85

[4] 徐美华，王振旗，韩秀娟 .利用WinPcap技术捕获数据包

[5] 谢希仁.计算机网络（第 4 版）[M].电子工业出版社.2003 6：94 － 96

[6] 刘文涛．网络安全编程技术与实例[M].机械工业出版社.2008.7

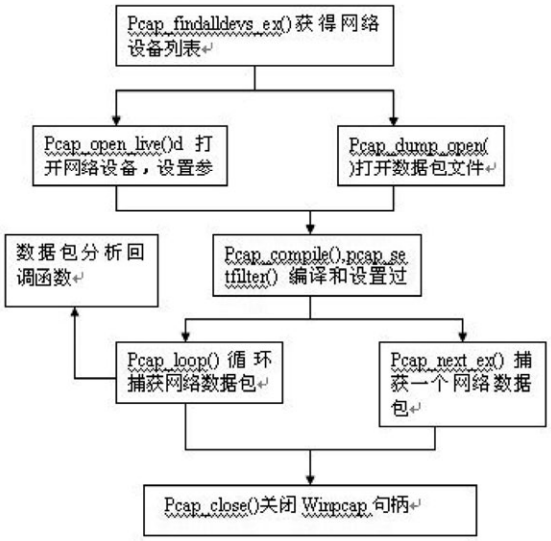

图5 基于Winpcap开发的编程模式

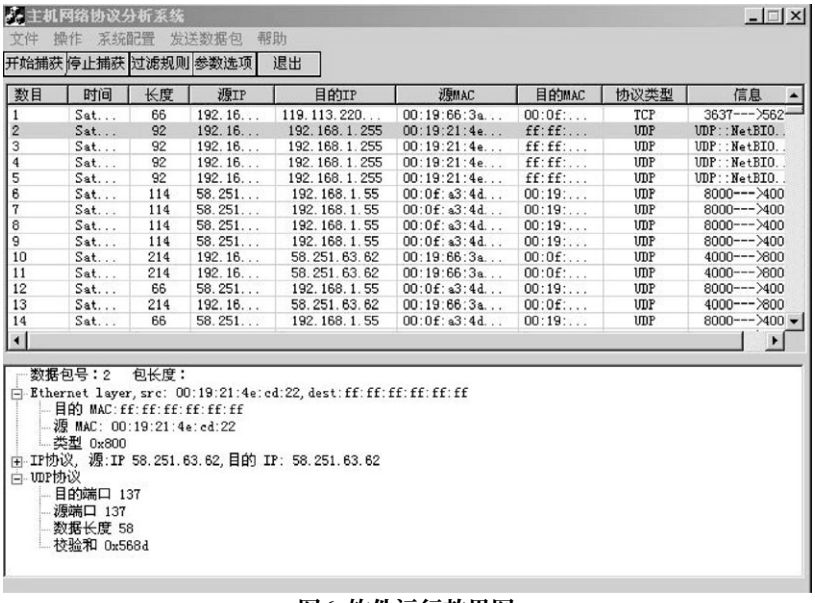

图6 软件运行效果图