<<互联网流测量>>

图书基本信息

书名：<<互联网流测量>>

13位ISBN编号：9787564115067

10位ISBN编号：7564115068

出版时间：2008-12

出版时间：东南大学出版社

作者：程光，龚俭　著

页数：309

前言

随着我国新一代互联网的建设和发展，互联网的用户数量和新的网络应用的持续增长，针对网络的流量攻击威胁问题也愈发严重，已给网络安全和管理带来极大威胁。
最近的互联网安全报告表明，安全攻击的频率及所造成的破坏都在持续增长，特别是DDoS（Distriuted I）enial of Service）和蠕虫攻击对互联网造成的危害则更为严重。
为了能够掌握网络中流量行为状况，更好地管理网络，对互联网这样一个复杂的工程系统，研究人员往往就需要对网络流量进行有效的监测和分析。
但由于新一代互联网具有“更大、更快、突变”的特性，对流量的全面测量、存储和分析将大量消耗昂贵的测量资源，使互联网的测量和管理也愈加困难。
因此测量和分析高速互联网的流量，以实现对高速网络流量行为的实时分析和检测，重点是摘要数据的快速采集，并从这些摘要数据中分析和提取相关必要信息。
目前在网络流量测量和分析过程中常常会遇到以下问题：（1）高速网络流量测量、分析的性能瓶颈。
由于存储和传输大量网络数据的代价非常大，特别是在OC48、OCl92的高速网络环境中，获取每个报文信息或者每个流信息并进行存储完全不符合实际情况，因此为了解决该性能瓶颈问题，使用限制测量资源的抽样和数据流算法目前已成为网络流测量分析技术研究的重点。
（2）流量的突变性问题。
由于测量资源（CPI_J、内存、带宽、硬盘等）的限制，在网络测量过程中常需要采用抽样或数据流等近似技术，但在一个时间段内到达的网络流量速率存在字节速率、报文速率和流速度的不稳定性因素，如蠕虫攻击和扫描、大文件下载等，这些速率的突变给抽样测量带来了测量资源的消耗，同时在同一测量时间段内也无法使用多个抽样比率。
为了解决这个问题，自适应抽样技术势必成为流量测量研究的重点之一。
（3）与此同时，为了适应高速网络测量，优化解决测量资源占用与测量精度之间的关系，重点获取高速流量数据中最具代表性的敏感性数据，如重尾流量、流量突变情况等作为反映流量异常的信息也是网络流量行为研究中的关键问题。
因此，本书讨论互联网流测量的相关技术，实现对互联网流行为的实时检测和分析，进行网络流的近似测量技术研究和流量行为分析。
根据互联网的流行为研究方向，本书分为4个部分：互联网流测量技术基础、抽样测量技术、互联网流测度行为规律、互联网流测量系统。

<<互联网流测量>>

内容概要

本著作讨论互联网流的测量相关技术，实现对互联网流行为的实时检测和分析，进行网络流的近似测量技术研究和流量行为分析。
本著作是作者在互联网流量测量领域长期的研究工作总结，也是作者承担国家各类科研项目的研究成果总结。
本著作的出版对互联网技术的研究具有重要的基础性贡献。
本著作分为四个部分：互联网流测量技术基础、抽样测量技术、互联网流测度行为规律、互联网流测量系统。
测量技术基础分两章介绍互联网流测量的相关研究状况和流测量研究中所涉及的数学基础理论。
抽样测量技术分别在第3章至第6章进行讨论，涉及内容为：基于分组标识的抽样测量模型、基于互联网流的哈希算法、互联网流长度估计方法、自适应超流检测方法等4个部分。
互联网流测度行为规律研究内容分别在第7章至第13章进行讨论，涉及内容为：网络行为测度、互联网流量统计行为、网络流流长度分布分析、网络流流速特征分析、网络流流速和到达行为分析与模型、网络流量行为分析模型、TCP宏观平衡性分析等7个部分。
互联网流测量系统包括高速网络报文测量器、高速网络流量测量平台等。
本著作适合作为网络测量、网络行为学、网络安全、网络体系结构相关研究人员的参考用书，也可作为网络测量相关课程的教材。

作者简介

程光，安徽黄山人，东南大学计算机科学与工程学院副教授，硕士生导师。
2003年3月东南大学计算机应用技术专业博士毕业，2006—2007在美国佐治亚理工大学电子与计算机工程学院进行博士后研究。
研究领域主要涉及：网络测量、流量模型、流量行为分析、网络安全、抽样技术等。
先后负责、参加国家973项目、863项目、国家科技支撑计划、国家自然基金项目、教育部重点基础研究项目、江苏省自然基础科学研究等10多项纵向课题研究。
近年来在国内外期刊及会议上发表论文50余篇，其中SCI、EI、ISTP等三大检索30篇。
获得项目鉴定1项，软件注册2项，专利申请5项，授权专利1项。
撰写教材3部，其中一部为“国家十一五”规划教材。
2004年获得“华英青年学者”称号，2006年获得“东南大学优秀青年教师教学科研资助计划”支持。

<<互联网流测量>>

书籍目录

<<互联网流测量>>

章节摘录

插图：1互联网流测量概述1.1流量测量的必要性早在1995年，当NSF停止对整个NSFnet资助以后，Internet出现多元发展的趋势，试图完整地跟踪和监控Internet行为已经不可能了。
NSF没有留下可以监测不同ISP之间的网络性能问题和安全事件的框架结构，同时ISP也没有重视收集或分析他们的网络数据，这就造成今天不但缺乏理想的测量和分析网络行为的工具，同时也缺乏用于分析网络行为变化的测度数据。
尽管网络测量没有得到足够的重视，但学术界对其的研究却一直没有间断。
因此现在有许多独立的网络端至端测量方法和相应的工具，这些测量方法主要是在端主机发送主动探测分组进入网络，然后记录分组返回的延迟。
但是这种测量涉及大量的难以独立建模的参数，同时测量结果的复杂性使得收集的数据难以比较或标准化。
有些研究组织正试图发展技术和体系结构来支持标准化测量、性能评估、选择网络路由的可靠性等，但这些工作进行得很慢，还不能满足用户、研究者和ISP的需求。
Internet是一个由上亿台计算机互联而成的全球性计算机网络，自20世纪80年代末以来，一直在以指数级的速度膨胀。
Internet具有以下三个特点：首先，TCP/IP技术将多种不同的网络技术和管理域统一成一个整体，这是Internet快速发展的主要原因。
但TCP/IP技术只是将各种多样性统一起来，并没有统一它们的行为成分。

<<互联网流测量>>

编辑推荐

《互联网流测量》适合作为网络测量、网络行为学、网络安全、网络体系结构相关研究人员的参考用书，也可作为网络测量相关课程的教材。

<<互联网流测量>>

版权说明