第33卷 第15期 计 算 机 工 程 2007年8月
Vol.33 No.15 Computer Engineering August 2007
·安全技术· 文章编号：1000—3428(2007)15—0160—03 文献标识码：A 中图分类号：TP393.08

一种基于效果评估反馈的入侵响应决策模型

李 杰[1]，龚 俭[2]
(1. 东南大学计算机科学与工程学院，南京 210096；2. 江苏省计算机网络技术重点实验室，南京 210096)

摘 要：响应决策技术是入侵响应领域中的关键技术，该文在综合分析目前应用于响应决策的主要方法的基础上，将响应效果评估和反馈机制引入响应决策中，并提出了一种基于反馈的入侵响应定量决策模型。同时借助于一个实例的分析和计算，证明该模型能够有效地改善人工决策的模糊性，并具有较好的自适应性。

关键词：响应决策；效果评估；反馈机制

Intrusion Response Decision Model Based on Effect Evaluation Feedback

LI Jie[1], GONG Jian[2]
(1. School of Computer Science and Engineering, Southeast University, Nanjing 210096;
2. Computer Network Technology Key Laboratory of Jiangsu Province, Nanjing 210096)

【Abstract】 Response decision is key to intrusion response. Based on the analysis of existing intrusion response decision models, a novel response decision model based on effect evaluation feedback is proposed. Analysis of an example is also presented, by which the accuracy and adaptation ability of the model is proved.

【Key words】 response decision; effect evaluation; feedback

入侵响应是指针对入侵检测系统的报警进行响应决策选择响应方案并执行响应的过程，响应决策是其中的关键部分。对响应决策模型的研究分为定性决策模型和定量决策模型。定性模型主要是基于响应分类技术，需要满足两个条件：(1)该分类必须是面向响应决策的；(2)该分类必须是唯一的。目前的分类技术很难同时满足这两个条件，基于分类的响应决策通常精确度较差。定量决策模型主要是基于代价评估技术，其基本思想是以最小的响应代价实现最大的安全目标[1]。该模型使得响应决策中定量计算成为可能，并使得决策过程更加合理、结果更准确，但同时它也存在一些问题，例如代价分类不够细致，代价量化是面向IDS代价评估而不是面向响应决策的。针对上述的问题，文献[2]对它进行了改进，对代价进行了更细致的分类和更合理的量化。

定量决策模型能够有效地消除响应决策过程中的模糊性和随意性，增强决策过程的准确性，但是其准确性的保证要依赖于响应参数的合理设置。由于响应参数通常由人工设置并带有人为的主观性，因此人的主观因素同样在很大程度影响着响应决策的效率。

反馈控制是控制理论中的一种能够有效动态修正系统的经典方法，因此，为了有效克服响应参数设置的合理性问题，本文以文献[1, 2]提出的代价模型为基础，并借鉴反馈控制的思想，将反馈引入响应决策模型中。由于响应方案的执行情况即执行效果客观地反映了响应决策的准确性，因此本文提出的反馈决策模型是基于响应效果评估的。

1 基于效果评估反馈的响应决策模型

1.1 模型概述

响应决策是入侵响应的重要环节，它通常包括确定响应目标、评价待选响应方案、选择最优方案等步骤。方案的选择依据方案评价的结果，因此，响应目标的确定和针对响应目标的方案评价是响应决策中的关键部分。响应目标一般包括多个方面，例如针对一次攻击事件，系统的响应目标可包括保障系统的可用性和完整性，入侵响应决策本质是一个多目标决策问题。本文根据决策理论[3]和反馈控制的思想，设计了一种基于反馈的入侵响应决策模型，如图1所示。

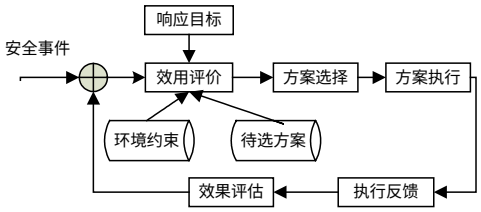

图1 基于反馈的入侵响应决策模型

根据图1，决策模型包括4个部分：效用评价，方案选择，执行反馈和效果评估。效用评价根据响应目标、环境约束和效果评估结果计算待选响应方案的效用值；方案选择则根据效用评价的结果从待选方案集中选择最优的响应方案；执行反馈根据方案的执行情况进行动态反馈；效果评估则根据反馈对响应方案的响应效果进行综合评估。

根据上述的模型，其基本执行流程如图2所示。

基金项目：国家“973”计划基金资助项目（2003CB314804）；江苏省网络与信息安全重点实验室基金资助项目（BM2003201）
作者简介：李 杰(1983－)，男，硕士研究生，主研方向：网络安全；龚 俭，教授、博士生导师
收稿日期：2006-08-17 **E-mail：**jli@njet.edu.cn

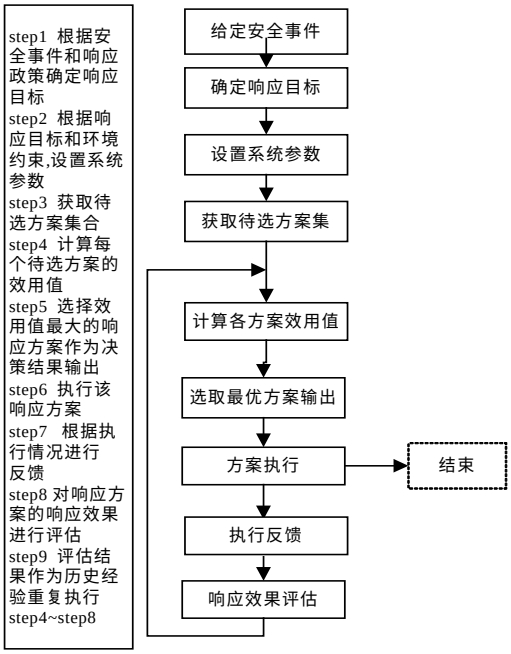

图 2　决策模型执行基本流程

1.2　响应效果评估

(1)评估指标的选取

入侵响应的目标是根除或抑制网络攻击事件对被保护系统的损害，提升被保护系统的安全性能，可以选取若干安全指标对系统的安全性能进行定量或定性的分析，且响应前后系统安全性能的变化可以用来刻画响应执行效果。文献[4]提出了评估网络攻击效果的指标体系和选取方法，由于入侵响应和网络攻击行为存在着对立的关系，本文基于文献[4]的方法并考虑响应目标的制定，从安全机制入手进行系统化地分析，选取评估响应效果的指标体系，表 1 中描述了指标取值类型、对应的安全机制、取值范围等。

表 1　响应效果评估指标体系

指 标	指标描述	安全机制	取值类型	取值范围
CPU 消耗	CPU 的占用比例	可用性	实数型	[0，1]
内存消耗	内存的占用比例		实数型	[0，1]
带宽消耗	带宽的占用比例		实数型	[0，1]
服务损失	系统提供服务的损失比例		实数型	[0，1]
系统免疫能力	系统对该攻击的免疫能力	保密性	实数型	[0，1]
根权限获取	是否泄露超级用户口令		布尔型	0 或 1
普通权限获取	是否泄露普通用户口令		布尔型	0 或 1
文件篡改	是否有文件被篡改	完整性	布尔型	0 或 1
文件删除	是否有文件被删除		布尔型	0 或 1

(2)网络熵与熵差的概念

文献[4]根据信息论中的熵的概念，提出了网络熵理论，网络熵是对系统安全性能的一种描述，网络熵越小则系统安全性越好。对于某一项安全指标来说，其网络熵的定义为 $H_i = -\log_2 V_i$，其中，V_i 为指标归一化参数。因为响应执行后系统的稳定性应该增加所以熵值应该减小，所以可以使用熵差 $\Delta H_i = -\log_2(V_2/V_1)$ 来对响应效果进行描述，其中，V_2 为响应前的指标归一化参数；V_1 为响应后的指标归一化参数。

(3)评估方法

根据网络熵的概念，响应效果可以通过单项指标熵差的加权和[4]描述，见式(1)。

$$\Delta H = \sum_{i=1}^{m} W_i * \Delta H_i \tag{1}$$

其中，ΔH_i 为单个指标的熵差；W_i 为指标i的权重系数。W_i 可以根据特层析分析法AHP[3]进行计算，下面描述其基本原理：

首先根据各项指标建立判断矩阵 A，建立 A 的过程中对指标进行比较的时候采用 1~9 标度作为比较的标准。然后采用专家评分法（Delphi），依重要性程度不同对一级指标层的各指标重要性分别赋值得到 A。设各指标的权向量为 $\overline{W}$，则 $\overline{W}$ 满足 $A\overline{W} = \lambda_{\max}\overline{W}$，$\lambda_{\max}$ 为 A 的主特征根。则 $\overline{W}$ 就为对应的特征向量。计算一致性指标 $CI = (\lambda_{\max} - n)/(n-1)$，并查表得出 n 阶平均随机一致性指标 RI 的值，当一致性比例 $CR = CI / RI < 0.1$ 时，认为判断矩阵具有满意的一致性，否则需要调整判断矩阵的元素取值。将获得的 $\overline{W}$ 进行归一化处理即可得到各指标的权重，最后用用递推的方法可以算得相对于总目标的各指标的权重。

根据式(1)计算得到的 ΔH 的值越大，则说明系统的安全性能在响应后变得越好，即响应效果越好。本文根据熵差的计算结果将响应效果分为 5 个等级，并初步给出 ΔH 对应的取值范围和相应的定量描述，如表 2 所示。

表 2　响应效果评估等级

ΔH	响应效果等级	响应效果定量描述
<0.05	几乎没有效果(5 级)	-2
0.05-0.25	有效果，但效果不理想(4 级)	-1
0.25-1	效果一般，符合预期效果(3 级)	0
1-2.5	效果较好，比预期稍好(2 级)	+1
>2.5	效果很好，大大超过预期(1 级)	+2

1.3　响应效用评价

根据效用理论，待选方案的效用值反映了用户对该方案的偏好程度。文献[1,2]中提出的代价模型是一种有效的效用评价模型。文献[2]将响应代价分为入侵残余代价，响应操作代价和响应负面代价，本文基于这种代价分类将响应效果的评估结果引入响应效用的评价当中。

根据文献[5]网络攻击对系统损害的危害程度和若干因素相关，包括：攻击类型，目标类型，受影响范围等，因此，基于响应目标和文献[2]中的响应代价分类和计算方法，本文将响应代价分为 3 类：可用性损失代价 $Cost_{\text{ava}}$，保密性损失代价 $Cost_{\text{sec}}$ 和完整性损失代价 $Cost_{\text{int}}$，计算方法见式(2)~式(4)，其中，定义 $import$ 为目标重要性系数；V_{sec}，V_{int}，V_{ava} 为攻击对目标保密性、完整性、可用性的损害；λ, ω, φ 分别为响应方案的残余系数、操作代价系数和方案损害服务比例，其取值范围均为[0,1]。

$$Cost_{\text{sec}} = import*(V_{\text{sec}}*\lambda + V_{\text{sec}}(dos)*(\omega+\varphi)) \tag{2}$$

$$Cost_{\text{int}} = import*(V_{\text{int}}*\lambda + V_{\text{int}}(dos)*(\omega+\varphi)) \tag{3}$$

$$Cost_{\text{ava}} = import*(V_{\text{ava}}*\lambda + V_{\text{ava}}(dos)*(\omega+\varphi)) \tag{4}$$

根据解决多目标决策问题的一般方法[3]和响应效用和响应损失代价的反比关系，本文采用加权法评价响应方案的初始效用，见式(5)。

$$E_0=\frac{1}{W_{\text{int}}*Cost_{\text{int}}+W_{\text{sec}}*Cost_{\text{sec}}+W_{\text{ava}}*Cost_{\text{ava}}} \tag{5}$$

其中，代价的计算参照式(2)~式(4)；$W_{\text{int}},W_{\text{sec}},W_{\text{ava}}$ 为损失代价对应的权值，通常根据响应政策设置。

响应决策是存在不确定性的，检测系统和响应系统本身都会产生不确定因素，例如响应方案的实际执行效果。为了克服系统的不确定性，响应方案的效用评价应和历史经验结合起来，本文将响应效果评估结果作为历史经验引入响应方案效用的迭代计算，见式(6)。

$$E_{t+1}(S)=E_t(S)+G*f(\Delta H) \tag{6}$$

其中，$t\geq 1$；G 为一个常数；$f(\Delta H)$ 为熵差的定量描述。

1.4 响应方案选择策略

响应方案选择环节从待选的响应方案集合种选择最优的响应方案作为决策结果输出。本文中的选择策略依据 1.3 节所述的响应方案的效用评价结果，其选择过程如下：

设待选方案集合为S，S_{result} 表示最终的决策结果，则若S中元素个数等于 1，则 S_{result} 即为S中唯一的响应方案；若S元素数大于 1，则 S_{result} 为满足 $E(S_i)=Max(E(S_{1\sim m}))$ 的方案S_i, m为待选方案数。

2 实例分析

本文选择一次典型的 Dos 攻击作为分析实例。该攻击的目标是一个 C 类子网中的邮件服务器，攻击由服务器的一个合法用户主机发起(服务器共有 1 000 个合法用户)，该主机在用户不知情的情况下感染了某种病毒，向服务器大量发送邮件，包括该用户的正常邮件和垃圾，企图消耗带宽和服务器资源，以使服务器服务失效。邮件服务使用的频率很高且使用时间具有随机性，该服务器针对这次攻击的响应目标是保障系统的可用性使其能够提供正常的邮件服务。根据响应经验，针对这样一次攻击行为，通常有如下响应方案。

方案 1　配置防火墙的 ACL，隔离该用户对目标服务器的访问；

方案 2　挂起服务器的 sendmail 进程，停止对所有用户的邮件服务；

方案 3　不进行任何响应。

根据人工响应经验，方案 1 和方案 3 都是可能的选择，方案 1 抑制了攻击但使服务器损失了一个合法用户，方案 3 保障了所有用户的服务但可能使服务器彻底失效，并不能直观上判定哪个方案更优。根据第 1 节所述的决策模型，进行 2 次试验。

首先，根据上述响应目标设置 $W_{\text{int}},W_{\text{sec}},W_{\text{ava}}$ 为 0、0、1，且根据文献[2]，该攻击的 V_{sec}，V_{int}，V_{ava} 为 0、0、30，设置其他参数，见表 3。

表 3　实例分析参数设置

方案	λ	ω	φ	$import$	G
方案 1	0	1/30	1/1000	5	0.05
方案 2	0	1/75	1	5	0.05
方案 3	1	0	0	5	0.05

根据上述的参数设置进行一次试验，根据 1.2 节和 1.3 节提出的公式，其计算结果如下：

$$Cost_{\text{sec}}(1)=V_{\text{sec}}*import*(\lambda+\omega+\varphi)=0$$
$$Cost_{\text{sec}}(2)=V_{\text{sec}}*import*(\lambda+\omega+\varphi)=0$$
$$Cost_{\text{sec}}(3)=V_{\text{sec}}*import*(\lambda+\omega+\varphi)=0$$
$$Cost_{\text{ava}}(1)=V_{ava}*import*(\lambda+\omega+\varphi)=5.15$$
$$Cost_{\text{ava}}(2)=V_{ava}*import*(\lambda+\omega+\varphi)=152$$
$$Cost_{\text{ava}}(3)=V_{ava}*import*(\lambda+\omega+\varphi)=150$$
$$Cost_{\text{int}}(1)=V_{\text{int}}*import*(\lambda+\omega+\varphi)=0$$
$$Cost_{\text{int}}(2)=V_{\text{int}}*import*(\lambda+\omega+\varphi)=0$$
$$Cost_{\text{int}}(3)=V_{\text{int}}*import*(\lambda+\omega+\varphi)=0$$
$$E_0(1)=\frac{1}{W_{\text{int}}*Cost_{\text{int}}+W_{\text{sec}}*Cost_{\text{sec}}+W_{\text{ava}}*Cost_{\text{ava}}}=\frac{1}{5.15}$$
$$E_0(2)=\frac{1}{W_{\text{int}}*Cost_{\text{int}}+W_{\text{sec}}*Cost_{\text{sec}}+W_{\text{ava}}*Cost_{\text{ava}}}=\frac{1}{152}$$
$$E_0(3)=\frac{1}{W_{\text{int}}*Cost_{\text{int}}+W_{\text{sec}}*Cost_{\text{sec}}+W_{\text{ava}}*Cost_{\text{ava}}}=\frac{1}{150}$$

根据初始效用值计算结果最优方案为方案 1，符合笔者的经验。执行该方案，方案得执行使得评估指标发生变化，见表 4，并将指标变化进行反馈。

表 4　响应前后的指标变化

时刻\指标	CPU 占用/%	内存占用/%	带宽占用/%	服务损失/%
响应前	90	90	60	0
响应后	45	45	30	0.1
根权限获取	**普通权限获取**	**文件删除**	**文件篡改**	**免疫能力/%**
0	0	0	0	0
0	0	0	0	0.1

根据上述指标评估响应效果，其中权向量 $\boldsymbol{W}$=(1/6, 1/6, 1/6, 1/6, 1/6, 1/12, 1/36, 1/36, 1/36)，由式(1)算得 $\Delta H=\sum_1^9 W_i*\Delta H_i\approx 2.18$，根据表 2 响应效果为 2 级，同时执行结果也是令人满意的，根据式(6)该方案产生了+0.05 的效用增益，每轮反馈后该方案被选中的几率都被增强。

改变参数设置，将方案 3 的残余系数修改为 0.02 时，此时对应人为造成的参数设置不合理情况，并进行第 2 次实验，与第 1 次试验同样的方式算得 3 种方案的初始效用如下：

$E_0(\text{方案1})=1/5.15, E_0(\text{方案2})=1/152, E_0(\text{方案3})=1/3$

因此根据初始效用计算结最优方案为方案 3 即不响应，结果并不违背响应经验，方案的执行情况如下所述。

由于没有采取任何措施，攻击将持续进行，系统资源和带宽大量被消耗，且随着攻击的进行已出现部分合法用户服务失效，因此系统熵差 $\Delta H<0.05$，响应效果为 5 级。根据式(6)该方案产生了-0.1 的效用增益，重复进行反馈，每轮反馈后该方案的效用变化如下：

$$E_1(2)=E_0(2)-0.05*2=0.567$$
$$E_2(2)=E_1(2)-0.05*2=0.467$$
$$E_3(2)=E_2(2)-0.05*2=0.367$$
$$E_4(2)=0.267$$
$$E_5(2)=0.167$$

根据上述计算结果发现经过 5 轮反馈后，方案 3 的效用值已经减小到 0.167，且小于方案 1 的效用值，方案 1 成为新的决策结果，执行该方案的过程同第 1 次试验。

通过上述的 2 次试验可以发现，该模型能够对响应方案进行定量的评价，由此消除了人为判断的模糊性和随意性。并且在响应参数设置不合理的情况下，该模型能够根据响应执行情况的动态反馈自适应地调整各响应方案的效用值，试验 2 有效地反映了自适应调整的过程，证明了模型是具有定量决策和动态修正的能力的。

3 结束语

目前对响应决策模型的研究主要集中在定量模型上，基

（下转第 204 页）