网络抗攻击性能的遗传投影寻踪评估模型

王会梅 李 旭 鲜 明 王国玉
(国防科技大学电子科学与工程学院 长沙 410073)

摘 要 抗攻击测试是进行系统安全测评的重要手段之一,对网络系统的抗攻击能力进行评估是抗攻击测试需要解决的一个关键问题。根据影响网络系统的安全属性,从抗攻击测试网络系统的攻击效果和模拟攻击方的攻击代价两个方面来构建网络抗攻击性能评估指标体系,提出了网络抗攻击性能的投影寻踪评估模型,投影指标函数采用基于实数编码的加速遗传算法进行寻优。最后进行了实例验证,结果表明,该方法不仅能够对网络的抗攻击性能进行很好的评价,还能对系统抵抗不同攻击方法的能力进行排序。

关键词 抗攻击测试,评估指标,投影寻踪,评估模型
中图法分类号 TP393.08 **文献标识码** A

Genetic Projection Pursuit Evaluation Method of Network Attack Resistance Ability

WANG Hui-mei LI Xu XIAN Ming WANG Guo-yu
(College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China)

Abstract Attack Resistance Test (ART) is an important security evaluation method and evaluating the system's attack resistance ability becomes a new domain of ART. Based on the security properties of the network, the network's attack resistance evaluation indexes were established from views of the goal system's attack effect and the hacker's cost. A projection pursuit evaluation model based on real coding based accelerating genetic algorithm was presented, and it was used in attack resistance ability evaluation for the first time. A simulation example was given, which showed that the approach was brief and effective. The approach can be used to evaluate the attack resistance ability, as well as to compare like kind attack's effect.

Keywords Attack resistance test, Evaluation index, Projection pursuit, Evaluation method

信息安全测评作为信息系统安全工程过程中的关键环节,在整个信息系统的生命周期中具有重要的作用,关系到信息系统安全建设的成败。抗攻击测试是进行系统安全测评的重要手段之一,在计算机网络攻击条件下,对系统的抗攻击能力进行定性或定量的评估是抗攻击测试需要解决的重要问题,为提高网络生存能力给出建议和方法,从而最终提高网络的安全防护能力。

安全测试是系统安全保障的重要环节,对增强系统安全性、提高系统防御攻击的能力有着重要的意义[1,2]。从测试的出发点来看,目前的安全测试方法主要包括两种:正向测试和反向测试。

正向安全测试又可分为形式化验证方法和非形式化验证方法。形式化验证是一种类似于数学证明的测评验证方法,是对系统的安全策略模型进行形式化证明,它的过程比较复杂,尤其对于复杂的系统效率会非常低。非形式化正向测试通常从标准出发,也可借助于专家经验,对测试目标进行对照检查,该类方法存在的主要问题是可实施性不好,而且对实施人员的专业水平要求较高。

反向安全测试主要是使用攻击的手段来对网络中的重要主机和安全设备进行安全测试,它的主要特点在于从黑客攻击的角度来对系统的安全性进行评价。目前的反向测试主要有渗透测试、可生存性测试等。目前的反向安全测试的研究主要集中在,如何通过渗透技术入侵目标系统,依据入侵结果给出安全改进建议。侯一凡[3]提出了基于层次分析法的抗攻击能力评价算法,但是评价指标的权重需要专家打分确定,带有主观性。为了消除专家打分的影响,将投影寻踪方法首次应用到网络抗攻击性能评估,依据评价指标样本值之间的相似性和差异性,对各评价对象进行分类从而达到评估的目的;并借鉴金菊良等[6]提出的基于实数编码的加速遗传算法对投影指标函数进行寻优。

本文第1节介绍了抗攻击性能评估的基本概念;第2节从攻击效果和攻击代价两个方面研究了网络抗攻击性能评估指标体系;第3节给出了网络抗攻击性能的遗传投影寻踪评估模型和评估算法;第4节给出了实例验证;最后进行了总结。

1 抗攻击性能评估

计算机网络的抗攻击性主要指网络系统及其硬件资源、软件资源和网络服务在遭到窃取、修改、阻塞、降低或破坏等

到稿日期:2009-07-10 返修日期:2009-09-15 本文受国家自然科学基金项目(60372039)资助。
王会梅(1981-),女,博士生,主要研究方向为信息安全、电子信息系统仿真与评估等,E-mail:freshcdwhm@163.com;李 旭(1984-),男,硕士生,主要研究方向为信息安全等;鲜 明(1970-),男,博士,研究员,主要研究方向为信息安全、无线传感器等;王国玉(1962-),男,博士生导师,主要研究方向为信息安全、电子信息系统仿真与评估等。

攻击后，网络系统仍能继续正常运行并提供主要服务甚至自动恢复的能力。抗攻击性能评估就是研究对网络系统抗攻击能力如何进行定性或定量评价的理论和技术。

从数学角度考虑，网络抗攻击性能评估过程即一个泛函映射过程[7]，$f:A\to B$，其中原象集 A 为评估的对象，一般没有约束，可以是数的集合，也可以是其它任意集合，对网络抗攻击性能评估来说，指的是评估指标；象集 B 为评估结果，一般是实数值、向量或矩阵；f 为从一般集合到数集的映射，即建立数学中的有序关系，具体到网络抗攻击性能评估中来说，f 为评估算法。

2 评估指标体系

网络抗攻击性能评估指标体系是网络抗攻击性能评估的一个重要组成部分，它是一套能够全面反映所评估对象的总体目标和特征并且具有内在联系、起互补作用的指标的集合。在评估时从攻击方和被攻击方两个方面对网络抗攻击性能评估指标进行提取，选取的指标必须能对网络性能参数有相当敏感的反映，同时能反映产生不同攻击效果的攻击代价的差异。

根据影响可用性、保密性和完整性等计算机网络系统安全性能的主要属性，对网络抗攻击性能测试中的攻击进行分类，如图 1 所示。

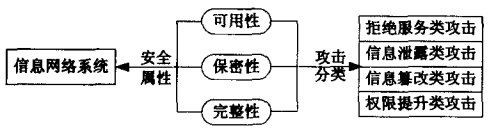

图 1 基于网络安全属性的攻击分类

其中，信息泄露类攻击主要破坏系统的保密性；信息篡改类攻击主要破坏系统的完整性；拒绝服务类攻击主要破坏系统的可用性；权限提升类攻击则破坏目标系统的保密性、完整性等多个安全属性。

借鉴网络攻击效果评估指标体系的建立[4,5]，从抗攻击测试网络系统方的攻击效果和模拟攻击方的攻击代价两个方面来建立网络抗攻击性能评估指标体系：$I_{RA}=\{I_{AE},I_{AC}\}$。其中，I_{AE} 表示攻击效果类指标，由图 1 中各个攻击分类的攻击效果指标集合而成，反映了抗攻击测试系统的安全属性的变化；I_{AC} 为攻击代价类指标，表示攻击方为完成攻击所需付出的努力，反映了攻击者破坏系统安全特性的难易程度。图 2 为按照此原则建立的抗攻击性能评估指标体系。

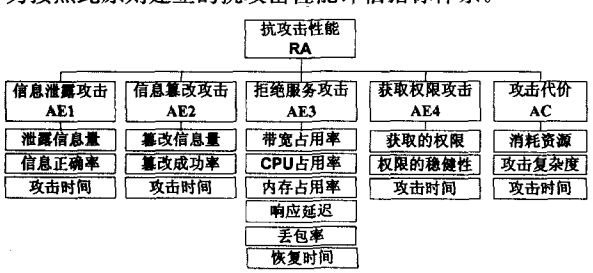

图 2 网络抗攻击性能评估指标体系

3 评估模型

对被测网络系统进行模拟攻击，用投影寻踪(PP)方法进行网络抗攻击性能评估，把攻击测试得到的高维网络抗攻击性能评估指标数据通过某种组合投影到低维子空间上。对于投影到的构形，采用投影指标数来衡量投影暴露某种结构的可能性大小，利用基于实数编码的加速遗传算法寻找出使投影指标函数达到最优的投影值，然后根据该投影值来分析高维数据的结构特征，对网络的抗攻击性能进行评估。网络抗攻击性能的遗传投影寻踪评估分析模型如图 3 所示。

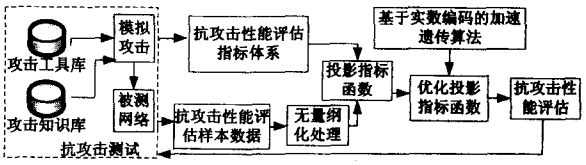

图 3 网络抗攻击性能评估分析模型

具体的评估算法如下：

(1)建立网络抗攻击性能评估指标体系

建立网络抗攻击性能评估指标体系，并对评估指标的样本数据进行一致无量纲化处理。

设网络抗攻击性能评估对象的评估指标样本集为$\{x(j,i)\mid j=1\sim p,i=1\sim n\}$，其中 n,p 分别为评估对象的数目和评估指标的数目。为消除各个评估指标的量纲效应，使建模具有通用性，需对$\{x(j,i)\mid j=1\sim p,i=1\sim n\}$进行一致无量纲化处理。

指标数据无量纲化的主要方法有 3 种。

1)直线型无量纲化方法：适用于规范化后的指标值与指标的测量值之间呈线性关系的指标。

2)折线型无量纲化方法：适应于指标变换呈阶段性，指标值在不同阶段变化对网络的抗攻击性能的影响是不同的指标。

3)曲线型无量纲化方法：适应于指标变化过程虽没有明显转折点，但是前后期的变化特点又确实不同的指标的无量纲化。

设标准化后评估指标样本集为$\{y(j,i)\mid j=1\sim p,i=1\sim n\}$。

(2)构造投影指标函数

投影寻踪分类方法就是把 p 维数据$\{y(j,i)\mid j=1\sim p\}$综合成以 $\omega=[\omega(1),\omega(2),\cdots,\omega(p)]$为投影方向的一维投影值 $z(i)$：

$$z(i)=\sum_{j=1}^{p}\omega(j)y(j,i) \tag{1}$$

然后根据 $z(i)-i$ 的一维散布图对网络抗攻击性能进行评估。式中，$\omega(j)>0$，$\sum_{j=1}^{p}\omega(j)=1$。可得，$\omega(j)$即为指标 j 的客观权重。

在综合投影值时，要求投影值的散布特征应为：局部投影点尽可能密集，最好凝聚成若干个点团(同一点团中的评估对象趋于同类)，而在整体上投影点团之间尽可能散开。为此，投影指标函数可构造为

$$Q(\omega)=S_zD_z \tag{2}$$

式中，S_z 为投影值 $z(i)$的标准差，D_z 为投影值 $z(i)$的局部密度，即

$$S_z=\left[\sum_{i=1}^{n}(z(i)-\bar{z})^2/(n-1)\right]^{0.5} \tag{3}$$

$$D_z=\sum_{i=1}^{n}\sum_{j=1}^{n}(R-r_{ij})u(R-r_{if}) \tag{4}$$

式中，$\bar{z}$为序列$\{z(i)\mid i=1\sim n\}$的均值；R 为局部密度的窗口半径，它的选取既要使包含在窗口内的投影点的平均个数不太

少，避免滑动平均偏差太大，又不能使它随着 n 的增大而增加得太快，R 的设置目前仍是经验性的，一般取 $0.1S_z$；距离 $r_{ij}=|z(i)-z(j)|$；$u(t)$ 为单位阶跃函数，当 $t<0$ 时函数值为 0，否则函数值为 1。

(3)优化投影指标函数

当给定评估对象的评估指标样本数据时，投影指标函数 $Q(\omega)$ 只随投影方向 ω 的变化而变化。不同的投影方向反映不同的数据结构特征，最佳投影方向可最大可能暴露高维样本数据的聚类特征结构。因此可通过求解投影指标函数最大化问题来估计最佳投影方向，即

$$\max Q(\omega)=S_zD_z$$
$$s.t.\ \omega(j)>0,\sum_{j=1}^{p}\omega(j)=1 \tag{5}$$

这是一个以 $\{\omega(j)|j=1\sim p\}$ 为优化变量的非线性优化问题，可用基于实数编码的加速遗传算法来进行求解。

(4)抗攻击性能评估

把步骤(3)求得的最佳投影方向 ω^* 带入式(1)后，可得各个评估对象的投影值 $z^*(i)$。$z^*(i)$ 值可反映各评价对象的综合特征，通过比较 $z^*(i)$ 的大小，亦可进行分类排序。

4 实例验证

4.1 评估实例

采用拒绝服务类攻击方法对被测网络系统进行抗攻击性能测试来验证评估算法的有效性。目标为一台 Web 服务器，分别采用 TCP SYN flood(TF)，UDP flood(UF)两类拒绝服务攻击方法对目标进行模拟攻击。每类攻击进行 3 种测试，分别为攻击主机 1 发起攻击、攻击主机 2 发起攻击、攻击主机 1 和 2 同时发起攻击。每种攻击重复攻击两次。

根据网络抗攻击性能评估指标体系，得到测试目标抵抗拒绝服务类攻击的性能指标为 $I_{dos}=\{a_1,a_2,a_3,\cdots,a_9\}$，其中 a_1-a_6 是从被测网络中获取的指标：a_1 表示网络带宽占用率，a_2 表示 CPU 利用率的变化量，a_3 表示内存利用率的变化量，a_4 表示响应延迟，a_5 表示丢包率，a_6 表示恢复时间；a_7-a_9 是从攻击方获取的指标：a_7 表示消耗资源，a_8 表示攻击复杂度，a_9 表示攻击时间。表 1 列出测试所得数据。

表 1 网络抗拒绝服务攻击性能数据样本

	攻击效果					攻击代价				投影值
	a_1	a_2	a_3	a_4(s)	a_5	a_6(s)	a_7(台)	a_8	a_9(s)	$z^*(i)$
UF11	0.01	0.02	0.01	0.8	0.01	1	1	0.2	6	0.9533
UF12	0.01	0.02	0.02	0.8	0.01	2	1	0.2	6	0.9526
UF21	0.03	0.05	0.02	0.9	0.03	3	1	0.2	6	0.9312
UF22	0.04	0.04	0.02	1.0	0.03	3	1	0.2	6	0.9328
UF31	0.12	0.13	0.04	1.5	0.11	5	2	0.2	6	0.8600
UF32	0.11	0.12	0.05	1.4	0.12	6	2	0.2	6	0.8675
TF11	0.27	0.41	0.02	1.2	0.12	69	1	0.2	10	0.6925
TF12	0.26	0.40	0.03	1.3	0.13	66	1	0.2	10	0.6986
TF21	0.33	0.43	0.03	1.3	0.14	72	1	0.2	10	0.6645
TF22	0.34	0.43	0.03	1.3	0.14	72	1	0.2	10	0.6614
TF31	0.41	0.62	0.15	2.0	0.27	96	2	0.2	10	0.5287
TF32	0.42	0.63	0.17	2.1	0.29	90	2	0.2	10	0.5179

首先对表中的数据进行一致无量纲化处理，指标 a_1，a_2，a_3，a_5 是负向性的百分比量，采用对 1 取余法进行量化。

对于指标 a_4 为负向性指标，采用曲线型归一化方法，可以得到归一化公式为

$$t_{delay}=e^{-k(a_4)^2} \tag{6}$$

假定当 a_4 大于 10 秒时认为网络性能已经很差，据此可以确定出式(6)中的 $k\approx0.02$。

对于指标 a_6 采用曲线型归一化方法，可以得到归一化公式

$$t_{recovery}=e^{-k(a_6)^2} \tag{7}$$

假定当 a_6 大于 30 分钟时认为网络性能已经很差，据此可以确定出式(7)中的 $k\approx0.002$。

对于指标 a_7，在拒绝服务攻击中，消耗的资源主要为参与攻击的主机，参照曲线型归一化方法进行无量纲化处理。

$$R_{dos}=1-e^{-k(a_7)^2} \tag{8}$$

对于指标 a_8，根据汪立东对弱点的攻击复杂性的分析来确定攻击复杂性[8]，TCP SYN flood，UDP flood 攻击属于有现成的攻击工具和较详细的攻击步骤，量化为 0.2。

对于指标 a_9，采用曲线型归一化方法，归一化公式为

$$t_{attack}=1-e^{-k(a_9)^2} \tag{9}$$

把一致无量纲化处理后的样本数据依次代入式(1)－式(4)，得到投影指标函数，利用实数编码的加速遗传算法求解由式(5)所确定的优化问题(群体规模 n 取 400，优秀个体数目 s 取 25)，得到最大投影指标函数值为 0.0543，最佳投影方向为

$$w^*=\{0.2555,0.5216,0.07506,0.0517,0.0061,0.0428,$$
$$0.0335,0.0039,0.0097\}$$

把 w^* 代入式(1)后得到各个抗攻击性能评估的投影值，如表 1 所列。

网络抗攻击性能评估值越大，表示网络抵抗该拒绝服务攻击的能力越强，各投影值的散布情况如图 4 所示。

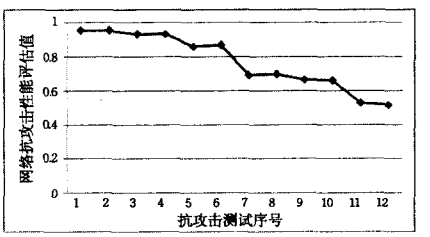

图 4 抗攻击性能评估数据投影值的散布图

4.2 结果分析

通过对表 1 和图 4 进行分析可以得出：

1)该 Web 服务器对两类拒绝服务攻击的抵抗能力 UDP flood>TCP SYN flood，这与公认的攻击形式有效性的评价相符合，即在各种拒绝服务攻击方式中，TCP SYN flood 攻击是最有效的。

2)被测 Web 服务器抵抗 DDOS 的能力明显低于抵抗单台主机发起的拒绝服务攻击的能力。

3)实验结果与侯一凡基于层次分析法的抗攻击能力评价算法实验结果一致[3]。但是投影寻踪评估方法减少了专家打分的过程，依据评估样本值之间的相似性和差异性进行评估，同时该模型对样本容量并无严格的要求，具有较强的适用性。

4)由实验结果可以看出，该 Web 服务器应该增强防火墙的配置，加强对 DOS 攻击的防范。

结束语 网络系统的抗攻击性能评估可以检验抗攻击测试的效果，为提高网络系统的抗攻击性和可生存性给出建议和意见。从网络系统安全属性出发，建立了表征攻击效果和

(下转第 163 页)

4类方法的优缺点进行了总结，并从多方面对它们的性能进行了比较。

Web应用的测试用例生成已取得了不少成果，但是与实际应用的需求还有很大的差距。在自动化测试时，如何填充表单项仍是需要解决的难点；Web2.0出现后，Ajax和RSS的测试对Web测试者提出了新的挑战。由于Web应用越来越多地融入社会生活，人们很多重要的活动都通过Web应用来实现，如电子商务、电子政务、安全性测试也会成为大家关注的研究热点。

参考文献

[1] Andrews A A, Offutt J, Alexander R T. Testing Web Applications by Modeling with FSMs[J]. Software Systems and Modeling, 2005, 4(2): 326-345

[2] 许蕾，徐宝文，陈振强. Web测试综述[J]. 计算机科学，2003，30(3)：100-104

[3] William G J H, Alessandr O. Improving Test Case Generation for Web Applications Using Automated Interface Discovery[C]// Proceedings of the 6th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering. New York, 2007: 145-154

[4] Xu Lei, Xu Baowen. Testing Forms in Web Applications Automatically[J]. Wuhan University of Natural Sciences, 2006, 11(3): 561-566

[5] Rational robot[OL]. http://www.rational.com/products/robot/index.jsp

[6] Jia X, Liu H. Rigorous and Automatic Testing of Web Applications[C]// 6th IASTED International Conference on Software Engineering and Applications (CTIRS). San Francisco, 2002: 280-285

[7] Elbaum S, Karre S, Rothermel G. Improving Web Application Testing with User Session Data[C]// International Conference on Software Engineering(ICSE2003). Portland, 2003: 49-59

[8] Sprenkle P S, Gibson P E, Sampath P S, et al. A case study of automatically creating test suites from web application field data [C]//Proceedings of the 2006 Workshop on Testing, Analysis, and Verification of Web Services and Applications. 2006: 1-9

[9] Kung D C, Liu C H, Hsia P. An Object-Oriented Web Test Model for Testing Web Applications[C]// Proceedings First Asia-Pacific Conference on Quality Software (COMPSAC2000). Taipei, Taiwan, China, 2000: 111-120

[10] Benedikt M, Freire J, Rice P, et al. VeriWeb: Automatically Testing Dynamic Web Sites[C]// Proceedings of 11st International WWW Conference. Honulolu, 2002

[11] 黄陇，李诺，金茂忠，等. 基于DataPool的Web测试数据生成与维护方法[J]. 计算机科学，2006，33(10)：272-274

[12] Sant J, Souter A, Greenwald L. An Exploration of Statistical Models for Automated Test Case Generation[C]// Proceedings of the Third International Workshop. St. Louis, Missouri, 2005: 1-7

[13] Ricca F, Tonella P. Analysis and Testing of Web Applications [C] // International Conference on Software Engineering (ICSE2001). Toronto, Ontario, Canada, 2001: 25-34

[14] Halfond W G, Orso A. AMNESIA: Analysis and Monitoring for NEutralizing SQL-Injection Attacks[C] // Proceedings of the IEEE and ACM International Conference on Automated Software Engineering (ASE 2005). Long Beach, CA, USA, 2005: 174-183

[15] Coar K, Bowen R. Apache Cookbook[M]. Sebastopol: O'Reilly Media, Inc, 2003

[16] Apache tomcat[OL]. http://tomcat.apache.org/

[17] 邓小鹏，邢春晓，蔡莲红. Web应用测试技术进展[J]. 计算机研究与发展，2007，44(8)：1273-1283

[18] Ash L, et al. The Web Testing Companion: The Insider's Guide to Efficient and Effective Tests[M]. New Jersey: John Wiley & Sons, Inc, 2003

[19] Nguyen H Q, Johnson B, Hackett M. Web application testing: test planning for mobile and internet-based systems[M]. New Jersey: John Wiley & Sons, Inc, 2003

[20] Powell T A, et al. HTML: The Complete Reference[M]. Columbus: McGraw-Hill Education, 2002

[21] Liu C, Kung D, Hsia P. Object-based Data Flow Testing of Web Application[C]// The First Asia-Pacific Conference on Quality Software. Hong Kong, China, 2000: 7-16

[22] Wassermann G, Su Z. Static detection of cross-site scripting vulnerabilities[C]// ICSE. 2008: 171-180

(上接第45页)

攻击代价的网络抗攻击性能评估指标体系，依据评估样本值之间的相似性和差异性提出了遗传投影寻踪评估模型，采用拒绝服务类攻击方法对被测网络系统进行抗攻击性能评估来验证了算法的有效性。投影寻踪评估算法既充分发挥了投影寻踪处理高维数据的突出优势，又避免了层次分析法等评估方法对人为确定参数或评价指标的不足。

在构造投影指标函数之前，对评估样本数据进行一致无量纲化处理以消除各个评估指标的量纲效应，如何使数据的无量纲化处理更加合理是一个努力的重点。

参考文献

[1] Wack J, Tracey M. Guideline on Network Security Testing [Z]. National Institute of Standards and Technology, 2002

[2] Herzog P. Open Source Security Testing Methodology Manual 2.0 [Z]. http://isecom.securentled.com

[3] 侯一凡. 抗攻击能力评价指标体系的构建与评价方法研究[D]. 郑州：解放军信息工程大学，2007

[4] 鲜明，包卫东，等. 网络攻击效果评估导论[M]. 长沙：国防科技大学出版，2007

[5] 王会梅，江亮，鲜明，等. 计算机网络攻击效果灰色评估模型和算法[J]. 通信学报，2009，30(11A)：17-22

[6] 金菊良，魏一鸣. 复杂系统广义智能评价方法与应用[M]. 北京：科学出版社，2008

[7] 周颖，王雪松，徐振海，等. 雷达电子战效果及效能评估的一般性思考[J]. 系统工程与电子技术，2004，26(5)：617-620

[8] 汪立东. 操作系统安全评估与审计增强[D]. 哈尔滨：哈尔滨工业大学，2002