共享上网检测技术原理分析

梅　娅

（盐城师范学院计算机系，盐城　224002）

摘　要：为了自身运营的需要，电信等网络服务提供商往往对共享上网方式加以限制，因此如何对共享上网方式进行检测成了当前研究的热点。对常用共享上网方式进行了介绍，在此基础上对多种检测技术的原理进行了分析，对各种技术的优缺点与适用场合做了阐述，最后对以后的研究方向做了预测。

关键词：共享检测；共享上网；检测系统；IP 协议；协议分析

0　引　言

出于成本的考虑，共享上网方式在中小企业和家庭网络中普遍存在，而电信等网络服务提供商出于利益、管理等方面的考虑，往往需要对这种上网方式加以识别与控制。因此，共享上网方式的检测技术成了研究的热点，吸引了越来越多的人对它进行研究。

1　常用共享上网方式

共享上网的方式有多种，总的来说可分为网关型、代理型和路由型三种[1]。网关型共享是一种最基本，也最简单的共享方式，这种方式一般在一台配置稍好的双网卡主机开启外网卡的连接共享功能来实现共享上网；代理型共享则是通过在主机上安装 WinGate、CCProxy、WinProxy 等代理软件来实现共享上网；路由型共享与前面两种共享方式完全不同，它通过一台具有 NAT 功能的路由器来实现共享上网，目前这种方式为广大用户普遍采用。

2　共享检测技术与原理分析

通过分析与研究，我们把各种检测技术归纳为协议分析法、应用特征检测法和行为统计检测法三种。

2.1　协议分析法

（1）IP 包 IPID 字段特征检测。IP 包结构如图 1 所示，每个主机都有个 IPID 系统变量作为本机发送 IP 包的计数器，系统每发送一个 IP 包，系统就做 IPID+1 运算[2]，同时，系统发送每个 IP 包的时候会把当前的 IPID 值填充到 IP 包 IP 首部的 16 位标识字段，如果在一段时间后，发现某个源 IP 地址有多段 IPID 在连续变化或者 IPID 值不连续，则说明此时多个用户在共享此 IP 地址进行上网；

（2）TTL 值检测[3]。经过统计分析发现，主机发出的 IP 数据包的 TTL 字段的值一般为 32、64、128，NAT 路由器往往会修改 TTL 值为其他数值，检查从下级 IP 出来的 IP 包的 TTL 值是否是 32、64、128 这几个值，如果不是，则说明多个用户在共享此 IP 地址进行上网。

检测方式（1）的优点在于经过统计分析，可以精确统计出有多少台主机在共享上网，方式（2）则只能检测出在共享上网，可以通过 TTL 值粗略判断主机的操作系统类型。

2.2　应用特征检测法

这类方法主要是通过检测下级 IP 发出的 HTTP 请求包中的一些特征值来进行判断。通过抓包分析，一次典型的 HTTP 请求主机的浏览器软件会发出以下命令，如图 2 所示。

（1）通过 User-Agent 字段来进行判断。HTTP 请求的 User-Agent 字段会随着操作系统、浏览器版本的不同而不同，同时不同浏览器软件发出的 HTTP 请求这个字段的值也不同，例如 Windows XP 的 HTTP 请求则有 Windows NT 5.1 字样，Windows 2003 系统的 HTTP 请求则有 Windows NT 5.2 字样。如果检测下级 IP 的数据包中有不同的 User-Agent 值，则可以认为用户在使用共享方式上网；

（2）通过大站 Cookie 方式进行检测。所谓大站 Cookie 就是通过监控访问新浪网等门户网站的 Cookie 值来进行判断。Cookie 一般用来在客户端（浏览器端）保存一些数据，是一个由网页服务器放在客

收稿日期：2008-01-07　修稿日期：2008-04-05

作者简介：梅娅（1980-），女，江苏盐城人，助教，研究方向为网络安全与网络管理

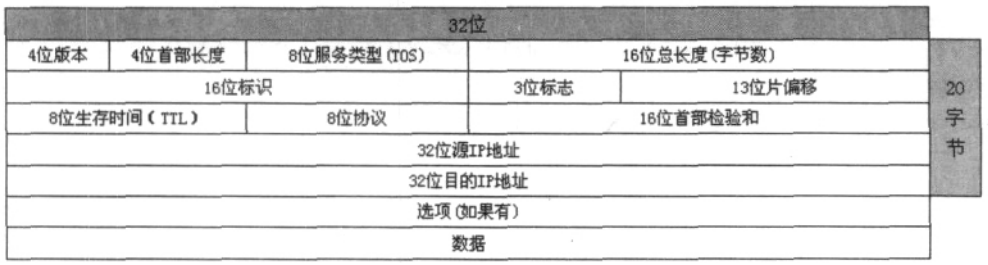

图 1 IP 首部结构[4]

```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
Host: www.sina.com.cn
Connection: Keep-Alive
Cookie: vjuids=6d44e7e50.1140c3bc250.0.d2aec6fb4e2d6; vjlast=1185715883
```

图 2 HTTP 请求命令

户端硬盘上的非常小的文本文件,它本质上就像客户端的身份证明一样[5,6]。因为用户访问这些门户网站几乎是肯定的,所以在一定时间内检测到针对同一网站同一类型相同的 Cookie 值, 则可以判定用户在使用共享方式上网。

方式(1)的优点在于可以即时判断,即只要有不同的用户在访问网页,就可以立即检测出来;缺点在于如果用户的操作系统、浏览器和其他相关软件版本完全一样,这种检测方式就失效了。

方式(2)克服了方式一的缺点,通过统计分析甚至可以检测出使用共享方式上网的主机数目;缺点在于如果主机数目比较小的情况下,在短时间内访问同一门户网站的几率比较小, 需要延长统计的时间,这一方式需要较好的算法支持。

两种方式都是通过检测 HTTP 请求的特征字符来进行工作的,共同的缺陷在于如果共享上网的主机没有进行 Web 资源访问, 这种检测方法就完全失效了。然而用户上网的主要行为就是访问 Web 资源,因此应用特征类检测方法具有很高的实用价值,目前已有使用这种检测技术的产品出现。

2.3 行为统计检测法

这类方法一般有以下几种方式:

(1)检测下级用户是否在设定的时间间隔内对同一网站发出访问请求,有则可以判定正在发生共享上网行为;

(2)检测下级用户是否在设定的时间间隔内对不同网站发出访问请求,有则可以判定正在发生共享上网行为。

这类方法的缺陷在于如果算法不够好,设置的参数不当,容易发生误报现象,一般用来作为其他方法的补充。

3 其他检测方法

为了提高检测的精确性与正确性,还有一些方法用来作为补充,例如检测下级用户的数据流量,检测并发连接数量等。

4 结 语

经过分析发现,在一定场合,还可以利用数据包中的 TCP 首部的序列号和窗口大小字段进行判断。随着相关研究的进一步深入,相信会有更多精确而有效的检测方法出现。

参考文献

[1]冯子祥. 多台电脑共享上网. 信息技术,2006,05:357~358

[2]程巍. 隐蔽端口扫描的原理及防御方法. 计算机应用与软件,2004,08:98~99

[3]Peter. Detecting NAT Devices Using sFlow. http://www.sflow.org/detectNAT/index.htm.

[4]Richard Stevens.TCP/IP Illustrated Volume 1 The Protocols[M]. U.S.2000-4

[5]胡忠望. Cookie 应用与个人信息安全研究. 计算机应用与软件. 2007,03:50~51

[6]杨文波. 基于 Cookie 的门户系统单点登录模型. 计算机应用研究,2006,08:100

(下转第 108 页)

复，凡从数据窗口中每取出一道符合组卷要求的试题，便将该试题存入系统的试卷表中，并把该试题从试题库窗口中删除，以免在随后的选题过程中选出重复的试题，保证整份试卷试题的重复比例为0。

4 结 语

本文通过对组卷的数学模型的分析，改进了随机组卷的数学模型，并利用正态分布概率函数计算出不同难度系数试题的最大分数，根据最大分数利用随机组卷算法生成试卷，组卷算法结构简单、单次组卷过程的运行速度较快，试卷难易程度符合用户需求。

参考文献

[1]毛秉毅. 基于遗传算法的智能组卷系统数据库结构的研究[J]. 计算机工程与应用，2003，6:230~232

[2]韩昆，杨小平. 自动组卷系统抽题算法研究[J]. 计算机工程与应用，2004，28:212~213

[3]林雪明. 基于知识点的试题库组卷算法的建立[J]. 微机发展，2001，2:77~80

[4]应暑儒，胡立新. 试题库随机选题数学模型及实现[J]. 计算机应用，2000，20(1):46~47

[5]华如海，王俊普，郑全，徐杨. 基于约束满足的智能组卷方法的研究与实现[J]. 计算机应用研究，2000，(11):20~22

Research and Realization of an Algorithm of Intelligence Assembling Paper in Test Paper Generation System

YAN Li[1] , JIANG Xiao-feng[2]

(1.HLJ August First Land Reclamation University, Daqing 163319)

(2.QKL Joint-Stock Trade China CO.,LTD , Daqing 163311)

Abstract: In order to reduce the teachers' burden, we use computers to form examination paper from the item pool. Designs the mathematical model based on the coefficient of difficulty, it uses the normal distribution function to the maximal score of different degree of difficulty question and realizes an algorithm of automatic test- question extraction.

Keywords: Normal Distribution; Coefficient of Difficulty; Intelligence Assembling Examination Paper

(上接第92页)

Analysis of ICS Detecting Technology Principle

MEI Ya

(Computer Department Yancheng Teachers College, Yancheng 224002)

Abstract: To meet up with the requirements of commercial operation, ISPs are always do strictly limit to share Internet connection, so share Internet connection detect become a hot topic. Introduces various types of ICS that are most common used, explaines the benefits, defects and best fit using scenario for each corresponding detection technique.

Keyworks: ICS Detecting; ICS; Detecting System; IP Protocol; Protocol Analysis