摘　要

互联网的迅速发展和普及，在给人们的工作和生活带来方便的同时，也为各种违法活动提供新的途径。由于 Internet 上的无政府状态，以及利用网络进行非法活动的高度隐蔽性，使得这种形式的作案行为日益蔓延。在这种形势下，建立城域网络信息实时监控系统显得尤为必要。

与一般的网络安全系统不同，网络信息监控主要不是针对黑客的入侵行为，而是通过检测、记录正常网络通信的部分特征参数以便为侦破某些网络案件提供辅助手段。信息监测点必须在城市范围内许多网络信息汇聚点广泛布设，这些分监测点可能是异构的，并且分别处于不同防火墙的保护范围内，如何实现分布监控点间信息的集成不是轻而易举的事情。

本课题主要研究在城域范围内实现网络信息监控的关键技术。论文首先比较详细地论述了在协议分析技术中，如何实现对网上传输的协议数据单元(PDU)进行深度的协议分析，不仅剖析了链路层、网络层和传输层的接口控制信息(ICI)，而且实现了对应用层 HTTP、SMTP 等协议不同结构报头信息的特征提取。其次，提出了采用负载均衡集群和 MPI 消息传递进行网络汇聚点上密集数据流协议分析的处理方法，以克服网络流量急剧增加时容易发生的丢包现象。最后，设计了一个分布式网络信息监控的原型系统。该系统架构在 J2EE 平台上，运用最新的 Web 服务软件技术，利用 XML 与 SOAP 解决了主、从监控点之间透明的任务通信。论文的研究结果可为建立高效实用的城域网络信息监控系统提供可行的解决方案。

关键词：协议分析；MPI；Web 服务

Abstract

With the development and popularization, Internet conveniences people's work and life and presents a new approach for all kinds of network crime. Because of anarchy and concealment for network crime, Internet is crime-ridden. It's very important to found a metropolitan-area network information Real-time monitoring system to restrain network crime and make network information criterion.

Unlike the generic network security system, the network information monitoring system does not detect the hacker's intrusion, but provide an assistant for detecting some kinds of network crime by observing and recording some characteristic parameters of the normal network communications. It is necessary for the network information monitoring system to array in the city range. These monitoring nodes may be isomerous, and lie in protection area by the firewall. It is difficult to integrate the information among these distributed monitoring nodes.

The main content of this paper is to provide the pivotal technologies research on monitoring metropolitan-area network information. Firstly, the paper discusses how to do a deeply protocol analysis from protocol data unite transferring through Internet. The task analyzes not only interface control information in link layer, internet layer and transport layer, but also all kinds of different structure datagram unit in application layer, such as HTTP, SMTP. Secondly, in order to resolve the problems of dropping data packet when network data stream is rushing, it brings forward the methods to attemper workflow among monitor groupware and to analyze protocol through the network dense data stream based on MPI. Finally，the paper illuminates the design idea and achievement method to set up a distributed network information monitoring system, which elucidates how to communicate in the transparency way between the control center and the monitoring nodes by the technologies of XML and

SOAP based on web services in J2EE platform. The research production of this thesis can proposes the solution to set up an effective and applied metropolitan-area network information monitoring system.

Key Words: Protocol Analysis; MPI; Web Service.

目　录

Contents

第 1 章　概论

1.1 课题的应用背景

随着网络的蓬勃发展，社会信息化的深入和电子商务的快速开展，计算机网络已经成为社会的重要基础设施。Internet 上如雨后春笋般冒出了不计其数的各种政府机构、商业公司及中小企业的网站，带来了丰富多彩的网络信息，与此同时上网的用户数量急剧增加。如今，人们已经进入了信息爆炸的时代， Internet 已经深入到人们生活的各个部分，极大方便了信息的传播，为我们带来一个全新的通信方式，通过 WWW 浏览、电子邮件等方式，我们可以及时地获得所需要的各种各样的信息。

然而 Internet 在给人们的工作和生活带来极大方便的同时，也为各种违法犯罪活动提供新的途径。由于 Internet 的无政府状态，以及利用网络进行非法活动的高度隐蔽性，使得这种形式的作案行为日益猖獗。通过网吧或其他公共上网场所来进行各种网络犯罪的手段比较隐蔽，不易察觉，例如通过网络散布非法资料或者通过电子邮件进行敲诈、邮箱攻击等各种网络犯罪层出不穷，网络信息安全成为日益严重的问题，因此，有必要通过在城域网络上各个公共上网场的若干个汇聚点设置分监测点，增加对城域网络活动的跟踪监测手段，利用协议分析技术对城域网络出口流量信息进行一定程度的监测。

与一般的网络安全系统不同，网络信息监控主要不是针对黑客的入侵行为，而是通过检测、记录正常网络通信的部分特征参数以便为侦破某些网络案件提供辅助手段。建立这种系统的难点在于：为了获得网络通信事件有价值的内在参数，需要对网上传输的协议数据单元(PDU)进行深度的协议分析。不仅分析链路层、网络层、传输层的接口控制信息(ICI)，更要分析应用层

各种不同结构数据单元的报头信息。

在通信活动中，网络监听是一种极重要的技术，同时在网络安全领域中扮演着一个越来越重要的角色，可以用来预防和抑制各种网络犯罪。Web 和 Email 是 Internet 现在占主导地位的两种服务，也是人们最常用的获得消息和传递消息的通信方式，因此对这部分的信息进行实时的监测具有重要意义。

1.2 目前的研究现状

现在的很多网络监听工具和协议分析软件虽然很多，但很多只实现了粗粒度的访问控制，其安全控制主要基于 IP 地址，只对网络层和传输层的协议进行分析，而真正对应用层的各种协议进行分析的系统并不多见，因为应用层的协议不仅种类众多，而且分析起来也更为复杂，因此这些工具已不能满足城域网络信息安全的需求。如何在完整的捕获所有通信的数据包后对其应用层的各种协议进行分析需要研究。

同时，大多数的监听工具都是单机运行，这样对于进行完整地监测网络流量有一定的影响。因为网络汇聚点的网络流量通常比较巨大，而捕获全部数据包和进行复杂的应用层协议分析的工作需要占用很大的系统资源，因此，单机工作有可能发生丢包的现象，这样不利于有效全面地监控城域网络流信息。

纵观现有的网络安全系统和产品，一定程度上存在着一些不足：不同的监控系统很难集成在一起，大多处于相对分离的状态；缺少通用的数据编辑和保存形式，不同操作系统和数据库平台上的子系统很难交互和共享数据；缺少有效的模块集成手段，基于不同平台的模块很难集成，系统的扩展性和伸缩性比较差。

1.3 论文的主要工作

由于信息监控不能局限于某个局域网，必须在城市范围内广泛布设。这些分监测点可能是异构的，并且分别处于不同防火墙的保护范围内，因此要考虑如何很好地实现分布监控点之间的通信。

随着更加强大的计算机和网络的出现，出现了分布式计算技术。通过 DCOM，CORBA 和 RMI 等都可以实现不同计算机上的进程之间的交互，但是它们要求进行交互的机器具有相似的系统，因此，这些技术之间的可互操作性（与不同供应商、不同平台的软件之间通信和共享数据的能力）是非常有限的。

Web 服务技术代表了分布式计算的下一个阶段，它胜过以往分分布式计算的一个最重要的优点是它使用了开放的标准。Web 服务扩展了有限的可互操作性而改进了分布式计算的能力，而且基于 Web 服务的应用程序比较容易调度。Web 服务促进了完全不同的应用程序和平台之间的通信。因此系统采用基于 Web 服务的系统集成技术，处理系统模块之间控制和数据的集成，很大程度上提高了系统数据的通用性，降低了模块间的耦合程度，从而提高了系统的扩展性、伸缩性和兼容性，便于系统分担负载，提高系统的服务质量。

论文首先分析了网络信息监测系统的应用背景和目前的研究现状，接着阐述了网络协议分析技术以及 MPI、Web 服务等技术的概念和发展，在此基础上提出了基于 Web 服务的城域网络信息监测系统的体系结构，最后给出了系统的架构，并进行了系统的建模，设计了原型系统。

论文对以下内容进行了深入研究：

1、在 Linux 平台上，用 C 语言实现网络信息监控系统的应用层协议分析程序设计，主要是通过检测、记录正常网络通信的部分特征参数，对网上传输的协议数据单元(PDU)进行深度的协议分析，不仅分析链路层、网络层、传输层的接口控制信息(ICI)，还分析应用层上的 HTTP 和 SMTP 等各种不同

结构数据单元的报头信息。

2、采用负载均衡集群系统和 MPI 消息传递机制处理网络汇聚点上密集数据流的包捕获以及网络协议分析，实现对城域网络信息高效全面的监测。

3、在 J2EE 平台上，运用最新的 Web 服务软件设计技术，利用 XML 与 SOAP 解决主、从监控点之间透明的任务通信，为建立高效而实用的城域网络信息监控系统提供可行的解决方案。

第 2 章 网络协议分析

TCP/IP（Transmission Control Protocol/Internal Protocol，传输控制协议/网际协议）是 70 年代美国国防部为其 APPANET 广域网开发的网络体系结构和协议标准，TCP/IP 协议族亦是当今网络通信的标准之一。TCP/IP 是不基于任何特定硬件平台的网络协议，既可用于局域网(LAN)，又可用于广域网(WAN)。

TCP/IP 是根据层来建模的，各层通过接口与上下层进行通信，为其直接上层提供服务，而通过服务原语调用其直接下层提供的服务。TCP/IP 协议的四层模型包括：应用层、传输层、网络层和网络接口层。

Internet 是由许多局域网连接起来的大网络，通信技术使用 TCP/IP 协议，而 TCP/IP 协议使用了包交换的通信技术，在 Internet 中所传输的数据，全部是以包（packet）为数据单位来发送和接收的。包是由“报头”和“报文（payload）”净荷所组成。在“报头”中，记载包的发送主机地址、接收主机地址及与报文内容有关的信息等。在“报文”中，记载着需要发送的数据。在发送包的时候，所经过的路由器阅读报头的信息，并通过报头中所记载的终点主机的信息，向目的主机进行转发处理。反复这样的操作，则包能够到达所要发送的终点主机。

2.1 以太网协议分析

以太网（Ethernet）已经在局域网市场占据了大部分位置，是现今最流行的局域网技术，也是一种普及最广的计算机网络。在上个世纪 80 年代和 90 年代，以太网面临着许多来自其他局域网技术的挑战，包括令牌环、FDDI 和 ATM。但是自以太网在上世纪 70 年代中期发明以来，它不断地演化和发

展，保持了它的支配性的市场地位。今天，以太网是最流行的局域网技术，而且在可预见到的将来也可能如此。

以太网的成功有许多原因。首先，以太网是第一个广为采用的高速局域网。其次，令牌环、FDDI 和 ATM 比以太网更复杂、更昂贵，这进一步阻碍了从以太网转变到采用其他技术。第三，改用其他局域网技术（例如 FDDI 或 ATM）最有吸引力的原因通常是新技术具有更高的数据速率，然而，以太网总是会抵抗，制造出具有同样的数据速率甚至更高速率的版本。在上世纪 90 年代早期，还引入了交换式的以太网，进一步提高了有效的数据速率。最后，以太网是如此的流行，以太网硬件（特别是网络接口卡）已经成为一个商品，而且非常便宜。

今天的以太网已经演变出许多形态和形式，一个以太网局域网可以在同轴电缆、双绞线或者光纤上运行。而且，以太网可以以不同速率传送数据，如 10Mbps、100Mbps 和 1Gbps，10Gbps。

虽然存在着许多不同的以太网技术，但是所有以太网技术都使用同样的帧结构。在以太网帧的报头中包含接收端及发送端的地址，帧的报文部分包含的是数据种类，最后放置的是错误检验和修正码。

以太网帧的结构如图 1 所示。

前同步和开始帧分界符（64 位）	接收端的 MAC 地址（48 位）	发送端的 MAC 地址（48 位）	类型字段（16 位）	数据（最大 12，000 位）	错误检验修正码（32 位）

图 1　以太网帧的构造

在以太网中，地址用 48 位二进制来表示，即 MAC 地址。在以太网上进行通信时，用 MAC 地址来区分机器。在以太网帧的构造中，开始的 64 位是前同步码（preamble）和帧首定界符(start frame delimiter)。前同步码

是使发送端和接收端在数据的交换上步调一致。

前同步码结束后是表示帧的真正开始的 8 位(10101011)位列。帧首定界符之后是地址等报头信息。

帧首定界符后面是接收端和发送端的 MAC 地址。只有在接收端的 MAC 地址是自己的 MAC 地址的情况下，才能进行帧接收；MAC 地址为其他机器的情况下，将不接收该帧而把它删除。但当接收端地址全部都为 1 时，在同一以太网内连接的所有设备，都要接收该帧。

接收端和发送端的 MAC 地址后面是 16 位的类型字段(type field)。类型字段中存放的是以太网帧中传送数据的上层协议的种类代码。这种代码是由规定以太网协议的 RFC(Request For Comments)1700 号规定的。

以太网帧的报文部最大能存放 12，000 位，即 1，500 字节。

帧的尾部是检查数据错误的错误检验及修正码。以太网中常使用循环冗余检验(CRC: Cyclic Redundancy Check)检查错误。

以太网是物理层及数据链路层的协议。以太网帧所传送的数据是网络层规定的数据包。如果要使用 IP 网络协议，则 IP 数据包就存储在以太网帧的报文处。

在上一层的协议为 IP 时，Ethernet 类型域的值为 0x0800。最后的帧检验序列（FCS）用于检查在数据发送过程中，从报头开始到数据结束，是否由于噪声等原因造成数据损坏。在发送时的 FCS 生成处理及在接收到时的 FCS 检查计算，都是由硬件自动完成，因此，不需要在程序设计中直接对 FCS 值进行设定。

2.2 网络层 IP 分析

网络层协议 IP（Internet Protocol）提供了网络层的协议，能在很多的局域网构成的网络上，从多台计算机中选择出作为通信对象的计算机。数

据包经过网络传输到目的计算机存在的网络中，需要路径上存在的网络依次对数据包进行中继，路由决定数据包前进方向，路由是网络层的重要功能之一。因此，IP 具有将包发送到接收终点主机的功能，在构成 IP 计算机网络的所有主机和路由器中，都事先赋予一个 IP 地址，IP 一边对 IP 报头进行解释，一边进行包的发送、接收和转发处理。

实际上，是使用数据链路层的功能进行 IP 数据报的交换。IP 数据报是用以太网的功能传送的。在路由经过的路由器对 IP 数据报中继时，IP 数据报暂且从以太网的报文中取出，而后路由器将其重新做成以太网帧的报文。

IP 数据报格式如图 2 所示。

0 15 16 31

<table>
<tr><td colspan="2">4 位版本</td><td colspan="2">4 位标题长度</td><td colspan="2">8 位服务类型</td><td colspan="4">16 位数据片长度</td></tr>
<tr><td colspan="6">16 位鉴定域</td><td colspan="2">3 位标志</td><td colspan="4">13 位碎片偏移</td></tr>
<tr><td colspan="3">8 位生存时间</td><td colspan="3">8 位传输协议</td><td colspan="4">16 位头部校正和</td></tr>
<tr><td colspan="9">32 位发送方 IP 地址</td></tr>
<tr><td colspan="9">32 位目标 IP 地址</td></tr>
<tr><td colspan="9">32 位选项和填充（若有）</td></tr>
<tr><td colspan="9">数据（可变长度）</td></tr>
</table>

图 2　IP 数据报格式

其中，数据片长度字段以 8 位为一个单位，即字节表示 IP 数据报的长度。鉴定域字段表示从 TCP 等上层协议调用时 IP 数据报的标识号。传输协议表示上一层（即传输层）协议的类型，因此，协议字段中存放着表示 TCP 等网络层的上层协议的值。

表 1 列出有代表性的协议编号：