网络攻击效果在线评估模型与算法研究*)

王永杰 江 亮 鲜 明 陈志杰 王国玉
(国防科学技术大学电子科学与工程学院 长沙 410073)

摘 要 为了顺利实现预定的攻击目标,在线评估攻击效果并制定适当的攻击策略都是非常重要的。本文讨论了网络攻击效果与目标网络系统安全性之间的关系,提了一种基于网络安全性改变量的攻击效果定义方法;重点研究了网络攻击效果在线评估的评估模型和评估算法;提出了网络攻击效果的评价准则和评估指标体系;设计并给出了网络攻击效果在线评估系统的框架模型;详细讨论了网络攻击效果在线评估的评估算法、状态图生成算法、攻击效果预测算法和攻击方案决策算法。

关键词 网络攻击,攻击效果,在线评估,状态图

Research of Online Evaluation Model and Algorithm for Network Attack Effect

WANG Yong-Jie JIANG Liang XIAN Ming CHEN Zhi-Jie WANG Guo-Yu
(School of Electronic Science and Engineering, NUDT, Changsha 410073)

Abstract In order to achieving the network attack object perfectly, it's very important to evaluating the attack effect in real time and making proper attack strategy. The relationship between attack effect and network security property is analyzed. A definition of the network attack effect based on the change of network security property is given. The online evaluation model and evaluation algorithm for network attack effect are mainly studied in this paper. The evaluation rule and evaluation metrics are brought forward. The framework and design method of the network attack effect online evaluation system are described. The evaluation algorithm, attack status graph generating algorithm, attack effect predicting algorithm and attack scenario decision-making algorithm are discussed carefully. Finally, some problems which should be researched thoroughly in the future are pointed out.

Keywords Network attack, Attack effect, Online evaluating, Status graph

1 引言

随着计算机技术和网络技术的迅猛发展,人类社会正迅速迈向信息时代。与此同时,"网络战"已不再仅仅是一个虚无的概念,正逐步变为现实,必将对未来的战争形态产生重要影响。"网络战"条件下的网络攻击显然不能等同于普通的黑客攻击,后者通常是一种炫耀技术的无特定目的的攻击行为,而前者则是一种目的性极强的攻击行为,更加注重攻击的效果、成功概率和攻击风险,因而通常有系统的理论做指导。

网络攻击的效果主要是通过被攻击目标安全性的改变来体现的,因此研究网络攻击效果就必须从研究网络系统安全性评估入手。网络系统产生安全性通常被理解为网络系统在受到恶意攻击时网络性能指标的反应。网络系统产生安全问题的根本原因是系统存在脆弱性,脆弱性被攻击者利用而导致网络系统的安全性被破坏。目前人们普遍关注安全性的6个基本属性,包括:可靠性(reliability)、可用性(availability)、保险性(safety)、可行性(performability)、完整性(integrity)、机密性(confidentiality)。要定量地描述网络的安全性,就需要研究给出可量化的评价指标的定义。网络攻击的效果就可以通过网络攻击前后目标网络系统安全性的变化量来定义。

网络攻击效果在线评估就是要对攻击方案进行效能预测,对网络攻击的实际效果进行在线的实时分析,其主要目的是根据网络攻击的进展情况,调整制定下一步的攻击策略,为网络攻击过程的顺利实施提供决策支持。目前国内外在此方面的相关研究成果主要体现在以下几个方面:

Chandana Lala 等人研究了网络攻击破坏程度的评估问题[1]。针对数据库系统,研究了数据遭受攻击后快速检测、评估破坏的算法,给出了一种利用数据库日志的评估模型和相应的数据结构。

Peng Liu 等人研究了网络攻击条件下网络防御策略的制定问题[2]。将网络攻击与防御看作一个博弈过程,通过求解博弈过程的纳什均衡来研究攻防双方的对抗策略和效用;以 DDOS 攻击为例介绍了博弈模型建立和纳什均衡的求解方法。D. S. Menasch'ea 等人. 提出了一种利用博弈模型进行网络拥塞控制的模型[3]。

文[4]深入研究了网络安全评估的评估标准、原理与方法,介绍了网络安全评估的一般过程和常用工具。文[5]详细分析了国内外在网络安全风险评估方面的研究现状,介绍了风险评估的主要标准、模型和工具。

文[6]研究了网络安全的随机模型和评价技术,分析了网络安全性的评价指标和评价模型,同时对各种网络攻击模型进行了分析和比较。文[7]对网络攻防对抗的原理、模型、战略、战术等方面进行了深入研究,提出了协同式网络对抗的概念。

*)国家自然科学基金项目(60372039)。**王永杰** 博士研究生,主要研究方向为信息网络安全;**江 亮** 硕士生;**鲜 明** 副教授,博士;**陈志杰** 副教授;**王国玉** 研究员,博导,博士。

目前在网络攻击效果在线评估方面的研究成果还不多。本文主要从评估准则、评估模型和评估算法等方面对网络攻击效果在线评估的原理和方法进行探讨。

2 在线评估准则

对于任何评估系统，评估所遵循的准则都是至关重要的一个问题，评估准则选取得合理与否将直接关系到评估结果的合理性和可靠性。在此，我们主要制定了网络攻击效果评价准则、网络攻击方案效果预测准则、网络攻击策略生成准则。

2.1 网络攻击效果评价准则

网络攻击效果评价准则是网络攻击效果在线评估的基础。在线评估过程中，目标网络的最大资源评价、既定攻击方案的攻击效果预测、最终效果评价以及攻击过程的方案决策都是建立在该准则的基础之上。

网络攻击的目的多种多样，同时对目标网络的描述也十分复杂。如从目标网络的重要性方面可分为军队、政府、大型企业、小型公司、学校网络等；攻击目标可分为通信连接或是计算机系统；计算机系统中又可分为服务器、工作站、路由器、防火墙等；从攻击的目的来分，可以分为信息窃取、信息篡改、资源破坏、拒绝服务、目标控制等。若直接将上述所有因素考虑进去，建立一个统一的层次评价体系，必然会导致评估指标体系过于庞大，难以操作。通过对网络攻击目标、目的和评估策略进行深入分析，兼顾评价指标的直观性，本文将一个评价指标体系分解为两个模型，如图 1、图 2 所示。

任何一个指标初始值经过量化和归一化后，先用图 2 的模型计算该指标的评价值。评价时用指标所属的网络类型和系统类型对该指标归一化值进行加权平均，因此评价值考虑了各种情况对该指标的影响，从而可以得出一个普遍意义上的评价结果。在这个指标评价值的基础之上用图 1 描述的层次分析法可以得出网络攻击效果评价值。

评估体系中一个重要环节就是确定每一级的权重。图 1 和图 2 中的权重可以用专家咨询的层次分析法计算得出。其中图 1 的专家咨询是在普遍意义的指标上进行的，不应带有任何目的偏向性。结合目标的重要程度把目标网络分为 4 个等级，图 2 中分别用 A、B、C、D 来表示。

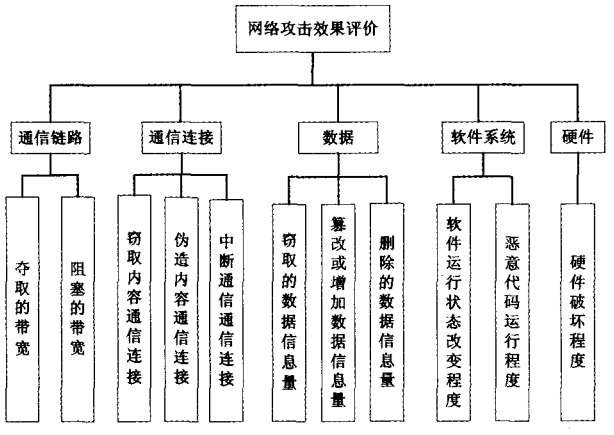

图 1 攻击效果指标体系

可以看到，这种评价准则直观性强、物理意义清晰、模型运算简单、易程序化。将评价指标体系分解为两部分简化了专家咨询工作的复杂度，降低了工作难度，也有利于提高权重计算的准确性。

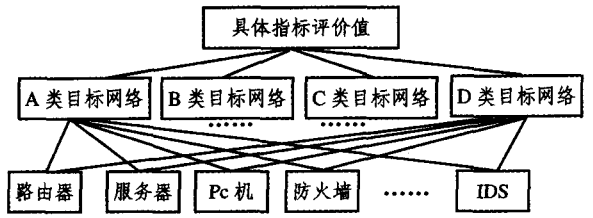

图 2 具体指标评价模型

2.2 攻击方案效果预测准则

在网络攻击方案开始实施前，需要对攻击方案的预期效果进行预测。预测主要从攻击能力、成功率、隐蔽性等 3 个主要影响因素进行分析。网络攻击成功率主要受网络状况、网络流量、先验知识多少、扫描结果可信度等影响；隐蔽性主要受目标网络管理员水平、检测系统敏感性、攻击手段自身特性等影响。由于攻防对抗过程中存在上述许多不确定性随机因素的影响，攻击前不能给出一个确定的攻击效果预测结果。在此，我们把攻击能力结合成功率、隐蔽性计算出攻击效果的数学期望值作为预测值。

2.3 网络攻击策略生成准则

攻击策略生成准则主要确定在攻击过程中每个攻击节点处将要采取的攻击动作。攻击策略主要根据继续攻击所冒风险和可获得的最大平均收益来确定，给出是否继续攻击的指导意见。

决策过程如下：第一步评估若停止攻击所得的攻击效果；第二步预测继续攻击最终的最大平均效果；第三步比较两者的大小，若后者大则继续攻击，否则停止。

图 3 给出了一个对某个既定方案，假设每一步攻击只有成功和被检测两种结果，得到的攻击效果转移图的示例，其中考虑了若后续攻击被检测出来，则可能失去某些前面已经取得的收益。

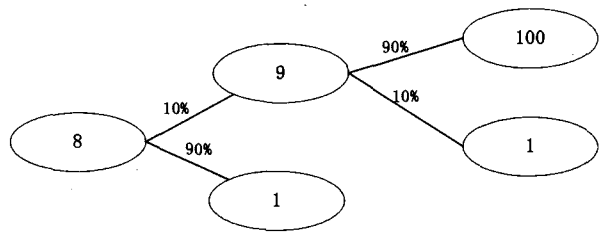

图 3 网络攻击效果转移图示例

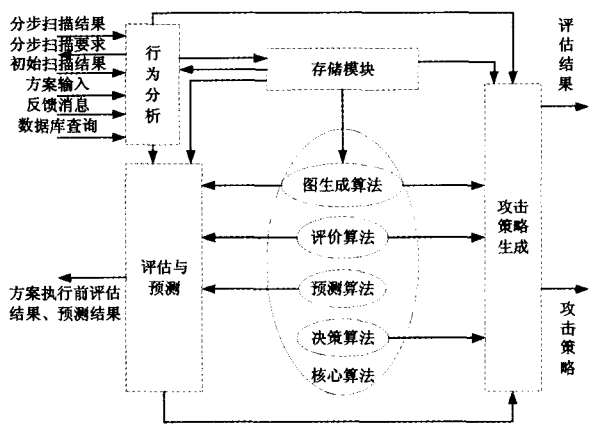

图 4 评估系统框图

前面提到的平均效果就是最终攻击效果的数学期望。如

图3所示例子，当攻击进行到效果为8的状态时，下一步继续攻击效果的数学期望为 $9*10\%+1*90\%=1.8<8$，但攻击状态到9还有后续步骤可以执行，实际上完全执行所有步骤的效果数学期望为

$$100*10\%*90\%+1*10\%*10\%+1*90\%=9.91>8$$

可以看出，虽然继续执行第一步攻击的风险很大，但冒险攻击却可能会产生更大的收益。

3 在线评估实现方案

网络攻击效果在线评估系统的总体实现方案如图4所示。评估系统分为行为分析模块、方案存储模块、评估及预测模块、攻击策略生成模块和核心算法模块。核心算法包括攻击图生成算法、攻击效果评价算法、攻击效果预测算法和决策算法。这里的决策算法指风险评估和策略生成算法。

·行为分析模块是在线评估系统的输入输出接口，负责在线评估系统的信息接收和任务调度。其主要功能包括：分析攻击步骤是否成功；分析当前攻击方案执行状态并更新存储模块；确定下一步的攻击策略；调度攻击策略生成模块和评估及预测模块的运行。

·存储模块的存储内容主要包括：目标网络拓扑分析结果、攻击方案、执行指针、当前方案执行状态、每个攻击步骤的执行结果等。

·评估和预测模块负责攻击方案执行前的目标网络最大可用资源、攻击方案的最大预期攻击效果和攻击结束后最终效果的评价；还有攻击前对攻击方案攻击效果的数学期望预测。

·攻击策略生成模块对行为分析模块得出的下一步攻击步骤进行深入分析，得出最终的攻击策略。

网络攻击效果在线评估系统的工作流程如下：

(1)行为分析模块首先获取关于目标系统的详尽扫描结果和攻击方案，分析扫描结果得出目标网络的拓扑信息，并把分析结果和攻击方案输入到存储模块。

(2)行为分析模块调用执行评估及预测模块进行攻击前的评估和预测。

(3)行为分析模块根据正在进行的攻击步骤属性，通过接收反馈消息、扫描结果、等待超时等因素确定当前攻击是否成功；分析当前攻击方案所处的状态；更新存储模块内容。

(4)行为分析模块根据目前攻击方案所处的状态，调用攻击策略生成模块，生成下一步攻击策略。

(5)行为分析模块重复(3)，直到所有可进行的攻击步骤完成或人工干预要求停止。

(6)行为分析模块调用执行评估及预测模块进行攻击后的效果评估。

4 核心算法

在线评估系统的核心算法主要有4个：攻击效果评价算法、方案攻击过程状态图生成算法、攻击效果预测算法和决策意见生成算法。

4.1 攻击效果评价算法

系统需要从攻击方案目前执行状态或某个假定的状态来计算出当前攻击效果，以此作为在线评估的基础。在效果评价准则中已经提到，对图2所示的模型，可以用加权平均法计算特定指标的评价值。对三层体系结构的加权平均算法如下：

$$r(x_i)=\sum_{j=1}^{m}w_j x_{ij} \tag{1}$$

$$r(x)=\sum_{i=1}^{n}w_i\sum_{j=1}^{m}w_j x_{ij} \tag{2}$$

其中 x_{ij} 为第三层指标的归一化值；m、n 为第二、三层指标的个数；w_i、w_j 分别为第二、三层的权重系数。权重系数可以通过层次分析法(AHP)得到，具体原理和计算方法可以参见文[8]。

4.2 攻击过程状态图生成算法

攻击过程状态图主要用来描述攻击过程所经历的攻击路径，以及继续进行攻击的所有可能攻击方案。由于网络攻击过程会受到各种随机因素的影响，攻击状态难以精确描述。为了降低问题的复杂度，我们对攻击过程状态图生成算法做了如下4个简化假设：

假设1 每个攻击步骤只有3种情况影响攻击后的方案状态：攻击成功、攻击失败、攻击行为被检测。

假设2 在每个状态下，下一步要执行的攻击步骤是攻击方案中第一个可以执行且尚未执行的原子攻击。

假设3 攻击会一直进行到没有可以执行的原子攻击为止。

假设4 一旦某个攻击步骤被检测到，则将失去已获得的控制权限，同时攻击过程不能继续。

为了描述方便，定义符号：

A_i：第 i 步攻击；

S'_i：A_i 攻击所需初始状态；

S'_{i+1}：A_i 成功，对初始状态贡献后的状态；

S_i^j：第 i 步攻击前方案可能的第 j 种状态；

S_i^{j-}：S_i^j 失去所有控制权后的状态；

A：找出的下一步攻击步骤。

图生成算法总以攻击方案的某一攻击步骤执行后的状态为起始点。此时方案状态已知，下一步攻击前的可能状态只有一个。在这4个假设原则限制下，图生成算法如下：

step1：$i=1,n=0$；

step2：若 $S_i^j\supseteq S'_{i+n}$，则 $A=A_{i+n}$，转 step4；否则转 step3；

step3：$n=n+1$，若 $i+n>$ 总步数，转 step5；否则转 step2；

step4：取 $S_{i+n+1}^{x1}=S_i^j\cup S'_{i+1}$，$S_{i+n+1}^{x1+1}=S_i^j$，$S_{i+n+1}^{x1+2}=S_i^{j-}$。其中 $x1=\max(j)+1$；

step5：对第 i 步攻击前的每个 S_i^j，都执行 step1～step4。

step6：$i=i+1$，若 $i>$总步数，转 step8；

step7：对第 i 步攻击前相同的 S_i^j 进行合并，并重新对 j 排序，转 step1；

step8：end

利用本算法生成的攻击状态图如图5所示。

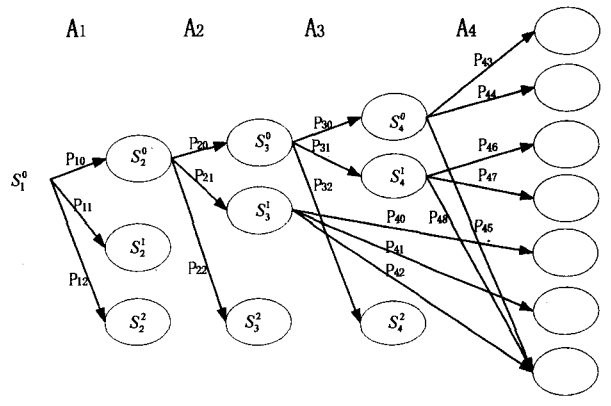

图5 攻击状态图

(下转第103页)

参 考 文 献

1 William S, Austin T. Ontologies. IEEE Intelligent Systems, 1999. 18～19
2 Martin D, Burstein M, Hobbs, J et al. OWL-S: Semantic Markup for Web Service. W3C Member Submission 22, November 2004
3 Akkiraju R, Farrell J, Miller J, et al. Web Service Semantics - WSDL-S. W3C Member Submission 7, November 2005
4 Battle S, Bernstein A, Boley H, et al. Semantic Web Servcies Language(SWSL). W3C Member Submission 9, September 2005
5 Miller G A, Beckwith R, Fellbaum C, et al. Introduction to WordNet: An On-line Lexical Database. International Journal of Lexicography, 1993
6 Paolucci M, Kawamura T, Payne T R, Mtching of Web Services Capabilities. In: Proc. of the First Intl Semantic Web Conference, June 2002
7 Tang S. Matching of Web Service Specifications Using DAML-S Descriptions: [Master dissertation]. Technische UniversitÄat Berlin, 2004, 3
8 Ankolekar A, Burstein M, Hobbs J R, et al. DAML-S : Web Service Description for the Semantic Web. The Semantic Web-ISWC, Springer 2002
9 Bramantoro A, Krishnaswamy S, Indrawan M. A Semantic Distance Measure for Matching Web Services. In: WWW2005, Web Service Semantics Workshop, 2005
10 张钋. 基于语义的网络服务匹配机制的研究与实现:[硕士论文]. 北京:清华大学计算机科学与技术系,2005,12
11 Sycara K, Widoff S, Klusch M, et al. Dynamic matchmaking among heterogeneous software agents in cyberspace. Autonomous Agents and Multi-Agent Systems, 2002, 5:173～203
12 吴健,吴朝晖,李莹,等. 基于本体论和词汇语义相似度的 Web 服务发现. 计算机学报,2005(4):595～602
13 Borst WN. Construction of Engineer Ontologies: [Ph D dissertation]. University of Twenty, Enschede, 1997

(上接第 74 页)

在图 5 中,每一个状态转换由检测率和成功率生成一个转移概率 P_{ij},其中 i 表示原子攻击 A_i,j 表示转移到状态 S_i^j。由于具体的攻击步骤只有 3 种结果,因此 3 种结果的状态转移概率之和为 1,如图 5 中有 $P_{10}+P_{11}+P_{12}=1$。

4.3 攻击效果预测算法

为了便于描述,取 $f(s_i^j)$为攻击效果评价值。没有后续攻击步骤的状态都是可能的最终状态。可以得出攻击效果为

$$P(f(s_5^3))=P_{10}P_{20}P_{30},P_{43},P(f(s_5^0))=P_{10}P_{21}P_{40},P(f(s_3^2))=P_{10}P_{22},\cdots \quad (3)$$

并且将效果评价值相同的状态合并,计算数学期望 E:

$$E=f(s_5^3)P(f(s_5^3))+f(s_5^0)P(f(s_5^0))+f(s_3^2)P(f(s_3^2))+\cdots \quad (4)$$

从而得出最终预测值。

4.4 决策意见生成算法

决策意见生成算法主要通过比较停止攻击所具有的攻击效果与继续攻击的最大数学期望来实现。其中停止攻击所具有的攻击效果容易计算,下面主要讨论继续攻击情况下攻击效果的最大数学期望的计算方法。用最大数学期望作为对比标准是合理的,如图 6 所示。

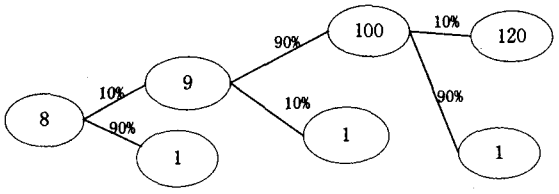

图 6 最大数学期望示例

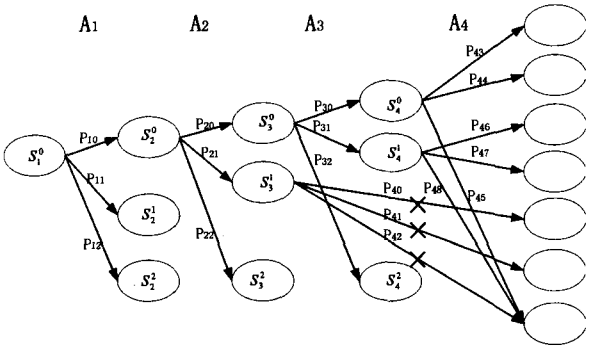

图 7 最大数学期望攻击图

与图 3 不同的是在攻击状态 100 后多了一个攻击步骤。当攻击状态为 8 时继续攻击最终的数学期望为

$$120*10\%*90\%*10\%+1*90\%*90\%*10\%+1*10\%*10\%+1*90\%=2.071$$

但是在状态 8 时我们的决策不变,仍是继续攻击。因为在状态 100 时,继续攻击的数学期望会很小,我们会在此处决策为停止攻击,在这样的攻击方案中最大数学期望仍为 9.91,所以在状态 8 时我们选择继续攻击。

用 $E(s_i^j)$表示 S_i^j 时继续攻击的最大数学期望。首先在从生成的攻击图中得出最大数学期望攻击图,如图 7 所示。决策意见生成算法如下:

step1:生成从当前状态开始的攻击图;

step2:计算最后一步攻击前所有状态的数学期望。如果 $E(s_i^j)<S_i^j$,则删除 S_i^j 的后续攻击步骤,生成一个新的攻击图;

step3:在此基础上计算倒数第二步攻击前的所有状态数学期望,同 step2 处理,直到当前需要决策的状态所在的攻击步骤为止。

step4:计算当前状态下继续攻击的数学期望。如果 $E(s_i^j)<S_i^j$,则决策为停止攻击,否则为继续攻击。

结束语 本文分析了网络攻击效果在线评估系统的目的,提出了直观有效的攻击效果评估准则和评估模型,给出了网络攻击效果在线评估的相关算法的实现方案,在实际应用中取得了良好的效果。由于网络攻击的具体情况十分复杂,如窃取数据信息量的初始值难以确定和归一化,针对软件的攻击时效性如何表现在指标初始值上等情况,使得指标权重的确定变得比较困难,同时攻击图生成算法中考虑到的隐蔽性和成功率在实际中难以精确得到,使得状态转移概率不精确,可能会影响最终的评估结果。上述这些难点问题都是以后研究中需要改进的地方。

参 考 文 献

1 Lala C, Panda B. Evaluating Damage from Cyber Attacks: A Model and Analysis[J]. IEEE Transactions on Systems, Man and Cybernetics-Part, A: Systems and Humans, JULY, 2001, 31(4)
2 Liu Peng, Zang Wanyu, Yu Meng. Incentive-based Modeling and Inference of Attacker Intent, Objectives, and Strategies [J]. ACM Transactions on Information and System Security, 2005, 8(1): 78～118
3 Menasch'ea D S, Figueiredob D R, de Souza e Silvaa E. An evolutionary game-theoretic approach to congestion control[J]. Performance Evaluation, 2005, 62: 295～312
4 Gregg M, Kim D. Inside Network Security Assessment: Guarding your IT Infrastructure[M]. Sams, 2005
5 冯登国,张阳,张玉清. 信息安全风险评估综述[J]. 通信学报,2004,25(7):10～18
6 林闯,汪洋,李泉林. 网络安全的随机模型方法与评价技术[J]. 计算机学报, 2005,28(12):1943～1956
7 卢显,等. 协同式网络对抗[M]. 北京:国防工业出版社,2003
8 刘进,王永杰,张义荣,等. 层次分析法在网络攻击效果评估中的应用[J]. 计算机应用研究,2005,22(3):113～115