Computer Science and Application 计算机科学与应用, 2015, 5, 18-24
Published Online January 2015 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2015.51003

Hans汉斯

Survey on Technology of Network Security Assessment

Meng Zhao, Yubo Tan

Department of Computer Science and Engineering, Henan University of Technology, Zhengzhou Henan
Email: 632370440@qq.com, benentan@163.com

Received: Jan. 27th, 2015; accepted: Feb. 10th, 2015; published: Feb. 16th, 2015

Abstract

With the rapid development of Internet and information technology, the network has been deeply integrated into our lives. However, the rich services and applications of the Internet bring more security problems. Technology of network security assessment is a strategy to deal with the problems of network security at present. The basic concepts and research significance are shed light on. This paper described the architecture of network security assessment, and analyzed the research status mainly focusing on the method based on mathematical model, the method based on knowledge reasoning and the method based on pattern recognition. Then the advantages and disadvantages were pointed out respectively. Finally, some future research directions were given at the end.

Keywords

Internet, Information Technology, Network Security, Network Security Assessment

网络安全评估技术综述

赵　孟，谭玉波

河南工业大学信息科学与工程学院，河南　郑州
Email: 632370440@qq.com, benentan@163.com

收稿日期：2015年1月27日；录用日期：2015年2月10日；发布日期：2015年2月16日

摘　要

互联网和信息技术的快速发展，使网络深深的融入到人们的生活中。然而，丰富的互联网服务应用也带来了更多的网络安全问题，网络安全评估技术是当前处理网络安全问题的一种策略。在阐述网络安全评估技术的基本概念、研究意义的基础上，给出了网络安全评估的体系结构，主要从基于数学模型的方法、基于知识推理的方法和基于模式识别的方法三方面分析其研究现状，讨论现有的技术的优势和不足，并探讨了未来的发展方向。

关键词

互联网，信息技术，网络安全，网络安全评估

1. 引言

随着互联网和信息技术的快速发展，计算机网络给人们的生产、生活、学习的方式带来了巨大变化，但是计算机网络就像一把双刃剑，给我们带来方便的同时，也给我们带来了一系列的问题，网络安全是其中一个比较严重且对我们危害极大的问题。从计算机发展之初到现在，网络安全问题始终伴随着计算机的发展。为了最大程度的保证网络的安全，不断检查、修复操作系统的漏洞，不断提高设备的安全性能，在设计、开发应用程序时，尽量设计的完整严谨，努力制定全面、完善的网络管理规范，加强网络管理的科学性与专业性，始终把网络安全放在重要的位置上，尽管如此，世界范围内每年仍然存在大量的网络安全事件。网络安全评估就是在这样的形势下出现的一种新的应对网络安全问题的策略。网络安全评估技术[1]是一种主动防御技术，在安全事件没有发生时主动分析和评估自身存在的安全风险和安全隐患，从而能够未雨绸缪，防范于未然；在安全事件发生时及时分析和评估安全事件的威胁态势状况，并根据评估结果采取适当的风险控制措施，从而能够及遏制威胁的蔓延。

2. 网络安全评估技术

2.1. 基本概念

1) 脆弱性：脆弱性[2]是系统本身的一组特性，而攻击者利用这些特性通过已授权的方式获得对系统上的资源的未授权访问，或对系统造成的不良影响。

2) 攻击概率：是指攻击发生的可能性的大小。攻击概率反映了网络或信息系统现在的安全状况，并预测了可能会发生的安全事件，是计算风险值的基础。

3) 风险值：风险值是指网络或信息系统面临的威胁以及威胁利用脆弱性对资产造成的影响。

4) 网络态势：是指由于各种网络设备运行状况、网络行为以及用户行为等因素所构成的整个网络的当前状态和变化趋势。

5) 网络态势感知：网络态势感知[3]是指在网络环境中，能对引起网络态势发生变化的安全要素进行获取、理解、评估、显示以及对未来发展趋势的预测。

6) 网络态势因子：态势因子是指能够引起网络态势发生变化的重要因素。

2.2. 网络安全评估技术的研究意义

为了应对日益突出的网络安全问题，学术界和工业界提出各种安全防御技术和方法。在应对网络安全问题的初级研究阶段，学术界和工业界普遍认为网络安全问题的出现主要是系统设计上存在漏洞，所

以试图通过改进系统细节和增加协议的复杂度，设计出绝对安全的网络系统来杜绝网络安全事件的发生，但是后来大家发现这是不切实际的。到中期研究阶段，提出了入侵检测系统和安全备份恢复技术，希望在攻击发生时能够迅速地发现攻击并及时采取相应的措施进行控制和制止，以及系统在被攻破后能够有效的进行恢复。到当前研究阶段，学术界和工业界认为在致力于设计出更加安全的系统的同时，还应该提高系统的攻击识别能力和系统恢复能力，应该加强对当前系统的扫描检测，针对网络和信息系统进行风险评估，并根据结果进行风险控制。

网络安全评估技术就是主动的防御技术，在设计出绝对安全的系统之前，加强系统本身的防御能力仍是应对网络安全最有效的方式，网络安全评估的意义[1]表现在：

1) 了解当前网络和信息系统所面临的安全风险状况和安全威胁；

2) 对网络和信息系统可能遭受的攻击的可能性进行预测，或者对网络和信息系统已经遭受的攻击所引起的网络威胁进行预测；

3) 安全评估的结果可以为系统管理者提供需要采取的防御措施或者处理意见。

3. 网络安全评估体系结构

网络安全评估系统主要是对网络和信息系统的态势感知，在现有的网络安全基础设施以及技术的基础上，借鉴态势感知的成熟理论和技术并将其应用于网络安全的管理领域，在复杂多变的网络安全环境中，准确的提取特征信息，并进行关联分析，使其能够表示网络的宏观、整体状态，从而加强对网络的管理和控制，提高网络管理员对网络的管理能力。

3.1. 网络安全评估内容

网络态势感知的原始信息主要来源于各种网络安全设备、网络管理设备和网络监控设备。网络态势感知通过对收集到的数据进行处理来判断网络的安全状况，反映网络和信息系统的安全变化趋势等。具体而言网络安全评估[3]主要包括以下几个方面：

1) 原始网络安全事件的搜集和预处理。将现有网络安全设备、网络管理设备和网络监控设备等产生的复杂、海量、冗余、异构的数据采集上来进行预处理，提取数据的特征信息，并进行简化及存储，为后面的数据分析和将来的数据审计提供数据基础。

2) 网络事件的关联和归并。基于预处理后的数据进行网络安全事件挖掘，从而从宏观角度去挖掘一些一般的网络安全设备所检测不到的网络攻击事件，提高网络安全检测的准确率，进一步降低漏报率。

3) 网络安全态势评估。网络安全态势评估主要是利用相应的数学评估方法对网络安全态势的指标进行量化计算，利用这个值来反映网络或信息系统某个时间段的安全状态。网络安全态势评估的要求是快速、客观、准确的反映网络的实际安全情况，能够让网络管理员及时准确地掌握网络安全动态，及时做出有效的防范。

4) 网络安全态势预测。网络安全态势预测是在网络态势评估的基础上，对未来网络安全态势的发展趋势进行预测，从而帮助管理员未雨绸缪，提前做好网络的安全防护工作，降低网络安全事件所带来的潜在损失。

5) 网络安全态势展示。网络安全态势展示是网络安全态势评估结果的显示，需要高效直观的对当前的网络安全态势进行全方位、全视角的显示，从而方便管理员从各个视角对网络安全状况进行判断。

3.2. 网络安全评估发展现状

网络安全评估技术经过多年的研究，其理论发展已经较为成熟。网络安全评估方法一部分是对传统方法的扩展，也有一些则是将当前的理论创新与态势评估相结合，评估方法或者评估思想具体有：故障树模

型，攻击树模型，特权图模型，攻击图技术，贝叶斯技术，向量机的方法，人工神经网络的方法，模糊逻辑的方法，层次化分析法，多元信息融合理论，攻防博弈理论，证据理论，集对分析理论，粗糙集理论和灰关联分析等。一个高效的、优秀的网络安全评估系统往往是几种网络安全评估方法融合在一起形成的。

根据网络安全评估技术的发展现状和发展趋势，评估方法[3]按照其原理来说可以分为以下三大类：基于数学模型的方法、基于知识推理的方法和基于模式识别的方法。

3.2.1. 基于数学模型的方法

基于数学模型的方法最早被用于态势评估。该评估方法根据影响网络态势的不同因素，构造评价函数，然后通过评价函数将多个态势因子聚集得到态势结果。基于数学模型的方法通过借鉴传统通用的多目标决策理论的一些方法来解决态势评估的问题，其优点就是可以形象直观的反映网络安全态势情况，比如传统的权重分析法，集对分析方法[4]都属于该模型的范畴。但是针对该方法也存在着许多的不足，比如说数学模型中核心评价函数的构造、参数的选择等没有统一的评价标准和衡量体系，往往借助该领域专家的知识和经验来进行评估，因此不可避免的带有专家的主观意见。

3.2.2. 基于知识推理的方法

基于知识推理的方法主要用来处理一些数学模型难以处理的情况。知识推理方法能够模拟人类的思维方式，相对于传统的数学模型而言，评价过程具有一定的智能性，在一定程度上避免了人的主观因素对态势评估客观性的影响。知识推理方法一方面借助模糊集[5]、概率论、D-S 证据理论等处理不确定性信息；另一方面通过推理汇聚多源多属性信息。在知识推理方面研究的热点有基于故障图模型的安全态势评估方法、基于攻击树的安全态势评估方法、基于特权图的安全态势评估方法、基于攻击图模型的安全态势评估方法、基于贝叶斯网络的安全态势评估方法、基于层次化的安全态势评估方法等。

故障树模型是用于描述系统内部的故障及其原因之间关系的模型，最早由 Helmer [6]提出用于对攻击者的入侵行为进行建模，Helmer 用故障树模型对攻击者的入侵的描述、标识和检测进行分析。在国内，张涛[7]利用故障树模型对计算机上存在的脆弱性关系进行描述和建模，用到了权限提升的理论。故障树模型用于脆弱性评估之中可以从逻辑上清晰地表达脆弱点之间的关系，然而故障树会随着逻辑门和基本事件数目的增加而呈指数增长，产生组合爆炸问题。

攻击树模型最早是由 Schneier [8]基于故障树模型的概念提出的。攻击树中的叶子节点表示攻击方法，根节点表示了攻击者的目标。攻击树中的节点分为 AND 节点和 OR 节点，其中 AND 节点表示只有所有孩子节点都实现，父节点才能实现，OR 节点表示任意一个孩子节点实现了，父节点就可以实现。Clark [9]等通过在攻击树上计算脆弱点的割集以及脆弱点被利用的概率来对攻击树进行定性分析和定量分析。在国内，王辉[10]提出改进的最小攻击树攻击概率算法，使得授权用户类的攻击行为也能够预测和计算。段友祥[11]对基于改进攻击树的网络攻击模式进行形式化研究，引入了先后顺序关系以及成功概率等概念。由于攻击树对各种可能的攻击路径有清晰的逻辑表达能力，所以攻击树模型对于攻击树上的概率计算等量化工作很方便，然而在攻击树的具体应用中，其结构可能变得非常庞大而复杂。攻击树模型的规模问题制约了该模型在实际脆弱性评估中的应用。

特权图模型首先由 Dacier [12]提出，特权图模型中的节点表示一组权限集合，特权图模型中的有向边表示使得权限集合发生变化的脆弱性。特权图上的一条路径表示攻击者利用一系列的脆弱性使得其获得的权限发生变化的过程，即表达了一条攻击路径。特权图模型用图的方式表达攻击者利用脆弱点进行权限提升的攻击过程，具有良好的语义和形象的表达方式，然而特权图只考虑了权限提升的脆弱性，使得其在实际中的应用受到了一定的限制。

攻击图以有向图的方式来表答攻击者利用存在的脆弱性对网络或信息系统进行攻击的所有可能的攻

击路径，全面的反映了网络或信息系统中脆弱点利用之间的依赖关系。攻击图最早由 Phillips 和 Swiler [13]提出，并使用所定义的攻击图和基于攻击图的算法对网络存在的脆弱性进行分析。方明等[14]提出的基于攻击图的分布式网络安全风险评估方法，为了克服攻击图中脆弱点之间联系不足的情况，引入了脆弱性关联技术，针对攻击图描述攻击路径对于定量指标的分析缺乏相应的处理能力，采用攻击路径形成概率对信息安全的风险因素指标进行量化。陈小军[15]等提出的基于概率攻击图的内部攻击意图推断算法中，针对单步攻击检测结果存在的不确定性，使得攻击图模型无法准确地推断攻击者的意图这一情况，在攻击图模型中引入了转移概率表，用其刻画单步攻击检测结果的不确定性。陈靖等[16]把动态实时评估的思想引入到攻击图的应用中，通过采集网络的脆弱性、网络拓扑、资产价值等安全属性信息，同时提取入侵检测系统的报警信息、防火墙策略、安全管理等动态攻防对抗信息，生成动态攻击图，实时调整防御手段对网络进行及时、有效的保护，实时地对网络系统的安全状态进行评估。攻击图模型是目前网络安全评估中，用于表达网络或信息系统中存在的脆弱点，以及脆弱点之间的关联关系最有效的模型之一，但是其忽略了网络或信息系统中资产分布和威胁分布状况等因素对攻击发生可能性的影响，使得评估结果不能客观的反映网络中的风险状况。

由于贝叶斯网络的方法可以充分利用攻击图的结构和弱点等信息，从而不需要对网络的结构和参数进行学习，另外由于贝叶斯网络在概率逻辑关联推理方面很有优势，使得基于贝叶斯网络的方法成为网络安全态势评估研究中的热点。在贝叶斯网络的方法中，Xie [17]等人和 Poolsappasit [18]等人做出了代表性的工作，他们在攻击图的基础上构建贝叶斯网络，然后建立报警节点作为证据节点，每个节点的攻击发生概率是这些证据的后验概率。Frigault 等[19]采用贝叶斯网络的方法对网络的内在风险进行分析，并提出动态贝叶斯网络来包含脆弱性随着时间变化等时间特性。吴金宇[1]在针对已有的贝叶斯攻击图模型无法表达网络运行环境因素对攻击发生可能性的影响，提出了广义贝叶斯攻击图模型，把攻击收益和威胁状态变量引入到此模型中，使得广义贝叶斯攻击图能够包括被评估网络或信息系统的业务应用环境和环境威胁信息对攻击可能性的影响，以及这些影响在广义贝叶斯网络上的传播。基于贝叶斯网络的方法充分利用了贝叶斯网络的因果关联优势和不确定性推理能力，使得评估结果比较准确。但是，基于贝叶斯网络的方法由于需要对所有的节点都建立条件概率表，因此需要较多的先验知识，另外，受贝叶斯网络推理算法复杂度的限制，基于贝叶斯网络的实时评估算法的性能不高，难以满足大型网络或信息系统实时评估的性能要求。

在基于 D-S 证据理论的方法的研究中，Sabata [20]和 Qu [21]等都提出基于 D-S 证据理论的评估方法对分布式的攻击事件进行融合，从而实现对网络态势的感知。国内的韦勇[22]和梅海彬[23]也提出采用 D-S 证据理论将多数据源的信息进行融合的方法进行网络安全态势评估。由于 D-S 证据理论对的方法对警报赋予了可信度，并利用 D-S 证据理论在具有噪声的信息融合方面的优势对相关的警报进行融合，因此在警报信息存在误报的情况下仍然较好的得到威胁态势结果，并且基于 D-S 证据理论的方法还具有需要先验知识少，算法性能高等优点。但是，已有的基于 D-S 证据理论的方法无法进行攻击场景的还原，无法识别攻击者的攻击意图和预测将要发生的具体攻击动作，并缺乏对警报的漏报问题的支持。

层次化评估思想也是网络安全态势评估中应用比较广泛的方法，陈秀珍等人[24]提出了层次化网络安全威胁态势量化评估的方法，利用 IDS 报警信息和网络性能指标，结合主机的脆弱性信息，对服务、主机和网络进行层次化的安全定量评估。刘丽军[25]把攻防博弈理论引入到层次化的网络安全态势评估模型中。陈锋等人[26]把威胁传播模型和层次化网络安全评估方法结合在一起，利用威胁传播模型识别目标网络系统的威胁主体、分析其产生的传播路径、预测对网络系统的潜在破坏，在此基础上利用层次化网络安全测度模型来计算服务、主机和网络系统的危险指数。层次化网络安全评估方法能从不同的层次显示出威胁的大小，使得系统威胁更加清晰准确，但是层次化分析法中层次的划分以及各个层次威胁所占的

比重需要较多的先验知识，这也一定程度上限制了其发展。

基于知识推理的网络安全评估方法虽然比较客观、全面，且具有一定的智能性，但是基于知识推理方法面临最大的挑战性问题在于推理规则、先验概率等知识比较难于获取。

3.2.3. 基于模式识别的方法

随着机器学习技术的发展，模式识别方法被引入到网络安全态势评估的研究中。该方法借鉴数据挖掘算法的理念，主要依靠从训练样本或者历史数据中挖掘态势模式来进行态势评估。该方法具有强大的学习能力，其过程主要分为建立模式和模式匹配两个阶段。在网络安全态势评估中使用该方法的代表性工作包括：支持向量机的方法、基于神经网络、灰关联度、粗集理论和基于隐马尔科夫模型的态势评估方法。Lu 等人[27]采用支持向量机(Support Vector Machine, SVM)的方法对多元、多属性的信息进行融合，从而获得网络态势的感知。王伟[28]把层次化分析法(Analytic Hierarchy Process, AHP)和支持向量机(SVM)的方法结合在一起，利用 AHP 对评估指标初步筛选，然后利用向量机对测试集进行预测，得到最佳的网络安全评估等级。Zhang [29]等人采用人工神经网络(Artificial Neural Network, ANN)的方法对数据进行融合，该方法利用了 ANN 处理非线性问题方面的能力进行评估。在基于隐马尔可夫模型(HMM)的方法中，Ourston 等人[30]都是采用了 HMM 对网络攻击过程进行建模，将网络安全状态的变化过程采用隐马尔科夫模型来描述，然后利用该模型评估网络的安全态势。基于模式识别的方法虽然在态势评估上具有客观性等特点，但是该方法需要大量的训练数据来学习模型中的参数，而一般的网络或信息系统往往较难获得这些数据，并且这些方法由于没有利用攻击关联等先验知识，从而难以实现具体攻击的预测。

4. 总结

网络和信息系统的快速发展使得安全问题变得越来越重要，同时也使得安全问题变得越来越严重，在没有设计出绝对安全的系统之前，网络安全防御系统仍旧是对抗网络威胁的最主要的方式，网络安全评估技术仍然是网络安全防御的重要力量。本文比较全面的介绍了网络安全评估的各种技术方法，基于数学模型的方法可以方便直观的反应网络系统的安全状况，但是函数的构造与参数的选择具有主观性，因人而异，受限于作者的知识储备及主观意愿；基于知识推理的方法仍旧是当前研究的热点，研究成果也比较多，它在一定程度上降低了作者的主观性对网络系统安全评价带来的风险，但是这种评估方法的智能性也很低，另外受限于推理规则的制定和先验概率的获取；基于模式识别的方法有很好的智能性，但是需要大量的训练数据来学习模型中的参数，当前的云计算和大数据处理技术可以运用到基于模式识别的评估方法中，解决训练样本的获取与培训这一问题。目前这些方法没有哪一种是可以完全通用的，或者是最优的，各有自己的长处，也有自己的不足，要想设计出一个执行效率高，运行可靠，同时又检测全面的网络安全评估系统，需要多管齐下、取长补短。

回顾网络安全评估的发展历程，网络安全评估技术由最初的手工评估发展到现在的自动评估，由先前的局部评估发展到现在的整体评估，由原来的单机评估发展到现在的分布式评估，网络安全评估技术正朝着智能化、全面化、规模化的方向发展。

基金项目

河南省教育厅自然科学项目，(编号：14B520059)；河南省科技攻关计划项目，(编号：132102210555)；河南省教育厅科学技术研究重点项目，(编号：14B413008)；郑州市科技局自然科学项目，(编号：20130692)。

参考文献 (References)

[1] 吴金宇 (2013) 网络安全风险评估关键技术研究. 博士论文, 北京邮电大学, 北京.

[2] 邢栩嘉, 林闯, 蒋屹新 (2004) 计算机系统脆弱性评估研究. *计算机学报*, **1**, 1-11.

[3] 张剑锋 (2013) 网络安全态势评估若干关键技术研究. 博士论文, 国防科学技术大学, 长沙.

[4] 韦勇, 连一峰, 冯登国 (2009) 基于信息融合的网络安全态势评估模型. *计算机研究与发展*, **3**, 353-362.

[5] Qi, Y.L. and An, H.L. (2010) The evaluation model of network security based on fuzzy rough sets. In: Qi, Y.L. and An, H.L., Eds., *Advances in Wireless Networks and Information Systems*, Springer, Berlin, 517-525.

[6] Helmer, G., Wong, J., Slagell, M., et al. (2002) A software fault tree approach to requirements analysis of all intrusion detection system. *Requirements Engineering Journal*, **4**, 207-220.

[7] 张涛, 胡铭曾, 云晓春, 等 (2005) 计算机网络安全性分析建模研究. *通信学报*, **12**, 100-109.

[8] Schneier, B. (1999) Attack Trees. *Dr. Dobb's Journal*, **24**, 21-29.

[9] Clark, K., Tyree, S., Dawkins, J., et al. (2004) Qualitative and quantitative analytical techniques for network security assessment. *Proceedings of* 2004 *Information Assurance Workshop of the* 5*th Annual IEEE SMC*, Hawaii, IEEE Press, 321-328.

[10] 王辉, 刘淑芬 (2007) 改进的最小攻击树攻击概率生成算法. *吉林大学学报*(*工学版*), **5**, 153-156.

[11] 段友祥, 王海峰 (2007) 基于改进攻击树的网络攻击模式形式化研究. *中国石油大学报*(*自然科学版*), **1**, 144-147.

[12] Dacier, M., Deswartes, Y. and Kaaniche, M. (1996) Quantitative assessment of operational security models and tools. Technical Report Research Report 96439, LAAS.

[13] Phillips, C. and Swiler, L. (1998) A graph-based system for network-vulnerability analysis. *Proceedings of the Workshop on New Security Paradigms*, Charlottesville, 22-26 September 1998, 71-79.

[14] 方明, 徐开勇, 杨天池, 孟繁蔚, 禹聪 (2013) 基于攻击图的分布式网络风险评估方法. *计算机科学*, **2**, 139-144.

[15] 陈小军, 方滨兴, 谭庆丰, 张浩亮 (2014) 基于概率攻击图的内部攻击意图推断算法研究. *计算机学报*, **1**, 62-72.

[16] 陈靖, 王冬海, 彭武 (2013) 基于动态攻击图的网络安全实时评估. *计算机科学*, **2**, 133-138.

[17] Xie, P., Li, J.H., Ou, X.M., Liu, P. and Levy, R. (2010) Using Bayesian networks for cyber security analysis. *Proceedings of the* 40*th IEEE/IFIP International Conference on Dependable Systems and Network*, Chicago, 28 June-1 July 2010, 211-220.

[18] Poolsappasit, N., Dewai, R. and Ray, I. (2012) Dynamic security risk management using Bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, **9**, 61-74.

[19] Frigault, M. and Wang, L. (2008) Measuring network security using Bayesian network-based attack graphs. *Proceedings of the* 32*nd Annual IEEE International Conference on Computer Software and Applications*, Turku, 28 July-1 August 2008, 698-703.

[20] Sabata, B. and Ornes, C. (2006) Multi-source evidence fusion for cyber-situation assessment. *Proceedings of Multisensor, Multisource Information Fusion Conference*, Bellingham, 18 April 2006, 1-9.

[21] Qu, Z.-Y., Li, Y.-Y. and Li, P. (2010) A network security situation evaluation method based on D-S evidence theory. *Proceedings of the* 2010 *International Conference on Environmental Science and Information Application Technology*, Wuhan, 17-18 July 2010, 496-499.

[22] 韦勇, 连一峰, 冯登国 (2009) 基于信息融合的网络安全态势评估模型. *计算机研究与发展*, **3**, 353-362.

[23] 梅海彬, 龚俭 (2011) 多 IDS 环境中基于可信度的警报关联方法研究. *通信学报*, **4**, 138-146.

[24] 陈秀珍, 郑庆华, 管晓宏, 林晨光 (2006) 层次化网络安全威胁态势量化评估方法. *软件学报*, **4**, 885-897.

[25] 刘丽军 (2014) 基于攻防博弈模型的层次化网络安全评估探析. *网络安全技术与应用*, **8**, 173-175.

[26] 陈锋, 刘德辉, 张怡, 苏金树 (2011) 基于威胁传播模型的层次化网络安全评估方法. *计算机研究与发展*, **6**, 945-954.

[27] Lu, J., Yang, X. and Zhang, G. (2007) Support vector machine-based multi-source multi-attribute information integration for situation assessment. *Expert Systems with Application*, **34**, 1333-1340.

[28] 王伟 (2011) AHP 和 SVM 组合的网络安全评估研究. *计算机仿真*, **3**, 182-185.

[29] Zhang, J., Wang, K. and Yue, Q. (2006) Data fusion algorithm based on functional link artificial neural networks. *Proceedings of the* 6*th World Congress on Intelligent Control and Automation*, Dalian, 21-23 June 2006, 2806-2810.

[30] Ourston, D., Matzner, S., Stump, W., et al. (2003) Applications of hidden Markov models to detecting multi-stage network attacks. *Proceedings of the* 36*th Hawaii International Conference on System Sciences*, Hawaii, 6-9 January 2003, 334-342.