网络抗拒绝服务攻击性能的集对评估方法

王会梅 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,对网络系统的抗拒绝服务攻击性能评估是抗攻击测试需要解决的一个关键问题。基于集对原理提出了网络抗攻击性能评估的新方法——集对评估法。系统地给出了网络抗攻击性能集对评估法的思路和步骤,考虑等级标准边界的模糊性,提出了采用模糊分析法确定同异反联系度,提出了基于粗糙集属性重要性的指标权重确定方法。最后通过实验验证了集对评估法的有效性和可靠性。

关键词 安全测试,抗攻击性能评估,集对,联系度,拒绝服务攻击
中图法分类号 TP393.08 **文献标识码** A

Set Pair Analysis Method for Evaluating Denial of Service Attack Resistance Ability

WANG Hui-mei 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. A new evaluation method of DoS attack resistance ability based on set pair was presented. The process of systematic analysis DoS attacks resistance ability was broadly put forward. Identity-discrepancy-contrary connection numbers were confirmed by fuzzy method. Using rough set theory, the nonlinear combination weight of evaluation indices was established. A simulation example shows that the approach is brief and effective.

Keywords Security test, Attack resistance ability, Set pair, Connection number, Denial of service attack

拒绝服务攻击已成为网络安全领域最为严重的问题之一,检验网络系统的抗拒绝服务攻击能力已成为安全测评领域亟待解决的问题[1]。从网络抗攻击测试的出发点来看,目前主要包括两种: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指使用攻击的手段来对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。根据各种指标等级标准和相应样本指标间的关系建立评价方法或模型,目前主要有层次分析法[2]、灰评估方法、模糊分析法、投影寻踪法[3]等。但是这些方法较复杂,实施较困难,应用不便。基于集对原理提出了网络抗攻击性能评估的新方法——集对评估法,系统地给出了网络抗攻击性能集对评估法的思路和步骤,采用模糊分析法确定联系度,提出了基于粗糙集属性重要性的指标权重确定方法,最后通过实验对集对评估法的有效性和可靠性进行了验证。

本文第1节从宏观上给出了网络抗拒绝服务攻击性能评估的过程;第2节从攻击效果和攻击代价两个方面研究了网络抗拒绝服务攻击性能评估指标体系;第3节给出了网络抗拒绝服务攻击性能的集对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 网络抗拒绝服务攻击性能评估

网络抗攻击测试是通过对目标实施攻击,来测试和评价系统抵御网络攻击的能力。网络抗攻击测试的主要目的是对目标系统抵御攻击的能力进行测试和评价,采用的主要手段是对目标系统实施真正的攻击,主要测评的思路是通过对攻击作用于目标系统的后果情况来评价目标系统的抵御攻击的能力[4]。网络抗拒绝服务攻击性能评估中实施的攻击为拒绝服务攻击。

网络抗拒绝服务攻击性能评估过程主要包括模拟DoS攻击、信息收集和性能评估。图1所示为网络抗攻击性能评估框架。模拟攻击阶段主要是对测试目标进行有组织协同攻击。为了测试的准确性,引入背景流量来表示测试目标在正常情况下的网络流量。信息收集主要用来检测、收集攻击前

到稿日期:2011-05-02 返修日期:2011-07-18 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;鲜 明(1970—),男,博士生导师,主要研究方向为信息安全、网电空间、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。

后测试网络系统和攻击平台各方面的性能指标。性能评估是在模拟攻击和性能指标数据的基础上，对信息网络系统的抗攻击能力进行定性或定量的评价，并给出测试结果。

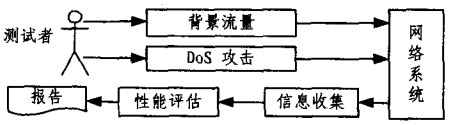

图 1　网络抗攻击性能评估框架

2　网络抗拒绝服务攻击性能指标

网络抗攻击性主要表现为模拟攻击方的攻击代价和抗攻击测试系统方的攻击效果两个方面，故可通过攻击效果和攻击代价来评估网络系统的抗拒绝服务攻击性能。由此，可将抗攻击性能看成是攻击效果和攻击代价的函数，即

$$P=f(I_{e1},\cdots,I_{ei},I_{c1},\cdots,I_{ci}) \tag{1}$$

式中，$I_{e1},\cdots,I_{ei}$ 为抗攻击测试方的攻击效果，$I_{c1},\cdots,I_{ci}$ 为模拟攻击方的攻击代价。

拒绝服务攻击的主要目的是使目标系统正常的服务受到影响或系统功能部分或全部丧失。可分为两种形式：一是利用目标系统或软件漏洞，向目标系统发送一个或多个精心构造的数据包，致使目标系统崩溃、运行异常或重启等，从而导致其无法为正常用户提供服务；另一类为泛洪攻击，使无用的信息占据系统带宽等资源，从而使系统不能服务于合法用户。本文主要研究第二种攻击方式，即利用网络中不同的主机同时发起 DoS 攻击，从而使攻击目标不能正常服务。影响攻击目标网络的性能指标描述如下[5]。

网络带宽利用率($V_{bandwidth}$)反映了网络攻击对目标计算机系统的网络带宽资源的占用情况，值越大表示网络攻击占据的网络带宽越大，则目标网络系统提供正常网络服务的能力就相应地下降越多，从而网络抗攻击性能越差。

CPU 利用率(V_{CPU})反映了网络攻击对目标计算机系统 CPU 资源的占用情况，值越大表示目标计算机系统的可用 CPU 资源越少，相应地可以认为抗攻击性能越差。

丢包率(V_{drop})为单位时间内目标计算机系统丢弃的数据包数量与接收到的数据包总数的比例，反映了网络攻击对网络链路的影响，值越大则表示网络链路状况越差，相应地可以认为抗攻击性能越差。

响应时间($T_{response}$)反映了目标网络负荷的变化情况，值越大表示目标系统处理正常应用的能力越低，从而网络抗攻击性能越差。

恢复时间($T_{recovery}$)是目标计算机从攻击停止到恢复正常工作的时间间隔，反映了攻击效果的延续性，值越大则表示网络攻击对目标计算机系统的影响越久，相应的网络抗攻击性能越差。

攻击代价的评价和分析是抗攻击能力评价的一个重要组成部分。攻击代价是指攻击发起方在攻击中所消耗的物力资源代价以及攻击者自身对实施攻击所消耗的人力操作代价，它反映了攻击者破坏系统安全特性的难易程度。主要包括：

资源消耗($C_{resource}$)主要是指攻击者为了达到攻击目的对本地系统资源的消耗情况。值越大，则网络系统抗攻击性能越好。

操作代价($C_{operate}$)主要指攻击者实施攻击的复杂度和攻击所要持续的时间，可以反映攻击的复杂程度和实施的难易程度。值越大，则认为目标系统的抗攻击性能越好。

3　网络抗拒绝服务攻击性能的集对评估方法

3.1　集对分析理论概述

集对分析理论是一种新型的处理模糊和不确定知识的数学工具，能有效地分析和处理不精确、不一致、不完整等各种不确定信息，并从中发现隐含的知识，揭示潜在的规律。集对分析的核心思想是对不确定性系统中的两个有关联的集合构造集对，对集对的特性做同一性、差异性和对立性分析，并建立集对的同异反联系度[6,7]。

设 A 和 B 为有联系的集合。$A=(a_1,a_2,\cdots,a_n)$，$B=(b_1,b_2,\cdots,b_n)$。A 和 B 构成集对 $H(A,B)$，则 $H(A,B)$ 的联系度为

$$\mu_{A\sim B}=\frac{s}{n}+\frac{f}{n}i+\frac{p}{n}j \tag{2}$$

式中，s 为同一性的个数，f 为差异性的个数，p 为对立性的个数。i 为差异不确定性系数，且 $-1\leqslant i\leqslant 1$；j 为对立系数，且 $j\equiv -1$。记 $a=s/n$，$b=s/n$，$c=p/n$，称 a,b,c 为某特性下的同一度、差异度和对立度，则

$$\mu_{A\sim B}=a+bi+cj \tag{3}$$

式中，$a+b+c=1$。

3.2　集对评估方法

将网络抗拒绝服务攻击性能指标样本中的指标值 x_l 看成集合 $A_l(l=1,2,\cdots,n)$，其中 n 为评价指标数；把相应指标的评价标准看成另一个集合 $B_k(k=1,2,\cdots,K)$，其中 K 为评价等级数，则可构成一个集对。根据集对分析原理，可用 K 元联系度 μ_l 描述集合对 $H(A_l,B_k)$ 的关系，即

$$\mu_l=\mu_{A_l\sim B_k}=a_l+b_{l,1}i_1+\cdots+b_{l,t}i_t+\cdots+b_{l,K-2}i_{K-2}+c_lj \tag{4}$$

式中，a_l 为指标值 x_l 与该指标第 k 级标准的同一度，$b_{l,1}$ 为指标值 x_l 与该指标第 k 级标准相差 1 级的差异度，$b_{l,t}$ 为指标值 x_l 与该指标第 k 级标准相差 t 级的差异度，c_l 为指标值 x_l 与该指标第 k 级标准的对立度。

网络抗拒绝服务攻击性能的集对评估方法的步骤主要包括：

(1)计算 K 元联系度 μ_l

借助三角模糊数来计算 μ：

$$a_l=\begin{cases}1, & x_l\leqslant s_1\\ \dfrac{s_2-x_l}{s_2-s_1}, & s_1<x_l\leqslant s_2\\ 0, & x_l>s_2\end{cases} \tag{5}$$

$$b_{lk}=\begin{cases}\dfrac{x_l-s_i}{s_{i+1}-s_i} & s_t<x_l\leqslant s_{t+1}\\ \dfrac{s_{i+2}-x_l}{s_{i+2}-s_{i+1}}, & s_{t+1}\leqslant x_l<s_{t+2}\\ 0, & \text{others}\end{cases}\quad(1\leqslant t\leqslant K-2) \tag{6}$$

$$c_l=\begin{cases}0, & x_l\leqslant s_{K-1}\\ \dfrac{x_l-s_{K-1}}{s_K-s_{K-1}}, & s_{K-1}<x_l\leqslant s_K\\ 1, & x_l>s_K\end{cases} \tag{7}$$

式中的联系度 μ 可以用图 2(以 $K=5$ 为例)来描述。

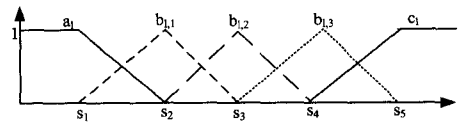

图 2 联系度 $\mu_l(K=5)$

(2)计算集对 $H(A,B)$的 K 元联系度 $\mu_{A\sim B}$

设评价样本为集合 A,评价标准为集合 B,则集对 $H(A,B)$的 K 元联系度 $\mu_{A\sim B}$可定义为

$$\mu_{A\sim B}=\sum_{l=1}^{n}\omega_l u_l=\sum_{l=1}^{n}\omega_l a_l+\sum_{l=1}^{n}\omega_l b_{l,1} i_1+\cdots+\sum_{l=1}^{n}\omega_l b_{l,m} i_m+\sum_{l=1}^{n}\omega_l c_l j \tag{8}$$

式中,ω_l 为指标 l 的权重,它是采用基于粗糙集属性重要性来确定的。

(3)基于粗糙集属性重要性的指标权重确定

把网络抗拒绝服务攻击性能看作一个属性值连续的决策系统 $S=\langle U,C\cup\{d\},V,f\rangle$,其中 $U=\{x_1,x_2,\cdots,x_n\}$是非空有限集合,表示网络抗拒绝服务攻击性能评估样本集;$C=\{a_1,a_2,\cdots,a_m\}$是非空有限条件属性集,即网络抗拒绝服务攻击性能评估指标集;d 表示结果属性,即网络抗拒绝服务攻击性能评估结果;$V=V_C\cup V_d$ 是属性值集合,$V_C=\{V_a\mid a\in C\}$是条件属性值集,V_d 是决策属性值集,第 i 个对象在第 j 个条件属性上的取值 $v_{ij}(i=1,2,\cdots,n;j=1,2,\cdots,m)$是连续变化的;$f:U\times C\cup\{d\}\to V$ 是一个信息函数,表示对 $\forall a\in C$,$x\in U$ 有 $f(x,a)\in V_a$。

利用粗糙集确定网络抗拒绝服务攻击性能评估中的各评估指标权重,实际上就是确定构成被评估各因素知识库中的各个条件属性的重要度。根据求得的各条件属性的重要度,进行权值归一化处理,就可以得到各评估指标的权重,从而达到确定评估指标权重的目的。具体计算方法如下:

a)计算属性重要性 $r(a_k)$

b)归一化处理:

$$\omega_j=\frac{r(a_j)}{\sum_{i=1}^{m}r(a_i)}(j=1,2,\cdots,m) \tag{9}$$

(4)判断样本的评价等级

采用置信度准则

$$h_k=(f_1+f_2+\cdots+f_k)>\lambda,(k=1,2,\cdots,K) \tag{10}$$

来判断样本所属的评价等级,即样本属于 h_k 对应的 k 级。其中 $f_1=\sum_{l=1}^{n}\omega_l a_l$,$f_2=\sum_{l=1}^{n}\omega_l b_{l,1} i_1$,$f_k=\sum_{l=1}^{n}\omega_l c_l j$,$\lambda$ 为置信度,一般在[0.50,0.70]内取值。λ 越大,则评价结果越趋向于保守。

4 实验验证

将集对评价法应用于网络抗拒绝服务攻击性能评价中,探讨其适用性。

4.1 网络抗拒绝服务攻击性能评估实验

测试目标为一台 Web 服务器,分别采用 TCP SYN flood、UDP flood 两类拒绝服务攻击方法对攻击目标进行模拟攻击。建立抗拒绝服务攻击性能评价指标体系:带宽利用率、CPU 利用率、丢包率、响应时间、恢复时间、消耗资源和攻击代价,用 x_1-x_7 表示。网络抗攻击性能评估数据样本如表 1 所列。

表 1 网络抗拒绝服务攻击性能评估数据样本

样本	网络抗拒绝服务攻击性能指标						
	x_1	x_2	x_3	x_4(s)	x_5(s)	x_6(台)	x_7
1	0.61	0.78	0.25	3	15	3	0.3
2	0.27	0.39	0.12	1.2	6	1	0.3
3	0.21	0.29	0.17	1.4	10	3	0.3
4	0.03	0.04	0.01	0.8	1	1	0.3

每个指标分为 5 级:1 级(好)、2 级(较好)、3 级(一般)、4 级(较差)、5 级(差),详见表 2。

表 2 网络抗拒绝服务攻击性能评估分级标准

评价指标	分级标准				
	1 级	2 级	3 级	4 级	5 级
x_1	0.1	0.3	0.5	0.7	0.9
x_2	0.2	0.4	0.6	0.8	0.95
x_3	0.05	0.1	0.3	0.5	0.7
x_4(s)	0.1	1	2	8	30
x_5(s)	2	8	30	100	480
x_6(台)	100	30	10	4	1
x_7	0.9	0.7	0.5	0.3	0.1

根据公式计算各指标与其标准的联系度,并通过粗糙集属性重要性确定指标权重为

$\omega=(0.119,0.102,0.134,0.225,0.201,0.132,0.087)$

计算各样本与标准的联系度,如表 3 所列。根据置信度准则,得到实验的网络抗拒绝服务攻击性能评估结果,依次为“较差”、“较好”、“较好”、“好”。

表 3 联系度

	a	b_1	b_2	b_3	c	评估结果
1	0	0.096	0.353	0.508	0.044	较差
2	0.113	0.607	0.059	0.132	0.087	较好
3	0.110	0.516	0.139	0.175	0.044	较好
4	0.606	0.173	0	0.132	0.087	好

4.2 结果分析

通过分析表 3 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[1,2]。可见集对评价法是简洁、可行而有效的,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 建立了网络抗拒绝服务攻击性能集对评估方法,考虑了等级标准分界的模糊性,避免了直接确定联系度中差异不确定系数。本文方法概念清晰,结构简单,计算简洁,易操作,评价结果可靠。通过实例验证表明,集对评估方法是有效的,可以广泛应用在网络抗攻击性能评估中。

参 考 文 献

[1] Mirkovic J, Reiher P, Papadopoulos C, et al. Testing a collaborative DDoS Defense in a Red Team/Blue Team Exercise[J]. IEEE Transactions on Computers, 2008, 57(8): 1098-1112

(下转第 83 页)

会随着分组发送率的增大而增大，但是由于可用信道数量较多，DIM 协议的固定信道算法对可用信道进行了合理分配，降低了干扰区域内的信道冲突。

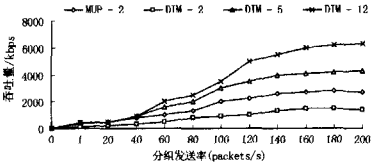

图 7　吞吐量

由此可见，在相同硬件配置情况下，通过增加网络可用信道数量，DIM 协议大大提高了其吞吐量。

(2) 平均分组延迟

分组延迟是指从发送方发出分组到接收方收到分组的这段时间，它是排队时延、退避时延和发送时延之和。平均分组时延是分组时延的平均值，也是衡量上述协议性能优劣的重要指标，可根据下式计算：

$$\text{平均分组延迟}=\frac{\sum\text{成功接收的分组延迟}}{\text{成功接收的分组个数}} \tag{3}$$

网络可用信道数为 2 时，如图 8 所示，DIM 协议数据分组的平均分组延迟始终大于 MUP 协议。这是由于 DIM 协议除了排队延迟、退避延迟和发送延迟等因素外，还要加上信道切换时延。但随着分组发送率的增大，节点间信道冲突增大，数据分组的排列延迟、退避延迟会进一步增大。如图 8 所示，平均分组延迟和分组发送率成正比。

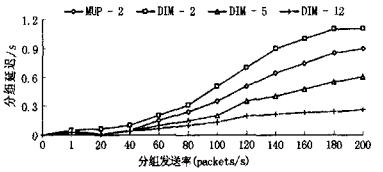

图 8　平均分组延迟

节点配置 DIM 协议，网络可用信道数量分别为 5、12，当分组发送率较小时，信道冲突对分组延迟的影响并不显著。虽然 DIM 协议具有信道数量方面的优势，但是与 MUP 协议相比，其对分组延迟的改善并不明显。但随着分组发送率的增大，信道冲突对网络性能的影响开始增大。此时，DIM 协议在信道数量方面的优势开始显现。由于 DIM 协议的固定信道选择算法在冲突区域内合理分布了信道，因此整个网络的信道冲突相对较少，降低了分组的排队延迟、退避延迟，平均分组延迟得到明显改善。

结束语　本文针对无线信道资源利用率和硬件成本这对矛盾，提出了一种低成本、高利用率的多信道 MAC 协议——DIM 协议。DIM 协议基于标准的 IEEE 802.11 双无线网卡，并且使用信道冲突模型来解决其信道分配问题，优化了网络的信道分布，提高了信道利用率，并在网络吞吐量和分组传输延迟方面有较好的性能改善。实际无线网络应用中，节点可能会配置更多数目的无线网卡，DIM 协议若增加无线网卡分配算法，便能得到有效扩展。无线网卡分配算法能够根据当前和未来一段时间内节点数据发送和接收的情况，合理地设定固定信道网卡和可变信道网卡的数目。这是本文下一步的研究工作。

参 考 文 献

[1] 赵蕴龙，马延龙，李香. 无线 Mesh 网链路不相交多路径路由策略[J]. 哈尔滨工程大学学报，2008，29(9)：967-972

[2] Jungmin S, Nitin V. Multi-channel MAC for Ad-hoc Networks: Handling Multi-channel Hidden Terminals Using A Single Transceiver[C]// Proc. ACM MobiHoc'04. Tokyo Japan, 2004: 222-233

[3] Adya A, Bahl P, Padhye J, et al. A Multi-radio Unification Protocol for IEEE 802.11 Wireless Networks[C]// First International Conference on Broadband Network. California, USA, 2004: 344-354

[4] Kyasanur P, Vaidya N H. Routing and Interface Assignment in Multi-channe Multi-interface Wireless Networks [C] // IEEE Wireless Communications and Networking Conference. USA, 2005: 2051-2056

[5] Raniwala A, Gopalan K, Chiueh T. Centralized Channel Assignment and Routing Algorithms for Multi-channel Wireless Mesh Networks [J]. ACM Mobile Computing and Communications Review, 2004, 8(2): 50-65

[6] Zhu Jing, Roy S. 802.11 Mesh Networks with Two Radio Access Points[C]// IEEE International Conference on Communications. USA, 2005: 3609-3615

[7] 束永安，洪佩琳，覃振权. 无线网状网中基于干扰模型的多信道分配策略[J]. 电子学报，2008，36(7)：1256-1260

[8] Cho S, Kim C-K. Interference-Aware Multi-channel Assignment in Multi-radio Wireless Mesh Networks [J]. IEICE Transactions on Communications, 2010, E91. B(5): 1436-1445

[9] 黄志杰，李峰，高强. 无线多媒体传感器网络实 MAC 协议[J]. 计算机科学，2010，37(11)：81-85

(上接第 55 页)

[2] 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

[3] 王会梅，鲜明，王国玉. 网络抗攻击性能的遗传投影寻踪评估[J]. 计算机科学，2010，37(6)：43-45

[4] Sachdeva M, Kumar K, Singh G, et el. Performance analysis of Web service under DDoS attacks[C]// IEEE International Advance Computing Conference. Patiala, India, March 2009: 1002-1007

[5] Halfond W G J, Choudhary S R, Orso A. Penetration testing with improved input vector identification [C] // International Conference on Software Testing Verification and Validation. Denver, CO, April 2009: 346-355

[6] 赵克勤. 集对分析及其初步应用[M]. 杭州：浙江科技出版社，2000

[7] 王文圣，金菊良，丁晶，等. 水资源系统评价新方法——集对评价法[J]. 中国科学，2009，39(9)：1529-1534