网络安全态势感知分析框架与实现方法比较

李 艳[1],王纯子[1],黄光球[2],赵 旭[1],张 斌[2],李盈超[1,3]
(1. 西安工程大学管理学院,陕西西安 710048; 2. 西安建筑科技大学管理学院,陕西西安 710055; 3. 联易软件有限公司,陕西西安 710000)

摘 要: 信息技术已经深入到全社会政治、经济、文化的方方面面,信息革命改变了全世界的沟通方式,促使人类社会有了巨大的发展,也使网络安全问题受到了前所未有的关注.针对网络安全问题的研究主要经历了理想化设计保证安全、辅助检测被动防御、主动分析制定策略、全面感知预测趋势4个主要阶段,在各国都在争夺数字控制权的新战略制高点背景下,针对网络安全态势感知的探讨无论是在学术研究上还是在产业化实现上都呈现出了全新的特点.本文对网络安全态势感知进行了尽可能详尽的文献调研,首先介绍了国内外研究现状及网络安全态势感知与传统态势感知之间的区别与联系;然后从数据价值链角度提出了网络安全态势感知的逻辑分析框架,将整个过程分解为要素采集、模型表示、度量确立、求解分析和态势预测五个连续的处理阶段,随后对每个阶段的作用,主流的方法进行了阐述,并对在实验对象上的应用结果以及方法间的横向比较进行了说明.本文意图对网络安全态势感知提供全景知识,为网络安全的产业化方案提供辅助思想,希望能够对此领域的科研和工程人员起到参考作用.

关键词: 网络安全; 网络态势感知; 攻击模型; 入侵检测; 数据融合分析
中图分类号: TN915.08 **文献标识码:** A **文章编号:** 0372-2112 (2019)04-0927-19
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.04.021

A Survey of Architecture and Implementation Method on Cyber Security Situation Awareness Analysis

LI Yan[1], WANG Chun-zi[1], HUANG Guang-qiu[2], ZHAO Xu[1], ZHANG Bin[2], LI Ying-chao[1,3]
(1. *School of Management, Xi'an Polytechnic University, Xi'an, Shaanxi* 710048, *China*;
2. *School of Management, Xi'an University of Architecture & Technology, Xi'an, Shaanxi* 710055, *China*;
3. *LianYi Software Co. Ltd., Xi'an, Shaanxi* 710000, *China*)

Abstract: Information technology has penetrated into all aspects of politics, economy and culture in the whole society. The information revolution has changed the way of communication all over the world, promoted the development of human society, and made the problem of network security get unprecedented attention. The research on network security has mainly experienced 4 main stages: idealized design ensures safety, passive defense after auxiliary detection, actively analyze and formulate security strategies, forecast trend after comprehensive perception. Under the background of the new strategic commanding point for the power of digital control in all countries, the research on the Cyber Security Situation Awareness Analysis (CSSA) has presented new features in both academic research and industrialization. This paper makes a detailed literature survey on CSSA. First, it introduces the status of the research and the difference and connection between CSSA and traditional awareness analysis. Then the logical analysis framework of CSSA is proposed from the perspective of data value chain. The whole process is decomposed into five continuous stages of processing, including factor collection, model representation, measurement establishment, solution analysis and situation prediction. After that, the role and the mainstream method of each stage are expounded, and the application results on the experimental object and the horizontal comparison between the methods are explained. The purpose of this paper is to provide a panoramic knowledge of CSSA, and to provide an auxiliary idea for the network security industrialization scheme, and hope that it can serve as a reference for scientific research and engineering personnel in this field.

Key words: network security; network situation awareness; attack model; intrusion detection; data fusion analysis

收稿日期:2018-04-23;修回日期:2018-09-25;责任编辑:李勇锋
基金项目:陕西省科学技术研究发展计划(No. 2013K1117);陕西省重点学科建设专项资金(No. E08001);西安工程大学博士科研启动基金

1 引言

针对网络安全方面的研究自信息网络诞生之日起就已经开始.网络规模和应用的指数级增长,尤其是在OSI模型为基础的静态Internet物理连接网络之上构建的随机动态访问关系,使得网络安全问题的研究更加复杂化.在上世纪60年代以前,人们针对网络安全问题的研究热点是面对破坏如何建立一个绝对安全的系统,减少设计上的漏洞来保证系统的保密性、完整性及可用性等要求,这可以视为网络安全研究的第一阶段;但人们很快意识到,在实际操作中这是不可能的[1],恶意入侵一定存在的现实,使人们开始思考构建一个安全辅助系统,目标是当入侵发生时能实时的检测到,并采取相应的措施,这其中最典型的应用就是入侵检测系统(Intrusion Detection System,IDS)的提出[2],入侵检测起源于Anderson的技术研究报告[3],之后的研究大体上可以分为异常检测和误用检测两类,目前大部分科研机构和商业组织的IDS也是基于这两类技术的,入侵检测技术在网络攻击发生时给出预警信息来保证网络安全,但其对绕墙隐秘攻击、多步复合攻击等无能为力,这样的被动防御技术在检测实时性上也差强人意;因此90年代以后第三阶段研究的关注重点从被动的防御转到主动分析[4,5]上来,其源于黑客技术的发展,意图是在网络攻击发生之前进行整体化安全评价,制定防御策略或保证网络遭受破坏的情形下仍能提供预定的服务功能;伴随着对可生存性研究的深入,1999年Bass首次提出了网络态势感知(Cyber Situation Awareness,CSA)的概念[6],意图感知时间和空间环境中的元素,使人们可以更好的把握网络整体安全状况及预测未来变化趋势,这在一定程度上促进了网络安全研究和其他学科的融合发展,尤其是和一些高级随机模型的结合取得了理论上的进展(如随机代数[7]、博弈论[8]、贝叶斯网络[9]等),但大部分都是在CSA概念模型基础上进行评估算法优化,很少有实践应用上的突破和系统性的阐述(表1对网络安全研究发展的四个主要阶段进行了简要的总结).

2 国内外研究现状

2.1 国外研究现状

态势感知(Situational Awareness)的研究来源于Endsley超过15篇文章以上的一系列研究与阐述[11~13],Bass[6]与网络空间相结合首次提出了网络态势感知的理念,在物联网、大数据、移动应用等新技术的推动下,互联网应用层面的创新和推广迅速扩大,拓扑结构也自然日趋繁杂,从公开资料的显示,各个国家都将网络安全上升到了国家战略层面,从各国公开的网络安全策略中可以看出虽然各国在对网络安全的理解、所实施的策略上有所不同,但是各国都意识到了需要行动起来保护关键信息和相关的基础设施,同时更需要研究新的方法和技术来实现网络安全态势预测智能化.

表1 网络安全研究发展的四个主要阶段

序号	时间区间	阶段	主旨思想	核心技术
1	1960年以前	设计保证	建立一个绝对安全的系统,保证攻击不会发生	软、硬件技术层面的架构设计
2	1970~1980年代	入侵检测	构建一个安全辅助系统,攻击发生时能检测到,并采取措施	入侵监测系统(误用检测、异常检测)
3	1990年代	主动防御	不只是被动防御,进行主动评价,在攻击发生之前制定防御策略	攻击模型(攻击树、攻击图、状态图等)
4	2000年以后	态势感知	感知时间和空间环境中的元素,把握网络整体安全状况及预测未来变化趋势	JDL, OODA,高级随机模型(复杂网络演化、博弈论等)

各国政府的高度重视会使其在基金支持等方面提供更多财力支撑,加之众多研究者对这个方面的自发持续关注,使得针对网络安全方面的研究成为了热中翘楚.为了能充分了解网络安全态势感知的研究现状,本文首先在2017年9月份对核心数据库中近10年关于此方面的外文Review文章进行了搜索,共整理了10篇被引量较大的综述类文献[14~23].通过对综述类文献进行总结可以看到国外针对此研究的主体脉络是将态势感知的模型和方法在网络安全态势感知领域的实例化,并在实践中不断检验和优化的过程.为了对网络安全态势感知的研究细节进行有效分析,本文又对近几年核心数据库中75篇文献进行了归纳,这些文章的研究点主要集中在9个方面(表2中将这9方面的关键研究内容与传统的Endsley模型[13],JDL模型[18]和OODA模型[23]的逻辑阶段进行了映射划分):

(1)模型的概念(与其他学科的融合)[17,23~27]

(2)数据采集变量的完备性和规则化[18,20,23,28,29]

(3)相关算法的优化[30~33]

(4)信息融合分析[18,20,28,34,35]

(5)过程工具的自动化[28,36~38]

(6)各阶段工作的可视化[4,9,26,31,34,35,39,40]

(7)实践检验及在大规模现实网络中的效率提升[41,42]

(8)感知方法的软件工程化实现[20,43~45]

(9)分析和预测结果在特定领域的实际应用[20,28,29,40,47,48]

表 2　根据摘要对外文 75 篇文献的统计分类

经典模型			核心关注点	文章数量
Endsley 模型[13]	JDL 模型[18]	OODA 模型[23]	概念升级细化或与其他学科相结合	15
元素感知	传感器	观察(拓扑和配置,用户和管理员活动,当前威胁,正在进行的攻击,软件和服务漏洞等)	信息采集对象的更完备和规则化信息采集工具的自动化	8
	数据预处理			
	对象精炼			
现状理解	情境细化	调整(业务流程 - 信息 - 基础设施 - 服务 - 应用)	情境感知算法优化 多源信息融合 结果可视化 大规模网络下效率提高 软件工程实现	60
未来状态感知	威胁细化			
感知决策	认知细化/HCI	决策	结果在特定领域的应用	25
动作执行		执行		

2.2　国内研究现状

在政策主导方面,我国从上至下都对网络安全异常的重视,和欧美国家相类似也在各个层级成立了网络安全相关的应急处理机构,2016 年 4 月 19 日,习近平总书记在《网络安全和信息化工作座谈会上的讲话》[92]中强调了网络安全的重要性、工作任务和工作目标,并明确提出感知网络安全态势是最基本,最基础的工作. 限于篇幅的原因,本文不对我国网络安全的政策和产业发展做过多的解读.

在学术研究方面,国内的学者更是倾注了极大的兴趣和热情,几乎每一个相关核心期刊都有“网络安全”相关专题,为了对国内研究现状进行总结,和外文文献研究思路一致,本文首先对综述类文献进行了整理,结合作者在此领域的研究积累和有效的搜索,共有 9 篇[49~57]综述类文献具有较大引用量或较强借鉴意义. 对比国内外的综述文档发现,我国学者对此方面的关注时间点和国外相差不多,但大多处于“跟随”状态,具有原创性的,有创新影响力的文章不多,ESI 国内高引的文章大都是针对模型算法优化和应用实现层面的突破[55,58],尤其是在态势量化计算感知方面[59~62],这可以视为国内针对此领域的研究主线. 同时针对国内的研究文献进行仔细甄别发现,有相当一部分文章的“信息融合、态势感知”等题目的说法只是停留在微观认知层面(这和外文文献一般都是在 Endsley 模型[13],JDL 模型[18]和 OODA 模型[23]基础上的改进不同),即在一定程度上自下而上对更多的数据源进行综合利用,而非自上而下的整体化考虑. 但这些先局部后整体的研究也取得了斐然的进展,对整个领域的促进作用也十分明显. 通过对 CNKI 核心期刊中 100 篇左右的文献进行归纳,这些文章的研究点主要集中在 5 个方面(表 3 中将这 5 方面内关键研究内容的总结和典型文章代表进行了列示):

表 3　根据题目和摘要对 100 篇左右中文文献的统计分类

序号	关注点	关键改进点	典型案例	文章数量
1	概念的定义或解释	一般性的概念解释和其他学科结合后的模型含义	态势感知领域内基本内容和研究范畴的界定[50,57]综述性文章[49~57]着色 Petri 网[63]、风险传播模型[65]	12
2	入侵检测数据融合	更多数据源的获取数据的融合利用	数据分类[66],数据时空属性的组合[83]数据融合示例[65]	26
3	主动评价模型尝试	交叉学科模型定义 模型求解算法求解结果应用	Petri 网[55],博弈论[84],贝叶斯网络[85] 算法优化及应用示例(如基于攻击图的分析[67,69,72,74])	42
4	量化后的体系化评价	评价指标体系化 指标量化 求解量化结果并利用	基于安全属性角度的分类[78] 基于攻击行为的分类[61,64,79~80] 风险评估结果的应用[59~60]	16
5	设计实现并在特定领域应用	软件工具的实现 特定领域的应用效果	ISACISAC,安全事故预案体系,大规模网络安全状态的仿真平台[51] ICS[81],ECP[82]	25

(1)概念的定义或解释[49,50,56,57,63,64]
(2)入侵检测数据融合[64,65]
(3)主动评价模型尝试[55,63,67~76]
(4)量化后的体系化评价[61,64,78~80]
(5)设计实现并在特殊领域应用[51,81,82]

3 整体框架

3.1 逻辑分析框架

网络安全态势感知通常涉及多个不同阶段,需要用系统化方法来处理网络安全的相关数据,在逻辑划分上主要有两种方法:一是工程层次化方法(如文献[23]中的图2,文献[56]中的图3,文献[66]中的图1,文献[70]中的图4等);二是概念层级化方法(如文献[23]中的图3,文献[12]中的图1等).但这两种方法都不能从数据处理阶段的角度出发提供理解容易的架构.本文从数据价值链角度,采用产业界广为接受的系统工程方法,将典型的网络安全态势感知过程分解为五个连续的处理阶段,包括要素采集、模型表示、度量确立、求解分析和态势预测,如图1所示.

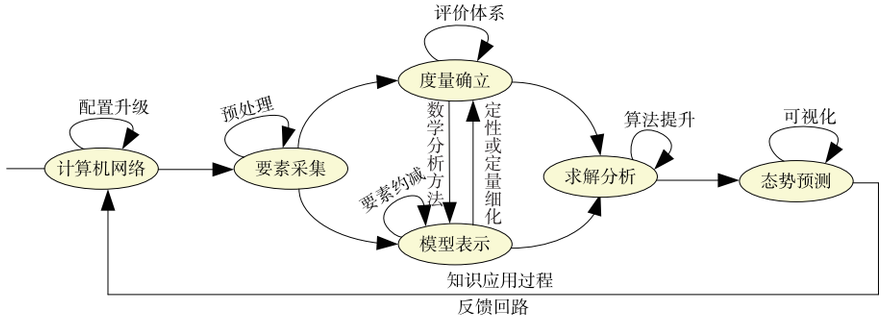


图1 网络安全态势感知运行机制

3.2 框架内方法间比较的实验环境

为了对所提整体框架上各阶段内的不同方法之间进行有效的对比和总结,这里将一家中型软件开发企业作为实验对象.图2为该企业的网络拓扑图,其通过电信的专用线路与外网连接,采用网神作为内外网之间的监视设备,10是一台Web服务器,对外提供公司宣传网站和产品演示的功能;140是可以外网访问的日志服务器(因为公司人员经常出差,所以无论内外网访问都需要经过外网);15是公司的数据库服务器,同时运行着SQL Server、Oracle两大关系型数据库及一个非关系型数据库MongoDB;16是测试服务器,公司已经交付及正在研发的产品都在测试服务器上有一个最新版本的部署;11是内部开发服务器,公司所有源代码及重要的项目方案、过程资料等都在此服务器上;公司有一个百人左右的开发团队,因开发技术不同主要分为两类,58代表采用.Net研发的技术团队,59代表采用Java研发的技术团队.

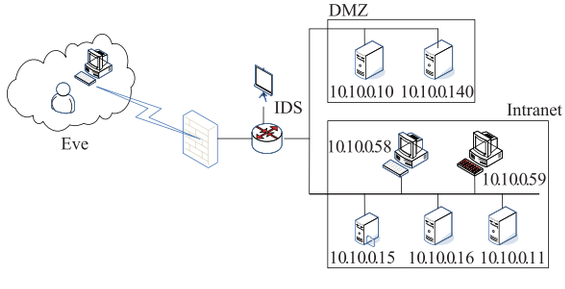


图2 实验网络拓扑结构图

4 阶段Ⅰ:要素采集

要素采集阶段的作用是将网络安全态势感知各个阶段中要用到的关键数据进行有效获取.广义上要素采集是指网络安全相关全要素的采集,狭义上要素采集是指某一感知过程中所涉及要素的采集,本文意图是对网络安全态势感知基础框架进行梳理,并对各阶段的核心实现方法进行横向比较,因此本文内要素采集指广义要素采集.毫无疑问,要素采集是网络安全态势感知的前提,没有基础数据收集,后续各阶段都无法工作.目前所搜集到的大部分文献都在框架逻辑描述上明确了此阶段的功能和重要作用,但在实现环节,大都只是提及通过自动化扫描工具或者预设传感器来进行数据获取,并按照后续模型的需要直接进行规约化或预处理,也有部分的文献对数据获取的方式或工具[36~38]等进行介绍.从严格意义上讲要素采集分为数据生成、数据获取和数据预处理三个部分,按照第3节逻辑分析框架的划分,数据预处理一般在模型定义或度量确立阶段开始后再进行;数据获取一般通过手动与自动相结合方式来完成,关注点一般在自动化工具研制上,本节重点从数据生成角度对数据分类进行归纳.

已有网络安全态势感知文献中,针对基础数据采集部分,大都是根据模型分析的需要逆推所用数据(狭义要素采集),这不利于数据标准统一和模型间比较验证.本文按照工程学的逻辑,从数据生成的角度出发对

网络安全分析中的数据进行简要统计和分类. 这里将数据分为两大类:静态数据和动态数据. 静态数据是指在图 1 所示一个网络安全态势感知分析循环中基本不会变化的数据,动态数据是指在图 1 所示一个网络安全态势感知分析循环中会随着分析过程深入有所改变的数据. 静态数据主要包括主机信息(如:主机 IP 地址或 MAC 地址唯一标识,运行的服务或程序,文件、数据等保密资产,操作系统,硬件组成,系统配置,权限配置等)、网络信息(如:网络设备信息,网络拓扑信息,协议信息,防火墙信息,网络配置信息等)和 IDS 信息(如:入侵检测系统基础信息,专家知识库,告警信息)等,动态信息主要包括活动信息(如:源地址,目标地址,活动描述等)、行为信息(如:源地址,目标地址,所用协议,传输数据大小,压缩算法等)、脆弱性信息(如:漏洞名称、标识、发布时间等基本信息,漏洞宿主信息,攻击方法,攻击影响,修复手段等)、攻击信息(如:攻击源地址,攻击方法等)和感知结果信息(如:上一次感知循环的感知结果信息,感知后的动作信息等).

5　阶段 Ⅱ:模型表示

形式化建模是网络安全态势感知运行机制中承上启下的关键环节,建模阶段针对要素的约减状态和形式化的描述能力会直接影响到后续的感知分析结果. 通过对现有文献的总结,网络安全态势感知模型主要分为 3 类:数学模型、随机模型和生物启发模型,各分类的核心理念和典型代表如表 4 所示.

表 4　网络安全态势感知的主要模型及其分类

序号	类型	核心思想	典型代表
1	数学模型	相关要素的公式化抽象,进而分析评价网络安全性	AHP 模型、贝叶斯网络、模糊集/粗糙集、可靠性/可生存性模型
2	随机模型	以交互描述为核心,通过行为刻画进行安全评价	Petri 网、博弈论、Markov 模型、攻击模型、D-S 证据模型、风险扩散模型
3	生物启发模型	与人工智能相结合,通过多层非线性拟合评估安全状况	神经网络、人工免疫、遗传算法/粒子群算法

5.1　数学模型

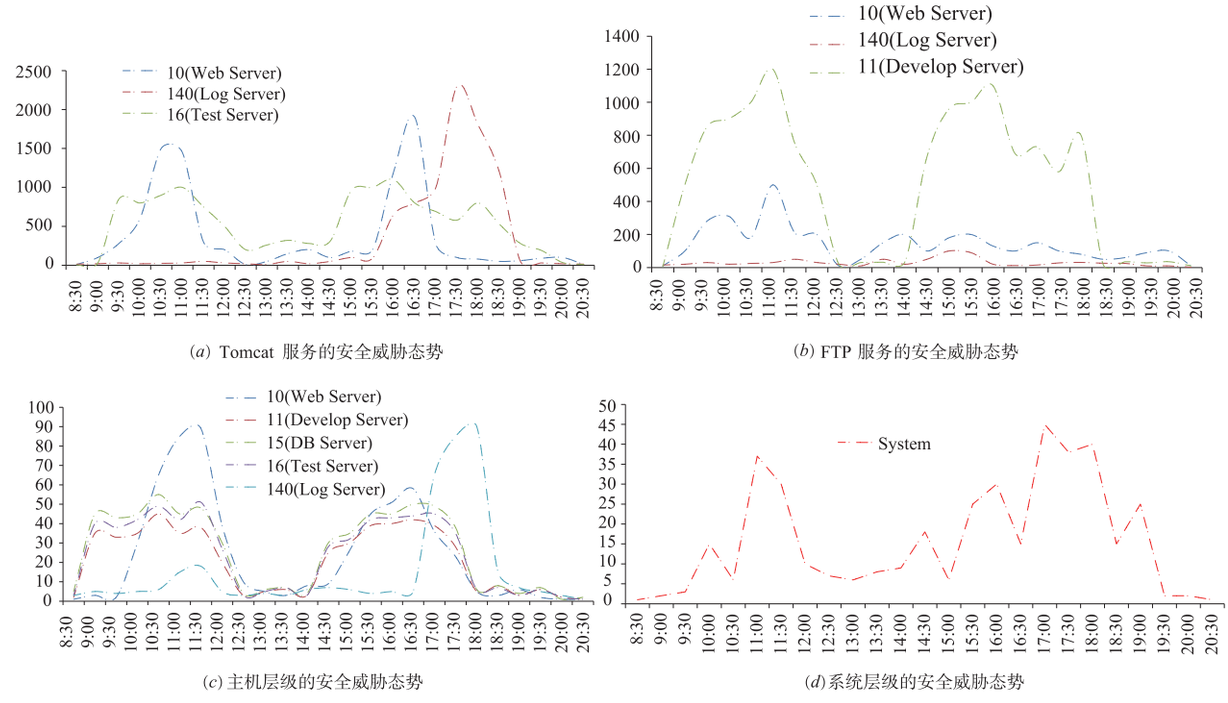
采用数学模型进行网络安全态势感知分析,主旨思想是用数学语言或者数学符号对计算机网络系统安全相关的特征或数量依存关系进行概括或近似描述. 这里的数学模型指狭义上的数学模型,即网络安全系统中各变量间关系的数学表达. 因此基于数学模型的感知分析方法更偏向于定量分析的形式. 主要包括:层次分析模型、贝叶斯模型、模糊集/粗糙集模型、可靠性/可生存性模型等.

层次分析法(Analytic Hierarchy Process,AHP)由 T L Saaty 教授提出,目前在决策领域得到了广泛的应用. 陈秀真等[58]人提出了层次化安全威胁评估模型,该模型自下而上将层级关系分为:漏洞、服务、主机和系统四个层次,并对各指数和参数给出了主观量化计算方法,最后按照先局部后整体的策略依次计算服务、主机及系统的安全状况. 图 3 是依据文献[58]中的主观量化方法进行运算后得出的 Tomcat 服务、FTP 服务、各主机及局域网络整体的安全态势量化结果. 层次化模型无论是在分析还是计算过程中都和决策者的思维过程保持一致,这保证结果直观理解性较强(例如,在图 3(*d*)中 17:30 分左右的安全态势指数都比较高,这是因为大部分人员都会在此时刻附近填写日志,频繁外网映射会导致安全隐患较高),构造有效的递阶层次结构是应用此模型的关键,也有文献针对层次结构的实例化进行了研究[128],但目前的要素量化过程基本都采用主观经验取值法,无法像经典层次分析法中通过两两因素排序进行比较量化,这导致模型客观性不够,而且目前的层次化结构只适用于局域网络,很难进行大规模推广,也缺乏对未来态势的有效预测.

为了对网络安全态势感知分析中不确定性和主观因素进行有效体现,通常使用概率方法进行定量说明[62,71],这其中贝叶斯逻辑是最常使用的模型,因为贝叶斯的因果关系规则及数学上的可靠性和人类思维推理的过程十分相似,贝叶斯计算可以综合最新的证据信息和先验信息,保证计算结果保持连续性和累积性两个重要特征. 有文献单独使用贝叶斯的数学方法进行网络安全态势评估[86],但大部分都将其作为量化计算工具与其他模型结合使用,尤其是将贝叶斯与攻击图相结合的研究较多[73,85],将图论和概率论相结合形成贝叶斯网络,使用图论展示定性层面上的结构和相互依赖关系,使用概率论进行定量层面的不确定性表达和推理,这个角度的研究取得了一定的进展,但贝叶斯网络在理论层面是联合概率分布的一种分解形式,实际求解中变量间相互不是独立的,联合概率的求解复杂度过高难以适用于大规模网络.

模糊集是针对传统集合而言的,在传统集合中对象与集合的关系是清晰的(非此即彼),但是现实中有些对象对集合的隶属关系是不明确的,存在着一种隶属程度的区间(隶属度函数),有文献将模糊相似度、模糊综合评判应用在网络安全态势感知分析中[87,88];粗糙集延拓了经典的集合论,其使用上、下近似两个集合来逼近任意一个集合,其可以在无先验知识的前提下分析不精确、不一致、不完整等各种不完备的信息,发

现隐含的知识,揭示潜在的规律,Zhao[89]和 Kong[90]等人将粗糙集中模式分类的思想应用在了网络安全态势评估中,将各安全评价指标作为条件属性集 C,根据 C 求出承载态势评估结果的决策属性 D,再根据 D 合成网络综合安全态势. 但目前在此方面的研究只限于用模糊集或粗糙集对过程中的不确定性进行表述,还无法将网络安全态势感知的目标或核心问题与模糊集或粗糙集方法深度结合,分析结果的实用性和研究的可延续性都有限,在与其他模型或方法的结合上也一般在分析过程中的某个环节上进行,更多是作为不确定性的量化工具出现.



(*a*) Tomcat 服务的安全威胁态势 (*b*) FTP 服务的安全威胁态势

(*c*) 主机层级的安全威胁态势 (*d*) 系统层级的安全威胁态势

图3 层次化安全态势感知结果

冯萍慧等人[91]将可靠性理论与脆弱性分析过程相结合来对分布式系统的安全性进行量化分析,意图通过可靠度函数 $R_s(c)$ 来确定在规定条件、规定代价 c 下系统维持安全状态的概率,图 4 是根据文献[91]对 10.10.0.11(内部开发服务器)上 FTP 服务进行攻击的脆弱性状态建模结果,针对此服务的平均攻击代价为 $E(C)=1/\lambda_1+1/\lambda_2+1/\lambda_3+1/\lambda_4+1/\lambda_5$. 文献[92]通过数学推演获得了复杂攻击网络完全概率可控或者部分概率可控的准则条件,从理论上证明了,如果网络中存在着有效防御的节点,复杂网络仍可在遭受攻击破坏的情形下提供正常的服务功能,并给出了防御节点选择及控制网络的建议方法. 使用可靠性或可生存性模型进行网络安全态势感知分析的优势是有数学理论上的推导过程来保证分析的严密性,但这些公式的前置约束条件也大大的限制了其在大规模网络条件下实际感知分析中的应用,现实网络中影响因素的多样性往往使得计算结果差强人意,而且模型在确定网络不安全状态后一般无法提供修复的方法使系统具备主动防御的能力.

5.2 随机模型

随机分析模型是一种非确定性模型,其主要特点是模型中的外生变量会随着具体条件而改变,这和网络安全相关行为的发生过程有很高的契合度,在攻击过程中,攻击者攻击手段的选择,防御者防御策略的选

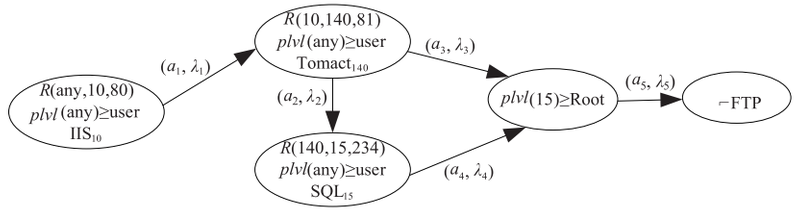
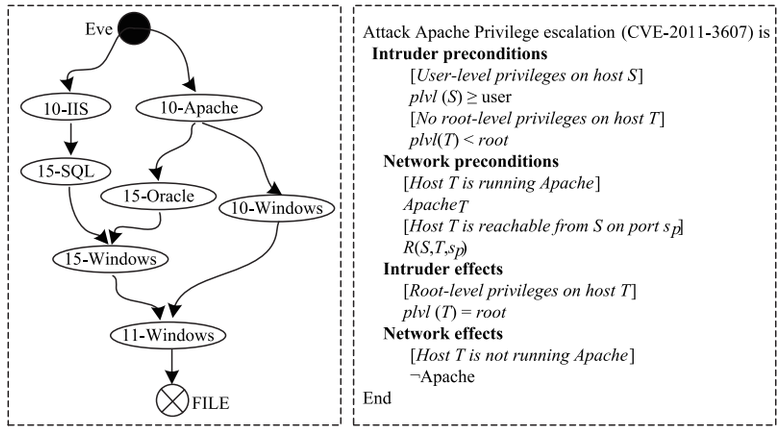


图4 可靠性量化模型建模结果

择以及正常用户的操作过程都是随机的. 使用随机模型进行网络安全态势感知,可以更清晰的刻画系统各要素的随机行为及行为之间的逻辑关系,也因此更易于对网络状态进行全面描述,同时其还可以包括未知行为的影响,基于随机模型网络安全态势感知是目前学术界的焦点,主要包括:攻击树/图模型、Petri 网、博弈论、Markov 模型、风险扩散模型等.

攻击树模型由 Scheier 等人[93]于 1999 年提出,其可以看作是故障树的一种扩展,直观也易于理解,但描述能力有限. 攻击图模型最早由 Swiler 等人[4]于 1998 年提出是目前应用最为广泛的方法,Sheyner[94]使用模型检测的方法生成攻击图,Ammann 等人[31]则通过图论的思想从初始状态开始正向搜索来生成攻击图,文献[95]以攻击为中心,给出了一种生成攻击图的工具,也有文献专注于攻击图的大规模构建和可视化呈现[74],早期的攻击图趋向于状态攻击图构建[4,31,74,94,95],但容易导致状态空间的爆炸,随着研究的深入越来越倾向于因果攻击图的构建[96],其边代表节点间的连接关系或者原子攻击的逻辑关系,扩展性强更易于大规模网络的应用,图 5 是第 2 节实验网络中攻击者 Eve 针对位于开发服务器上(10.10.0.11)的 FTP 服务进行攻击的攻击图结果,其中图 5(a)是图形化的描述,图 5(b)是攻击步骤形式化的描述,攻击图模型有着直观性和描述能力强的优点,而且容易和其他方法相结合是目前网络安全态势感知分析的基础模型,目前研究热点集中在原始模型上的细化[69]或改进[97]以增强描述能力和与其他学科进行融合[9]来增强分析能力两个方面.



(a)攻击图的图形化描述　　(b)攻击步骤中针对Apache攻击的形式化描述

图5　针对11服务器上FTP的攻击图

和攻击图相近的模型还包括特权图和状态转移图两类. Dacier[98]等人将图中的节点抽象为权限状态,提出了特权图模型,Ortalo[99]依托于特权图的概念建立了马尔可夫模型,给出了系统的安全演化过程,汪立东博士[150]对此进行了细化,但特权图模型很难描述状态或者随机事件之间的依赖关系,使得后续对此模型的扩展研究鲜有影响力的成果;Kemmerer[100]首次提出了基于状态转移图的入侵检测方法,图中的每个节点代表系统的一个临时状态,边代表状态的变迁和转移过程,文献[101]的概率模型、文献[102]的半马尔可夫过程模型等都是在此基础上的扩展,状态图的优点是其描述能力更强,但都存在着大规模网络下状态空间爆炸的问题,已有的针对此挑战的解决方法[71,74]仍都是差强人意.

Petri 网(Petri Net,PN)最早由卡尔·A·佩特里于 1962 年提出,可以对离散并行系统进行有效的数学模拟,其由三个要素:库所(Place),变迁(Transition)和有向弧(Arc)组成,$N=(P,T;F)$在库所内可以有任意数量的令牌代表资源(Token),最初的应用场景是通过 Token 在库所中的流动来检测协议中的错误(死锁状态). 在 Petri 网与网络安全态势感知的结合中,库所 P 通常代表可描述的系统局部状态,变迁 T 代表能够使系统状态发生改变的攻击事件或者正常活动,有向弧 F 将局部状态和事件之间进行有效的关联,它一方面引用能够促使变迁发生的局部状态,一方面指向由变迁所引起的局部状态的改变,图 6 所示的是第 2 节的实验网络中针对 11 上的 FTP 服务进行攻击的 Petri Net 模型建模结果,与经典 Petri Net 有差别的是,库所内不是 Token,而是某局部状态下变迁发生的概率,附着在变迁上的数字代表某攻击或活动成功的概率,在此基础上可以进行定性的可达标识分析或者通过关联矩阵,状态方程等进行量化分析,例如采用风险最大预估的"或"原则(不同路径间的概率取最大值),则中间库所 P_7 的发生概率为 $\max(0.4\times0.4,0.7\times0.5,0.8\times0.1)=0.35$. 可以看到,Petri 网不但具有图形化建模的直观和形象等特点,同时更适合于异步,并行的攻击发生过

程,在此方向的研究进展包括:增加模型描述能力的着色 Petri 网[103],针对变迁增加随机发生时间的随机 Petri 网[104],针对建模过程中不确定性描述的模糊 Petri 网[105]等.

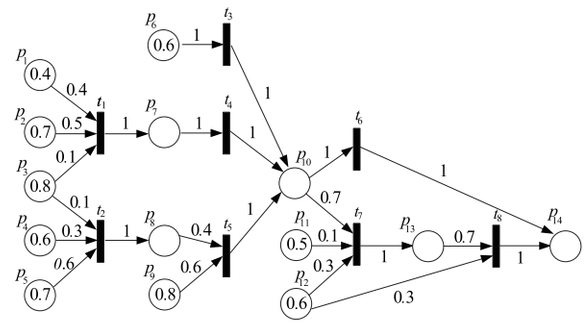


图6 针对11服务器上FTP攻击的Petri网建模结果

随着网络安全态势感知研究的深入,研究者意识到了两个问题:一是网络安全对抗过程中不单单是技术因素,同样的技术实现手段,不同的人应用在不同的场景会产生截然相反的结果;二是网络安全的分析一定不是一方的行为,在具有主动防御的环境中,安全态势会随着两方或多方的选择而发生变化,这与博弈论的策略依存思想有着极高的吻合度,一经提出便成为了研究的热点[106]. 传统针对入侵检测或者攻击行为的研究多数是建立在一次博弈分析基础上的[107],考虑到真实环境中的应用,定然是重复多阶段的不完全信息动态博弈[108],存在着精炼贝叶斯纳什均衡. 每一个基于博弈论的网络安全态势感知模型都至少包含五部分内容:$N=\{1,2,\cdots,n\}$是局中人的集合(一般将多个同类对象进行合并处理,分为攻击者、防御者、正常用户三类,$|N|=3$)、$S=\{S_1,S_2,\cdots,S_k\}$是攻防过程中的博弈状态集合、$\theta=\{\theta_A,\theta_D\}$是攻防双方的行动策略集合、$P$是博弈状态$S$间的转移概率、$R_n=S_i\times\theta\times S_j\in(-\infty,+\infty)$表示局中人$n$在状态$S_i$转移到状态$S_j$时的收益函数,$GM=\{N,S,\theta,P,R\}$,基于此基础定义,经过有限步($k$步)的博弈过程之后,系统在不同状态之间进行转化会形成一个树形结构,局中人的目标都是使各自的目标函数最大化,通过 Shapley 算法或问题转化求解[75]等方式可以获得模型的纳什均衡策略f^*. 博弈论的结合使网络安全态势感知的关注点从技术上升到管理策略层面,而且可以对各参与方的心理活动进行刻画,这极大提高了模型的描述能力和分析结果的科学性,目前的改进方向集中在:静态博弈转向动态博弈[109],模型相关要素量化[8]或与其他方法结合[110]以及实际应用效果体现[61,84]等方面.

Markov 模型的基本思想是下一状态的转移只与当前状态有关与历史状态无关,马尔可夫模型由三个要素组成:S是系统所有可能的状态所组成的非空状态集,P是系统状态转移概率矩阵,Q是系统初始概率分布,$M=\{S,P,Q\}$,将 Markov 模型应用在网络安全态势感知中的意图是在初始条件具备的情况下对攻防演化有效的进行预测,但攻击过程中会存在着大量的伪装攻击或者隐蔽攻击,强制施加无后效性会使统计的结果走向极端化(过分夸大某一偶然动作的影响或者忽略某一关键步骤的作用),因此一般将 Markov 与其他模型结合在一起使用[75,77],通过 Markov 的方法获取因果知识,并通过一步转移概率矩阵简化运算的过程,使模型可以在大规模网络下进行有效运算.

风险传播模型由张永铮等人[64]提出,其核心思想是由于网络系统的高度关联性,某一网络主体的风险会扩散到无漏洞的主体甚至整个网络,需要有效的手段来对整个网络信息系统的风险状态进行有效的评估. 风险传播模型(脆弱性扩散模型)一般由网络抽象和传播算法两部分组成,网络抽象部分描述的是系统逻辑访问关系结构,传播算法描述的是风险扩散的规则. 图 7 是第 3.2 节实验网络中攻击者对 Web 服务器攻击后,对开发服务器,数据库服务器及测试服务器所产生的风险扩散逻辑访问抽象建模结果,其中有向边的权重代表攻击收益. 若采用保证最终风险扩散结果最优的累积效应算法来确定节点间扩散估值λ_{uv},即

$$\lambda_{uv}=\frac{w(u,v)}{\sum_{m\in N(v)}w(m,v)}$$

其中$w(u,v)$代表节点u,v之间的权重,可得表 5 所示的计算结果. 从结果可以看出网络的风险状态不单单与存在着漏洞的主体有关,同时和逻辑访问结构与漏洞的分布状态有关,采用风险传播模型能够找到最具安全威胁的主体或风险传播路径.

5.3 生物启发模型

以自然界生物的自然现象或过程为灵感而提出的智能计算方法称之为生物启发计算方法,其基本原理是根据已知信息来探索某问题的解决方案,在探索过程中将相关信息进行有效记录和积累,并根据越来越多的已知信息指导下一步动作和修正以前的步骤,进而获得整体上更好的结果. 攻击者的攻击过程及防御者的防御过程也是如此,都是基于当前的知识状态来寻求以最小的代价获取最大的收益,这可视为人工智能在网络安全态势感知领域的具体应用,是极具前景的方法. 目前此方面的研究处于起步阶段,将攻防过程中的高维、非线性数据进行抽象并通过启发式计算求解的结果,无论是在可行性还是在最优性上都有待实践的检验和提高. 取得一定进展的模型主要包括:神经网络模型和人工免疫模型.

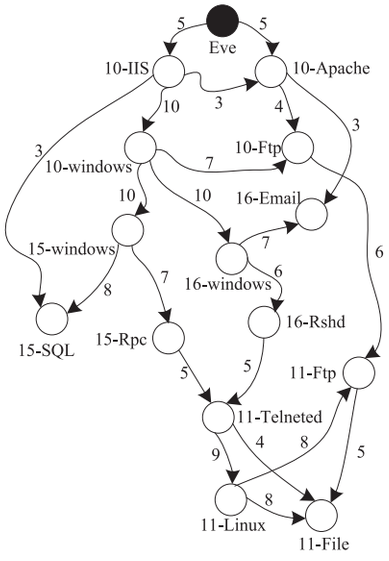


图7　风险扩散逻辑访问抽象建模结果

表 5　图 7 中各节点 λ_{iw} 计算结果

10-IIS	10-IIS	10-IIS	10-Apache	10-Apache	10-windows
0-Apache	10-windows	15-SQL	10-Ftp	16-Email	10-Ftp
3/8	1	3/11	4/11	3/10	7/11
10-Ftp	15-Windows	15-Windows	15-Rpc	16-Windows	16-Windows
11-Ftp	15-SQL	15-p. pc	11-Telneted	16-Email	16-Rshd
6/14	8/1 1	1	5/10	7/10	1
10-windows	10-windows	11-Ftp	16-Rshd	11-Linux	11-Linux
15-Windows	12-Windows	11-File	11-Telneted	11-Ftp	11-File
1	1	5/17	5/10	8/14	8/17

基于神经网络的一般方法是,将采集到的实时安全状态指标(如:脆弱性信息、攻击方法、防御手段等)作为输入向量 X,将代表态势感知结果的指标(如:机密性、完整性、可用性等)作为输出向量 Y,通过有效的训练构建起自 X 到 Y 的非线性映射[111,112]. 文献[113]在 IDS 研究中引入了神经网络的学习方法,有效的提高了报警的准确率,文献[114]将自编码网络与深度信念网络结构技术融入到风险识别的模型中,提出了一种轻量级入侵检测模型,可以在一定程度上降低训练时间和测试时间,降低了误报率.

模仿生物免疫系统的计算机免疫学[115]已经被广泛的应用在了网络安全态势感知分析中,文献[116]提出了将动态克隆选择算法应用在网络入侵检测系统的免疫模型,李涛依据人体免疫系统抗体浓度的变化与病原体入侵强度的对应关系,提出了基于免疫的网络安全风险检测模型[117],并通过免疫记忆的动态模型和响应的递推方程建立了基于免疫的网络监控模型[118]. 文献[119]将人工免疫算法作为风险评估的多目标求解方法,可以在一定程度上展示不同攻击策略下网络安全状态的变化. 但作为网络安全态势感知分析的新途径,免疫模型要充分的模拟免疫学的机理才能发挥作用,免疫学的复杂性和不可知性会使建模及求解过程过分的复杂化,能否有效反应安全态势演化过程还有待实践检验.

6　阶段Ⅲ:度量确立

度量确立的核心目的是在进行求解分析之前对网络安全态势感知所涉及到的各个要素对象细化分类或量化取值. 根据图 1 中网络安全态势感知运行机制所示,度量确立阶段可能会发生在模型形式化表述之后,也可能是在要素采集的基础上直接进行,这样此阶段主要分为两种情况:一是模型要素量化,二是评价指标体系和指数.

6.1　模型要素量化

在第 5 节形式化建模的过程中已经对相关的各要素进行了详细的定义,要进行网络安全态势感知所需要的求解分析,还需要对模型中的各个要素进行量化处理(从模型描述能力的角度来讲要素量化取值的过程也是描述能力细化的过程),因此,此阶段和模型构建的思路有很强的相关性,通过现有的文献统计和分析发现,各模型虽着眼点不同,但每个模型中都会有包含攻击行为的描述,针对攻击严重度、攻击发生/成功概率、攻击收益这 3 个要素的量化已经基本上形成了一定标准或者规范.

攻击严重度量化的前提是攻击类型的定性分类,网络攻击种类的多样性导致了攻击的分类方式也有多种,目前实用性较强而且被大多数人所接受的是 Christy[79]所提出的六元组表示方法,在定性分类方法的基础上划分为若干等级,来量化衡量威胁的严重程度[61,64],这种方法一般和 IDS 的告警机制相关联,在入侵检测中有广泛应用;在攻击模型中应用较为广泛的是 CVSS 的漏洞评价机制[8,80],其对每一个公开的漏洞分基本评价标准,生命周期评价和环境评价三个方面进行,最终的运算结果是一个 0 ~ 1 的数值,分值越高表明漏洞的威胁程度越大.

针对攻击发生\成功概率量化的目的是对攻击发生的真实性\攻击成功的可能性进行度量,网络攻击过程中会充斥着大量的虚假和无用信息,各主机和安全设备所提供的信息往往是不精确的,这就给信息融合模型进行综合估算带来了极大困难,目前在各实验模型中主要采用专家主观概率估计的方法[8,71,75],贝叶斯网络可以对不确定性知识的概率推理进行有效的表达,因此在此方面的研究中,基于贝叶斯的估算方法[26]

也取得了一定的进展.

攻击收益的量化是攻击效果评估中的重要组成部分,一般情况下是先对攻击的破坏性大小进行定性的衡量(例如:攻击获取了某一服务的 Root 权限[4,5]等),然后根据定性分类来给出损坏程度的量化值,量化研究可以从攻击者和防御者的两个角度进行,从攻击方的角度是在一定攻击成本下攻击所获取的回报,防御方是指在一定防御代价下系统免受的损失,一般情况下攻击收益均小于网络系统损失,为简便起见,大部分模型中均使用防御损失作为攻击收益,在本文后续分析中也采用此方法[61].

6.2 指标体系和指数

指标体系用于评价和反映某个领域的某种态势,在各个层面都有广泛的应用. 和对模型中的各个要素进行点上的量化不同,网络安全态势评估指标体系要从整体出发,意图对与网络安全态势评价相关的属性进行穷尽分类,给出每一类的明确含义,在相互联系、互相补充的体系化指标基础上进行量化操作,并通过数学计算方法获得待评估的网络安全态势指数值,通过指数值的变化来反映网络安全状况的变化.

网络安全态势指标体系和指数可以使网络管理员的关注点从分散或海量的日志数据监测中解放出来,便于直观的反应网络安全状态,尤其是变化程度的相对数可以帮助更好的发现异常,进而确定主要影响因素,做到有效的防护. 其主要包括两方面的工作:一是全面、系统的确定网络安全态势感知相关的要素(图 1 中评价体系以及各个度量要素量化的部分);二是建立体系化要素到结果指数之间的映射模型(图 1 中确定数学分析方法和求解分析部分).

林闯等人[55]在对网络安全性具体含义的解释进行有效综合的基础上,依托于可信赖性的研究,将安全性中普遍关注的属性分为了可靠性、可用性、保险性、机密性、完整性六个组成部分,分别给出了每一个指标在安全性领域的具体含义,并讨论了量化的方式. 可生存性超出了安全性的概念,它量化了一种正确执行预定功能的能力,是在安全性评价的基础上分析系统面临威胁时提供正常服务的能力. 可行性量化了网络系统在可能发生失效情况下的运行性能,提供了安全性与系统性能之间一种综合定量评价标准.

文献[120]在层次化指标体系的基础上[58],提出了基于配置指标体系的网络安全态势评估方法. 该方法中将指标分为综合指数、评估维度和态势因子三个层级展开,网络安全态势综合指数分为“优(0-1)、良(1-2)、中(2-3)、差(3-4)、危(4-5)”五个等级,评估维度主要在基础运行指数(反映网络设备及服务的安全运行情况)、脆弱性指数(反映在没有攻击的情况下,网络自身的脆弱情况)和风险指数(反映网络攻击对网络的影响)三个维度展开,每个维度可以选择不同的态势评估因子,并给出了每个因子的建议量化方法(如基础运行指数中的因子采用过载率进行量化等).

张永铮等人[121]提出了 10 个关键分类属性以及指数分类的通用概念模型 $ICM,M=(I,A,\Delta)$,其中 I 表示指数集合,包括指数的名称、计算公式和描述等信息;A 表示分类属性的集合,主要包括安全特性、数据特征、计算依据、对象规模、数据对象、计算形式、现象性质、基期、地域、网络对象等 10 个关键分类属性;Δ 代表由 I 到 A_m 的分类映射. 此分类方法可以提供较强的分类描述能力(理论上可以支撑 233280 个指数),同时也较易与层次化分类[100]相结合构建细粒度的指标体系.

7 阶段Ⅳ:求解分析

通过阶段Ⅱ的模型形式化描述和阶段Ⅲ的要素细化度量取值,基本上完成了网络中相关感知对象的细粒度抽象,接下来是网络安全态势感知中最核心的步骤:求解分析,其主要目的是对相应模型和数据经过有效分析计算,进而获得能反应网络安全状态的定性或定量结果,以数学语言来表述其是从要素及其量化的特征集合到网络安全状况判断性结果的映射过程. 在研究文章中,此部分一般以“模型求解算法”的形式出现,有文章是将传统方法扩展到网络安全态势感知领域,也有文章是将新理论或方法引入到此方面的研究中. 目前所搜索到的国内外网络安全态势感知文献中,有六成以上的文献是针对求解方法环节的改进,试图在分析结果的准确性或求解效率上有所提高.

7.1 求解方法分类

虽然网络安全态势感知过程中,求解方法呈现出了多样性的特点,但按照理论总结起来,总体可以分为:公式分析方法、逻辑推理方法和信息融合分析方法三类,如图 8 所示.

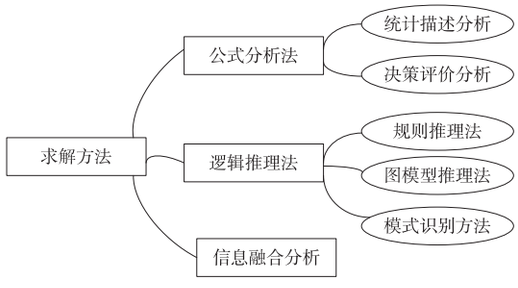


图8 网络安全态势感知求解分析方法分类

公式分析法也可称之为数学计算法,是最早应用于网络安全态势感知的方法,包括统计描述分析和决策评价分析两种类型. 统计描述分析方法使用基础的

数学统计计算的方式来反映网络安全状态,例如:网络实时发生的安全事件个数统计[36~38]、网络拥塞状况[38,51]、漏洞 top-k 排序[8,80,120]等,被广泛应用在各层级的网络安全监测系统中,此方法客观性高,可操作性强,但只能对结果展示,不能对状态发生的原因进行有效回溯;决策评价分析方法借鉴多目标决策理论,依托于前三个阶段的要素抽象和指标体系构建评价函数,通过评价函数获得态势感知结果,Dapoigny 提出的静态统计数据的快速计算方法[33],文献[58]中层次分析法的式(1)~(12),模糊评价法[88]的式(1)~(4),文献[91]中提出的平均攻击代价计算公式等都是此方法在网络安全态势感知方面的应用范畴. 公式分析法一般和阶段Ⅱ中的数学模型结合使用,同时也是本节中其他求解方法量化分析的基础,该方法的优点是可以直观形象的反应感知结果,计算复杂度在多项式内容易在大规模网络下推广,但是评价函数和相关参数的选择没有统一的标准具有很强的主观性,容易导致从要素指标集合 X 到感知结果集合 Y 的映射 $Y=F(X)$ 与实际情况偏差较大.

针对公式分析法的缺点,逻辑推理法逐渐成为了问题解决的突破口,其可以汇聚多源多属性的不确定信息,模拟人类的思维方式,智能性的获得评估结果,包括规则推理法、图模型推理法和模式识别法三种类型. 规则推理法由基于规则的专家系统发展而来,通过模仿专家在求解中的关联推理能力进行试探性的求解,在网络安全态势感知领域的研究中主要是和入侵检测系统相结合,提高入侵检测的效率或准确度,例如:鲍旭华等[122]人提出的针对复合攻击模检测的模型,Ilgun K 等[123]人提出的基于类别的主成分分析的有效参数选择方法,文献[124]提出的多功能仿真平台,文献[125]通过对底层警报的聚类和分类建立的基于本体的攻击知识模型,伏晓等[126]人提出的层次化入侵场景重构方法等;图模型推理分析法是目前探讨网络安全态势感知中相关要素关联关系的最有效方法之一,通过有向图的状态转换来包含逻辑关系、推理方法、概率计算等知识,攻击图模型[4,63,67,71]、贝叶斯模型[9,63,85,73]、马尔可夫模型[75,77]等都会用到此方法,此求解方法主要包括可达性分析和量化计算分析两个步骤:可达性分析主要说明当前网络系统或某一服务组件是否存在被攻击的可能性,包括攻击可达性和攻击路径等分析结果,图 9 是使用文献[4]中的分析方法对实验网络中内部开发服务器进行可达性分析的结果,可以看到①位于服务器 11 上的文件是存在被攻击的可能性的;②共存在 9 条攻击路径(图 9 中左 3 条,中 2 条,右 4 条),这些攻击路径可以分为 3 类(图 9 中左中右),量化计算分析在可达性分析的基础上,经过进一步量化计算提供相互比较的标准,如最大攻击概率[5,62,73]、最大攻击收益[64]、最小割集分析[59,60]等,下图 9 中每个节点内的数字是使用阶段Ⅲ中模型要素量化的方法对攻击收益[61]的取值结果,结合表 5 中的概率值,使用文献[62]中的最大可达概率计算算法,可知每一类攻击路径中的最大概率路径(图 9 中用虚线表示). 图模型推理的分析过程清晰,符合人类的逻辑思维易于理解,但也增加了推理的复杂度(如:图存储开销较大、不确定表示的合理性等),因此在大规模网络下的推广是此方法的最主要待突破点;随着机器学习的发展,模式识别求解方法用于求解要素指标集 X 和感知结果集合 Y 之间无法通过函数或逻辑推理来建立联系的感知过程,其以历史监测数据(同时包括要素数据和结果数据)作为训练样本确定态势模板,通过隐式的模式匹配进行态势评估,将此方法和入侵检测相结合对未知攻击检测等取得了一些进展[6,116],但该方法计算量大,对感知结果无法提供科学证据,离具体使用还有较大差距.

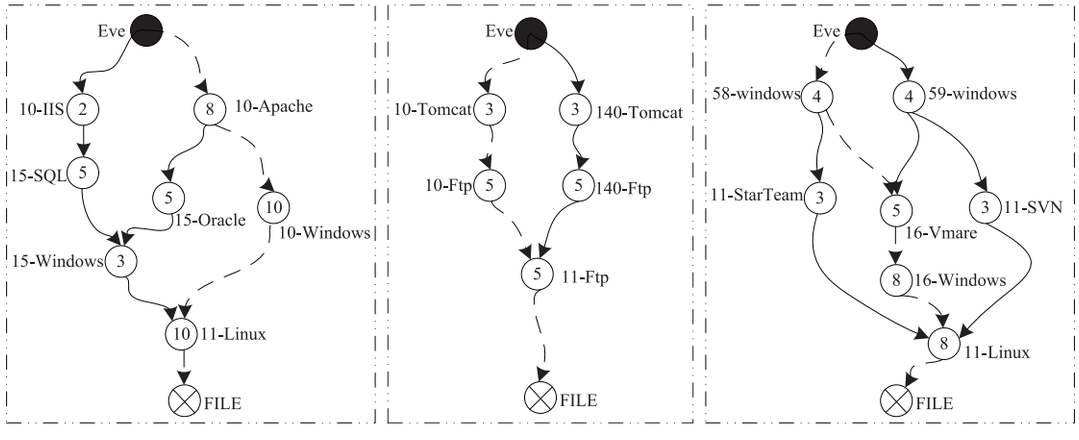


图9　实验网络图模型推理分析结果

公式分析法和逻辑推理法各有优缺点,还没有一个通用的求解方法可以解决目前所遇到的所有问题,因此,将各种求解方法的优点进行结合,试图用优势互补的方式对求解方式进行尝试,这就是信息融合分析法的初衷.一类是在求解方法基本不变的前提下,提供更多的数据源,通过数据的多样性及关联度获得更精准的感知结果,如:Bass[6]将异构分布式网络传感器的数据融入到入侵检测系统中,韦勇等人[66]将漏洞信息和服务信息通过 D-S 证据理论进行多源融合,文献[124]中对实时感知切片及其融合的方法进行了综合介绍;另一类是在输入的要素及度量值基本不变的前提下,进行求解算法的相互补充,如:Poolsappasit N 等人[9]将贝叶斯网络与攻击树/图中的定性因果分析法相结合,形成了多目标优化平台,文献[105]将模糊集中可信度的概念引入到 Petri 网模型中,并通过层次化方法进行综合评估,张勇等人[75]将 Markov 的无后效性分析和攻防博弈相结合,并提出了包含 3 个子算法的安全态势评估算法等.

7.2 验证与优化

在求解方法之后的环节是对前四个阶段进行验证,在文章中一般以实验的方式出现.验证工作主要分为两个部分:一是对模型抽象的有效性进行验证,二是对分析结果的合理性进行验证.模型抽象的有效性验证是判断网络要素及其关联的形式化表达和实验真实情况是否相吻合,同时验证是否能满足对应求解分析方法的需要;分析结果的合理性既包括对 7.1 节中求解方法的正确性进行验证,也包括验证求解分析的初步结果是否符合当前网络的真实安全状态.

验证是模型内实验结论和预期目标之间的比较,优化是模型间描述能力、求解效率或分析结果等方面的比较.有文献对形式化抽象环节有所改进,意图以更简洁的描述反应网络安全态势感知的关键要素,如:Ammann 等人[31]在对攻击图进行核心理念审视的基础上,提出了更简洁并可以扩展的模型,Hamid 等人[69]将 Take-Grant 保护模型与攻击图相结合,将图中节点粒度细化到了组件级,罗智勇等人[127]以底层数据为依托,构建分层攻击图来提高入侵意图检测的精度,通过博弈论刻画攻防双方的随机策略选择等;有文献针对求解算法层面进行优化,力求使分析结果更加精准或者降低算法复杂度以适应大规模网络,Poolsappasit N 等人[9]基于贝叶斯网络的风险管理框架,可以保证在资源受限的条件下获得更多的决策信息,吴迪等人[63]给出了一种基于攻击图的安全危险识别方法,文献[67]将最优弥补集问题转换为单一的加权碰集问题进行求解,并证明这样基于转换的分析方法有更好的性能,文献[62]的攻击图简化算法和最大可达概率算法可以更好的适应于大规模复杂网络,叶云等人[74]提出了大规模网络的攻击图自动构建算法等;也有文献针对形式化抽象和求解算法同时进行改进,以求获取更好的分析效果,此方面更多是第 5 节模型表示中的形式化方法和 7.1 节中的求解方法间的组合,如文献[9,85]将贝叶斯运算与攻击图相结合进行动态安全风险评估,Dietterich 等人[32]将机器学习的理论应用在了网络安全态势感知过程中,Petri 网与模糊集的结合应用[105],博弈论与 Markov 相结合[75],信息融合方法在网络安全态势方面的综合应用[6,33,66]等.

8 阶段Ⅴ:态势预测

按照本文第 3 节中网络安全态势感知运行机制的阶段划分,最后一个环节是态势预测阶段,其核心作用是在前四个阶段所得求解分析结果的基础上进行知识运用进而提升网络安全程度,形成反馈回路的过程.但大部分文献中针对此阶段的研究是缺失的,在简单实验网络或一些特殊情景下,求解分析结果可以直观的反应当前态势,分析结论也可以直接对应到防御决策措施上,在真实网络环境下从求解结果到态势判断再到决策措施的应用过程还有一定的距离,也需要有效方法论的支撑,不能将决策知识有效验证并形成反馈回路是目前大部分网络安全态势感知方法无法推广的主要原因之一,应引起重视.

8.1 结果可视化

如图 1 所示,网络安全态势感知运行机制中的前 4 个阶段,充分运用了理性思维和机器的计算优势,但无法充分利用人类的感知能力,将模型抽象或语言表述进行图形化,更能轻易的表述内在含义,增强认知效果,通过可视化图形呈现数据中隐含的信息和规律是信息可视化的主要作用也是研究重点[128].可视化分析是多研究领域交叉产生的新方向,这无疑与网络安全态势感知研究多学科融合现状有极大的相似点,目前的结合主要在,阶段二的模型表示之后或阶段四的求解分析之后两个点上开展.

在阶段二之后进行的主要是要素及其关系的可视化,简单的如本文中的图 5(a)、图 7 等都是实验网络模型化抽象后的直观图形表达结果,网络物理连接及逻辑连接的可视化[36~38]是所有分析方法的基础,Plan 等人[129]提出的可自建结构的时间可视化系统以及各类攻击图的图形化描述[62,71,94,95]都属于此范畴;分析结果的可视化在阶段四求解分析之后进行,通过图形化可以将关注点进行聚焦更易于理解,Tamassia[130]针对安全感知的可视化进行了基础的调查统计,本文中的图 9 是分析结果可视化的一个简明示例,尤其是在大规模网络的分析过程中,分析结果可视化可极大的提高分

析效率,图 10 中所示的是将攻击图的分析结果进行可视化约减后的效果.

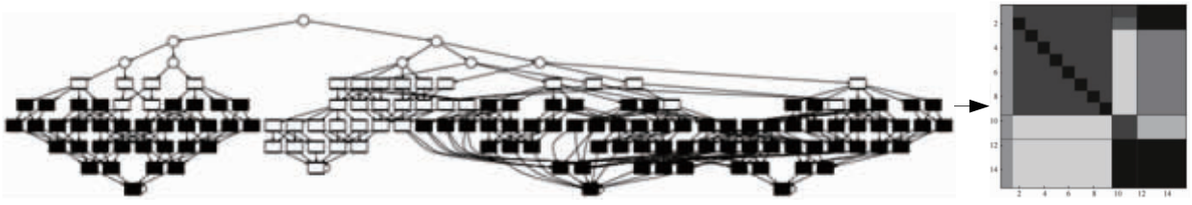


图10 攻击图形式化分析[94]与可视化简化[131]

图形化的表达是信息可视化的重要组成部分,但也是可视化的初级阶段,可视化不单单是信息被动挖掘的过程,更是人主观意识参与后的作用过程[128],针对可视化映射的人机交互过程,D' Amico 等人[44]采用认知任务分析创建了一个可视化框架,Erbacher R 等人[132]提出的框架可以允许网络管理人员在分析回路中进行人工参与,借助于参与者的独特专业知识来进行即时评估,也有文献将人工智能与可视化相结合[39],但这些文章大都停留在技术视角内[22],以有效的方法获取和开发人类内心的感知能力,对通用情景下的网络安全态势感知进行柔性分析还有很长的研究里程.

8.2 知识应用

通过前述几个阶段的有效分析,可以获得网络安全状态的感知结果,若结果内存在着潜在的威胁或者攻击,网络安全管理员就需要采取相应的防御措施来对目标网络进行安全加固,在本文图 1 所示的网络安全态势感知运行机制中称为感知知识的应用反馈回路过程. 显然完全将感知结果中的漏洞或者威胁因素消除是不现实的,这样基于感知分析结果的知识应用反馈过程就转化为了一个最优加固决策的选择问题. 目前针对此方面的研究主要分为关键目标最小代价加固、全网络最大收益加固和多目标安全加固三类.

基于关键目标最小代价加固的理念是以网络中重要的关键资产作为加固出发点,寻求以最小的代价来保证安全的方法. 大部分文献中都会在实例分析结束后给出保证关键目标不遭受损失的防御措施[9,63,94,95],以本文实验网络的分析结果(图 7,图 9)为基础,假设位于10.10.0.11内部开发服务器上的资料是关键目标,则加固目标 g 可以表示为

g = (10-Apache ∧ 10-Windows ∧ 10-Linux) ∨ (10-Tomact ∧ 10-Ftp ∧ 11-Ftp) ∨ (58-Windows ∧ 16-Vmare ∧ 16-Windows ∧ 11-Linux),

通过求解可以获得 36 种加固解 $\{D_i, D_j, D_k\}$,最小加固代价为

$$\min_{i,j,k}[Cost(D_i) + Cost(D_j) + Cost(D_k)]$$

其中 $D_i \in \{$10-Apache,10-Windows,10-Linux$\}$,

$D_j \in \{$10-Tomact,10-Ftp,11-Ftp$\}$,

$D_k \in \{$58-Windows,16-Vmare,16-Windows,11-Linux$\}$.

文献[76]在此基础上以网络初始条件逻辑表达式的组合来表示网络中的重要资产,从攻击源出发获得加固方案,Wang 等人[133]通过 Markov 模型量化脆弱性导致状态转移的概率关系,分析可能的攻击手段及对应的防御成本,提出了加固成本最小化的方案. 此方法从网络管理员的关注视角出发,可以以相对最小的代价保证核心资产不受损失,但此方法忽略了防御措施与其他正常访问间的相关性,容易导致部分其他未列为关键目标的资产或服务等不能正常响应.

全网络最大收益加固的关注点是在当前感知分析结果下如何保证网络整体达到最大的安全性. Steven Noel 等人[134]从网络的初始条件出发,通过计算逻辑表达式的真值来求解最大化地保障关键资产安全需要采取的安全措施,Sushil Jajodia 等人[135,136]从作为防御方的网络管理员的角度出发,着眼于企业网络的最大化安全防护,寻求最有效的防御措施来保证部署的安全措施的最大回报. 此方法可以在一定程度上保证网络安全效能的最大化,但完全以安全为出发点会导致实际应用中时间复杂度过大或为了安全而损失正常服务功能的问题.

多目标安全加固试图结合关键目标最小代价加固和全网络最大收益加固的优点,在保证网络关键目标和基础功能正常的前提下达到全网络的最大安全性. Frigault M 等人[137]和贝叶斯攻击图相结合,计算攻击过程中的攻击行为与防御报警指标间的概率关系,以安全指标为指导建立多组加固措施,并通过定量分析对不同加固措施进行比较,Rinku Dewri 等人[138]运用博弈的思想,通过多目标分析和竞争协同演化理论,构建了双方竞争的最优安全加固问题模型,在攻击决策和防御决策的共同进化中,确定安全控制措施保证在一定安全开销和功能正常的前提下求得最大安全回报. 该方法能够从不同角度考虑决策的应用效果,但该方法目标矩阵中的开销或回报主观因素过大,会导致知识应用反馈的客观性不足,而且在大规模网络的推广中,该方法在存储和计算上也会有很大的局限性.

9 结论

本文介绍了网络安全态势感知的基本概念和核心方法,突出了数据价值链角度的系统工程学感知框架.该框架由要素采集、模型表示、度量确立、求解分析和态势预测5个阶段构成.本文详细介绍了不同阶段的基本作用、主要方法及应用效果.在要素采集阶段,对感知数据进行了分类归纳,并对要素数据库的标准化设计与实现进行简要说明;在模型表示阶段,讨论了每一类模型的核心理念,代表性技术及建模结果;在度量确立阶段,按照模型要素量化和评价指标体系两个方面进行了说明;在求解分析阶段,讨论了典型求解算法的应用前提和分析结论,并对算法间进行了横向比较;在态势预测阶段,强调了知识应用反馈回路的重要性,讨论了分析结果可视化和防御措施选择的基本方法.最后对网络安全态势感知的研究方向进行了探讨和总结.

参考文献

[1] Miller B P. Fuzz-revisited:A re-examination of the reliability of UNIX utilities and services[J/OL]. ftp://grilled.cs.wisc.edu/technical_papers/fuzz-revisited.ps.Z,2001.

[2] Smaha S E. Haystack:an intrusion detection system[A]. Aerospace Computer Security Applications Conference[C]. US:IEEE,2002.37-44.

[3] Anderson J P. Computer security threat monitoring and surveillance[A]. James P Anderson Co Fort[C]. Washington,1980.26-32.

[4] Phillips C,Swiler L P. A graph-based system for network-vulnerability analysis[A]. The Workshop on New Security Paradigms[C]. US:IEEE,1998.71-79.

[5] Ritchey R W,Ammann P. Using model checking to analyze network vulnerabilities[A]. Proceedings of IEEE Symposium on Security and Privacy[C]. IEEE,2000.156-165.

[6] Bass T. Multisensor data fusion for next generation distributed intrusion detection systems[A]. Proceedings of the Iris National Symposium on Sensor & Data Fusion[C]. US:Hopkins University Applied Physics Laboratory,1999.24-27.

[7] Mcdermott J. Attack-potential-based survivability modeling for high-consequence systems[A]. IEEE International Workshop on Information Assurance[C]. US:IEEE Computer Society,2005.119-130.

[8] Wang Yuanzhuo,Lin Chuang,Cheng Xueqi,et al. Analysis for network attack-defense based on stochastic game model[J]. Chinese Journal of Computers,2010,33(33):1748-1762.

[9] Poolsappasit N,Dewri R,Ray I. Dynamic security risk management using Bayesian attack graphs[J]. Dependable and Secure Computing,2012,9(1):61-74.

[10] Theureau J. Nuclear reactor control room simulators:human factors research and development[J]. Cognition Technology & Work,2000,2(2):97-105.

[11] Endsley M R. Design and evaluation for situation awareness enhancement[J]. Proceedings of the Human Factors & Ergonomics Society Annual Meeting,1988,32(1):97-101.

[12] Endsley M R. Toward a theory of situation awareness in dynamic systems[J]. Human Factors,1995,37(1):32-64.

[13] Endsley M R,Garland D J. Situation Awareness:Analysis and Measurement[M]. Lawrence Erlbaum Associates,2000.1740-1741.

[14] Tadda G P,Salerno J S. Overview of Cyber Situation Awareness. Cyber Situational Awareness[M]. Springer US,2010.15-35.

[15] Kopylec J,D'Amico A,Goodall J. Visualizing Cascading Failures in Critical Cyber Infrastructures. Critical Infrastructure Protection[M]. US:Springer,2007.351-364.

[16] Goodall J R. Introduction to Visualization for Computer Security[A]. The Workshop on Vizsec[C]. DBLP,2008.1-17.

[17] Jajodia S,Liu P,Swarup V,et al. Cyber Situational Awareness[M]. Springer US,2010.132(2):1-4.

[18] Giacobe N A. Application of the JDL data fusion process model for cyber security[J]. Proc Spie,2010,7710(5):1-10.

[19] Klein G,Tolle J,Martini P. From detection to reaction-A holistic approach to cyber defense[A]. Defense Science Research Conference and Expo[C]. US:IEEE,2011.1-4.

[20] Schreiber-Ehle S,Koch W. The JDL model of data fusion applied to cyber defense-A review paper[A]. Sensor Data Fusion:Trends,Solutions,Applications[C]. US:IEEE,2012.116-119.

[21] Manuel Cheminod,Luca Durante,Adriano Valenzano. Review of Security Issues in Industrial Networks[J]. IEEE Transactions on Industrial Informatics,2013,9(1):277-293.

[22] Franke U,Brynielsson J. Cyber situational awareness-A systematic review of the literature[J]. Computers & Security,2014,46:18-31.

[23] Lenders V,Tanner A,Blarer A. Gaining an edge in cyberspace with advanced situational awareness[J]. IEEE Security & Privacy,2015,13(2):65-74.

[24] Mukherjee B,Heberlein L T. Network Intrusion Detection[M]. US:IEEE Network,1994.26-41.

[25] Stevens-Adams S, Carbajal A, Silva A, et al. Enhanced Training for Cyber Situational Awareness. Foundations of Augmented Cognition[M]. Berlin Heidelberg: Springer, 2013. 90 – 99.

[26] Roschke S, Cheng F, Meinel C. High-quality attack graph-based IDS correlation[J]. Logic Journal of the Igpl, 2013, 21(4): 571 – 591.

[27] Liang X, Xiao Y. Gametheory for network security[J]. IEEE Communications Surveys & Tutorials, 2013, 15(1): 472 – 486.

[28] Sanfilippo F. A multi-sensor fusion framework for improving situational awareness in demanding maritime training[J]. Reliability Engineering & System Safety, 2017, 161: 12 – 24.

[29] Adhikari U, Morris T H, Dahal N, et al. Development of power system test bed for data mining of synchrophasors data, cyber-attack and relay testing in RTDS[A]. Power and Energy Society General Meeting[C]. US: IEEE, 2012. 1 – 7.

[30] Hinman M L. Some computational approaches for situation assessment and impact assessment[A]. International Conference on Information Fusion[C]. US: IEEE, 2002. 687 – 693.

[31] Ammann P, Wijesekera D, Kaushik S. Scalable, graph-based network vulnerability analysis[A]. ACM Conference on Computer and Communications Security 2002[C]. Washington DC: DBLP, 2002. 217 – 224.

[32] Dietterich T G, Bao X, Keiser V, et al. Machine Learning Methods for High Level Cyber Situation Awareness. Cyber Situational Awareness[M]. US: Springer, 2010. 227 – 247.

[33] Dapoigny, Richard, Barlatier, et al. Formal foundations for situation awareness based on dependent type theory[J]. Information Fusion, 2013, 14(1): 87 – 107.

[34] Paffenroth R, Toit P D, Nong R, et al. Space-time signal processing for distributed pattern detection in sensor networks[J]. IEEE Journal of Selected Topics in Signal Processing, 2013, 7(1): 38 – 49.

[35] Mathews M L, Halvorsen P, Joshi A, et al. A collaborative approach to situational awareness for cybersecurity[A]. International Conference on Collaborative Computing: Networking, Applications and Worksharing[C]. US: IEEE, 2012. 216 – 222.

[36] Bearavolu R, Lakkaraju K, Yurcik W. NVisionIP: An animated state analysis tool for visualizing netFlows[EB/OL]. http://www. cert. org/flocon/2005/presentations/NVisionIPFlocon2005. pdf, 2005.

[37] Yin X, Yurcik W, Slagell A. The design of VisFlowConnect-IP: A link analysis system for IP security situational awareness[A]. IEEE International Workshop on Information Assurance[C]. US: IEEE, 2005. 141 – 153.

[38] Zhenmin Li, Jed Taylor, Elizabeth Partridge, et al. UCLog: A unified, correlated logging architecture for intrusion detection[J]. Telecommunication Systems – TELSYS, 2004. 12 – 27.

[39] Ross K J, Hopkinson K M, Pachter M. Using a distributed agent-based communication enabled special protection system to enhance smart grid security[J]. IEEE Transactions on Smart Grid, 2013, 4(2): 1216 – 1224.

[40] Giles K, Hagestad W. Divided by a common language: Cyber definitions in Chinese, Russian and English[A]. International Conference on Cyber Conflict[C]. US: IEEE, 2013. 1 – 17.

[41] Adam Doupé, Egele M, Caillat B, et al. Hit 'em where it hurts: a live security exercise on cyber situational awareness[A]. Twenty-Seventh Computer Security Applications Conference[C]. Orlando, Fl, USA: DBLP, 2011. 51 – 61.

[42] Fink G, Best D, Manz D, et al. Gamification for Measuring Cyber Security Situational Awareness. Foundations of Augmented Cognition[M]. Berlin Heidelberg: Springer, 2013. 656 – 665.

[43] Klein G, Günther H, Träber S. Modularizing cyber defense situational awareness – Technical integration before human understanding[J]. Communications in Computer & Information Science, 2012, 318: 307 – 310.

[44] D'Amico A, Whitley K. The real work of computer network defense analysts[A]. The Workshop on Vizsec[C]. US: DBLP, 2008. 19 – 37.

[45] Erbacher R F, Frincke D A, Wong P C, et al. A multi-phase network situational awareness cognitive task analysis[J]. Information Visualization, 2010, 9(3): 204 – 219.

[46] Ralston P A, Graham J H, Hieb J L. Cyber security risk assessment for SCADA and DCS networks[J]. Isa Transactions, 2007, 46(4): 583 – 594.

[47] Kirillov I A, Metcherin S A, Klimenko S V. Metamodel of shared situation awareness for resilience management of built environment[A]. International Conference on Cyberworlds[C]. US: IEEE, 2012. 137 – 143.

[48] Adams K, Wassell A, Ceruti M G, et al. Emergency-management situational-awareness prototype (EMSAP)[A]. IEEE First International Multi-disciplinary Conference on Cognitive Methods in Situation Awareness & Decision Support[C]. US: IEEE, 2011. 110 – 114.

[49] Liu XW, Wang HQ, Lü HW, Yu JG, Zhang SW. Fusion-based cognitive awareness-control model for network security situation[J]. Journal of Software, 2016, 27(8): 2099 – 2114. (in Chinese)

[50] Gong J, Zang XD, Su Q, Hu XY, Xu J. Survey of network security situation awareness [J]. Journal of Software, 2017, 28(4): 1010 – 1026. (in Chinese)

[51] Shen Changxiang, Zhang Huanguo, Feng Dengguo, Cao Zhenfu, Huang Jiwu. Overview of information security [J]. SCIENCE IN CHINA Ser E Information Sciences, 2007, 37(2): 129 – 150. (in Chinese)

[52] Liu J, Su P, Yang M, He L, Zhang Y, Zhu XY, Lin H. Software and Cyber Security-A Survey [J]. Journal of Software, 2018, 29(1): 42 – 68. (in Chinese)

[53] Jian-chun Jiang, Heng-tai Ma, Dang-en Ren, Si-han Qing. A survey of intrusion detection research on network security[J]. Journal of Software, 2000, 11(11): 1460 – 1466. (in Chinese)

[54] Ying-xu LAI, Zeng-hui LIU, Xiao-tian CAI, Kai-xiang YANG. Research on intrusion detection of industrial control system [J]. Journal of Communications, 2017, 38(2): 143 – 156. (in Chinese)

[55] Lin Chuang, Wang Yang, Li Quanlin. Stochastic modeling and evaluation for network security[J]. Chinese Journal of Computers, 2005, 28(12): 1943 – 1956. (in Chinese)

[56] Wang HQ, Lai JB, Zhu L, Liang Y. Survey of network situation awareness system [J]. Journal of Computer Science, 2006, 33(10): 5 – 10. (in Chinese)

[57] Gong ZH, Zhuo Y. Research on cyberspace situational awareness[J]. Journal of Software, 2010, 21(7): 1605 – 1619. (in Chinese)

[58] Chen XZ, Zheng QH, Guan XH, Lin CG. Quantitative hierarchical threat evaluation model for network security [J]. Journal of Software, 2006, 17(4): 885 – 897. (in Chinese)

[59] HU Hao, YE Run-guo, ZHANG Hong-qi, YANG Ying-jie, LIU Yu-ling. Quantitative method for network security situation based on attack prediction[J]. Journal on Communications, 2017, 38(10): 122 – 134. (in Chinese)

[60] Lei Kenan, Zhang Yuqing, Wu Chensi, Ma Hua. A system for scoring the exploitability of vulnerability based types [J]. Journal of Computer Research and Development, 2017, 54(10): 2296 – 2309. (in Chinese)

[61] Jiang Wei, Fang Bin-Xing, Zhang Hong-Li. Evaluating network security and optimal active defense based on attack-defense game model[J]. Chinese Journal of Computers, 2009, 4(1): 817 – 827. (in Chinese)

[62] Ye Yun, Xu Xi-shan, Jia Yan. An attack graph based probabilistic computing approach of network security[J]. Chinese Journal of Computers, 2010, 33(10): 1987 – 1996. (in Chinese)

[63] Di Wu, Yi-feng Lian, Kai Chen, Yu-ling Liu. A security threats identification and analysis method based on attack graph[J]. Chinese Journal of Computers, 2012, 35(9): 1938 – 1950. (in Chinese)

[64] Zhang YZ, Fang BX, Chi Y, Yun XC. Risk propagation model for assessing network information systems [J]. Journal of Software, 2007, 18(1): 137 – 145. (in Chinese)

[65] Tang Chenghua, Liu Pengcheng, Tang Shensheng, Xie Yi. Anomaly intrusion behavior detection based on fuzzy clustering and features selection[J]. Journal of Computer Research and Development, 2015, 52(3): 718 – 728. (in Chinese)

[66] Wei Yong, Lian Yifeng, Feng Dengguo. A network security situational awareness model based on information fusion [J]. Journal of Computer Research and Development, 2009, 46(3): 353 – 362. (in Chinese)

[67] YAN Feng, LIU Shu-fen, LENG Huang. Study on analysis of attack graphs based on conversion[J]. Acta Electronica Sinica, 2014, 42(12): 2477 – 2480. (in Chinese)

[68] Ma Chunguang, Wang Chenghong, Zhang Donghong, Li Yingtao. A dynamic network risk assessment model based on attacker's inclination [J]. Journal of Computer Research and Development, 2015, 52(9): 2056 – 2068. (in Chinese)

[69] Shahriari H R, Jalili R. Vulnerability take grant (VTG): An efficient approach to analyze network vulnerabilities [J]. Computers & Security, 2007, 26(5): 349 – 360.

[70] Tianfield H. Cybersecurity situational awareness [A]. IEEE International Conference on Internet of Things [C]. IEEE, 2017. 782 – 787.

[71] CHEN Xiao-Jun, FANG Bin-Xing, TAN Qing-Feng, ZHANG Hao-Liang. Inferring attack intent of malicious insider based on probabilistic attack graph model [J]. Chinese Journal of Computers, 2014, 37(1): 62 – 72. (in Chinese)

[72] Cisco. OpenSOC: Big data security analytics framework [EB/OL]. http://opensoc.github.io/, 2017-03-20.

[73] Zhang SJ, Li JH, Song SS, Li L, Chen XZ. Using Bayesian inference for computing attack graph node beliefs[J]. Journal of Software, 2010, 21(9): 2376 – 2386. (in Chinese)

[74] Ye Yun, Xu Xishan, Qi Zhichang, et al. Attack graph generation algorithm for large-scale network system[J]. Journal of Computer Research and Development, 2013, 10: 2033 – 2139. (in Chinese)

[75] Zhang Y, Tan XB, Cui XL, Xi HS. Network security situation awareness approach based on Markov game model [J]. Journal of Software, 2011, 22(3): 495 – 508. (in Chinese)

[76] Wang Lingyu, Noel S, Jajodia S. Minimum cost network

hardening using attack graphs[J]. Computer Communications,2006,29(18):3812 – 3824.

[77] Feng Xuewei, Wang Dongxia, Huang Minhuan, Li Jin. A mining approach for causal knowledge in alert correlating based on the Markov property[J]. Journal of Computer Research and Development, 2014, 51(11):2493 – 2504. (in Chinese)

[78] Wang Jinrong, Fang Dingyi, Chen Xiaojiang, Wang Huaijun, He Lu. Taxonomy of software attack technique oriented to automated modeling[J]. Journal of Sichuan University:Engineer Science Edition, 2015, 47(Z1):91 – 98. (in Chinese)

[79] J Christy. Cyber threat & legal issues[A]. Shadowcon Conference[C]. USA:1999. 29 – 50.

[80] CVSS. Common Vulnerability Scoring System[EB/OL]. http://nvd. nist. gov/cvss. cfm, 2008-01-01.

[81] HUANG Jia-Hui, FENG Dong-Qin, WANG Hong-Jian. A method for quantifying vulnerability of industrial control system based on attack graph[J]. Acta Automatica Sinica, 2016, 42(5):792 – 798.

[82] WANG Yufei, GAO Kunlun, ZHAO Ting, QIU Jian. Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph[J]. Proceedings of the CSEE, 2016, 36(6):1490 – 1499.

[83] LI Min-zheng, LAN Jian-ping. Smart home intrusion detection algorithm based on spatial-temporal field information fusion[J]. Journal of Beijing University of Posts & Telecommunications, 2017, 40(3):76 – 84.

[84] Wang Yichuan, Ma Jianfeng, Lu Di, Zhang Liumei, Meng Xianjia. Game optimization for internal DDoS attack detection in cloud computing[J]. Journal of Computer Research and Development, 2015, 52(8):1873 – 1882. (in Chinese)

[85] Ni Gao, Ling Gao, Yue-yi He. Dynamic security risk assessment model based on Bayesian attack graph[J]. Journal of Sichuan University: Engineering Science Edition, 2016, 48(1):111 – 118. (in Chinese)

[86] Wang L, Wang B, Peng Y. Research the information security risk assessment technique based on Bayesian network [A]. International Conference on Advanced Computer Theory and Engineering[C]. US:IEEE, 2010. 600 – 604.

[87] Liao Y T, Ma C B, Zhang C. A new fuzzy risk assessment method for the network security based on fuzzy similarity measure[A]. The 6th World Congress on Intelligent Control and Automation[C]. US:IEEE, 2006. 8486 – 8490.

[88] Chen T P, Zhang X Y, Zheng L Q. Network security risk assessment based on fuzzy integrated judgment[J]. Journal of Naval University of Engineering, 2009:38 – 41.

[89] Zhao L, Xue Z. Synthetic security assessment based on variable consistency dominance-based rough set approach [J]. High Technology Letters, 2010, 16(4):413 – 421.

[90] Kong L S, Ren X F, Fan Y J. Study on assessment method for computer network security based on rough set[A]. IEEE International Conference on Intelligent Computing and Intelligent Systems[C]. US:IEEE, 2009. 617 – 621.

[91] Feng PH, Lian YF, Dai YX, Bao XH. A vulnerability model of distributed systems based on reliability theory [J]. Journal of Software, 2006, 17(7):1633 – 1640. (in Chinese)

[92] Li Yan, Huang Guangqiu, Cao Lixia. The probability controllability of complex network via attack[J]. Journal of Frontiers of Computer Science & Technology, 2016, 10(10):1407 – 1419.

[93] Scheier B. Attack trees:modeling security threats[J]. Dr Dobb's Journal, 1999, 12(24):21 – 29.

[94] Sheyner O, Haines J, Jha S. Automated generation and analysis of attack graphs[A]. Proceedings of the IEEE Symposium on Security and Privacy[C]. Oakland:IEEE Computer Society Press, 2002. 273 – 284.

[95] Swiler LP, Phillips C, Ellis D, Chakerian S. Computer attack graph generation tool[A]. Proceedings of the DARPA Information Survivability Conference and Exposition II[C]. Anaheim, CA, 2001. 307 – 321.

[96] Ingols K, Chu M, Lippmann R, Webster S, Boyer S. Modeling modern network attacks and counter measures using attack graphs[A]. Proceedings of the 25th Annual Computer Security Applications Conference[C]. Honolulu, Hawaii, USA, 2009. 117 – 126.

[97] Liu Weixin, Zeng Kangfeng, Wu Bin. Alert processing based on attack graph and multi-source analyzing[J]. Journal on Communications, 2015, 36(9):135 – 144. (in Chinese)

[98] Dacier M. Towards Quantitative Evaluation of Computer Security[D]. Institut National Polytechnique de Toulouse, France, 1994.

[99] Ortalo R, Deswarte Y, Kaaniche M. Experimenting with quantitative evaluation tools for monitoring operational security[J]. IEEE Transactions on Software Engineering, 1999, 25(5):633 – 650.

[100] Porras P A, Kemmerer R. A penetration state transition analysis:a rule-based intrusion detection approach[A]. Proceedings of the Eighth Annual Computer Security Applications Conference[C]. US: IEEE, 1992. 220 – 229.

[101] Stevens F, Courtney T, Singh S, Agbaria A, Meyer JF, Sanders WH, Pal P. Model-based validation of an intrusion-tolerant information system[A]. Proceedings of

23rd Symposium on Reliable Distributed Systems(SRDS 2004)[C]. Florianópolis, Brazil, 2004. 184 – 194.

[102] Madan B, Go eva-Popstojanova K, Vaidyanathan K, Trivedi KS. A method for modeling and quantifying the security attributes of intrusion tolerant systems[J]. Performance Evaluation, 2004, 56(1 – 4): 167 – 186.

[103] Gao Xiang, Zhu Yue-fei, Liu Sheng-li. Attack composition model based on generalized stochastic colored Petri nets[J]. Journal of Electronics & Information Technology, 2013, 35(11): 2608 – 2614. (in Chinese)

[104] LIN Chuang, WANG Yuan-zhuo, YANG Yang, QU Yang. Research on network dependability analysis methods based on stochastic Petri net[J]. Acta Electronica Sinica, 2006, 34(2): 322 – 332. (in Chinese)

[105] GAO Xiang, ZHU Yue-fei, LIU Sheng-li, FEI Jin-long, LIU Long. Risk assessment model based on fuzzy Petri nets[J]. Journal on Communications, 2013, (s1): 126 – 132. (in Chinese)

[106] ANDERSON R. Why information security is hard-an economic perspective[A]. Proceedings of 17th Annual Computer Security Application Conference[C]. Washington, DC, USA: IEEE Computer Society, 2001. 39 – 40.

[107] REDDY Y B. A game theory approach to detect malicious nodes in wireless sensor networks[A]. 3rd International Conference on Sensor Technologies and Application[C]. Washington, DC: IEEE Computer Society, 2009. 462 – 468.

[108] SHEN S G, LI Y J, XU H Y. Signaling game based strategy of intrusion detection in wireless sensor networks [J]. Computers & Mathematics with Applications, 2011, 62(6): 2404 – 2416.

[109] Jia Chunfu, Zhong Anming, Zhang Wei, Ma Yong. Incomplete informational and dynamic game model in network security[J]. Journal of Computer Research and Development, 2006, 43(s2): 530 – 533. (in Chinese)

[110] ZHU Jian-ming, SONG Biao, HUANG Qi-fa. Evolution game model of offense-defense for network security based on system dynamics[J]. Journal on Communications, 2014, 35(1): 54 – 61. (in Chinese)

[111] Ran J X, Xiao B. Risk evaluation of network security based on NLPCA – RBF neural network[A]. International Conference on Multimedia Information Networking and Security[C]. US: IEEE, 2010. 398 – 402.

[112] Liang Y, Wang H Q, Lai J B. Quantification of network security situational awareness based on evolutionary neural network[A]. The 6th International Conference on Machine Learning and Cybernetics[C]. US: IEEE, 2007. 3267 – 3272.

[113] Wang G, Hao J, Ma J, et al. A new approach to intrusion detection using artificial neural networks and fuzzy clustering[J]. Expert Systems with Applications, 2010, 37(9): 6225 – 6232.

[114] Gao Ni, Gao Ling, He Yiyue. A lightweight intrusion detection model based on autoencoder network with feature reduction[J]. Acta Electronica Sinica, 2017, 45(3): 730 – 739. (in Chinese)

[115] S A Hofmeyr, S Forrest. Architecture for an artificial immune system[J]. Evolutionary Computation, 2000, 7(1): 45 – 68.

[116] J Kim, J B Peter. Towards network intrusion detection: artificial immune system for investigation of dynamic clone selection[A]. Proceedings of the World Congress on Computational Intelligence[C]. Piscataway: IEEE Press, 2002. 1015 – 1020.

[117] Li Tao. Network security risk detection based on immune [J]. SCIENCE IN CHINA Ser E Information Sciences, 2005, 35(8): 798 – 816.

[118] Li Tao. An immune based model for network monitoring [J]. Chinese Journal of Computers, 2006, 29(9): 1515 – 1522.

[119] Fangfang Dai, Kangfeng Zheng, Shoushan Luo, Bin Wu. Towards a multi objective framework for evaluating network security under exploit attacks[A]. Proc of 2015 IEEE International Conference on Communications[C]. New York: IEEE Press, 2015. 8814 – 8819.

[120] Zhang J, Liu F, Han W, et al. Research and implement of configurable network security index system[A]. International Conference on Applied Robotics for the Power Industry[C]. US: IEEE, 2012. 645 – 648.

[121] Zhang Y Z, Yun X C. Network operation security index classification model with multidimensional attributes [J]. Chinese Journal of Computers, 2012, 35(8): 1666 – 1674. (in Chinese)

[122] Bao XH, Dai YX, Feng PH, Zhu PF, Wei J. A detection and forecast algorithm for multi-step attack based on intrusion intention[J]. Journal of Software, 2005, 16(12): 2132 – 2138. (in Chinese)

[123] Ilgun K, Kemmerer RA, Porras PA. State transition analysis: A rule-based intrusion detection approach[J]. IEEE Trans on Software Engineering, 1995, 21(3): 181 – 199.

[124] Shifflet J. A technique independent fusion model for network intrusion detection[A]. Proceedings of the Midstates Conference on Undergraduate Research in Computer Science and Mathematics[C]. IEEE, 2005, 3(1): 13 – 19.

[125] REN Wei-wu, HU Liang, ZHAO Kuo. Intrusion alert correlation model based on data mining and ontology

[J]. Journal of Jilin University (Engineering Science), 2015,45(3):899 – 906.

[126] Fu X, Shi J, Xie L. Layered intrusion scenario reconstruction method for automated evidence analysis[J]. Journal of Software, 2011, 22(5): 996 – 1008. (in Chinese)

[127] LUO Zhi-yong, YOU Bo, XU Jia-zhong, LIANG Yong. Automatic recognition model of intrusive intention based on three layers attack graph[J]. Journal of Jilin University (Engineering Science), 2014, 44(5): 1392 – 1397.

[128] Keim D, Konlhammer J, Ellis G, Mansmann F. Mastering the information age: Solving problems with visual analytics[J]. Goslar: Eruographics Association, 2010. 1 – 168.

[129] Phan D, Gerth J, Lee M, Paepcke A, Winograd T. Visual analysis of network flow data with timelines and event plots[A]. Viz SEC 2007[C]. GER: Springer, 2008. 85 – 99.

[130] Tamassia R, Palazzi B, Papamanthou C. Graph drawing for security visualization[A]. Graph Drawing[C]. GER: Springer, 2009. 2 – 13.

[131] YE Yun, XU Xi-shan, JIA Yan, QI Zhi-chang, CHENG Wen-cong. Research on the risk adjacency matrix based on attack graphs[J]. Journal on Communications, 2011, 32(5): 112 – 120.

[132] Erbacher R. Visualization design for immediate high-level situational assessment[A]. ACM International Conference Proceeding Series[C]. US: IEEE, 2012. 17 – 24.

[133] Wang Shuzhen, Zhang Zonghua, Youki Kadobayashi. Exploring attack graph for cost-benefit security hardening[J]. Computers & Security, 2013, 32: 158 – 169.

[134] Steven Noel, Sushil Jajodia, O'Berry B, et al. Efficient minimum-cost network hardening via exploit dependency graphs[A]. Proc of the 2003 Annual Computer Security Applications Conference[C]. New Jersey: IEEE Press, 2003. 86 – 95.

[135] Sushil Jajodia, Steven Noel. Topological vulnerability analysis: a powerful new approach for network attack prevention, detection, and response[J]. Algorithms, Architectures and Information Systems Security, Indian Institute Platium Jubilee Series, 2009: 285 – 305.

[136] Ingols K, Chu M, Lippmann R, et al. Modeling modern network attacks and countermeasures using attack graphs[A]. Proc of the 2009 Annual Computer Security Applications Conference[C]. New Jersey: IEEE Press, 2009. 117 – 126.

[137] Frigault M, Wang L Y, Singhal A, Jajodia S. Measuring network security using dynamic Bayesian network[A]. Proceedings of the 4th ACM Workshop on Quality of Protection[C]. US: IEEE, 2008. 23 – 30.

[138] Rinku Dewri, Indrajit Ray, Nayot Poolsappasit, et al. Optimal security hardening on attack tree models of networks: a cost-benefit analysis[J]. International Journal of Information Security, 2012, 11(3): 167 – 188.

作者简介

李　艳　男,1984 年生,河北承德人,蒙古族,CCF 会员,博士,副教授,研究方向为:信息对抗、网络安全.
E-mail:sy_liyan137@126.com

王纯子　女,1983 年生,陕西西安人,汉族,博士,副教授,研究方向为:网络安全.

黄光球　男,1964 年生,湖南桃源人,汉族,博士,教授,研究方向为:网络安全、复杂系统建模、分析与控制、系统工程.