网络新技术系列丛书

WANGLUO XINGWEI DE
QUANXI CELIANG FANGFA

网络行为的全息测量方法

程 光/吴 桦◎著

东南大学出版社
SOUTHEAST UNIVERSITY PRESS

网络新技术系列丛书

网络行为的全息测量方法

程　光　吴　桦　著

东南大学出版社
SOUTHEAST UNIVERSITY PRESS
·南京·

内 容 提 要

本书主要针对网络行为的全息测量问题，系统介绍了作者在网络测量和行为分析方面的理论及实践的研究成果，从多层面和多角度的协同测量和关联分析入手，建立可扩展的稳定的测量结构体系，以解决测量资源的增长和海量测量数据的增长之间的矛盾，在网络中出现异常突变等极端情况下，采用抽样和数据流算法等近似测量技术，通过自适应调整测量参数，控制测量资源的使用，实时地检测高速网络中的全息信息；从宏观上掌握网络运行情况，分析反映网络总体行为状况的流量指标的聚类方法；随着网络规模的扩大和需要观测的测度数量的增加，从海量的数据中发现异常的数据或特征，采用图形化手段表示各种类型的数据特征。本书的成果对深入研究网络测量和分析方法具有重要的借鉴意义，为网络安全和网络管理，特别是校园网的管理提供了参考。

本书可供计算机科学、信息科学、网络工程及流量工程等学科的科研人员、大学教师和相关专业的研究生和本科生，以及从事计算机网络管理领域、网络工程及网络安全保护的技术人员阅读参考。

图书在版编目(CIP)数据

网络行为的全息测量方法/程光，吴桦著. —南京：东南大学出版社，2013.12

网络新技术系列丛书

ISBN 978-7-5641-4666-5

Ⅰ.①网… Ⅱ.①程… ②吴… Ⅲ.①计算机网络—计算机应用—测量 Ⅳ.①P209

中国版本图书馆 CIP 数据核字(2013)第 286274 号

网络行为的全息测量方法

出版发行	东南大学出版社
出 版 人	江建中
社　　址	南京市四牌楼 2 号
邮　　编	210096
经　　销	全国各地新华书店
印　　刷	南京京新印刷有限公司
开　　本	787 mm×1092 mm　1/16
印　　张	16.5　彩插：8 面
字　　数	429 千字
版　　次	2013 年 12 月第 1 版
印　　次	2013 年 12 月第 1 次印刷
书　　号	ISBN　978-7-5641-4666-5
定　　价	39.00 元

（本社图书若有印装质量问题，请直接与营销部联系。电话：025-83791830）

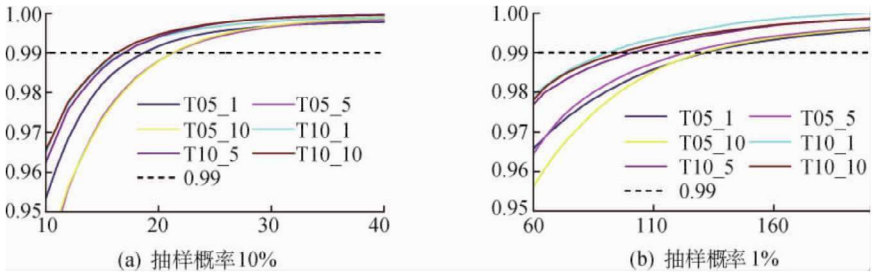

图 2.7　原始流长和未被抽样流的概率

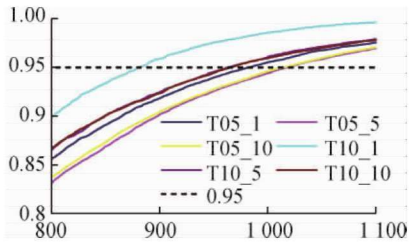

图 2.9　影响短流的最大原始流长

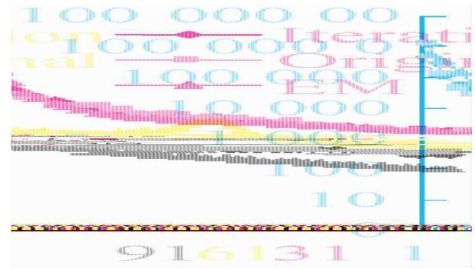

图 2.18　前 100 个流长估计的比较

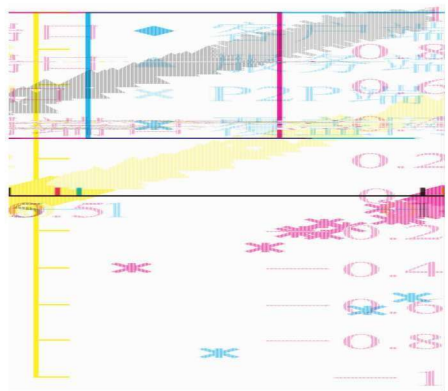

图 4.19　正常端口通信差异性测度二维图

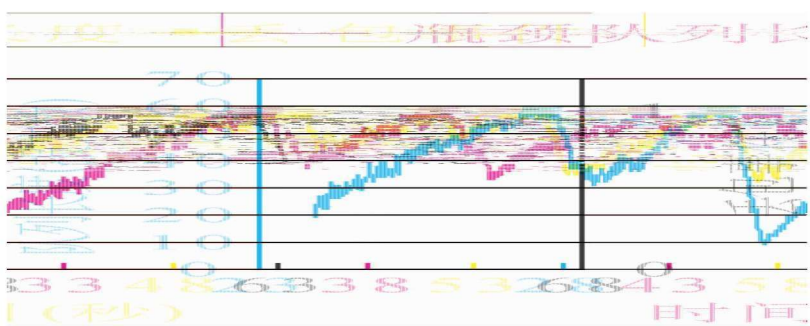

图 7.2　拥塞点队列长度变化和丢包事件关系

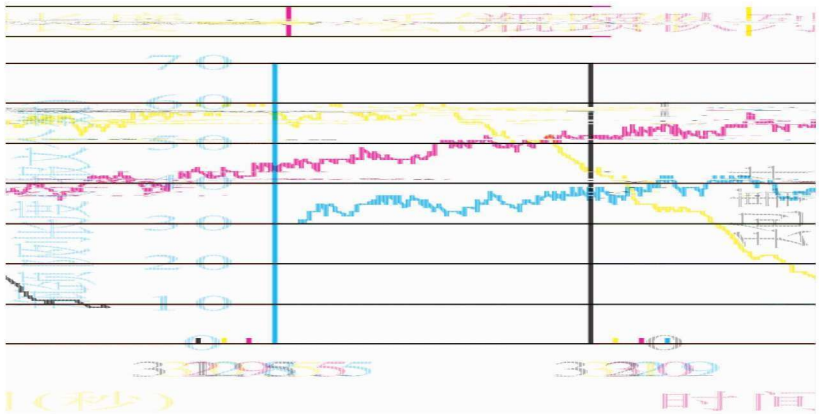

图 7.3　一次丢包平台细节

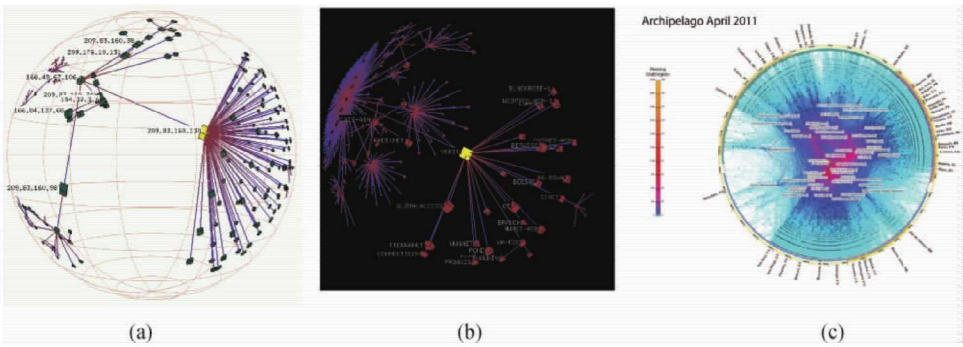

图 8.1　CAIDA 网络拓扑结构图

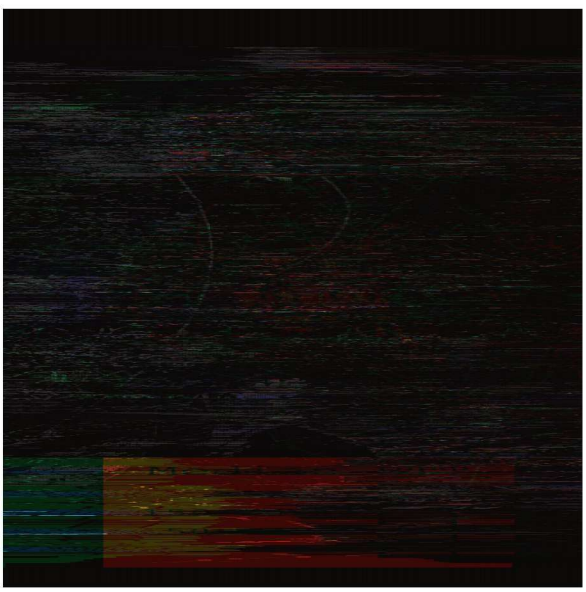

图 8.2　Walrus 拓扑图

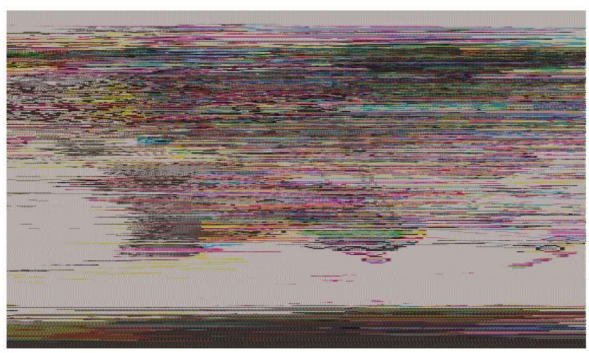

图 8.3　Mapnet 的显示效果

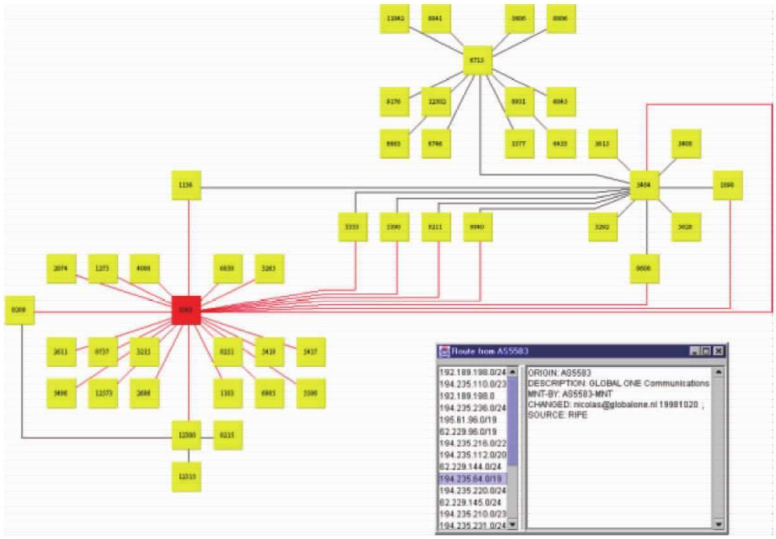

图 8.4　HERMES 拓扑图

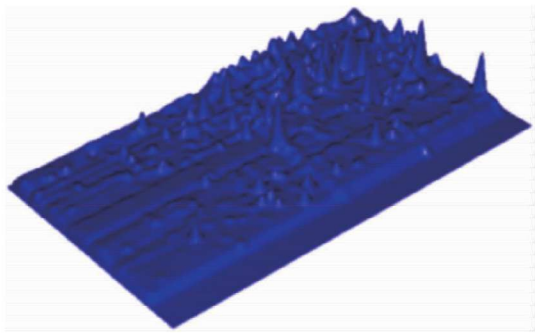

图 8.5　Cichlid 显示的网络地形

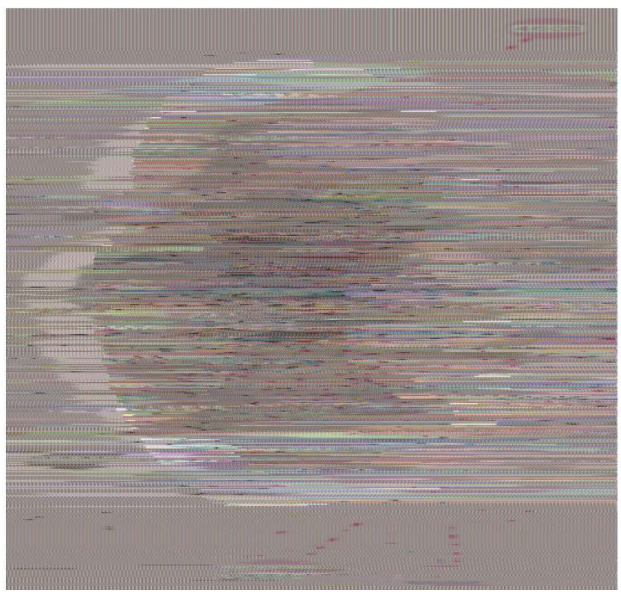

图 8.6　AS 分层等高线划分

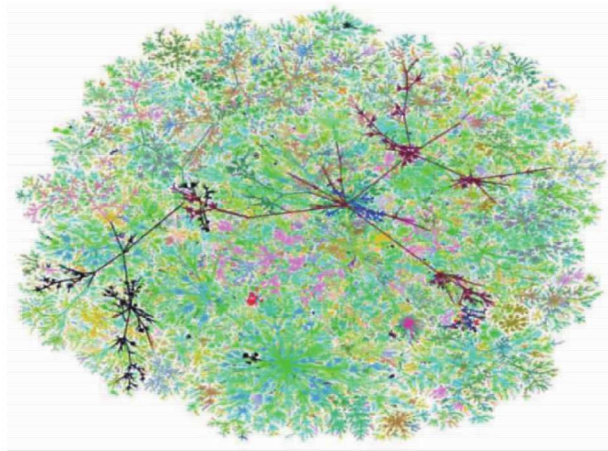

图 8.7　采用力导向布局生成的拓扑

图 8.8　The Internet map 网站

图 8.9　Internet Map 地球视图和互联网分级视图

图 8.14　地标显示效果

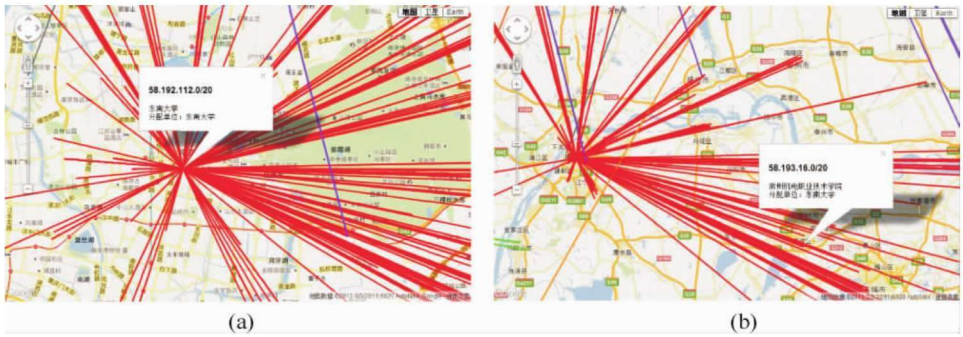

图 8.18　折线显示效果

图 8.19　CERNENT 所有网段分布导致视觉灾难

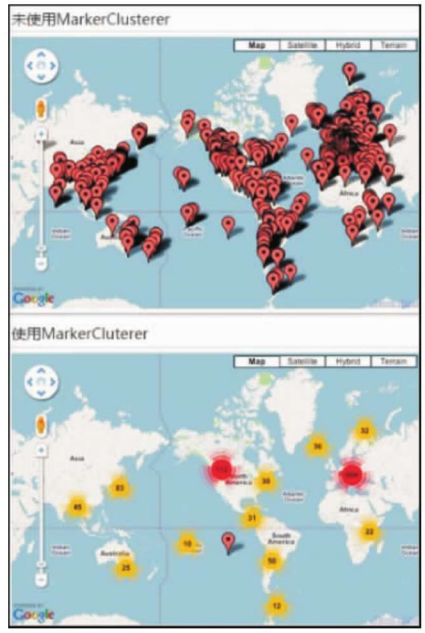

图 8.20　MarkerClusterer 的使用效果图

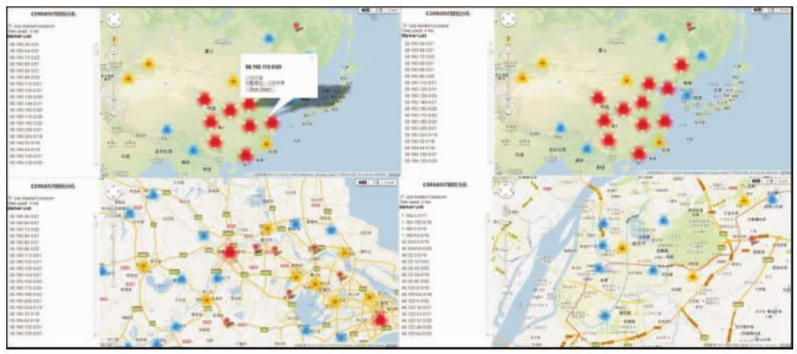

图 8.24　使用 MarkerCluster 网络标注化

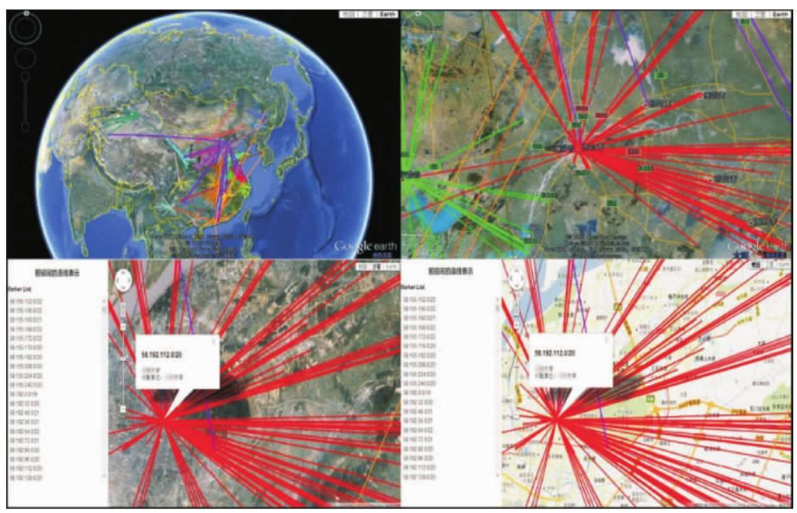

图 8.25　连线表示

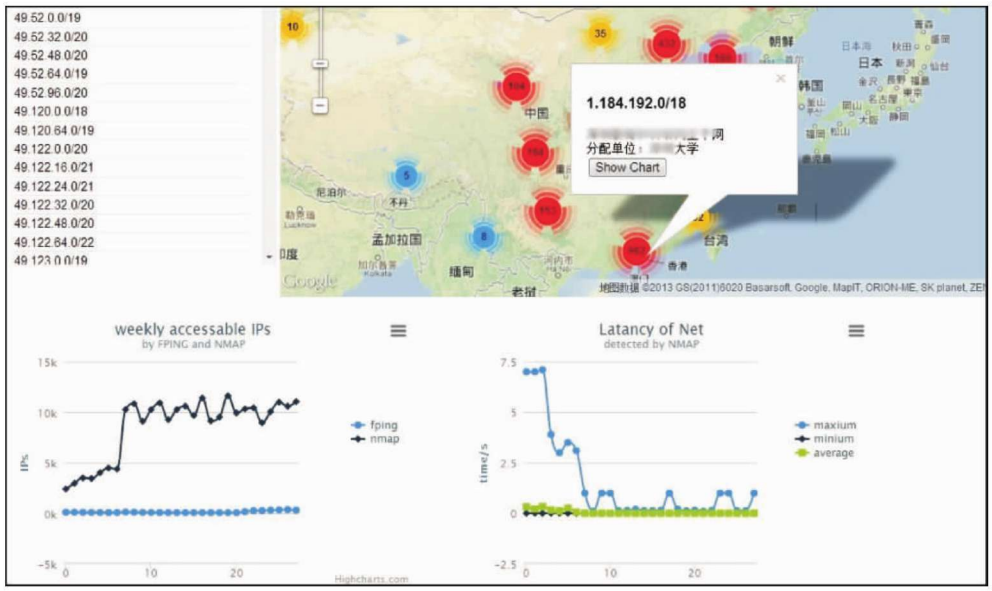

图 8.26　网络状态可视化效果

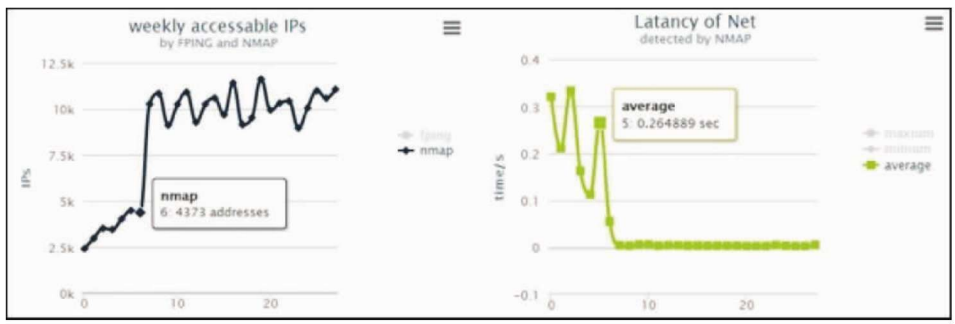

图 8.27　Highcharts 的交互功能展示图

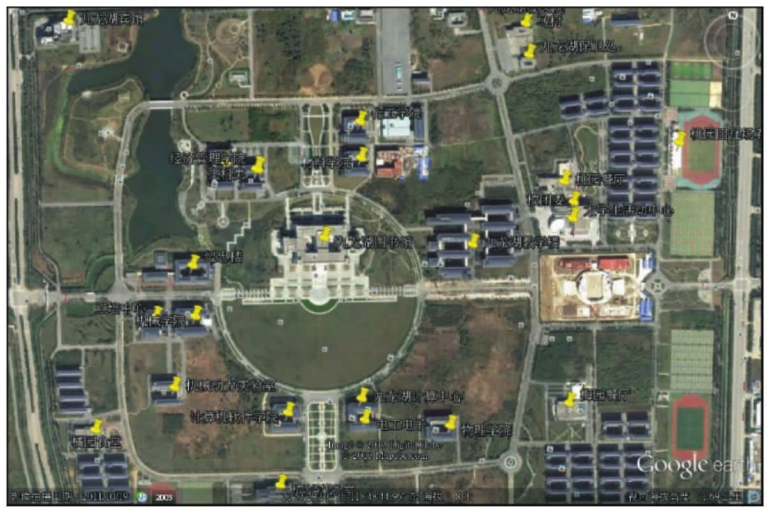

图 8.28　从 Google Earth 获取建筑物坐标

图 8.29　九龙湖网络地理位置可视化

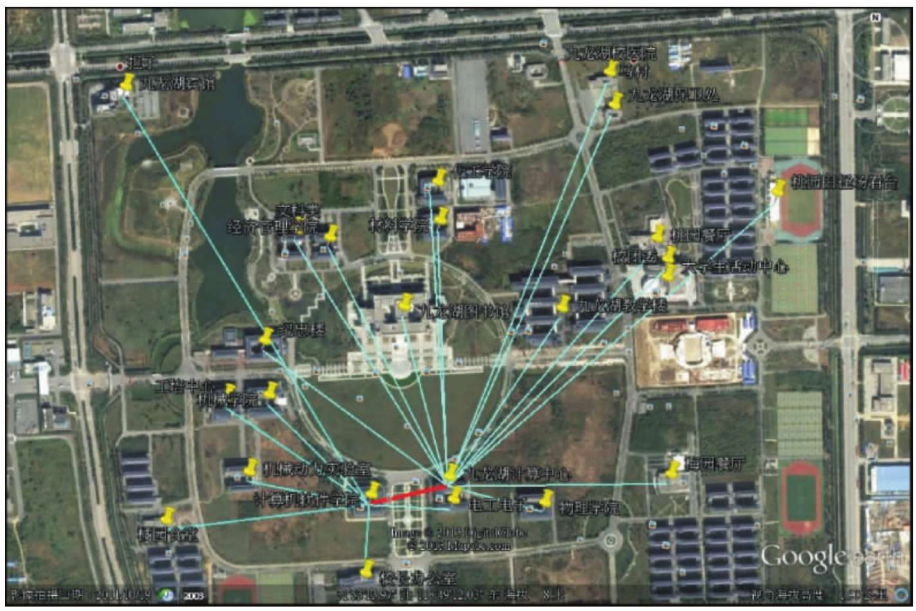

图 8.30　九龙湖校区子网逻辑拓扑

前　言

近年来，互联网的快速发展和新应用的不断出现，网络流量测量已经被广泛应用于网络计费、流量工程、网络安全等领域。随着网络链路速率不断提高和网络数据流急剧增加，当前在高速骨干网链路上，网络流量测量需要极高的计算和存储资源，从而给网络流量测量研究开发带来了技术挑战。在高速链路上，处理每个分组需要在纳秒内完成。例如，在 OC-768(40 Gbps)链路上，设分组的平均大小为 40 byte，则分组的平均处理时间为 8 ns。传统的网络流量测量方法面临的主要问题是可扩展性，不能够适应高速网络环境。美国已经在高速网络试验床上开展了下一代高速计算机网络及其典型应用的研究，在其他国家和地区也相继开展了下一代高速互联网络及其应用的研究，如英国、加拿大。与国际同类研究相比，我国的下一代互联网的研究内容涵盖了高速互联网络涉及的大部分研究领域，包括基础设施、网络服务与网络应用，并取得了一定的理论与应用成果。高速网络流量测量技术是下一代互联网研究的重要组成部分，成为网络测量的发展趋势之一。目前，高速网络流量测量问题主要有三种解决方案：① 利用高性能的专用硬件，如 TCAM、ASIC 等，实现高速链路上网络流量数据处理，然而，高性能的硬件设备极其昂贵；② 利用抽样技术只对部分有代表性的网络流量数据进行采集处理，降低系统的负荷，但这种方法存在较大的测量误差；③ 利用数据流技术对所有网络流量数据进行处理，有效减少存储资源的需求，同时保持一定的准确性。

高速链路上持续到达的海量的网络流量，给网络流量测量与分析带来了极大的困难。因此，需要采取一些可行的措施既能够对网络流量数据进行缩减又能够保留网络流量数据的特征信息。根据网络流量测量的应用需求，数据缩减技术主要分为抽样和数据流。抽样技术的目的是选择具有代表性的网络流量数据分组子集，通过该子集推断网络流量总体数据分组的特征信息。数据流技术可将庞大的信息压缩到较小的存储空间并保持一定的精确度，数据流技术具有在线实时处理和有限存储空间的特性。各种网络流量测量方法是针对具体的应用需求提出的，具有一定的局限性，目前还没有一种通用的网络流量测量方法。

围绕“用户跨域访问的自治网络管理和安全问题”的科学问题，重点解决“如何在竞争中形成有序的平衡状态，最大限度地利用资源同时保障每个实体公平使用资源的权利”这一关键问题。通过网络行为的全息测量方法研究，使热点测量和宏观测量相结合，以实现对网络非公平使用资源的热点实体监测，从多层面和多角度进行宏观协同测量和关联分析。

本书针对全息测量的数据的采集方法、数据的建模方法和数据的表示方法三个主要问题进行研究。全书分为三个部分包括 8 章内容，其中第 1 章为绪论，

第 2～4 章是数据的采集方法，第 5～7 章是数据的建模分类方法，第 8 章是数据的可视化方法。第 1 章综述了近年来国内外主要的高速网络流量测量方法的研究进展，第 2 章给出基于报文信息的流量抽样估计方法，第 3 章讨论网络流量聚合方法，第 4 章基于多维的活跃节点检测算法，第 5 章基于会话模式的网络流量分类方法，第 6 章基于 HTTP 流量分类方法，第 7 章基于 TCP 流的网络性能评估，第 8 章讨论网络的可视化方法。

本书主要是作者在网络测量和行为分析领域长期的研究成果的总结，也包括了作者培养的研究生参与的科研项目部分相关科研成果和论文。在本书撰写过程中，周爱平、臧家宁、江洁欣、李翔、刘军、王松、吴昊、赵欣、张阳、张涛、潘吴斌、张杰、王艳、王会羽、程志等给予了大力支持，参与了本书部分章节的编写工作以及本书的整编及校验，在此表示感谢，全书由程光、吴桦统稿。感谢东南大学龚俭教授、丁伟教授、曹争副教授、杨望讲师、吴珺助工，以及解放军理工大学的张国敏等帮助和支持。

本书的研究成果受国家 973 计划[基于自治治理模型的网络管理与安全研究(No. 2009CB320505)]、国家自然科学基金[高速网络活跃节点检测及其流量分类研究(No. 60973123)]江苏省科技支撑计划——工业部分[基于分布式通信机理的主干网僵尸网络追踪系统(No. BE2011173)]等国家省部级项目的资助，在此表示感谢！同时感谢江苏省“青蓝工程”优秀骨干教师及“六大人才高峰计划”的支持。

在本书的撰写过程中，得到了东南大学计算机科学与工程学院、东南大学计算机网络和信息集成教育部重点实验室、东南大学出版社等单位领导和专家的大力支持，在此深表谢意！

同时对作者所引用的参考文献的作者及不慎疏漏的引文作者也一并致谢！

由于作者水平有限，编写过程中难免存在很多不足及顾此失彼之处，敬请读者给予批评指正！

著　者

2013 年 8 月

目　录