

网络威胁安全数据可视化综述

张繁, 谢凡, 江颀

(浙江工业大学计算机学院, 浙江 杭州 310023)

摘要: 在网络空间威胁手段日益复杂化的背景下, 网络安全数据分析技术亟待提高。数据可视化技术已成为各类数据分析的理论框架和应用中的必备要素, 并成为科学计算、商业智能、安全等领域中的普惠技术。网络威胁安全数据可视化通过提供有效的信息可视化交互手段, 有效提升网络安全专家在分析网络空间安全问题过程中的认知能力。介绍了网络威胁安全数据可视化技术的研究现状和面临的问题, 并对未来的发展趋势进行了展望。

关键词: 网络空间安全; 关联分析; 可视分析; 人工智能

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018013

Survey on the visualization technologies of threatening security data in cyber space

ZHANG Fan, XIE Fan, JIANG Jie

College of Computer Science, Zhejiang University of Technology, Hangzhou 310023, China

Abstract: With the rapid development of the cyber threatening methods, the requirements of network security data analysis become more and more imperative. Data visualization has already evolved as a requisite tool among all kinds of data analysis theory framework and applications, especially in the fields of scientific computation, business intelligence and cyber security. Threatening security data visualization provides various effective interaction means which improve the perception ability for the cyber security specialists to get a distinctive insight into the large amount of complicated cyber security problems. The state-of-art cyber security data visualization technologies were introduced. Some existing problems that were still challenging research topics were investigated. Some directions for future studies were outlined.

Key words: cyber space security, associate analysis, visual analysis, artificial intelligence

1 引言

随着“互联网+”时代的到来, 网络安全威胁的范围和内容不断扩大和演化, 传统的安全边界

逐步失效。云计算、移动互联网的普及不仅带来APT、DDoS攻击、叉式网络钓鱼、水坑式攻击、物联网攻击等高级威胁, 诸如震网病毒、蠕虫病毒、僵尸网络、勒索软件、信息泄露等安全事件

收稿日期: 2017-12-26; 修回日期: 2018-01-29

通信作者: 江颀, jj@zjut.edu.cn

基金项目: 国家自然科学基金资助项目(No.U1736109, No.61772456, No.U1609217); 浙江省自然科学基金资助项目(No.LY18F020034)

Foundation Items: The National Natural Science Foundation of China(No.U1736109, No.61772456, No.U1609217), The Natural Science Foundation of Zhejiang Province(No.LY18F020034)

也迅速增加。新攻击类型的出现和攻击复杂度的提高,使很多传统的分析方法和分析模型不再有效。网络安全大数据的研究和开发方兴未艾^[1,2]。

可视化是大数据分析的重要方法,能够有效地弥补自动化分析方法的不足,整合计算机的分析能力和人类对信息的感知和判断能力,利用人机交互技术辅助用户更好地发现模式、检测异常、识别关系和协同分析^[3,4]。国内外很早就有针对网络安全数据的可视化技术研究,比如 IEEE 举办的最具代表性的学术界盛会——网络安全可视化研讨会(VizSec, IEEE symposium on visualization for cyber security)。自2004年以来,很多研究已经在网络监控、关联分析、态势感知等方面取得了重要成果^[5,6]。

2 网络安全数据可视化分析现状

可视化具备三大功能:记录信息、传播交流、分析推理^[7]。可视化在支持人的宏观概览、态势感知、证据关联、模糊搜索等方面展示了其天然强大的赋能能力^[8]。由于网络攻击具有持续性和隐蔽性,将关联融合、时间序列、流数据分类等技术运用于大数据环境下的网络威胁数据分析能够提高获取高价值威胁特征的能力^[9],如何将多源异构网络安全数据关联,并将可视化技术有效应用于网络安全分析场景中是复杂且急需解决的问题。

2.1 网络安全数据关联分析模型

网络威胁安全数据来源于防毒软件、防火墙、入侵检测系统、攻击防御系统、主机监控系统、异常检测系统和攻击预测系统等各种安全产品,不能相互融合、互相验证,产生了大量重复的警报和日志。各检测系统报警信息格式不一致,各检测系统的误报率、漏报率以及重复报警率偏高,对于分步骤的攻击,或端口扫描攻击,检测系统短时间内会产生大量重复报警,给管理员带来巨大的工作量。利用关联分析方法研究网络威胁安全数据通常包括以下工作^[10]:1) 利用正则表达式匹配将多源异构数据规范化;2) 对大量 IDS 告警数据进行统计分析,发现误报与真实警报的区别特征,对警报数据进行初筛;3) 通过相似隶属度函数计算每条报警的源 IP、目的 IP、源端口、目

的端口的相似度,采用模糊聚类进行警报融合;

4) 对报警信息进行关联分析,把杂乱的、无意义的报警信息最终变为有意义的攻击规则,利用多步攻击中每步攻击之间的内在关联,得到完整的攻击路径;5) 通过杀伤链模型和模糊聚类生成攻击模型。

2.2 网络安全数据可视化研究现状

网络安全数据可视化通过交互式工具,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^[11]。赵颖等^[12,13]将堆叠流图引入网络安全可视化中,并根据网络安全事件的多源关联性,研究了基于统一格式的事件元组和统计元组的数据融合模型,并提出了擅长事件关联分析的雷达图和擅长统计时序对比分析的对比堆叠流图的设计方法。张胜等^[14]分别采用信息熵、加权法、统计法等不同算法进行特征提取,引入树图和符号标志从微观上挖掘网络安全细节,引入时间序列图从宏观展示网络运行趋势。赵立军^[15]等提出了基于熵的堆叠条形图设计方法和基于平行坐标的安全可视化方法,将总图浏览和细节分析相结合,降低了分析人员的认知困难。吴亚东等^[16]提出了一种异构树网络安全数据组织方法,在此基础上设计了一种针对大规模网络的三维多层球面空间可视化模型,大大增强了分析系统的可交互性,并提高了对网络安全数据的分析效率。

2.3 已有商业软件和开源软件

近年来,出现了一大批新颖的商用和开源数据可视化系统和工具,如 Maltego、Palantir、Tableau、LabVIEW 等。Maltego 是一款针对网络信息的互联网情报聚合可视化工具,面向所有基于网络和资源的实体组织,将这些组织发布在互联网的信息进行聚合,提供一个能够清晰展示某个组织经营环境安全隐患的平台。Palantir 是一款情报分析软件,其核心要素是采用动态本体管理器的思想,用于对领域相关的事物进行基于本体的建模、操作、管理、关联、分析、推理和可视化。Tableau 是一个商业智能分析软件,以可视的形式动态呈现关系型数据之间的关联,并允许用户以所见即所得的方式完成数据分析、可视图表与报告的创建。LabVIEW 开发环境集成了工程

师和科学家快速、方便地构建各种应用所需的所有工具,旨在帮助工程师和科学家解决问题、提高生产力和不断创新。通过对比不难发现,有些系统工具专注于处理结构化数据,如 Excel 表格等。进一步考虑在受到中断、截获、修改或伪造等形式的网络攻击时,网络安全数据会不完整、缺失、不真实,面向结构化数据开发的系统和工具很难直接应用于复杂网络威胁安全事件分析专业领域。

3 网络威胁安全数据可视化研究存在的问题

尽管数据可视化技术取得了很大的进步,但是由于网络安全事件数据量大、类型丰富、变化快等特点,网络安全数据可视化在实际应用中还存在许多困难。

1) 网络威胁安全数据联动分析模型有待完善

网络威胁安全数据底层数据实体之间缺乏交叉参考,仍然缺乏有效手段来整合多源、异构、高维网络数据。早期基于数据分组和数据流的可视化研究工作^[17]和工具 PortVis^[18]、NVisionIP^[19]、TNV^[20]、RUMINT^[21]等集中用于网络监控与异常检测,大量利用直方图、线图、柱状图、矩阵图和散点图等方法展示不同网络端口的请求和响应次数。当攻击导致网络端口流量发生异常变化时,这些方法可以帮忙分析人员快速定位异常网络行为。自动化入侵检测系统以及防火墙技术出现以后,人们开始通过分析各种网络报警日志数据理解网络攻击特征,此类数据的可视化分析工具包括 NIVA^[22]、VisAlert^[23]、IDS RainStorm^[24]、SpiralView^[25]等。但是更多的网络攻击,如 APT 攻击,通常采取证书盗取手段。而攻击者利用窃取得到的证书登录系统行为非常隐蔽,并不会引起网络端口流量的异常变化,所以在海量登录事件中检测出恶意系统登录非常困难。纽约大学研究人员设计了交互可视化工具 APT-Hunter^[26],通过分析企业网络的登录数据,利用预先设定的可疑和正常两组规则集及可视化方法帮助用户过滤并发现所有可疑登录事件。Bigfoot 可视分析系统^[27]尝试利用二维多边形将路由变化数据投影到世界地图上的方式展示全球范围内日常复杂的网络路由变化数据,成功识别出了 139 个可能的

网络威胁安全事件。但是上述研究工作都是基于单一数据源,分析人员无法开展联动分析,也无法跟踪网络攻击的横向移动。

2) 网络威胁安全数据分析需要积累专家知识和经验

本体理论和知识图谱为整合异构数据、利用知识改进分析模型提供了一种可能性。斯坦福大学研究人员最早通过陈述性知识表进行网络流量分类和可视分析^[28],用于检测暴力入侵或网络扫描等行为。针对网络安全数据异构特性,加州大学戴维斯分校 Ma 等^[29]利用本体拓扑结构表达恐怖组织网络中的恐怖组织、恐怖分子、国家和地区、组织分类、法律案件、恐怖攻击、攻击目标、手段和武器 9 种不同类别节点,通过节点语义和结构抽取及过滤,极大地简化了可视化大规模异构数据的负担。美国橡树林国家实验室、太平洋西北国家实验室、斯坦福大学和华盛顿大学 4 家单位在网络安全知识图谱构建上开展了一项有意义的联合研究工作^[30],尝试通过 JSON 格式组织数据元信息将海量结构化、非结构化数据统一入库。Aupetit 等^[31]构建了针对 DRDoS 攻击的可行知识库,Yao 等^[32,33]尝试利用语义知识和语义关联辅助合并、处理和分析多数据源安全数据,并针对国内注册信息安全专业人员(CISP, certified information security professional)认证构建了信息安全知识图谱。前述工作重点在语义网络、知识图谱的构建上,而如何利用知识图谱内在的知识推理能力有效发现网络威胁安全事件特征,以及如何结合分析人员的新发现快速动态更新知识图谱,这些问题还有待进一步研究。

3) 网络威胁安全可视化系统设计思想还不完善

网络威胁安全可视化系统设计大多采用以技术或模型为中心的思想,如何通过人机交互界面将人机智能融合是一个长期的研究目标。网络威胁具有很强的隐蔽性,网络攻击主体和客体的复杂性、时效性和多变性决定了网络攻击过程的不确定性和复杂性^[34]。早期研究工作通过形式化方法刻画系统安全和网络攻击特征,如 Schneier 于 1999 年提出的攻击树(attack tree)是一种基于树结构的系统安全测评方法,有助于提高分析人员

发现新漏洞的能力^[35]。攻击图(attack graph)最早由美国桑迪亚国家实验室学者提出,在综合分析多种网络配置和脆弱性信息的基础上,通过漏洞与漏洞关联可视化帮助防御者直观地分析攻击者可能选取的攻击路线^[36]。后续研究在分析攻击模式和攻击路径可视化方面进行了大量探索,例如,使用半透明四边形连接的柱形图符号指示复杂攻击在不同阶段的状态,利用圆柱尺寸和颜色编码攻击类型和严重级别等信息^[37]。又如,Wang等^[38]设计了一个用于研究病毒传播的新模型SADI,将真实物理网络和虚拟逻辑网络分开,基于社交蠕虫病毒的消息提示和人类移动的时间特征,通过概论统计求解用户在不同层上移动的可能性,进而估算蠕虫病毒的传播路径。但是以上方法都采用固定技术或模型,计算模型参数很难调整或根本不可调,所以分析过程相对孤立,分析人员只能被动接受结果,效果并不十分理想。

4 网络空间安全数据可视化发展趋势

4.1 多视图关联和动态表达

可视化在支持人的宏观概览、态势感知、证据关联、模糊搜索等方面展示了其天然强大的赋能能力^[8],多视图关联和动态表达方法是数据可视化诸多行之有效方法中的2个代表。LogSpider^[39]将可视过滤概念引入安全可视化领域,通过设计驾驭式可视查询和保持上下文选择子集等操作帮助分析人员识别出安全问题。MVSec^[40]尝试用故事线的方式呈现网络安全态势演化过程,Zhao等^[41]通过时序化的平行坐标视图、多主体的矩阵视图、多主体的时序视图、相似度扩展树视图分析网络流量日志数据。ENTVis^[42]利用雷达图、矩阵图等可视化方法支持基于信息熵的网络攻击流量特征分析,Shi等^[43]利用改进雷达图进行网络事件关联分析。虽然这些改进算法通过特征抽取、降维、采样或聚合的方法减少了数据项和数据维度,但数据挖掘算法往往很难与可视化方法有机结合,交互性并不好。因此,如何改善网络安全分析领域人机交互模型,有效融合分析人员的先验知识,更新计算分析模型,是一个急需解决的问题。

4.2 人工智能的新一轮研究热潮带动预测性可视分析研究

世界著名咨询公司Gartner从信息经济学角度定义了一个重要技术进化模型,从低级到高级依次为:探索过去的描述性分析、探索原因的诊断性分析、可以预言未来的预测性分析^[44]。预测网络威胁安全事件未来移动对于遏制横向移动和减少威胁停留时间至关重要,但如何对攻击趋势做出预测并采取预防措施,还是一个远期的研究目标。将人工智能技术及可视分析技术结合是一个值得尝试的解决思路。例如,Correa等^[45]早期利用可视推理技术研究社交网络中的不确定性问题,Arietta等^[46]将数据挖掘技术应用于城市计算中,结合可视推理方法成功预测了部分城市属性。Wang等^[47]运用可视推理技术对大量出租车轨迹数据进行可视分析,有效评估了城市道路利用率。Cao等^[48]研究在线社交网络异常用户行为过程中,定义了行为特征、内容特征、交流特征、活动时间特征、网络特征、头像特征6类用户特征,引入非监督学习模型计算和检测异常用户并排序,取得了显著的效果。美国乔治亚理工大学研究人员^[49]首次提出了一个名为“演示式可视化”的数据可视分析通用交互范式,通过量化计算用户的交互意图,从位置、大小和颜色3方面递进式地推荐给用户下一步图形转化建议。由此看来,基于智能技术的可视推理是预测性可视分析发展的一个重要研究方向,但目前在网络安全相关领域尚未有研究工作报道。

5 结束语

网络空间安全的重要性与日俱增,网络空间安全关联数据可视化是网络空间安全领域一个新的研究热点。本文在分析网络安全数据可视化分析现状基础上,深入讨论了当前网络威胁安全数据可视化研究存在的问题,并进一步探讨了网络空间安全数据可视化的发展趋势。数据可视化技术已经在很多领域研究得到深入应用,数据可视化技术也必将在网络空间安全领域发挥越来越重要的作用。

参考文献:

- [1] FISCHER F, FUCHS J, MANSMANN F, et al. BANKSAFE: visual

- analytics for big data in large-scale computer networks[J]. *Information Visualization*, 2015, 14(1): 51-61.
- [2] 张焕国, 韩文报, 来学嘉, 等. 网络空间安全综述[J]. *中国科学: 信息科学*, 2016, 46(2): 125-164.
- ZHANG H G, HAN W B, LAI X J, et al. Survey on cyberspace security[J]. *SCIENTIA SINICA Informationis*, 2016, 46(2): 125-164.
- [3] 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.
- [4] ZHANG T Y, WANG X M, LI Z Z, et al. A survey of network anomaly visualization[J]. *Science China: Information Sciences*, 2016, 59(1): 1-17.
- [5] STAHELI D, YU T, JORDAN C R, et al. Visualization evaluation for cyber security: trends and future directions[C]//*IEEE Workshop on Visualization for Computer Security (VizSec)*. 2014.
- [6] POST T, WISCHGOLL T, BRYANT A R, et al. Visually guided flow tracking in software-defined networking[C]//*IEEE Workshop on Visualization for Computer Security (VizSec)*. 2016.
- [7] WARD M O, GRINSTEIN G, KEIM D. Interactive data visualization: foundations, techniques, and applications[M]. A K Peters Press, 2010.
- [8] 陈为, 沈则潜, 陶煜波. 数据可视化[M]. 北京: 电子工业出版社, 2013.
- CHEN W, SHEN Z Q, TAO Y B. Data visualization[M]. Beijing: Publishing House of Electronics Industry, 2013.
- [9] 李建华. 网络空间威胁情报感知、共享与分析技术综述[J]. *网络与信息安全学报*, 2016, 2(2): 16-29.
- LI J H. Overview of the technologies of threat intelligence sensing, sharing and analysis in cyber space[J]. *Chinese Journal of Network and Information Security*, 2016, 2(2): 16-29.
- [10] 李燕, 曹宝香, 马兆丰, 等. 关联分析算法在安全管理平台中的研究与应用[J]. *计算机技术与发展*, 2013, 23(10): 107-110, 114.
- LI Y, CAO B X, MA Z F, et al. Research and application of correlation analysis in security management platform[J]. *Computer Technology and Development*, 2013, 23(10): 107-110, 114.
- [11] 赵颖, 樊晓平, 周芳芳, 等. 网络安全数据可视化综述[J]. *计算机辅助设计与图形学学报*, 2014, 26(5): 687-697.
- ZHAO Y, FAN X P, ZHOU F F, et al. A survey on network security data visualization[J]. *Journal of Computer-Aided Design & Computer Graphics*, 2014, 26(5): 687-697.
- [12] 赵颖, 樊晓平, 周芳芳, 等. 大规模网络安全数据协同可视分析方法研究[J]. *计算机科学与探索*, 2014, 8(7): 848-857.
- ZHAO Y, FAN X P, ZHOU F F, et al. Research on collaborative visual analysis of large scale network security data[J]. *Journal of Frontiers of Computer Science and Technology*, 2014, 8(7): 848-857.
- [13] 赵颖, 樊晓平, 周芳芳, 等. 多源网络安全数据时序可视分析方法研究[J]. *小型微型计算机系统*, 2014, 35(4): 906-910.
- ZHAO Y, FAN X P, ZHOU F F, et al. Visualization of multi-source network security data based on stacked stream graph[J]. *Journal of Chinese Computer Systems*, 2014, 35(4): 906-910.
- [14] 张胜, 施荣华, 赵颖. 基于多元异构网络安全数据可视化融合分析方法[J]. *计算机应用*, 2015, 35(5): 1379-1384, 1416.
- ZHANG S, SHI R H, ZHAO Y. Visual fusion and analysis for multivariate heterogeneous network security data[J]. *Journal of Computer Applications*, 2015, 35(5): 1379-1384, 1416.
- [15] 赵立军, 张健. 基于堆叠条形图和平行坐标的网络数据安全可视化分析方法研究[J]. *装备学院学报*, 2015, 26(5): 86-90.
- ZHAO L J, ZHANG J. Study on network data security visualization based on stacked bar chart and parallel coordinates[J]. *Journal of Equipment Academy*, 2015, 26(5): 86-90.
- [16] 吴亚东, 蒋宏宇, 赵思蕊, 等. 网络安全数据 3D 可视化方法[J]. *电子科技大学学报*, 2015, 44(4): 594-598.
- WU Y D, JIANG H Y, ZHAO S R, et al. 3D visualization method for network security data[J]. *Journal of University of Electronic Science and Technology of China*, 2015, 44(4): 594-598.
- [17] 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.
- [18] MCPHERSON J, MA K, KRYSTOSK P, et al. PortVis: a tool for port-based detection of security events[C]//*IEEE Symposium on Visualization for Cyber Security (VizSec)*. 2004.
- [19] LAKKARAJU K, YURCIK W, BEARAVOLU R, et al. NVisionIP: an interactive network flow visualization tool for security[C]//*IEEE International Conference on Systems, Man and Cybernetics*, 2004.
- [20] GOODALL J R, LUTTERS W G, RHEINGANS P, et al. Preserving the big picture: visual network traffic analysis with TNV[C]//*IEEE Workshop on Visualization for Computer Security (VizSec)*. 2005.
- [21] CONTI G, ABDULLAH K, GRIZZARD J, et al. Countering security analyst and network administrator overload through alert and packet visualization[J]. *IEEE Computer Graphics and Applications*, 2006, 26(2): 60-70.
- [22] NYARKO K, CAPERS T, SCOTT C, et al. Network intrusion visualization with NIVA, an intrusion detection visual analyzer with paptic integration[C]//*The 10th Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems*. 2002.
- [23] LIVNAT Y, AGUTTER J, MOON S, et al. A visualization paradigm for network intrusion detection[C]//*IEEE SMC Information Assurance Workshop*. 2005.
- [24] ABDULLAH K, LEE C, CONTI G, et al. IDS RainStorm: visualizing IDS alarms[C]//*IEEE Workshop on Visualization for Computer Security (VizSec)*. 2005.
- [25] BERTINI E, HERTZOG P, LALANNE D. SpiralView: towards security policies assessment through visual correlation of network resources with evolution of alarms[C]//*IEEE Conference on Visual Analytics Science and Technology (VAST'07)*. 2007.
- [26] SIADATI H, SAKET B, MEMON N. Detecting malicious logins in enterprise networks using visualization[C]//*IEEE Symposium on Visualization for Cyber Security (VizSec)*. 2016.
- [27] SYAMKUMAR M, DURAIRAJAN R, BARFORD P. Bigfoot: a geo-based visualization methodology for detecting BGP threats[C]//*IEEE Symposium on Visualization for Cyber Security (VizSec)*. 2016.
- [28] LING X, GERTH J, HANRAHAN P. Enhancing visual analysis of network traffic using a knowledge representation[C]//*IEEE Symposium on Visual Analytics Science and Technology*. 2006.
- [29] SHEN Z Q, MA K L, ELIASSI-RAD T. Visual analysis of large heterogeneous social networks by semantic and structural abstraction[J]. *IEEE Transactions on Visualization and Computer Graphics*, 2006, 12(6): 1427-1439.
- [30] IANNAcone M, BOHN S, NAKAMURA G, et al. Developing an

- ontology for cyber security knowledge graphs[C]//The Cyber and Information Security Research. 2015.
- [31] AUPETIT M, ZHAUNIAROVICH Y, VASILADISM G, et al. Visualization of actionable knowledge to mitigate DRDoS attacks[C]//IEEE Symposium on Visualization for Cyber Security (VizSec). 2016.
- [32] YAO Y G, WANG X, MENG X J, et al. ISEK: an information security knowledge graph for CISP knowledge system[C]//The International Conference on IT Convergence and Security (ICITCS). 2015.
- [33] YAO Y G, ZHANG L, YI J, et al. A framework for big data security analysis and the semantic technology[C]//The International Conference on IT Convergence and Security (ICITCS). 2016.
- [34] CIAPESSONI E, CIRIO D, KJØLLE G, et al. Probabilistic risk-based security assessment of Power systems considering incumbent threats and uncertainties[J]. IEEE Transactions on Smart Grid, 2016, 7(6):2890-2903.
- [35] 彭勇, 江常青, 谢丰, 等. 工业控制系统信息安全研究进展[J]. 清华大学学报, 2012, 52(10): 1396-1408.
- PONG Y, JIANG C Q, XIE F, et al. Industrial control system cyber security research[J]. Journal of Tsinghua University, 2012, 52(10): 1396-1408.
- [36] KAYNAR K, SIVRIKAYA F. Distributed attack graph generation[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(5): 519-532.
- [37] YELIZAROV A, GAMAYUNOV D. Visualization of complex attacks and state of attacked network[C]//IEEE Workshop on Visualization for Computer Security (VizSec). 2009.
- [38] WANG T B, XIA C H, WEN S, et al. SADI: A novel model to study the propagation of social worms in hierarchical networks[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 99: 1-17.
- [39] STANGE J, DÖRK M, LANDSTORFER J, et al. Visual filter: graphical exploration of network security log files[C]//IEEE Symposium on Visualization for Cyber Security (VizSec). 2014.
- [40] ZHAO Y, LIANG X, FAN X P, et al. MVSec: multi-perspective and deductive visual analytics on heterogeneous network security data[J]. Journal of Visualization, 2014, 17(3):181-196.
- [41] 赵颖, 王权, 黄叶子, 等. 多视图合作的网络流量时序数据可视分析[J]. 软件学报, 2016, 27(5):1188-1198.
- ZHAO Y, WANG Q, HUANG Y Z, et al. Collaborative visual analytics for network traffic time-series data with multiple views. Journal of Software, 2016, 27(5):1188-1198.
- [42] ZHOU F F, HUANG W, ZHAO Y, et al. ENTVis: a visual analytic tool for entropy-based network traffic anomaly detection[J]. IEEE Computer Graphics and Applications, 2015, 35(6):42-50.
- [43] SHI L, WANG C, WEN Z, et al. 1.5D Egocentric dynamic network visualization[J]. IEEE Transactions on Visualization and Computer Graphics, 2015, 21(5):624-637.
- [44] LANEY D. Information economics, big data and the art of the possible with analytics[EB/OL]. [https://www-950.ibm.com/events/wwc/grp037.nsf/vLookupPDFs/Gartner_Doug-%20Analytics/\\$file/Gartner_Doug-%20Analytics.pdf](https://www-950.ibm.com/events/wwc/grp037.nsf/vLookupPDFs/Gartner_Doug-%20Analytics/$file/Gartner_Doug-%20Analytics.pdf).
- [45] CORREA C D, CRNOVRANIN T, MA K. Visual reasoning about social networks using centrality sensitivity[J]. IEEE Transactions on Visualization and Computer Graphics, 2012, 18(1): 106-120.
- [46] ARIETTA S M, EFROS A A, RAMAMOORTHY R, et al. City forensics: using visual elements to predict non-visual city attributes[J]. IEEE Transactions on Visualization and Computer Graphics, 2016, 20(12):2624-2633.
- [47] WANG F, CHEN W, WU F R, et al. A visual reasoning approach for data-driven transport assessment on urban roads[C]//IEEE Conference on Visual Analytics Science and Technology (VAST). 2014.
- [48] CAO N, SHI C L, LIN S, et al. TargetVue: visual analysis of anomalous user behaviors in online communication systems[J]. IEEE Transactions on Visualization and Computer Graphics, 2016, 22(1): 280-289.
- [49] SAKET B, KIM H, BROWN E T, et al. Visualization by demonstration: an interaction paradigm for visual data exploration[J]. IEEE Transactions on Visualization and Computer Graphics, 2017, 23(1): 331-340.

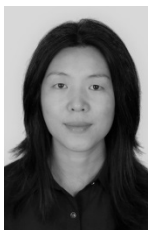
[作者简介]



张繁 (1978-), 男, 浙江绍兴人, 博士, 浙江工业大学副教授, 主要研究方向为网络安全、信息可视化。



谢凡 (1997-), 男, 广东梅州人, 浙江工业大学本科生, 主要研究方向为网络安全、数据挖掘。



江颀 (1972-), 女, 浙江平湖, 博士, 浙江工业大学计副教授, 主要研究方向为信息安全、服务计算。