网络安全数据可视化综述

赵 颖[1)]，樊晓平[1,2)]，周芳芳[1)]，汪 飞[3)]，张加万[4)]

[1)](中南大学信息科学与工程学院 长沙 410083)

[2)](湖南财政经济学院网络化系统研究所 长沙 410205)

[3)](湖南师范大学数学与计算机学院 长沙 410081)

[4)](天津大学软件学院 天津 300072)

(zff@csu.edu.cn)

摘 要：网络安全可视化是一个新兴的交叉研究领域，它通过提供交互式可视化工具，提升网络安全分析人员感知、分析和理解网络安全问题的能力.通过近些年来的研究，该领域的很多研究成果已经在网络监控、异常检测、特征识别、关联分析和态势感知等方面取得了重要进展.文中介绍了网络安全可视化的必要性和发展历史，以及主要的网络安全数据源，并重点从网络安全问题和网络安全可视化方法 2 个角度对已有研究成果进行了系统的梳理；最后对未来的发展趋势进行了展望.

关键词：信息可视化；可视分析；网络安全；安全可视化

中图法分类号：TP391

A Survey on Network Security Data Visualization

Zhao Ying[1)], Fan Xiaoping[1,2)], Zhou Fangfang[1)], Wang Fei[3)], and Zhang Jiawan[4)]

[1)](*Information Science and Engineering School, Central South University, Changsha* 410083)

[2)](*Laboratory of Networked Systems, Hunan University of Finance & Economics, Changsha* 410205)

[3)](*College of Mathematics and Computer Science, Hunan Normal University, Changsha* 410081)

[4)](*School of Software, Tianjin University, Tianjin* 300072)

Abstract: As a young community of network security research, visualization for network security focuses on taking advantage of the power of the human perceptual and cognitive processes by bringing robust visual tools into hands of humans in solving computer network security problems. Amounts of visual tools have played very significant roles in helping network security analysts to detect anomalies, discover patterns, identify correlations, and assess network security situation. In this paper, we offer a comprehensive review of network security visualization. First, we introduce the necessity and the phased development of this field; then we provide taxonomies from network security visualization technology and visual application in network security; at last we outline some guidelines and directions for future studies.

Key words: information visualization; visual analytics; network security; security visualization

随着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的要求.一直以来，各种网络监控设备采集的大量日志数据是人们掌握网络状态和识别网络入侵的主要信息来源.网络安全分析

收稿日期：2014-01-09；修回日期：2014-02-18.**基金项目**：国家自然科学基金(61103108，60673196)；湖南省科技计划博士后专项(2012RS4049)；湖南省自然科学基金(12JJ3062)；中南大学博士后专项.**赵 颖**(1980—)，男，博士研究生，讲师，CCF 会员，主要研究方向为可视化与可视分析等；**樊晓平**(1961—)，男，博士，教授，博士生导师，主要研究方向为网络系统与智能交通等；**周芳芳**(1980—)，女，博士，副教授，CCF 会员，主要研究方向为科学可视化与信息可视化等；**汪 飞**(1979—)，男，硕士，讲师，主要研究方向为可视化和可视分析等；**张加万**(1975—)，男，博士，教授，博士生导师，主要研究方向为图形学与可视化等.

人员在处理网络安全问题时,首先通过分析相应的数据来了解网络状态和发现异常现象,然后对异常事件的特征以及对网络的影响进行综合诊断,最后采取对应的响应措施.然而,随着网络安全需求的不断提升,网络安全分析人员在分析网络安全数据时遇到了很多新的困难:1)异构的数据源和持续增长的数据量给分析人员带来了繁重的认知负担;2)新攻击类型的出现和攻击复杂度的提高,使得很多传统的数据分析方法不再有效;3)大量漏报和误报是一些自动化异常检测系统的弊病;4)侧重于局部异常分析的传统思路,使得分析人员很难掌握宏观网络态势.如何帮助网络安全分析人员更高效地分析网络安全数据,已成为网络安全领域一个十分重要而且迫切的问题.

在解决网络安全问题的过程中,人的认知和判断能力始终处于主导地位,一个能帮助人们更好地分析网络安全数据的实用办法就是将数据以图形图像的方式表现出来,并提供友好的交互手段,建立人与数据之间的图像通信,借助人们的视觉处理能力观察网络安全数据中隐含的信息,以进一步提高分析人员的感知、分析和理解网络安全问题的能力.因此,许多学者提出将可视化技术引入到网络安全研究领域中来,并逐步形成了网络安全可视化这一新的交叉研究领域[1-3].

早在 1995 年 Becker 等[4]就提出对网络流量状况进行可视化,之后 Girardind 等[5]在 1998 年曾使用多种可视化技术来分析防火墙日志记录.从 2004 年开始举办的国际网络安全可视化年会[6](visualization for cyber security, VizSec),标志着该领域的正式建立,并且在 2004～2006 年集中涌现了一批高质量的研究成果,如图 1 所示.从 2011 年开始,国际可视分析挑战赛[7](VAST challenge)连续 3 年都采用了网络安全数据作为竞赛题目,推动着该领域呈现出一个新研究热潮.国内网络安全可视化的研究起步相对较晚,哈尔滨工程大学、天津大学、北京邮电大学、吉林大学、北京大学和中南大学等研究机构的一些团队已开展了相关研究.

经过十多年的发展,在网络安全可视化领域,学者们提出了许多新颖的可视化设计,并开发了诸多实用的交互式可视分析工具,这也为传统的网络安全研究方法和分析人员的工作方式注入了新的活力:1)分析人员的认知负担得以减轻;2)异常检测和特征分析变得更为直观;3)人们可以更自主地探索事件关联和复杂攻击模式,甚至发现新的攻击类型;4)网络安全态势的察觉和理解效率得以提高.

本文首先介绍网络安全分析人员需要处理的各种网络安全数据源,并重点从网络安全问题和网络安全可视化方法这 2 个角度,对已有研究成果进行了系统的梳理,最后对网络安全可视化的发展趋势进行了展望.

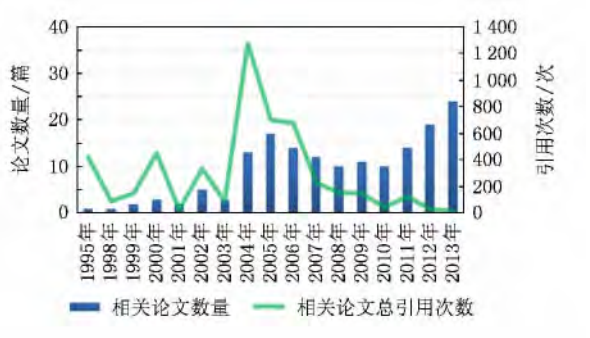


图 1 网络安全可视化领域相关研究年度汇总表

1 网络安全数据介绍

网络安全分析人员需要处理的网络安全数据种类非常多,其中最重要数据源来自各种网络监控设备.根据位于不同逻辑层次和不同物理位置的各种网络监控设备所采集信息的特点,可以将网络监控数据分 3 类:流量监控数据、状态监控数据和事件监控数据,如表 1 所示.

表 1 网络安全数据分类表

分类	数据名称	数据源举例
流量监控	网络数据包日志	Tcpdump,WireShark
	网络数据流日志	Cisco NetFlow
状态监控	状态监控日志	Big Brother,vSphere
事件监控	入侵检测系统日志	Cisco,SNORT
	防火墙日志	Cisco,Checkpoint,华为
	入侵保护系统日志	Cisco,IBM,天融信
	网络应用操作日志	Apache,Exchange,DNS
	弱点扫描与监控日志	Honeypots,eEye,Nessus
其他数据	系统配置文件、病毒样本等等	

流量监控数据主要来自包级和流级 2 个采集层次.包级的流量监控会记录每个数据包的 TCP/IP 包头信息和载荷内容;流级的流量监控会将一次网络会话的数据流聚合起来,只记录会话信息的方式数据量更小,也更加易于理解和管理.

状态监控数据是指网络中各种软硬件资源的运行状态信息,如 CPU 利用率、网络吞吐率、邮件服

务是否正常等等，它们可以通过 SNMP 协议或者通过安装一些专业的状态监控产品获得.

事件监控数据又分为异常检测日志和日常操作记录. 异常检测日志主要来自自动化的网络防御设备产生的报警事件，如防火墙和入侵检测系统，它们是以流量数据、状态数据等原始监控数据为基础，通过规则匹配和算法处理生成. 日常操作记录来自各种网络服务和应用在运行过程中获取的用户操作信息，如管理服务器的用户登陆记录、域名服务器的域名解析请求记录等等. 另外，也可以将网络漏洞扫描数据和通过蜜罐获取的攻击者信息看作事件监控数据.

网络安全分析人员在日常工作中还需要面对一些非监控型网络安全数据，如防火墙配置文件、网络路由表、病毒样本等. 针对这些数据的可视化可以为分析人员提供多方面的帮助，如 Nataraj 等[8]将恶意软件样本可视化为灰度图像，并利用图像特征对样本进行分类. Mansmann 等[9]采用 Sunburst 图形将防火墙配置规则树可视化，帮助管理员理解复杂的规则和辅助调优.

2　主要研究方法与发展现状

网络安全可视化的研究，首先是确定网络安全分析人员关心的问题，也就是有什么数据，需要从数据中获取什么信息；然后是设计可视化结构来表示数据，建立数据到可视化结构的映射；最后是设计缩放、聚焦、回放和关联更新等人机交互功能，完成人与可视化工具的交流，从而帮助分析人员观察网络安全数据中隐含的信息，进一步提高分析人员的感知、分析和理解网络安全问题的能力. 无论是针对网络扫描、拒绝服务攻击、蠕虫传播等具体的网络入侵事件，还是针对网络监控、特征分析、态势感知等抽象的网络安全需求，面对不同的网络安全问题和数据源，设计不同的可视化结构和交互手段、采用不同的技术路线和分析思路，便可以形成不同的网络安全可视化研究方法.

从网络安全分析人员的角度出发，按照从简单到复杂、从单一到整体、从低层到高层的思路，可以将人们关心的网络安全问题和网络安全可视化在网络安全中的应用分为 5 类：网络监控、异常检测、特征分析、关联分析和态势感知. 本节将逐类介绍主要的网络安全可视化研究方法和发展现状，表 2 所示为常见的网络安全问题和主要的网络安全可视化研究方法结合情况的整体概览.

2.1　网络监控

从各种网络监控设备获取的数据中了解网络运行状态是网络安全分析人员关注的最基本问题，也是网络优化、异常检测、态势感知的基础. 可视化的网络监控主要研究是按照时间顺序，如何将主机和端口等监控对象、流量和事件等监控内容使用图形图像的方式表达出来，以帮助分析人员快速了解网络运行状态.

主机是网络活动的主体，也是最重要的监控对象. 在网络空间中，IP 地址是主机的唯一标识，针对 IP 地址的非物理位置特性和分段特性，学者们尝试了多种方式来实现基于 IP 地址的网络监控. IPmatrix[10]采用了二维坐标定位和颜色映射的方法监控某 B 类网络中发生的事件，如图 2 a[10]所示，X 和 Y 值构成的坐标确定 IP 地址，不同事件类型映射为不同的颜色，但是这种方法表示的 IP 地址空间有限. Quantree[11-12]技术将正方形进行多次四分后形成的 512×512 矩阵来表示 4 个字节的 IPv4 地址空间，图 2 b[11]显示了基于该方法的 IPv4 全地址空间的流量监控，流量大小使用颜色编码；但其缺点是点阵太密集，不便于交互. Treemap[13]在表示 IP 地址的分层特性时具有更好的交互性，如图 2 c[13]所示，用户可以通过交互自由地查看分级汇总或细节信息，还能将其扩展到 IPv6 地址的表示[14].

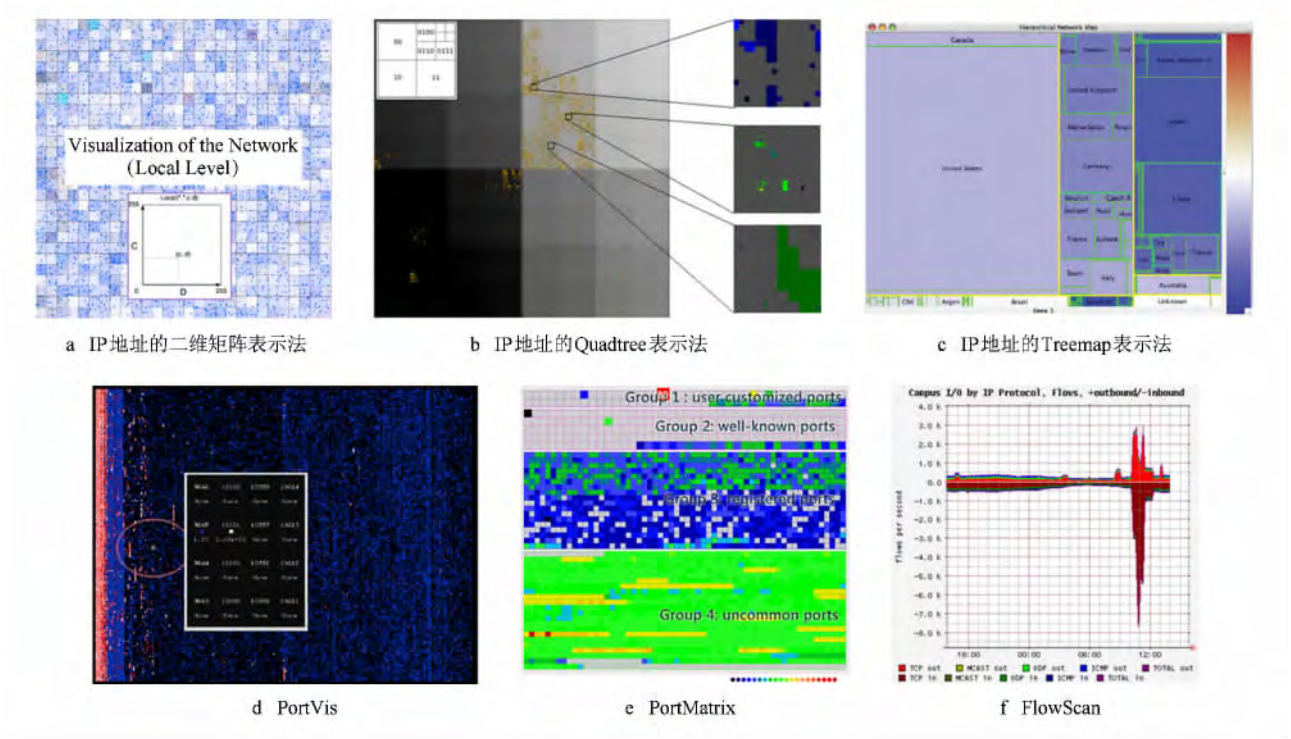
IP 地址标识了主机，端口则标识了不同的网络应用，因此端口监控和主机监控有着同等重要的地位. PortVis[14]用一个 256×256 的网格矩阵和颜色映射方法表示 65 536 个端口的流量情况，如图 2 d[14]所示，为防止过密的数据点的交互困难，系统还提供了区域选择和放大观察的交互方式. 考虑到不同端口号区段的重要程度不同，可以将不太重要的端口号用较小的图元表示；如 PortMatrix[15]将网络端口号分为如图 2 e[15]所示 4 类，其中 100 个连续的动态端口使用同一个方格表示.

网络监控数据都具有时序特点，线条图、柱状图、堆叠图等适合时序数据表示的基本统计图形在网络安全可视化中应用很广，图 2 f[16]显示了 FlowScan[16]使用堆叠图可视化某校园网流量的时序变化情况，不同网络协议的流量用不同颜色编码，在进行统计时还区分了流入和流出的流量. 为了实现整体和细节的统一，设计者通常会结合统计分析方法，将描述网络整体状态变化的时序图形与描述某时段网络具体状态的监控图形联动起来. 因此，传统统计图形和统计方法一定程度上成为了各种新颖的可视化系统中不可或缺的标准配件[17-18].

表2 网络安全问题与网络安全可视化主要研究方法分类汇总表

网络安全问题		网络安全可视化采用的主要图形分类									网络安全可视化常见的技术特点分类								横向汇总
		节点连接图	网格图矩阵图点阵图	柱状图堆叠图线图	雷达图径向图环状图	平行坐标轴	树图	散点图	地图	热力图	结合统计分析方法	结合数据挖掘和机器学习方法	多视图协同分析	多数据源协同分析	大规模网络处理	大规模数据处理	实时分析	使用三维图形	
网络安全问题分类	网络监控	■	■	■	▪	■	▪	_	▪	▪	■	_	■	▪	▪	▪	▪	■	
	异常检测	■	■	■	■	■	▪	▪	▪	▪	■	▪	■	▪	_	▪	▪	▪	
	特征分析	■	■	■	▪	■	▪	▪	_	▪	■	▪	▪	_	_	_	_	▪	
	关联分析	▪	_	▪	▪	_		_	_	_	▪	_	_	▪		_	_		
	态势感知	_	▪	▪	▪	_	_		_	_	▪	_	▪	▪	_	_	_		
常见的一些具体网络安全问题	端口与网络扫描分析	▪	▪	▪	▪	▪		_		_	▪	_	▪	▪		_	_	▪	
	拒绝服务攻击分析	▪	▪	▪	▪	▪	_	_		_	▪	_	▪	▪	_	_	_	_	
	僵尸网络分析	▪	_	▪	_	▪	_	_	_	_	▪	_	▪	▪	_	_	_	_	
	恶意软件和病毒分析	▪	_	_	_	_	▪	_	_		_	_	▪						
	蠕虫传播分析	_	▪	▪		▪		_	_	_	▪	_	▪	_			_	_	
	边界网关协议路由分析	▪	▪	▪		_	_	_	▪		▪	_	▪		▪		_	_	
	网络弱点分析	▪	_	▪	_	_	▪	_	_	_	▪	_	▪	_			_	_	
	垃圾邮件分析	_	_	_	_					_	_		_	_		_			
纵向汇总		▮	▮	▮	▮	▮	▮	▮	▮	▮	▮	▮	▮	▮	▮	▮	▮	▮	

说明：▮ ■ ▪ _ 代表相关研究数量



a　IP地址的二维矩阵表示法　　b　IP地址的Quadtree表示法　　c　IP地址的Treemap表示法

d　PortVis　　e　PortMatrix　　f　FlowScan

图 2　可视化的网络监控

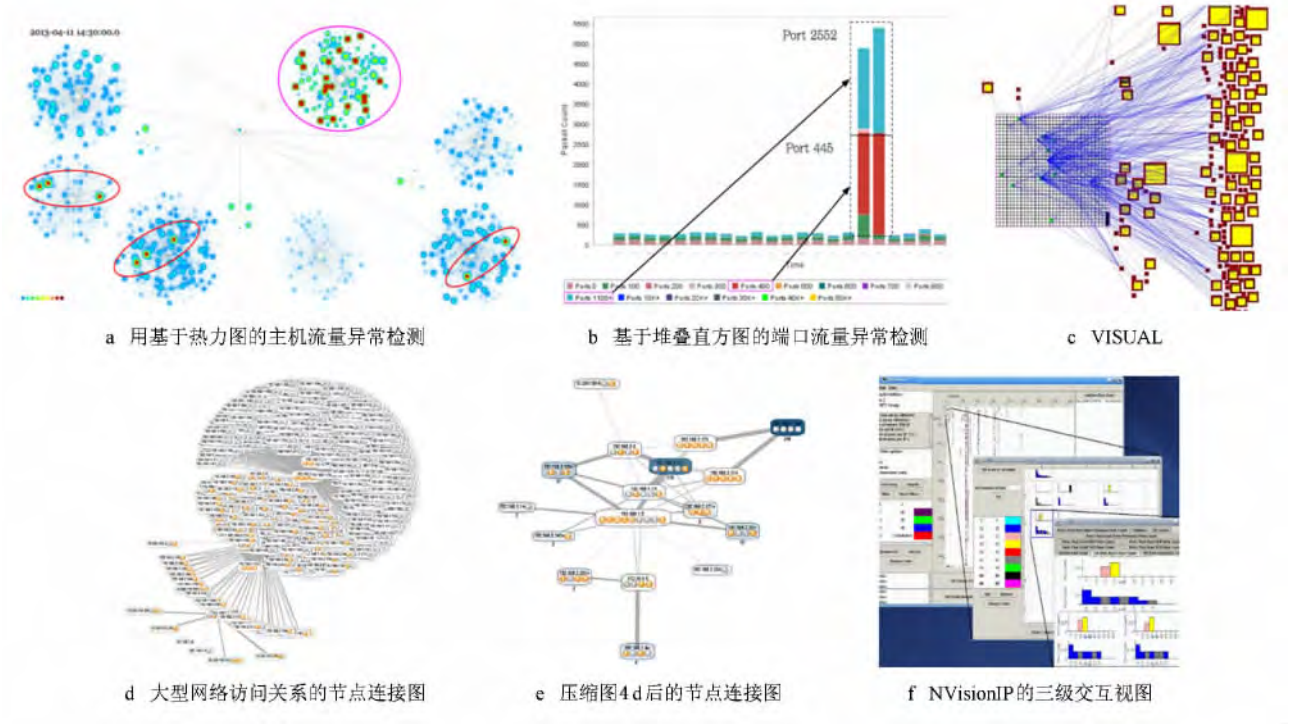
2.2　异常检测

网络异常包括的范围很广,如流量的突变、设备的失效、越权的资源访问、可疑的主机行为等. 有的异常是由于恶意攻击产生,而有的则是由于普通网络故障或者用户操作不当造成. 检测和定位各种网络异常是网络安全分析人员的日常工作,也是进一步诊断异常原因、识别网络攻击类型的基础. 可视化的异常检测经常与网络监控联系在一起,主要方法是通过对网络状态和网络访问等信息的图形化表示,帮助分析人员从"正常状态"中快速准确地发现"异常情况",而不是像传统的自动化检测方法那样只抛出异常检测结果.

流量是主要的网络状态之一,拒绝服务攻击和蠕虫传播等网络入侵行为发生时,往往首先会在网络流量上出现明显的变化. 网格矩阵图和颜色编码是最常见的以主机和端口为对象的可视化流量异常检测方法,因此 2.1 节中介绍的多个可视化监控系统也都能胜任流量异常检测. 除此之外,学者们也提出了很多其他行之有效的可视化流量异常检测方法,如图 3 a[15] 显示的是一个采用热力图技术的流量监控系统,从中可以很直观地观察到在当前时刻有一些流量热点主机出现,友好的拓扑布局还可以帮助分析人员迅速定位热点主机和观察子网分布特点;图 3 b[19] 显示了一个根据端口流量进行分组聚合分析的可视化系统,横轴表示时间,每个时段各端口的流量通过堆叠柱状图表示,图中明显的峰值时段是由端口 445 和 2552 产生的,而这 2 个端口和蠕虫传播有较大关系.

网络应用主要通过主机之间的互访实现,当主机遭到误用、滥用和病毒感染时,常常会出现网络访问的异常. 节点连接图是检测网络访问异常的重要可视化方法,它又分 2 种不同的处理策略:主机位置相对固定和主机位置动态布局. TNV[17],VISUAL[20] 和 NflowVis[21] 是典型的使用主机位置固定策略的可视化系统,图 3 c[20] 显示了 VISUAL 可视化的内外网主机通信情况,内网主机的网格矩阵在中心区域,外网主机分布在四周,从连线的多少和外网主机方块大小可以很直观地发现一些异常活跃的内外网主机. 主机位置固定策略便于保持主机的逻辑拓扑关系,而主机位置动态变化策略可以实现聚类效果,图 3 d[22] 是使用力导引布局的网络访问图,图中几个明显的中心点将网络中的主机分成了几个区域,而这几个中心很可能是由于存在异常的网络扫描行为而形成的. 针对大型网络的节点连接图难免会出现连线混杂的问题,代表性的解决方法包括边绑定技术[21]、抽象图技术[23] 和图压缩技术[22],或者改用邻接矩阵[24] 表示网络访问. 图 3 e[22] 所示为通过基于网络拓扑信息的图压缩方法对图 3 d 简化后效果,它大大简化了连接复杂度,并且凸显了关键主机.

对于具有动态性、随机性和隐蔽性的复杂网络异常，为了达到更好的异常检测效果，需要将多种可视化方法结合起来，以支持不同粒度和角度的选择，提供多层次和多维度的交互，形成多视图的合作分析. SpiralView[18]，NVisionIP[25]和 VisTracer[26]都是多视图工具的代表，如图 3 f[25]所示，NVisionIP 通过 3 级交互视图，将主机监控和端口监控以及全局概览和局部分析有机地结合了起来.



a 用基于热力图的主机流量异常检测 b 基于堆叠直方图的端口流量异常检测 c VISUAL

d 大型网络访问关系的节点连接图 e 压缩图4 d后的节点连接图 f NVisionIP的三级交互视图

图 3 可视化的网络异常检测

2.3 特征分析

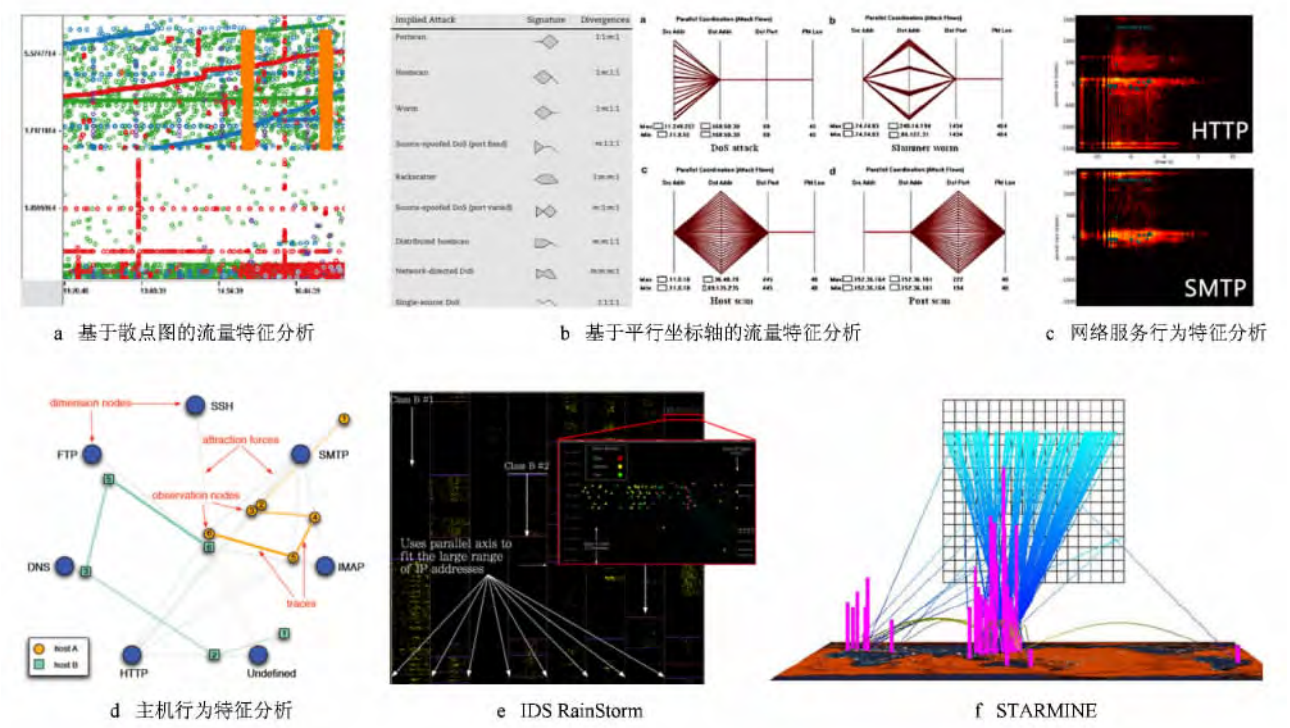
网络安全中的特征分析和异常检测相辅相成，一方面分析人员需要对检测到的网络异常进行进一步的特征分析，从而达到识别网络攻击类型和选择防范措施的目的；另一方面，特征分析也可以帮助分析人员更好地进行异常检测. 可视化技术将复杂的特征描述转化为图形模式，通过人类视觉对图形模式的强大识别能力，帮助分析人员快速完成特征发现和模式匹配. 网络安全中的特征分析对象主要包括流量、行为和事件.

流量监控数据包含时间、协议、源 IP、目的 IP、源端口、目的端口、包大小等多个维度的信息，很多网络攻击都会引发流量大小的异变，同时还会在其他维度上表现出更多的攻击特征. Xiao[27]等使用散点图对多种网络攻击的流量特征进行了两两维度的组合分析，图 4 a[27]显示了 SSH 攻击(橙色)和网络扫描(红色)产生的网络流量在时间(X 轴)和端口(Y 轴)2 个维度上的特征. 为了实现更多维度的特征同步分析，平行坐标轴技术[5,28]被广泛采用，代表性的例子是 Choi 等[29]对网络扫描、DDoS 攻击等多种网络攻击的流量特征的分析. 图 4 b[29]总结了这些攻击类型在平行坐标轴上图形模式，如端口扫描产生的流量记录在平行坐标上会出现 1:1:M:1(源 IP:目的 IP:目的端口:包大小)图形区域，这是因为端口扫描通常是从单源 IP 发出大量相同大小的探测数据包，以检测目的 IP 的可访问端口.

以主机和网络服务为对象的监控记录中隐含了它们的行为模式，通过对行为模式的分析，可以帮助分析人员更好地区分正常和异常的网络活动. Wright 等[30]通过对数据包的时序可视化，揭示了不同网络服务的行为模式. 如图 4 c[30]所示，横轴表示时间，纵轴正值和负值分别表示服务请求方发出和收到的数据包字节数，图例反映了主机在请求 HTTP 服务时收到的包大小要大于发出的包大小，而在请求 SMTP 服务时发出的包大小要大于收到的包大小. Mansmann 等[31]提出了一种主机行为分析方法，如图 4 d 所示，它将各种网络服务分布在四周，根据主机在不同时间对各种网络服务的访问顺序绘制出相应的路径，具有相同行为模式的主机路径将会呈现出形态的相似性和位置聚集效果，异常的主机行为路径得以凸显.

入侵检测系统是重要的网络安全工具，它将网

络数据包和事件规则库进行比对，如果匹配成功就会发出相应报警记录，它可以部分代替分析人员从原始数据中寻找异常并分析特征的入侵检测过程，但其弊端是规则设置技巧性高、不能检测未知事件和大量产生的误报漏报. 很多学者使用可视化技术管理入侵检测日志和分析事件特征，帮助分析人员优化规则设置、鉴别误报漏报和发现可能存在的新攻击类型，提高入侵监测系统的实用性. 早期的 SnortView[32] 可以帮助人们鉴别误报和漏报，但它只适合小规模网络. IDS RainStorm[33] 针对大规模网络采用了两级视图的设计方式：使用分层网格矩阵和颜色编码的概览视图和对选定时段和 IP 段进行事件特征分析的细节视图，如图 4 e[33] 所示. 图 4 f 所示 STARMINE[34] 将 IP 矩阵与地图结合起来，分析 Sasser 蠕虫爆发事件在网络空间和地理空间中的传播特征. Alsaleh 等[35] 开发了 PHPIDS 的扩展组件，该组件在 Web 环境下提供了近 10 种可视化图形，用来管理入侵检测日志和分析事件特征.



a 基于散点图的流量特征分析　b 基于平行坐标轴的流量特征分析　c 网络服务行为特征分析

d 主机行为特征分析　e IDS RainStorm　f STARMINE

图 4　可视化的特征分析

2.4　关联分析

复杂的网络攻击都具有多步性和协作性的特点，如攻击者首先会通过端口和主机扫描寻找网络中的漏洞，然后利用漏洞注入木马、僵尸或其他恶意软件；当对网络有一定的控制能力后就会进行文件窃取、广告推送，甚至将网络中主机当作傀儡机，共同发起对其他网络资源的蛮力攻击. 因此，将现有的事件信息合理地组织起来，建立基于上下文关系的可视分析，可以帮助分析人员发现网络安全事件之间的关联，理解当前的网络安全形势，尽量将网络危机化解在早期阶段.

事件之间的关联一般存在于类型、位置和时间 3 个维度，称为 3W(what，where，when)模型. 雷达图在描述 3W 模型时具有很好的图形表现力和多样的交互空间，是事件关联可视化的主要研究方法. VisAlert[36] 首先采用 3W 模型和雷达图来分析事件关联，如图 5 a 所示，圆的内部是主机布局，圆周上每段圆弧代表一种事件类型，时间维度从内到外用多个圆环表示，通过交互选择，用户就可以轻松地组合 What，Where，When 3 个维度去寻找事件关联. 随后有许多相关研究对 VisAlert 进行了改进和应用拓展，如 NetSecRadar[37] 和 AlertWheel[38] 调整了雷达图的主机布局和连线方式，IDSRadar[39] 探讨了某企业网络中僵尸病毒感染事件和文件窃取事件可能存在的关联，Avisa[40] 使用雷达图分析了复杂网络入侵的多步攻击过程.

分析网络漏洞造成的关联影响也非常重要，因为攻击者经常利用有漏洞的主机作为跳板来到达攻击目标，网络中任意一台有漏洞的主机都会引来连锁反应. 网络攻击图是一种可视化漏洞关联影响的技术，它以现存的网络安全漏洞为基础，找出攻击者能够在网络中走通的所有攻击路径，从而达到评估

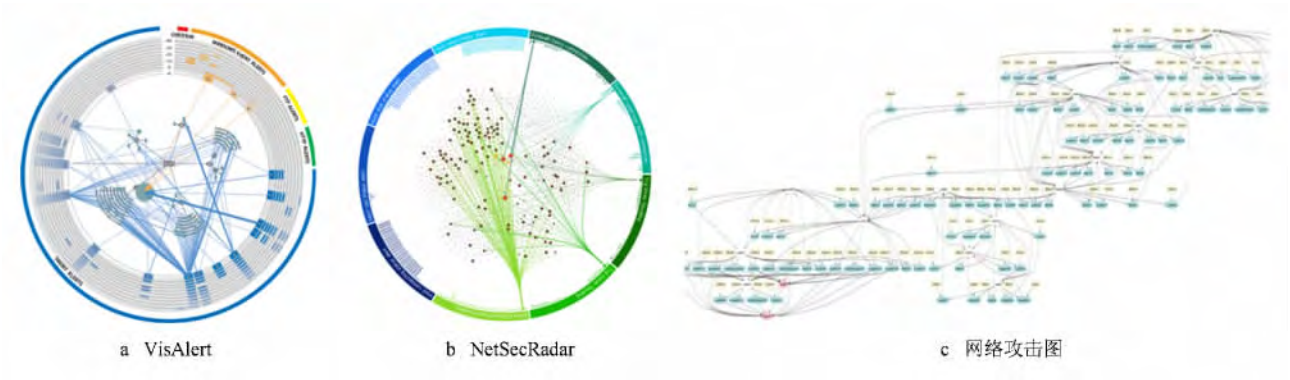


图 5 可视化的关联分析

网络安全性的目的. 图 5 c[41] 就显示了一幅使用树形结构来绘制的网络攻击图,其中各种形状的节点代表源主机、目的主机和漏洞类型,每条边就代表一次漏洞利用. 传统的树形图在表现大型网络攻击图时空间利用率不高,GARNET[42] 使用 Treemap 改进了攻击图的表示方法,该方法具有更好的空间利用率和交互性.

2.5 态势感知

在大规模网络环境中,网络安全分析人员往往更倾向于首先掌握宏观的网络态势,即网络整体的运行状态和变化趋势,然后由整及分、由急到缓地解决网络安全问题. 针对这一重要的网络安全需求,Bass[43] 在 2000 年首先提出了网络安全态势感知的概念:通过融合各种网络安全设备收集的状态记录和报警记录,评估当前网络整体运行状态,并预测变化趋势. 可视化的网络安全态势感知首先由 VisFlowConnect[44] 在 2004 年提出来,它通过提供描绘大规模网络状态和海量事件的高层次视图,帮助人们更快地察觉和理解网络安全态势、缩短决策时间. 早期对网络安全态势可视化相关研究相对较少,但随着数据融合、态势评估、大规模数据处理和大屏幕等技术的发展,近几年涌现了一批优秀成果.

多数据源的融合与协同是网络安全态势感知的特点之一,也是网络安全可视化常见的分析策略. BANKSAFE[45] 使用 Treemap,Clockmap 和 AlertTimeline 3 种图形,分别将网络状态、入侵检测日志和 Firewall 日志用 3 个屏幕可视化出来,如图 6 a[45] 所示,从而实现大规模网络的可视化态势感知. AnNetTe[46] 融合了 NetFlow,IPS 和 BigBrother 3 种数据,通过提供描绘健康指标、报警数量、流量、IP 和端口活跃度等网络状态变化的一组时间线来刻画网络安全态势,如图 6 b 所示;它还通过提供分层的弦图与平行坐标轴,交互分析用户选中时段的细节信息.

大屏幕为态势感知中需要表达的众多信息元素带来了更广阔的展示空间. 如图 6 c 所示,NOCturne[47] 在大屏幕上的设计思路是使用时间线、连接矩阵、地

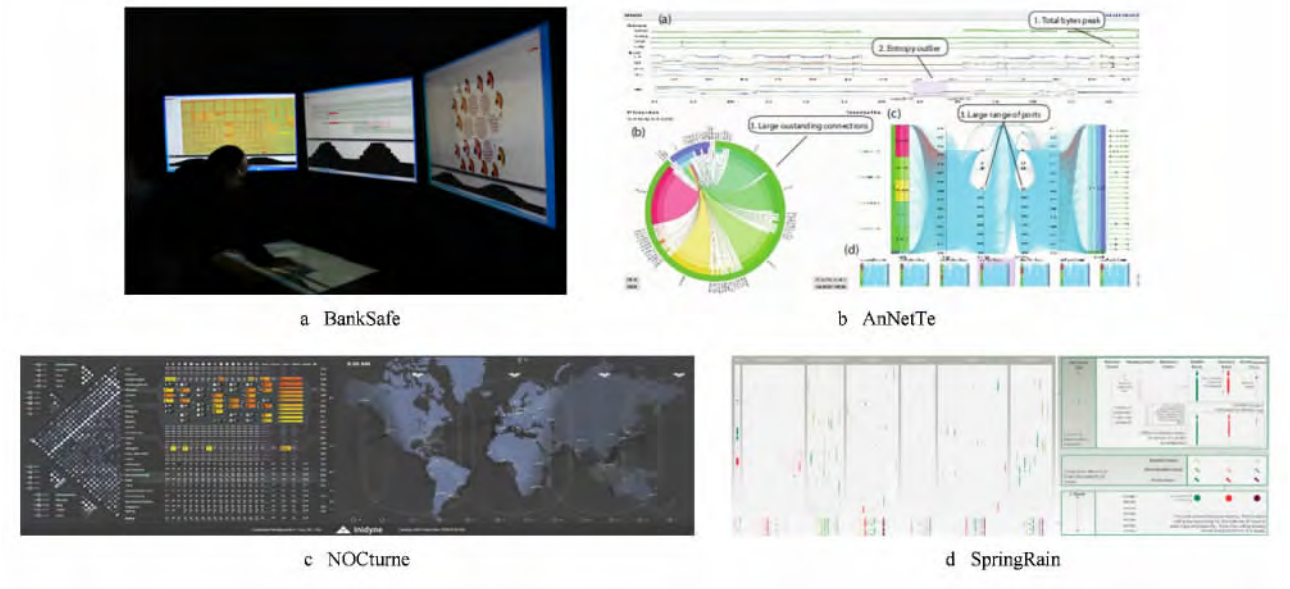


图 6 可视化的网络安全态势感知

图等多种图形将多源信息有机地组织在一起，但这种方式缺乏整体感. 如图 6 d 所示，SpringRain[48] 提出了一种新颖的大屏幕设计思路，它将不同网络区域看作是大型瀑布的水流簇，每个簇内从上至下充满了通过颜色和形状编码的网络安全信息元素，整体和细节很好地融合在了这一可视隐喻之中；另外它还提供与 Google Glasses 的连接，从而加强了人与画和人与人的协同交互.

3　总结与展望

网络安全可视化将网络安全数据分析和可视化技术结合起来，通过提供图形化的交互工具，提高网络安全分析人员感知、分析和理解网络安全问题的能力. 从本文的介绍中可以看出，网络安全可视化已经取得了丰硕的研究成果，但是面对越来越严重的网络安全威胁和越来越复杂的攻击手段，研究者们还面临着诸多的挑战：

1) 如何实时显示和处理大规模网络数据. 目前大部分研究仍然停留在离线数据的分析上，但是实时分析远比离线分析重要. 实时的网络安全可视化需求对数据预处理速度、图形绘制速度、交互响应速度都提出了更高的要求.

2) 如何搭建网络安全可视化的协同工作环境. 解决大范围的复杂网络问题往往需要多数据源、多视图、多人的协同分析，因此现有的数据融合和多视图技术以及多人参与的网络安全协同可视分析环境都有较大的发展空间.

3) 如何提高网络安全可视化系统的易用性. 对于目前大部分网络安全可视化系统，即使是有丰富经验的分析人员，都需要一定程度的培训后才能熟练使用，但网络安全可视化的受众本应更为广泛，因此需要加强网络安全可视化的易用性研究.

4) 如何研究出一套完整的理论体系. 可视化方法研究主观性很强，解决网络安全问题的经验性要求高，网络安全可视化的有效性验证非常困难，因此在相关数学模型、基础理论和设计原则等方面开展深入研究势在必行.

参考文献(References)：

[1] Lü Liangfu, Zhang Jiawan, Sun Jizhou, *et al*. Survey of network security visualization techniques [J]. Journal of Computer Applications, 2008, 28(8): 1924-1927 (in Chinese)
(吕良福，张加万，孙济洲，等. 网络安全可视化研究综述 [J]. 计算机应用，2008，28(8)：1924-1927)

[2] Shiravi H, Shiravi A, Ghorbani A A. A survey of visualization systems for network security [J]. IEEE Transactions on Visualization and Computer Graphics, 2012, 18(8): 1313-1329

[3] Harrison L, Lu A. The future of security visualization: lessons from network visualization [J]. IEEE Network, 2012, 26(6): 6-11

[4] Becker R A, Eick S G, Wilks A R. Visualizing network data [J]. IEEE Transactions on Visualization and Computer Graphics, 1995, 1(1): 16-28

[5] Girardin L, Brodbeck D. A visual approach for monitoring logs [C] //Proceedings of Large Installation System Administration Conference. New York: ACM Press, 1998: 299-308

[6] VizSec Homepage [EB/OL]. [2014-01-09] http://www.vizsec.org. 2013

[7] VAST Challenge Homepage in vacommunity [EB/OL]. [2014-01-09] http://www.vacommunity.org/VAST+Challenge+2013. 2013

[8] Nataraj L, Karthikeyan S, Jacob G, *et al*. Malware images: visualization and automatic classification [C] //Proceedings of the 8th International Symposium on Visualization for Cyber Security. New York: ACM Press, 2011: 4-11

[9] Mansmann F, Göbel T, Cheswick W. Visual analysis of complex firewall configurations [C] //Proceedings of the 9th International Symposium on Visualization for Cyber Security. New York: ACM Press, 2012: 1-8

[10] Koike H, Ohno K, Koizumi K. Visualizing cyber-attacks using IP matrix [C] //Proceedings of Visualization for Computer Security. Los Alamitos: IEEE Computer Society Press, 2005: 91-98

[11] Atkison T, Pensy K, Nicholas C, *et al*. Case study: visualization and information retrieval techniques for network intrusion detection [M] //Data Visualization. Hedelberg: Springer, 2001: 283-290

[12] Le Mal E, Kohara M, Hori Y, *et al*. Interactively combining 2D and 3D visualization for network traffic monitoring [C] //Proceedings of the 3rd International Workshop on Visualization for Computer Security. New York: ACM Press, 2006: 123-127

[13] Mansmann F, Keim D A, North S C, *et al*. Visual analysis of network traffic for resource planning, interactive monitoring, and interpretation of security threats [J]. IEEE Transactions on Visualization and Computer Graphics, 2007, 13(6): 1105-1112

[14] McPherson J, Ma K L, Krystosk P, *et al*. Portvis: a tool for port-based detection of security events [C] //Proceedings of the ACM Workshop on Visualization and Data Mining for Computer Security. New York: ACM Press, 2004: 73-81

[15] Zhao Y, Liang X, Wang Y, *et al*. MVSec: a novel multi-view visualization system for network security [C] // Proceedings of Visual Analytics Science and Technology. Los Alamitos: IEEE Computer Society Press, 2013: 7-8

[16] Plonka D. FlowScan: a network traffic flow reporting and visualization tool [C] //Proceedings of Large Installation System Administration Conference. New York: ACM Press, 2000: 305-317

[17] Goodall J R, Lutters W G, Rheingans P, *et al*. Preserving the big picture: visual network traffic analysis with tnv [C] // Proceedings of Visualization for Computer Security. Los Alamitos: IEEE Computer Society Press, 2005: 47-54

[18] Bertini E, Hertzog P, Lalanne D. SpiralView: towards security policies assessment through visual correlation of network resources with evolution of alarms [C] //Proceedings of Visual Analytics Science and Technology. Los Alamitos: IEEE Computer Society Press, 2007: 139-146

[19] Abdullah K, Lee C, Conti G, *et al*. Visualizing network data for intrusion detection [C] //Proceedings of Information Assurance Workshop. Los Alamitos: IEEE Computer Society Press, 2005: 100-108

[20] Ball R, Fink G A, North C. Home-centric visualization of network traffic for security administration [C] //Proceedings of the ACM Workshop on Visualization and Data Mining for Computer Security. New York: ACM Press, 2004: 55-64

[21] Fischer F, Mansmann F, Keim D A, *et al*. Large-scale network monitoring for visual analysis of attacks [M]. Heidelberg: Springer, 2008

[22] Liao Q, Shi L, Wang C. Visual analysis of large-scale network anomalies [J]. IBM Journal of Research and Development, 2013, 57(3/4): 13: 1-13

[23] Tsigkas O, Thonnard O, Tzovaras D. Visual spam campaigns analysis using abstract graphs representation [C] // Proceedings of the 9th International Symposium on Visualization for Cyber Security. New York: ACM Press, 2012: 64-71

[24] Yu T H, Fuller B W, Bannick J H, *et al*. Integrated Environment Management for Information Operations Testbeds [M] //Visualization for Computer Security. Heidelberg: Springer, 2008: 67-83

[25] Lakkaraju K, Yurcik W, Lee A J. NVisionIP: netflow visualizations of system state for security situational awareness [C] //Proceedings of the ACM Workshop on Visualization and Data Mining for Computer Security. New York: ACM Press, 2004: 65-72

[26] Fischer F, Fuchs J, Vervier P A, *et al*. VisTracer: a visual analytics tool to investigate routing anomalies in traceroutes [C] //Proceedings of the 9th International Symposium on Visualization for Cyber Security. New York: ACM Press, 2012: 80-87

[27] Xiao L, Gerth J, Hanrahan P. Enhancing visual analysis of network traffic using a knowledge representation [C] // Proceedings of IEEE Symposium On Visual Analytics Science And Technology. Los Alamitos: IEEE Computer Society Press, 2006: 107-114

[28] Lee C P, Trost J, Gibbs N, *et al*. Visual firewall: real-time network security monitor [C] //Proceedings of IEEE Workshop on Visualization for Computer Security. Los Alamitos: IEEE Computer Society Press, 2005: 129-136

[29] Choi H, Lee H, Kim H. Fast detection and visualization of network attacks on parallel coordinates [J]. Computers & Security, 2009, 28(5): 276-288

[30] Wright C V, Monrose F, Masson G M. Using visual motifs to classify encrypted traffic [C] //Proceedings of the 3rd International Workshop on Visualization for Computer Security. New York: ACM Press, 2006: 41-50

[31] Mansman F, Meier L, Keim D A. Visualization of host behavior for network security [M]. Heidelberg: Springer, 2008

[32] Koike H, Ohno K. SnortView: visualization system of snort logs [C] //Proceedings of the ACM Workshop on Visualization and Data Mining for Computer Security. New York: ACM Press, 2004: 143-147

[33] Abdullah K, Lee C P, Conti G J, *et al*. IDS RainStorm: Visualizing IDS Alarms [C] //Proceedings of IEEE Workshop on Visualization for Computer Security. Los Alamitos: IEEE Computer Society Press, 2005: 1-8

[34] Hideshima Y, Koike H. STARMINE: a visualization system for cyber-attacks [C] //Proceedings of the Asia-Pacific Symposium on Information Visualisation-Volume 60. Sydney: Australian Computer Society, Inc., 2006: 131-138

[35] Alsaleh M, Alqahtani A, Alarifi A, *et al*. Visualizing PHPIDS log files for better understanding of web server attacks [C] //Proceedings of the 10th Workshop on Visualization for Cyber Security. New York: ACM Press, 2013: 1-8

[36] Livnat Y, Agutter J, Moon S, *et al*. Visual correlation for situational awareness [C] //Proceedings of IEEE Symposium on Information Visualization. Los Alamitos: IEEE Computer Society Press, 2005: 95-102

[37] Zhou F, Shi R, Zhao Y, *et al*. NetSecRadar: a visualization system for network security situational awareness [M] // Cyberspace Safety and Security. New York: Springer International Publishing, 2013: 403-416

[38] Dumas M, Robert J M, McGuffin M J. Alertwheel: radial bipartite graph visualization applied to intrusion detection system alerts [J]. IEEE Network, 2012, 26(6): 12-18

[39] Zhao Y, Zhou F F, Fan X P, *et al*. IDSRadar: a real-time visualization framework for IDS alerts [J]. Science China Information Sciences, 2013, 56(8): 1-12

[40] Shiravi H, Shiravi A, Ghorbani A A. Situational assessment of intrusion alerts: a multi attack scenario evaluation [M] // Information and Communications Security. Heidelberg: Springer, 2011: 399-413

[41] Noel S, Jacobs M, Kalapa P, *et al*. Multiple coordinated views for network attack graphs [C] //Proceedings of IEEE Workshop on Visualization for Computer Security. Los Alamitos: IEEE Computer Society Press, 2005: 99-106

[42] Williams L, Lippmann R, Ingols K. GARNET: a graphical attack graph and reachability network evaluation tool [M]. Heidelberg: Springer, 2008

[43] Bass T. Intrusion detection systems and multisensor data fusion [J]. Communications of the ACM, 2000, 43(4): 99-105

[44] Yin X, Yurcik W, Treaster M, *et al*. VisFlowConnect: netflow visualizations of link relationships for security situational awareness [C] //Proceedings of the ACM Workshop on Visualization and Data Mining for Computer Security. New York: ACM Press, 2004: 26-34

[45] Fischer F, Fuchs J, Mansmann F, *et al*. BANKSAFE: visual analytics for big data in large-scale computer networks [J]. Information Visualization Journal, 2013, 6: 1-10

[46] Chen S, Merkle F, Schaefer H, *et al*. AnNetTe collaboration oriented visualization of network data [C] //Proceedings of Visual Analytics Science and Technology. Los Alamitos: IEEE Computer Society Press, 2013: 1-2

[47] Benson J R, Ramarajan J. NOCturne: a scalable large format visualization for network operations [C] //Proceedings of Visual Analytics Science and Technology. Los Alamitos: IEEE Computer Society Press, 2013: 3-4

[48] Promann M, Ma Y A, Wei S, *et al*. SpringRain: an ambient information display [C] //Proceedings of Visual Analytics Science and Technology. Los Alamitos: IEEE Computer Society Press, 2013: 5-6