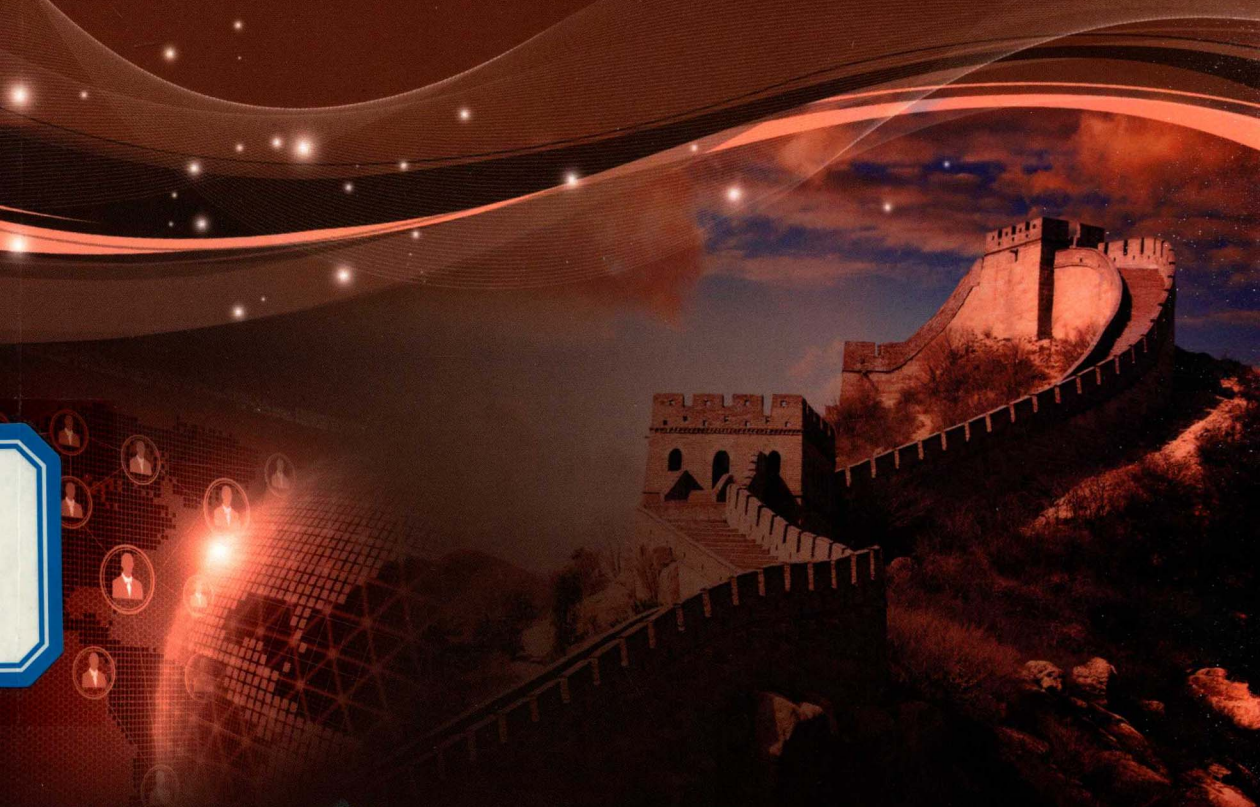
网络空间安全丛书

网络安全监测数据可视化分析关键技术与应用

◎张 胜 赵 珏 著



中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

国家自然科学基金(61402540)
湖南省社会科学基金(17VBA242)
湖南省自然科学基金(2016JJ2070)
湖南省普通高校教学改革(湘教通〔2017〕452号)
新零售虚拟现实技术湖南重点实验室出版基金
湖南商学院北津学院学术著作出版基金资助出版

网络安全监测数据可视化分析关键技术与应用

张 胜　赵 珏 著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书从信息科学的角度出发，系统地介绍了安全监控数据可视化分析系统的基本理念、各种处理技术和作者的最新研究成果。本书以人的认知模式为本源，以网络安全监测数据为研究对象，以可视化技术为研究手段，以快速发现网络安全事件并做出响应为目的，构建人、事、物三元世界高度融合的可视化人机分析系统，并针对网络安全中的异常检测、特征识别、关联分析和态势感知等需求，提出并设计新颖实用的可视化模型和算法。

本书可以为网络安全、计算机科学、信息科学及相关领域研究人员和专业技术人员提供参考，也可作为本科生或研究生的教学用书，还可供数据分析师、视觉设计师和对数据感兴趣的开发人员学习提高使用。

图书在版编目(CIP)数据

网络安全监测数据可视化分析关键技术与应用 / 张胜，赵珏著. — 北京：电子工业出版社，2018.5
ISBN 978-7-121-34087-1

I. ①网… II. ①张… ②赵… III. ①计算机网络－网络安全－数据处理 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 078911 号

策划编辑：张小乐
责任编辑：郝黎明　　特约编辑：王　炜
印　　刷：北京虎彩文化传播有限公司
装　　订：北京虎彩文化传播有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1092　1/16　　印张：7.25　字数：186 千字
版　　次：2018 年 5 月第 1 版
印　　次：2018 年 5 月第 1 次印刷
定　　价：48.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：(010)88254462，zhxl@phei.com.cn。

前　言

随着计算机网络通信技术的进步，飞速发展的网络应用对网络安全提出了很高要求。同时，现代网络安全威胁的范围和内容也不断扩大并演化，网络安全形势与挑战变得日益严峻和复杂。中国工程院沈昌祥院士认为，网络空间已经成为继陆海空天之后的第五大主权领域空间，应加快建设我国的网络安全保障体系，捍卫国家网络安全主权。

各种网络监控设备采集的大量日志数据是网络安全分析人员掌握网络状态和识别网络入侵的主要信息来源。网络安全可视化作为新兴的交叉研究领域，为传统的网络安全数据分析方法注入了新的活力，它通过提供交互式分析工具，建立人与数据之间的图像通信，借助人的视觉处理能力，进一步提高了分析人员的感知、分析和理解网络安全问题的能力。它能够将抽象的网络和安全监测数据转化为可视图呈现，帮助用户快速掌握网络状况，识别网络异常和入侵，全方位感知网络安全态势。

因此，向读者提供网络安全监测数据可视化分析领域相关算法、技术和问题解决过程中的实践经验，是本书的撰写宗旨。本书以人的认知模式为本源，以网络安全监测数据为研究对象，以可视化技术为研究手段，以快速发现网络安全事件并做出响应为目的，按照从简单到复杂、从单一到整体的思路，形成人、事、物三元世界高度融合的可视化人机分析系统。按照从单源到多源、从低层次视图到高层次视图的思路，针对网络安全中的异常检测、特征识别、关联分析和态势感知等需求，提出并设计新颖实用的可视化模型和算法。

本书系统地介绍了网络安全监测数据可视分析的概念、基本技术和应用，从主机状态、网络流量、入侵检测与防御数据、多源数据融合可视分析等方面阐述了各种处理技术和作者的最新研究成果。全书共分 7 章，内容包括网络安全监测数据分析概论，网络安全监测数据及图技术，主机健康状态变迁热图及异常检测分析技术研究，基于树图和信息熵时序的网络流时空特征分析算法研究，入侵检测与防御可视化中辐状图改进技术研究，多源异构网络安全监测数据可视化融合技术研究，网络安全监测数据可视分析关键技术总结与展望。

本书的撰写得到了国家自然科学基金(61402540)、湖南商学院北津学院学术著作出版基金、湖南省社会科学基金(17VBA242)、湖南省自然科学基金(2016JJ2070)、湖南省普通高校教学改革(湘教通〔2017〕452 号)、新零售虚拟现实技术湖南重点实验室的大力支持和出版基金资助，在此谨致以最诚挚的感谢。同时感谢中南大学施荣华教授、周芳芳教授、赵颖博士的指导和帮助；感谢赵珏等专家学者所付出的辛勤劳动；感谢作者家人的大力支持和理解。

由于网络安全监测数据可视化技术是一个新兴的交叉领域，很多理论方法和应用技术问题还有待进一步深入探索和发展，加上作者学识所限，因而书中一定存在不足之处，敬请专家和读者批评指正。

目　录

第 1 章　网络安全监测数据分析概论 …… 1

1.1　引言 …… 1

1.2　网络安全监测数据分析技术概况 …… 3

1.2.1　传统的网络安全监测数据分析技术 …… 3

1.2.2　数据可视化及分析技术 …… 5

1.2.3　网络安全监测数据可视化分析技术 …… 5

1.3　小结 …… 17

第 2 章　网络安全监测数据及图技术 …… 18

2.1　网络安全监测数据 …… 18

2.1.1　主机和应用状态日志 …… 18

2.1.2　流量负载数据 …… 19

2.1.3　防火墙日志 …… 20

2.1.4　入侵检测与防御日志 …… 21

2.1.5　其他数据 …… 21

2.1.6　安全监测数据比较 …… 22

2.2　测试数据集介绍 …… 23

2.2.1　校园网 Snort 数据集 …… 23

2.2.2　VAST Challenge 2013 数据集 …… 24

2.3　网络安全可视化图技术 …… 27

2.3.1　基础图 …… 27

2.3.2　常规图 …… 29

2.3.3　新颖图 …… 33

2.3.4　图技术的比较 …… 35

2.4　小结 …… 36

第 3 章　主机健康状态变迁热图及异常检测分析技术研究 …… 37

3.1　热图技术 …… 37

3.2　主机热图设计与实现 …… 39

3.2.1　颜色映射模式设计 …… 39

3.2.2　主机状态指标建模 …… 39

3.2.3　主机健康状态故事变迁热图技术实现 …… 42

3.3 实验数据分析与异常检测 …… 42
3.4 结果分析与评估 …… 45
3.5 小结 …… 47

第 4 章 基于树图和信息熵时序的网络流时空特征分析算法研究 …… 48
4.1 网络流可视化技术 …… 48
4.2 网络流可视化分析算法 …… 49
4.2.1 树图算法的选择 …… 49
4.2.2 树图层次规划 …… 50
4.2.3 树图空间特征的分析方法 …… 52
4.2.4 信息熵算法 …… 52
4.2.5 网络流时序算法 …… 53
4.2.6 时序图时间特征分析方法 …… 55
4.3 实验与数据分析 …… 55
4.4 结果分析与评估 …… 58
4.5 小结 …… 59

第 5 章 入侵检测与防御可视化中辐状图改进技术研究 …… 60
5.1 辐状图技术 …… 60
5.2 辐状汇聚图设计与实现 …… 62
5.2.1 用户接口界面设计 …… 62
5.2.2 色彩选择与混合算法 …… 63
5.2.3 汇聚曲线算法 …… 64
5.2.4 端口映射算法 …… 65
5.2.5 入侵检测系统实验数据分析 …… 66
5.3 辐状节点链接图设计与实现 …… 68
5.3.1 节点链接图改进技术 …… 68
5.3.2 基于节点链接图的辐射状表示方法 …… 69
5.3.3 可视化映射与筛选方法 …… 70
5.3.4 入侵防御系统用例数据分析 …… 71
5.4 结果分析与评估 …… 75
5.5 小结 …… 76

第 6 章 多源异构网络安全监测数据可视化融合技术研究 …… 77
6.1 数据融合技术现状 …… 77
6.2 多源异构数据可视化融合设计与实现 …… 80
6.2.1 多源异构数据集的选择与预处理 …… 80

6.2.2 数据融合分层框架 …… 81
6.2.3 标记树图数据级融合方法 …… 82
6.2.4 时间序列图特征级的融合方法 …… 85
6.2.5 人机交互决策级的融合方法 …… 87
6.3 融合实验与数据分析 …… 88
6.3.1 正常状态分析 …… 88
6.3.2 异常状态分析 …… 89
6.3.3 特殊状态分析 …… 92
6.4 结果分析与评估 …… 93
6.5 小结 …… 96
第 7 章 网络安全监测数据可视分析关键技术总结与展望 …… 97
参考文献 …… 101

第1章

网络安全监测数据分析概论

1.1 引言

近年来，随着计算机网络规模不断扩大、信息高速公路不断提速以及网络应用的不断增加，网络安全面临着越来越严峻的考验。特别是进入大数据时代以来，网络攻击呈现出大数据的“3 V”特征(Volume、Variety、Velocity)，即攻击规模越来越大，如分布式拒绝服务攻击，往往可以控制成千上万台设备攻击主机；攻击类型越来越多，新的攻击模式和病毒木马的变种叫人防不胜防；攻击变化越来越快，如一次有预谋的网络攻击往往包含多个步骤和多种应变的方案。

纵观我国互联网络安全态势[1~5]，如图 1-1 所示，网络安全问题不断攀升，主要表现为：

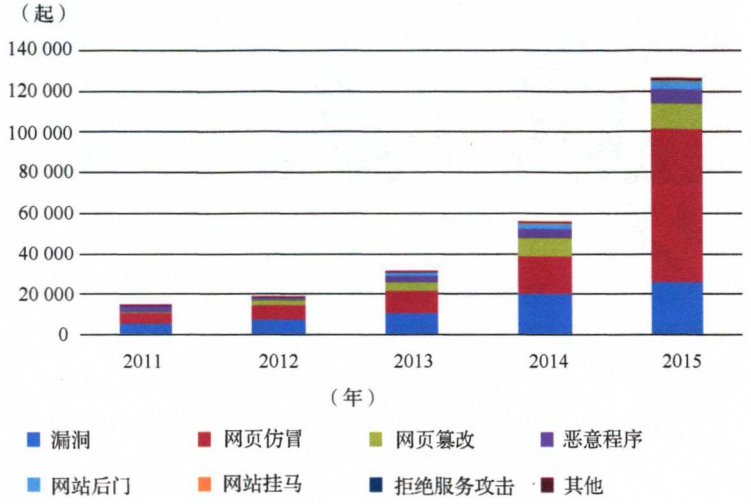


图 1-1 我国近 5 年安全事件分布

(1)网络基础设施面临严峻挑战。通用的硬件和软件漏洞较多、风险大，容易被探测、攻击和渗透，导致网络设施或主机被操控、用户信息泄密、恶意代码泛滥、攻击网络软/硬件资源、破坏网络稳定运行等安全事件。特别是随着网络技术的不断发展，处于新生和不断完善阶段的智能家电、智能穿戴、智能交通等设备，安全防护能力普遍较弱，存在安全隐患，如不及时更新和修复，易被大量使用，造成严重危害。同时，随着云计算、大数据等新技术应用与发展，部署到云平台上的政务系统和企业系统，由于涉及大量国计民生、企业运营和用户个人信息，将会更多地吸引有目的、有预谋的精准攻击。

(2)网站植入后门、钓鱼攻击和其他隐蔽事件呈不断上升趋势。网站用户信息已成为黑客攻击的重点，如用户信息、产品信息、消费者信息频繁泄露，网络钓鱼事件日渐猖狂，严重影响电子商务网站和金融业务的成长，危害公共服务平台的安全。

(3)拒绝服务攻击仍然是中国互联网安全最严重的威胁，其技术也变得越来越复杂。攻击形式从直接攻击变换为分布式反射攻击，攻击对象从网站本身转变为网站所使用的域名系统，严重威胁到我国互联网的整体运转安全。根据 2015 年 1～9 月统计，攻击流量超过 1000Mbit/s 的分布式拒绝服务攻击数量约 38 万次，平均每日攻击次数达到 1490 多次。

横观世界各国情况，以亚太地区为例，如图 1-2 所示，情况惊人的类似，网站被篡改、仿冒、病毒、木马攻击、网络入侵、攻击等成为主要问题[6]。事实证明：为最大限度地保护网络空间安全，必须优化和改进传统的安全防御方式，构建能应对复杂化和持久威胁的安全防护和响应体系[7、8]。

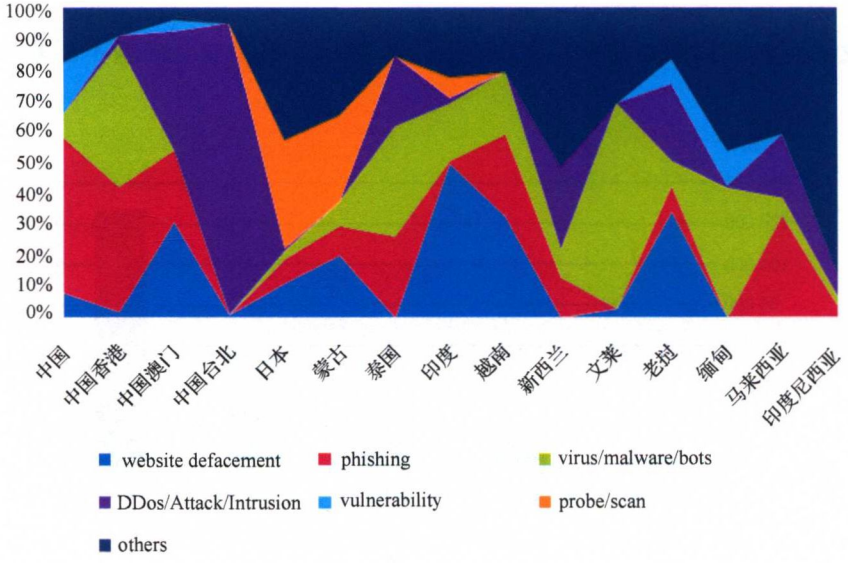


图 1-2　2015 年亚太地区网络安全事件分布

当前世界各国相继集中部署网络安全核心战略，如美国在 2012 年签署了“美国行

动网络政策”，在 2013 年发布“加强关键基础设施网络安全”白皮书，“2014 年国防预算优先项和选择”拟重组 133 个网络防御单位计划；加拿大在 2014 年“全面数字化国家计划”中提出了加强网络空间安全防控能力等近 40 项新措施；日本在网络安全领域通过“网络安全基本法”，发挥政府和民间的互补优势来更好地应对网络攻击。我国在 2014 年成立了中央网络安全和信息化领导小组统筹各个领域的网络安全和信息安全问题。国务院重组了国家互联网信息办公室，负责全国网上信息的内容整理、监管、审核等工作。工业和信息化部信息中心发布了“关于加强电信和互联网行业网络安全工作的指导意见”，明示了八项重点工作，包括提升基础设施防护能力和提高数据保护措施等，着力构建网络安全空间的保障体系。

综上所述，网络空间安全问题已经引起了世界各国的高度重视，各种研究方法纷纷涌现。对可视化的研究分析技术不但使网络安全威胁看得见、摸得着，还能在人和技术中间架起一座良好的沟通桥梁，保护着日益重要的网络空间，更加重要的是图形图像比枯燥的数据更容易被人识别和认同，为决策者制定网络安全政策提供了可靠而形象的数据来源。网络安全数据可视化技术的研究改进不仅对我国国家安全、政府办公、企业经营和社会生活等具有广阔的应用前景，更对我国自主研发核心网络安全产品、构建网络安全防御体系具有深远的科学意义。

但是，目前这个新兴的研究领域还有很多关键技术问题急待解决。比如，如何快速提取网络资源状态特征，直观展示异常问题；如何解决网络负载数据量大、影响因素广、分析困难的问题，精确表达时空特征；如何直观发现入侵行为，满足视觉性和实用性需要；如何解决海量多维数据的信息融合，实现多源分析，感知网络安全态势等。

本书将从主机状态数据可视化、网络流量可视化、入侵检测防御数据可视化和多源数据融合分析可视化四个方面，深入进行网络安全监测数据可视化的分析设计研究，提出易用、实用、美观的技术解决方案，实现对网络安全威胁的风险评估和实时响应。

1.2　网络安全监测数据分析技术概况

1.2.1　传统的网络安全监测数据分析技术

针对安全威胁日益加剧的网络空间战争，业界开发出各种网络安全技术来监控、分析、掌控网络环境，其代表有：

(1)防火墙(Firewall)，主要目的是保护内部网络资源，防止用户未经授权访问。防火墙以网络安全访问策略或规则为依据，对进/出网络的数据包进行检测，符合访问策略的被允许通过，不符合的予以阻断，采用了在边界上控制流量的策略。作为一种网络隔离手段，防火墙对提高内网的安全发挥了重要的作用。

(2)入侵检测与防御技术(IDS/IPS)，主要目的是检测和识别网络中的恶意行为，发现潜在的对网络或主机的攻击行为，包括内部和外部的网络入侵或未经授权的行为。入

侵系统作为一种主动安全防御系统，可以有效弥补静态防御技术中的一些问题，并已成功应用于网络安全管理中。

(3)网络负载检测(Network Traffic)，主要目的是检查、识别和分析网络流量是否异常，根据检测技术分为基于特征的检测和基于统计的检测。基于特征的检测是指通过匹配已知异常特征模式来检测，基于统计的检测是指通过学习历史流量得到正常的流量模型，通过正常模型来检测不符合此模型的流量。继防火墙、入侵检测与防御技术之后，流量检测成为网络安全技术研究的新热门。

(4)恶意代码检测(Malware)，主要目的是检测和消除系统中的恶意程序，保护主机和网络免受感染或减少对系统的破坏，是保护网络安全不可缺少的工具。

传统网络安全技术在实际运用中往往会产生海量的监测数据文件，网络的保护方式、攻防足迹、效果和不足等有效信息往往隐藏在这些数据中。网络安全监测数据分析技术就是利用监测数据找出有效信息，对其进行深度分析挖掘。

从目前的研究情况看，传统数据分析主要建立在机器的自动化分析上，往往采用简单的统计图形，或者晦涩难懂的专业报表，使分析的有效性难以保证。如防火墙受数据分析技术的制约，通常只是对日志数据简单地进行查询、汇总，导致有价值的信息不能进行深入挖掘和直观展示；入侵检测系统误报率很高，这些误报往往掩盖了攻击的真实目的；网络负载分析难以满足大规模网络实时处理的要求，给海量流量的实时处理和未知攻击的检测带来极大的挑战；恶意代码分析的本质是一种事后处理，分析技术在准确性和完备性上还不够，存在着假阴性和假阳性等问题。

随着当今社会网络威胁不断呈现出复杂化、隐蔽化、扩大化态势，传统数据分析技术无法完全满足“看得见，管得好，防得住，应得急”的网络安全目标。要想实现将网络安全从过去的严密防控转变为符合当代需求的实时分析加响应的需求，只依靠以上技术和方法还是存在不少缺陷的[9~11]。

(1)缺乏实时显示、分析和处理大规模网络数据有效管理的手段。诸多安全设备运行时会产生海量警告或日志数据，难以直接解读，需要耗费管理员大量人力、物力对其进行分析处理。这些日志数据看起来很丰富，但使用却很烦琐，如何使管理人员实时、准确、形象地把握全局和威胁态势是一个挑战。

(2)缺乏感知和应对实际威胁的能力。在警告和日志数据中充斥着大量误报、漏报、重复报，隐匿着真实威胁，传统的分析方法使得管理员无法及时辨识，甚至直接忽略了某些重要的报警，安全事件应急响应无从保证。

(3)缺乏安全监测数据之间的协同分析。不同功能安全设备以各自方式独立工作，产生的安全数据针对全局来说是片面和孤立的，而网络是一个整体，不能割裂地对待安全事件。如每一次入侵都会在防火墙系统、网络负载、主机日志上留下证据。如何解决大范围的复杂网络问题，让多个数据源、多种安全视图、多个管理员共同参与网络安全威胁分析是一个难题。

(4)网络安全设备的易用性和实用性低，日志数据难以解读。每种网络安全设备都

需要经过一定的人员培训才能使用，而且大部分系统都需要专业知识作为支持，即使是有丰富经验的分析人员也很难驾轻就熟。然而，网络安全的受众应该更加广泛，起点应该更低，因此有必要加强对网络安全设备和技术的易用性研究。

1.2.2　数据可视化及分析技术

数据可视化的基本思路是将数据集中绘制成单个图元素，大量的数据集可以构建为复杂有序的图像，其中数据属性值以多维数据的形式表示，可以在图像上观察不同维度的数据，从而对数据进行更深入的观察和分析。

数据可视化起源于 20 世纪 50 年代的计算机图形学，经过科学可视化、信息可视化两个阶段，现在发展为数据可视化阶段。科学可视化是指科学计算组成部分的可视化，主要针对科学与工程实践中计算的建模和模拟运用。信息可视化旨在为各应用领域中抽象、异质的数据集提供分析支持工作，面向的是应用领域。数据可视化技术是对前两种技术的扩充和完善，指利用图形和图像处理、计算机视觉以及用户界面，通过表达、建模以及对立体、平面、动画的显示，对数据加以可视化解释。现在主要的研究领域包含文本数据可视化、网络(图)数据可视化、时空数据可视化、多维数据可视化[12]。

支持可视化分析的认知理论模型包括意义建构、人机交互分析、分布式认知三种模式。意义建构认为信息是在特定时空环境中认知主体主观建构的意义，构建过程是人的内部认知与外部环境交互行为共同作用的结果，如数据分析就是搜索和获取信息的行为。人机交互分析认为搜索信息是人主观发起的，新知识的构建可以通过显式交互操作建立，计算机将相关、有价值的信息显示出来，分析者对信息进行取舍。分布式认知是将认知的领域从个体延伸到与之相关的时空环境，数据可视化是将信息和知识进行外部化的一种手段，用户可以直接从符合用户心理映像的外部表征中提取信息和知识。不管是哪种模式，充分利用人的主观能动性来弥补自动化检测的不足，在人机之间建立良好的合作接口是最终目的。

随着社会信息化的高速增长，数据的可视化显示和分析需求也急剧扩大，特别是一些监控中心、指挥中心、调度中心等重要场所，大屏幕显示分析系统已经成为数据可视化不可或缺的核心基础系统。进入大数据时代以来，数据呈指数级增长，对大数据的可视化呈现与分析将进一步得到应用，特别是关乎国家安危的海陆空天以及网络安全领域，切实实现大数据价值，可以帮助各行业各领域管理决策者从政策制定、决策把握、业务管理、事前预警、事中指挥调度、事后分析研判等多个方面提升智能化决策能力。

1.2.3　网络安全监测数据可视化分析技术

网络安全问题首先是人本身的问题，不管是网络威胁的发起、检测还是制衡，人的知识和判断始终处于主导地位。经过多年的发展，将以人为本的可视化技术引入网络安全领域已经形成了新的研究方向，网络安全监测数据可视化就属于其中一个分支。它利用人类生理视觉对图像的获取能力强于文字、数字的特点，将抽象的网络和日志数据以图形/图像的方式展现出来，帮助业务人员分析监测网络状况，识别网络异常、入侵，

预测网络安全事件发展趋势[13]。从 2004 年开始，学术界和工业界每年都要召开一次国际会议 Visualization for Cyber Security，这代表着业界已开始注重网络安全可视化的研究。网络安全监测数据可视化如式 1-1 所示：

$$网络安全监测数据可视化=人+事+物 \tag{1-1}$$

“人”包括决策层高度重视、管理层把控质量、执行层落实到位，其中安全团队(专家)实时有效的分析和快速响应是关键；“事”指网络安全事件，主要包括事前预防、事中接管，事后处理，其中如何快速地掌握事件真相并做出响应是关键；“物”包括防火墙、入侵检测与防御系统、病毒防护、交换设备、虚拟局域网、堡垒隔离设备等网络安全设备，其中合理的配置规则、调优、联动是关键。

从式(1-1)中可以看出，“人”是关键，“物”是基础，“事”是网络安全要查找和解决的对象。网络安全监测数据可视化研究首先要分析监测数据或日志(来自“物”)结构，进行预处理，先选择基本的视觉模型，建立数据到可视化结构的映射，不断改善表示方法，使之更容易视觉化并绘制视图，再通过人机交互功能和“人”认知能力来观察和分析隐藏在数据中的有用信息(网络安全“事”件)，从而提高感知、分析、理解和掌控网络安全问题的能力，如图 1-3 所示。

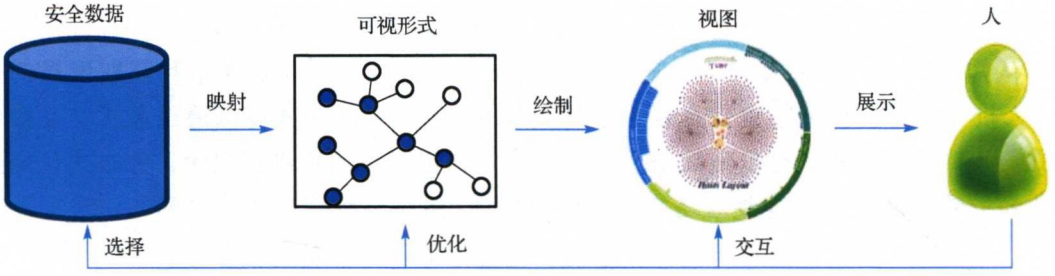


图 1-3　网络安全监测数据可视化流程

根据网络安全监测数据对象的不同，可视化系统主要分为以下 5 种：

1．主机状态数据可视化

主机状态日志可视化主要致力于展示主机和服务器的状态，包括网络状态、用户数、系统负载、异常进程等，主要作用是检查恶意软件和保证主机服务能力。一般由日志接收代理、数据库、过滤分析中心等几部分构成，由于收集代理不同，导致收集内容有所偏重；同时，信息传输和分析使用的数据格式不同，阻碍数据在不同平台及系统间自由交换。主机状态日志可视化主要解决日志格式不统一带来的理解差异，从而提高管理效率和质量。

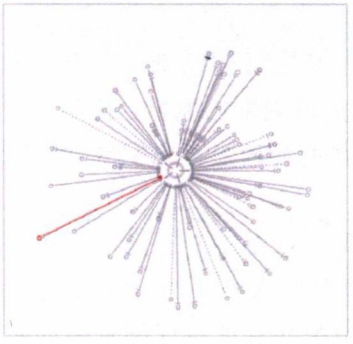
早期的工作有用 Erbacher 设计的可视系统，如图 1-4(a)所示，服务器排列在中间，主机以同心圆的方式环绕着服务器，同一子网的主机和服务器更靠近一些，系统用不同的符号标识来表示主机不同的属性，主机和服务器的连接类型用不同的连接线段来表示，该系统目的是发现不确定的数据连接[14]。

Tudumi 也是早期系统，不同于 Erbacher 的设计，Tudumi 采用 3D 技术，系统节点采用 3D 符号标志，主机之间的服务采用不同的线段，如粗线表示终端服务，细线表示文件传输等。该系统关注一个或少数几个主机和服务器的活动，用于监视和审计服务器上的用户行为[15]。

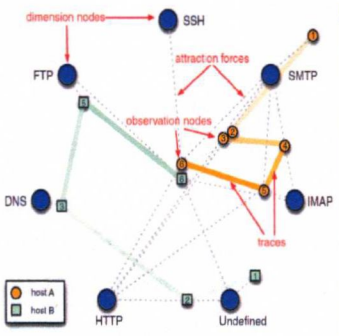
Mansmann 采用了节点链接图来展示主机行为，如图 1-4(b)所示，各种网络服务被排列在力导向布局的视图上，被观察的节点通过虚拟弹簧来连接相关的服务，节点的大小根据传输数据量的对数指标计算。该系统能监视主机行为，主机状态非正常的变化被定义为可疑事件[16]。

之后，主机的可视化产品被不断开发出来，可用于商业。产品如 Mocha(摩卡)能实现不同主机和不同的操作系统关键资源的自动监测，Visualized Management 模块将主机实时运行的情况以及多个主机参数以符号、时序图等方式展现出来，包括各 CPU 的使用率、物理内存和虚拟内存利用率、进程操作、进程优先级、网络流速流量等，如图 1-4(c)所示，可以帮助管理员找到主机异常和故障[17]。

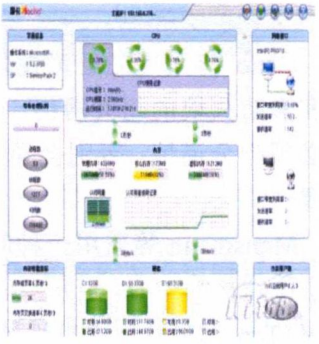
CCGC 采用了仪表盘的可视化技术，如图 1-4(d)所示，仪表盘上展示了现在和过去主机和网络状况因子，如网络因子、CPU 因子、内存因子、磁盘因子等，允许管理员审查网络状态和定位潜在的异常问题，通过下钻操作，还可以获取更多信息，便于故障分析和网络恢复[18]。



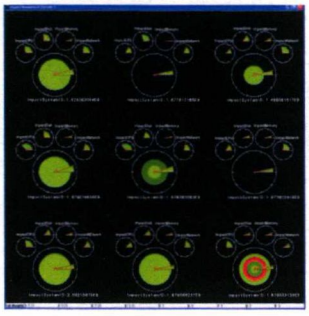
(a) Erbacher



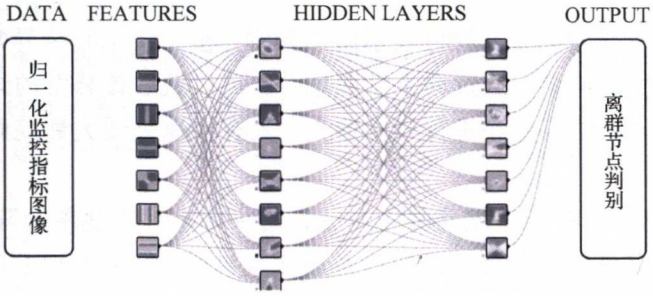
(b) Mansmann



(c) Mocha BSM



(d) CCGC



(e) 吴頔

图 1-4　主机状态数据可视化

进入了云时代以后，我国阿里云、盛大云和腾讯云都推出了可视化云主机服务，采用企业级虚拟化技术和管理平台，给用户提供了高性能、高可用、高安全、高弹性的云服务[19~21]。同时，为了保证服务质量，系统还提供了可视化资源使用情况的监控平台，可以实时监测内存、处理器、存储、网络带宽的调整和变化，用户可随时掌握云主机的服务质量，为用户调整、优化云服务，按需使用、按需付费提供了依据。

吴峒从时间、节点号、性能指标类型三个维度出发[22]，如图 1-4(e)所示，提出了基于维度压缩与维度切面的云主机性能数据集可视化方法，应用动态时间规划和卷积神经网络实现离群节点自识别。

2．防火墙数据可视化

防火墙作为使用最为广泛的安全设备之一，对于阻断外部攻击作用明显。它面临的主要问题是：如何设置防火墙记录级别，既能保证记录的全面又可防止数据过于巨大；防火墙数据进/出方向包括内部与外部接口的进与出四个方向，如何防止重复记录；因防火墙规则配置困难，如何进行验证和审计规则的改变。防火墙可视化的主要作用是简化防火墙操作、合理调整防火墙策略、发现网络出口的可疑日志、监控上网行为等。

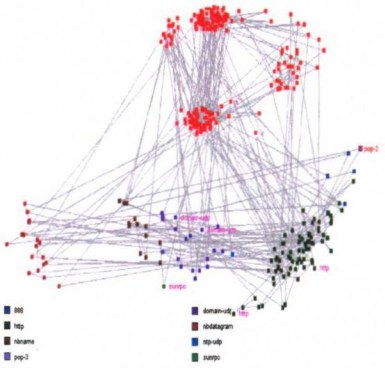
Girardin 等采用散点图来显示防火墙事件，如图 1-5(a)所示，用有色方块表示主机，方块的颜色表示不同的协议类型。数据点按时间顺序排列，类似事件会聚在一起。该系统能清楚地显示事件中的相似性和相关性，用户可直观地发现进程是否启动、被谁启动、请求是否可疑等[23]。

Chao 等采用三层可视化结构来显示防火墙规则以及规则之间的联系，适合于大规模和多防火墙的超大网络，特别是在多防火墙系统中，防火墙规则的编辑、排序、发布都必须十分谨慎，否则会导致网络功能紊乱，该系统旨在帮助管理员事先发现并去除误配置[24]。

Mansmann 等采用一种叫日照图技术来显示防火墙规则，如图 1-5(b)所示，根节点在层次结构的中心，表示“对象组”，接下来的同心环依次排列防火墙动作(允许和拒绝)、协议(Tcp、Udp)、主机地址、端口，该系统的主要功能是帮助管理员理解复杂的防火墙规则配置[25]。

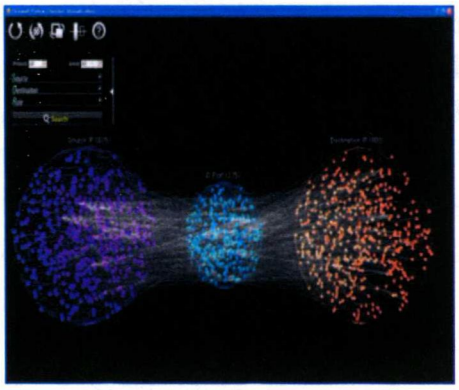
FPC 的主视图采用 3D 技术检查防火墙策略，如图 1-5(c)所示，用 3D 球体的颜色来表示异常类型，红色表示阴影异常，橙色表示冗余异常，暗黄色表示泛化异常，黄色表示关联异常。通过向下钻取球体，可以获取该异常的详细视图，该系统用于发现风险服务、非法服务和进行异常检查，具有快速处理大量规则的能力，降低使用者的技术门槛[26]。

VAFLE 采用聚类热图来分析防火墙事件，热图矩阵可视采用时间×主机、时间×端口等组合用来发现活跃的服务器或主机等，如图 1-5(d)所示，用深色的热点显示了两天中网络用量最高的主机，该系统通过增强互动的集群可视化热图来进行异常检测和网络态势分析[27]。

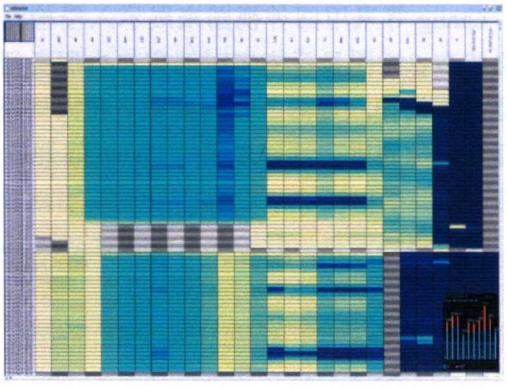


(a) Girardin 等

(b) Mansmann 等



(c) FPC



(d) VAFLE

图 1-5　防火墙数据可视化

3．网络入侵数据可视化

入侵检测与防御系统主要用于发现网络或系统中是否有违反安全策略的行为和被攻击的迹象，帮助管理人员快速识别和抵御分布式拒绝服务、网络蠕虫及木马等攻击行为。但是，入侵检测机制导致产生了大量的重报、误报，海量日志数据使得管理人员无从下手，甚至会忽略重要的警报，实时的安全响应无法保证。因此，网络入侵系统日志可视化主要功能是帮助分析人员降低认知负担，去除误报，提高检测攻击的能力。

Snort View 采用的可视化技术是散点图和符号标志，如图 1-6(a)所示，系统由三个面板组成：源地址、警报和源/目标，警报用不同颜色的符号标记，颜色表示优先级，符号类型表示不同攻击的类型，适合于小型网络。该系统用于帮助管理员减少错误警报，检测隐藏攻击和攻击序列[28]。

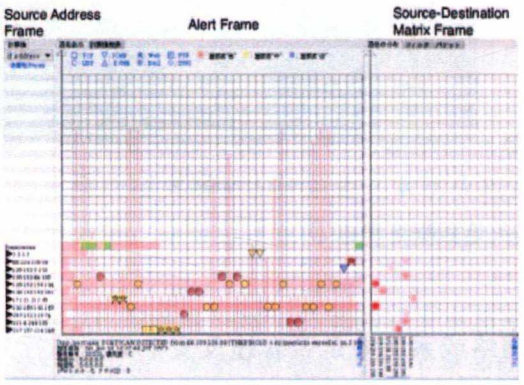
IDS Rainstorm 采用的可视化技术是散点图，如图 1-6(b)所示，系统由一个主视图(显示整个网络的表现)、一个缩放视图(显示用户选择的 IP 地址范围)组成。主视图由 8 列构成，每列可显示连续的 20 位 IP 地址，整个视图可显示 2.5 个 B 类地址 24 小时的监控数据，报警的等级采用颜色来表示。用户可以用主视图分析整个网络情况，发现可疑

事件，用缩放视图获取详细攻击信息。该系统用于发现非正常的网络事件、僵尸网络的感染和蠕虫病毒的传播[29]。

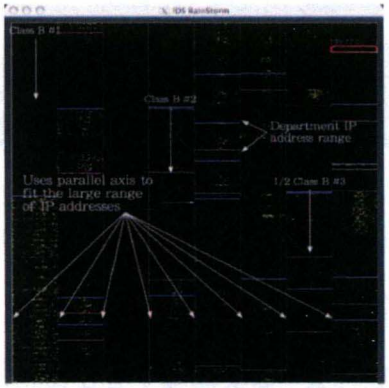
Vizalert 系统采用的可视化技术是雷达图，如图 1-6(c)所示，系统关注警报时间、地点、事件三个方面的特征，主视图在中间显示网络的拓扑，而周围的圆环用于显示不同的警报，圆环的宽度表示时间，连线从圆环指向内部触发的主机。该系统可以提高网络攻击的检测、分析和处理速度，减少攻击的影响[30]。

Avisa 采用的可视化技术是辐状汇聚图，如图 1-6(d)所示，辐状图由外部环和内部弧构成，环分为两部分，较小的一边用于显示网络警报分类，较大的一边用于显示子网或自定义的分组。弧用于显示真正的报警，弧的一边指向报警类型，另一边指向有关联的主机。该系统采用启发式算法，用来洞悉攻击模式，促进潜在数据的理解[31]。

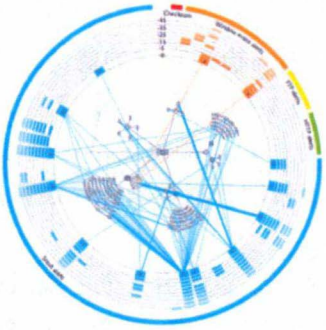
Zhang 等采用四种视图来展示入侵检测系统的日志，包括甘特图显示服务器连接的变化状态、树图显示指定时间窗口内服务器报警的数量、节点图表示事件间的关联、堆叠直方图统计服务器各指标参数。在大规模的网络中，通过多种可视化方法的互补，可以有效去除误报，同时，基于 Web 的开放平台能简化管理，提高研究人员协同分析的能力[32]。



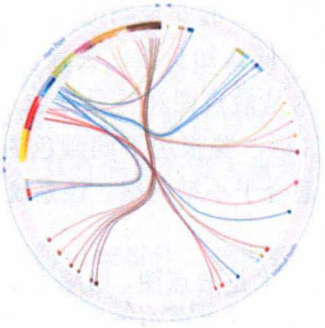
(a) Snort View



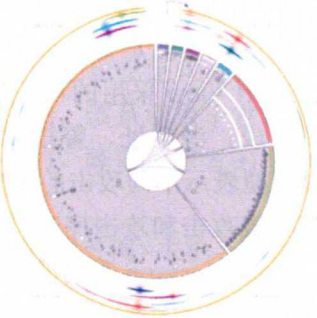
(b) IDS Rainstorm



(c) Vizalert



(d) Avisa



(e) IDSPlanet

图 1-6　网络入侵数据可视化