一种基于智能规划的信息安全风险过程建模方法

王桢珍,武小悦,刘 忠
(国防科技大学信息系统与管理学院,湖南长沙 410073)

摘 要: 为了评估网络信息系统的安全风险,提出了基于智能规划的信息安全风险过程建模方法:使用规划领域的定义语言描述信息安全的风险领域和风险问题,修改后的 bifrost 规划引擎调用相关算法构建系统所有的渗透路径,最后通过 Graphviz Toolkit 接口绘制出规划渗透图表现系统安全风险过程.

关键词: 智能规划; 风险过程; 规划领域定义语言
中图分类号: TP309.2 **文献标识码**: A **文章编号**: 0372-2112 (2008) 12A-076-05

A Planning-based Method of Risk Process Modeling for Information Security

WANG Zhen-zhen, WU Xiao-yue, LIU Zhong
(*Institute of Information System and Management, Changsha, Hunan* 410073, *China*)

Abstract: To evaluate the information security risk, a planning-based information security risk process modeling approach (PISRPMA) was proposed to model the risk process of Information Security. PISRPMA described risk domain and risk problem in planning domain definition language, a modified bifrost engineer reasoned all exploit paths using correlative algorithms and Graphviz Toolkit built a planning exploit graph to model the risk process.

Key words: planning; risk process; planning domain definition language

1 引言

信息安全风险是对某个威胁主体利用网络信息系统的一种或一组脆弱性导致信息系统发生某种安全失效的潜在概率及危害后果的一种度量[1],任何一个网络信息系统都不可能完全消除其中存在的信息安全风险,只能针对系统需求,将信息安全风险掌控在可接受范围内,实现"适度安全",达到信息系统的"可用性"和"安全性"的平衡.信息安全风险渗透过程建模是达到识别系统风险形成原因、描述风险渗透过程、分析风险渗透后果的关键技术,是当前信息安全领域的热点研究问题之一.

研究者们提出了多种网络信息系统风险过程的建模方法[2~7],展示攻击者对目标系统进行安全破坏的所有可能的攻击路径,这些方法都遇到了无法应用于大中型网络系统的问题,究其原因有两个方面:首先,计算复杂度高、网络扩展性差使得这些方法无法适用于现实网络[8];其次,大多建模方法的输入输出采用了非形式化的描述,风险过程难以被系统安全管理员理解,也是很多方法无法应用于现实系统的一个重要原因[9].

本文首次将智能规划[10]的思想引入信息安全风险分析领域,提出了基于智能规划的信息安全风险过程建模方法 PISRPMA (Planning-based Information Security Risk Process Modeling Approach):对系统本身及其安全属性要求进行参数抽象,并采用形式化的规划域定义语言 PDDL (Planning Domain Definition Language) 语言进行描述,归纳推理规则并使用相关算法构建代表网络信息系统信息安全风险过程的规划渗透图 PEG (Planning Exploitation Graph),最后调用 Graphviz Tootkit[7] 接口绘制规划渗透图.相较于以往的信息安全风险过程建模工作,本文提出的建模方法具有以下两点优势:(1) 对风险过程的形式化描述规范直观;(2) 规划渗透图的绘制算法复杂度较低.

2 基本概念

2.1 智能规划

智能规划 (Planning) 是人工智能研究领域近年来发展起来的一个热门分支,它的主要思想是将问题分解为对周围环境进行认识与分析,根据自己要实现的目标,对若干可供选择的动作及所提供的资源限制施行推理,综合制定出实现目标的规划 (Plan). PDDL 语言是智能规划问题设计的标准语言,用于描述一个领域.

收稿日期:2008-08-11;修回日期:2008-11-10

经典的智能规划问题可表述为一个三元组形式 $D=\langle I,A,G\rangle$[11],其中 I 表示初始状态集合,A 表示动作的集合,G 表示目标状态集合. 这类问题要求分别明确给出初始状态、动作特征以及目标状态的描述,动作在这里被描述成为一种改变系统状态的行为,动作序列形成了系统状态的演变,如图 1 所示.

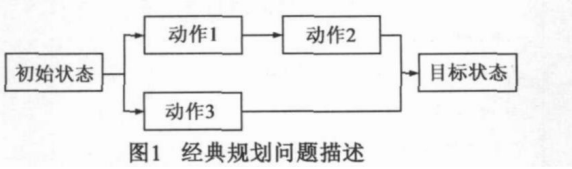

图1　经典规划问题描述

2.2　规划渗透图模型 PEG

定义 1　$PEG=\langle S,s_i,s_g,AE,AEP,L,\delta\rangle$为规划渗透图模型. 其中,$S$ 表示系统状态集合,s_i 表示系统初始状态,s_g 表示风险渗透完成的目标状态,AE 表示原子风险渗透集合,AEP 为所有风险渗透路径集合,L 为标签函数,δ表示单个原子风险渗透实例化的集合.

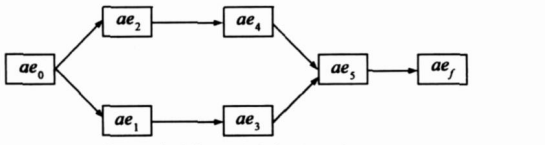

图2　规划渗透图表达形式

规划渗透图的结构如下图 2 所示,满足如下属性:

(1) for $\forall s\in \mathrm{pre}(ae_1)$, $s\subset s_i=ae_0$,表示 $ae_0=s_i$,且渗透路径的第一个风险渗透原子的发生前提集合被 s_i 满足;

(2) $ae_f=s_g\subset \mathrm{post}(ae_{f-1})$,表示 $ae_f=s_g$,且目标状态集合一定包含于最后一个风险渗透原子的后果集合;

(3) if $i\neq j$,then $ae_i\neq ae_j$,即风险渗透路径中不存在重复的两个风险渗透原子,也不存在回路.

3　基于智能规划的信息安全风险过程建模方法

3.1　PISRPMA 系统框架

PISRPMA 方法的系统框架如图 3 所示由三个基本模块组成:信息支持模块、信息收集模块和规划渗透图 PEG 构建模块. 其中信息支持模块负责构建原子风险渗透信息库,其数据来源为目前通用的脆弱性数据库[2],如 CVE、ICAT 等,将在 3.2 节中具体介绍. 信息收集模块使用信息嗅探器[2]如 Nessus 等收集系统本身信息和脆弱性信息,并将其实例化为风险渗透原子模型符合的格式,具体将在 3.3 节介绍. 规划渗透图构建模块包含规划图推理规则和规划图构建算法,并利用 Graphviz Tootkit 绘制出规划渗透图,具体在 3.4 节介绍.

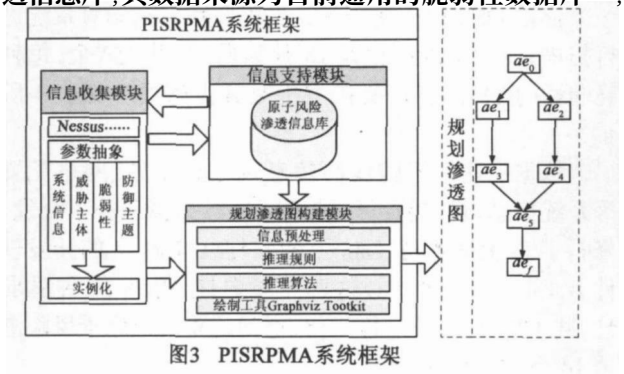

图3　PISRPMA系统框架

3.2　原子风险渗透信息库

原子风险渗透是导致系统状态变化的动作,也是寻求渗透路径这一规划问题中的基本元素,其本质是脆弱性触发的规范表示. 本文选取 CVE 和 ICAT 创建原子风险渗透信息库,并作如下定义.

定义 5　原子风险渗透模型 $AE=\langle \mathrm{pre}(ae),\mathrm{effect}(ae)\rangle,ae$,其中 ae 表示单个原子风险渗透,$\mathrm{pre}(ae)$ 为其发生的前提条件,$\mathrm{effect}(ae)$ 为其发生后产生的影响.

则原子风险渗透表示如下:

$ae=(ae\_ID=\text{“ ”})\wedge(ae\_\mathrm{Name}=\text{“ ”})$

$\mathrm{pre}(ae)$:

$(\mathrm{Service})=\text{“ ”})\wedge(\langle \mathrm{Host}\_s,\mathrm{Host}\_d,port\rangle)$

$\wedge(\mathrm{Attpri}\_pri.[\mathrm{Host}\_s]\geq\text{“ ”})\wedge(\mathrm{Attpri}\_pri.[\mathrm{Host}\_d]\leq\text{“ ”})$

$\mathrm{post}(ae)$:

$(\mathrm{Attpri}\_pri.[\mathrm{Host}\_d]=\text{“ ”})\wedge(\neg(Ser\_\mathrm{Name}=\text{“ ”})$

$(\mathrm{Priescalation}=\text{“ ”})\wedge(Sec\_\mathrm{Loss}=\text{“ ”})$

3.3　信息收集模块

信息收集模块负责两个功能:系统参数抽象和原子风险渗透信息实例化.

3.3.1　系统参数抽象

系统参数抽象是指对目标网络信息系统的主机、网络设备及其之间的关系利用信息嗅探器工具如 Nessus 进行收集,并且按照 3.2 部分中原子风险渗透模型的模式对收集的信息进行参数抽象.

(1) 主机配置

主机配置信息一般包括:系统中存在哪些活动主机、主机上运行了哪些网络服务等,这些配置信息通过转换后用 PDDL 语言描述如下:

(:objectIP_1IP_2-host) 描述了网络中的主机定义,object 为对象定义,host 为预先定义的种类“主机”. 该语句表示系统中有标识为 IP_1 和 IP_2 的两台主机,也可以用主机编号来表示.

(:constants web_apach ftp-service) 描述了系统内存在的服务定义,其中 constants 为常量定义,service 是预先定义的种类“服务”. 该语句表示系统中运行的服务有 web_apach 和 ftp.

(:predicates(runservice ?s-host ?v-service)) 描述了主机 s 上运行了 v 服务,其中 runservice 是预先定义的谓

词,表示某主机上运行了某项服务.

(2) 主机联通关系

主机联通关系描述了主机与主机之间的通信关系,用 PDDL 语言描述如下:

(:predicates(access ?s ?d-host ?v-service)) 描述了主机 s 通过主机 d 上的服务 v 进行两台主机的通信. access 是预先定义的谓词.

(3) 脆弱性信息

脆弱性信息描述了系统中某主机上存在某些脆弱性.用 PDDL 语言描述如下:

(:predicates vulner ?s-host ?m-vulnerability),该语句表示主机上 s 存在脆弱性 m. 其中,vulnerability 是预先定义的谓词.

(4) 攻击者能力

攻击者能力主要以攻击者在主机上获得的权限来表示,一般来说权限有三种:none ,uesr ,root. 用 PDDL 语言描述如下:

(:predicates(none ?s-host)) 表示攻击者在主机 s 上没有权限,即 none.

(:predicates(user ?s-host)) 表示攻击者在主机 s 上拥有 user 权限.

(:predicates(root ?s-host)) 表示攻击者在主机 s 上拥有 root 权限.

3.3.2 系统信息实例化

借助 PDDL 语言的特点,PISRPMA 对系统的实例化工作分为两个部分:风险过程的领域描述和风险过程的问题描述,如图 4 所示.

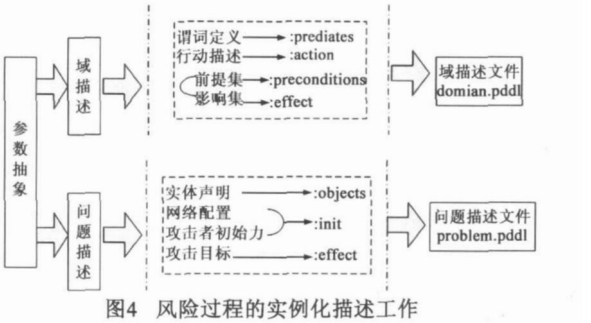

图4 风险过程的实例化描述工作

依据领域定义解决实际问题时,谓词 predicate 和动作 action 构成了完整的领域描述,领域内部实体 objects、领域初始状态 init 和问题目标 goal 构成了完整的基于领域的问题描述. 这种做法可以根据目标系统本身的特定信息,仅从原子风险渗透信息库中提取和目标系统相关的原子风险渗透构成相关渗透路径,减小规划过程中的搜索范围,极大提高了风险过程分析的效率.

3.4 构建规划渗透图

规划渗透图构建模块主要负责如下工作:参照原子风险渗透执行的推理规则及规划渗透图构建算法,调用 Graphviz Tootkit 接口绘制规划渗透图,其绘制算法如下:

算法:规划渗透图绘制算法
输入:规划渗透图模型 PEG
输出:图形化的规划渗透图模型
设 N 为已经绘制的节点集合,E 为已经绘制的边集合,
令 $E=\Phi, N=\Phi$.
for each $aep_i \in AEP$ do
for each $ae_j \in aep_i (j>0)$ do
if $ae_j \notin N$ then
CreateNode(ae_j);
$N = N + ae_j$;
end if
if $e(ae_{j-1}, ae_j) \notin E$ then
CreateEdge(ae_{j-1}, ae_j);
$E = E + e(ae_{j-1}, ae_j)$;
end if
end for
end for

注:绘制规划渗透图算法的时间复杂度与原子风险渗透集合元素的数目和每条渗透路径的原子风险渗透数目相关,其最大时间复杂度为 $O(|AEP| * |AE|)$.

4 应用实例

试验网络信息系统环境[21]由一个信息中心、5 个实验施和一个管理部门组成. 信息中心中共有 4 台服务器,分别运行 S_1:Apached; S_2:Ftpd; S_3:Sendmail; S_f:Mysqld 四个服务程序. 每个实验室有 20 台工作站,同一个实验室的计算机软件配置基本相同. 管理部门中也有 20 台计算机. 防火墙将外部网络和内部网络隔开,只允许外部主机 a_1 访问服务区 S_1 上的 Apached 服务和 S_2 上的 Ftpd 服务,其它外部访问均被禁止. 攻击者位于外部网络主机 a_1 上,渗透目标为获取主机 S_f 上的数据库文件,即获取 S_f 主机的 root 权限. 试验系统的测试环境如下:CPU 为 Pentium 4 1.8GHz 以及 512MB 内存,操作系统为 windows xp sp2,PISRPMA 使用的推理引擎为修改后的 bifrost[12].

4.1 原子风险渗透信息库的建立

依据 PISRPMA,使用 Nessus 脆弱性扫描器对系统进行扫描,发现系统中存在 18 种脆弱性,共 150 个,每种脆弱性的 CVE 编号、所在主机及其渗透类型如表 1 所示.

依据上述系统脆弱性信息及主机配置、网络配置等系统信息,对实验系统进行了病毒扫描和补丁分发,修补了 S_2 上的木马、Lab_1 上的软件 A、Lab_4 上的开发软件 B、Lab_5 上的软件 C 这四类脆弱性,得到 14 种脆弱性,共 119 个. 对其进行简化,得到试验系统原子风险渗透 14 个,如表 2 所示.

表 1　系统脆弱性信息

序 号	脆弱性编号	运行的服务	所在主机	脆弱性的渗透类型
1	CVE-2004-0646	Apache	WebServer	远程缓冲溢出
2	CVE-2005-3524	Ftpd	FileServer	远程缓冲溢出
3	DEF-2007-0001	Linux、Ftpd	FileServer	木马渗透
4	CVE-2001-0588	Sendmail	MailServer	本地缓冲溢出
5	CVE-2002-1337	Sendmail	MailServer	远程缓冲溢出
6	DEF-2007-0002	Linux	DBServer	信任渗透
7	CVE-2004-0628	MySQL	DBServer	远程缓冲溢出
8	CVE-2004-0836	MySQL	DBServer	远程缓冲溢出
9-20	CVE-2007-3825	alert.exe	Lab_1	远程缓冲溢出
21-30	DEF-2007-0003	某开发软件 A	Lab_1	远程缓冲溢出
31-50	CVE-2006-3441	DNS Client	Lab_2	远程缓冲溢出
51-70	CVE-2005-1984	Spoolsv.exe	Lab_3	远程缓冲溢出
71-80	DEF-2007-0004	某开发软件 B	Lab_4	远程缓冲溢出
81-90	CVE-2006-2382	iexplore.exe	Lab_4	远程缓冲溢出
91-100	DEF-2007-0005	某开发软件 C	Lab_5	远程缓冲溢出
101-110	CVE-2006-3440	Winsock API	Lab_5	远程缓冲溢出
111-130	DEF-2007-0006	某办公软件 D	Man_i	远程缓冲溢出
131-150	CVE-2006-4702	WMP	Man_i	远程缓冲溢出

表 2　简化后的原子风险渗透信息

原子风险渗透编号	脆弱性 ID 号	所在主机	原子风险渗透编号	脆弱性 ID 号	所在主机
ae_1	CVE-2004-0646	WebServer	ae_8	CVE-2007-3825	Lab_1
ae_2	CVE-2005-3524	FileServer	ae_9	CVE-2006-3441	Lab_2
ae_3	CVE-2001-0588	MailServer	ae_{10}	CVE-2005-1984	Lab_3
ae_4	CVE-2002-1337	MailServer	ae_{11}	CVE-2006-2382	Lab_4
ae_5	DEF-2007-0002	DBServer	ae_{12}	CVE-2006-3440	Lab_5
ae_6	CVE-2004-0628	DBServer	ae_{13}	DEF-2007-0006	Man_i
ae_7	CVE-2004-0836	DBServer	ae_{14}	CVE-2006-4702	Man_i

```
Domain.pddl
(define (domain network)

/ *定义本系统内常量的类型主机、服务及脆弱性 */
(:types host service vulnerability)
/ *定义表述系统状态的谓词 */
(:predicates (trust ? s ? d-host) / *定义主机间信任关系 */
    (user ? s-host) / *定义攻击者权限 */
    ……
    (access ? s ? d-host ? v-service) / *定义主机间连接关系 */
    ……
    (vulner ? d-host ? m-vulnerability)) / *定义主机上有脆弱性 */
/ *定义系统内常量:主机和脆弱性 */
(:constants Telnetd Apached Ftpd Mysqld-service CVE-2005-3524 DEF-
2007-0001 ……-vulnerability)
/ *定义推理规则 */
(:action local-bufOverflow
  :parameters (? d-host)
  :precondition (and (vulner ? d CVE-2006-2451)
        (user ? d)
        (not (root ? d)))
  :effect (root ? d)
)
) / *本地缓存溢出渗透 */
```

图 5　试验系统领域描述的显示

4.2　试验系统的领域描述和问题描述

在此,试验系统的领域描述和问题描述只给出了部分信息的描述,从对试验系统的领域描述和问题描述不难看出,PDDL 的系统信息实例化表现方式直观易懂,而且,可以自定义谓词,随着系统规模的扩大,其语法结构可以保持相对稳定.

(1) 试验系统的领域描述(见图 5)

(2) 试验系统的问题描述(见图 6)

```
Problem.pddl
(define (problem fixit)
  (:domain network)
  / *定义 host 对象 */    (:objects S1 S2 S3 Sf ……-host)
  / *定义系统初始状态 */
  (:init (user S1)
  ……
  (:goal (root Sf))) / *定义攻击者目标为获取 Sf 上的 root */
```

图 6　试验系统问题描述的 PDDL 显示

4.3　试验性能分析

为了验证 PISRPMA 方法的实用性,我们将系统的网络连接关系分为服务区主机都能访问工作区(E_1)、$s1$ 和 $s2$ 能够访问工作区(E_2)、$s1$ 能够访问工作区(E_3)和都不能访问工作区(E_4)四种情况,观察不同情况下

方法的实验效果.

图 7 显示了随着网络脆弱性数目的增加,四种网络连接关系下的渗透路径条数的变化趋势. 在脆弱性数目为 400 的情况下, E_1 产生的渗透路径为 4500 条, E_2 为 700 条, E_3 为 85 条, E_4 为 10 条,说明网络连接关系是影响网络安全的重要因素,合理的安全策略应该阻断一切没有必要的网络连接,如从服务区主动连向工作区的请求.

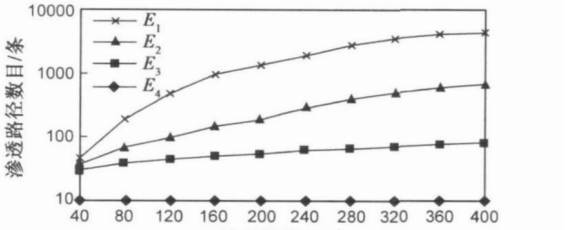

图7 网络连接—渗透路径数目变化情况

图 8 反映了在两种网络连接关系下随着脆弱性数目的增加,绘制规划渗透图所需 CPU 消耗时间的变化趋势. 在网络连接关系 E_1,400 个脆弱性的情况下,所需时间为 34.6 秒,从时间复杂度的角度证明了 PISRPMA 完全适应对大规模网络的进行安全分析,同时也表明网络连接时间效率.

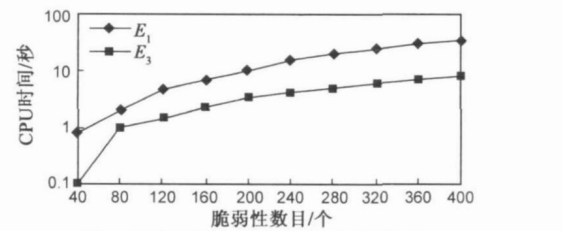

图8 网络连接—CPU时间变化情况

5 结论和展望

本文提出了一种基于智能规划的信息安全风险过程建模方法 PISRPMA,采用形式化的逻辑语言 PDDL 描述了系统本身及其安全属性的要求,调用 Graphviz Tootkit 接口绘制规划渗透图. 相较于以往的信息安全风险过程建模工作,本文提出的建模方法具有以下优势:(1) 对风险过程的形式化描述规范直观;(2) 规划渗透图的绘制算法复杂度较低.

PISRPMA 目前也存在一些不足之处,后续的工作主要在以下几个方面:(1) 原子风险渗透信息库的继续完善,目前仅是针对具体系统进行了原子风险渗透信息的转变,要增强其适用性需要信息库知识的不断完善、维护和更新;(2) 系统信息的进一步全面抽象,实际网络信息系统中的网络连接关系非常复杂,涉及到网络设备、安全设备等多个方面的因素,尤其是安全设备的使用后会导致连接关系复杂性的爆发;(3) 原子风险渗透推理规则的归纳简练及规划渗透图的构建算法的可扩展性、完备性的研究,而且我们相信随着规划引擎的进一步完善,规划渗透图的构建效率会进一步提高.

作者简介:

王桢珍 女,1980 年出生于安徽合肥,博士研究生,主要研究方向为信息安全风险评估、风险分析与决策.

E-mail:wangzhenzhen_2005@hotmail.com

武小悦 男,1963 年出生于山西平遥,博士生导师,研究领域包括装备系统论证与决策分析、系统工程.

E-mail:xiaoyuewucn@yahoo.com.cn

参考文献:

[1] 陈光. 信息系统信息安全风险管理方法研究[D]. 长沙:国防科技大学研究生院,2006.
Chen Guang. Research on method of information system information security risk management [D]. Changsha: Graduate School of National University of Defense Technology,2006.

[2] 毛撼东. 基于逻辑渗透图模型的网络安全风险评估方法研究[D]. 长沙:国防科技大学研究生院,2008.
Mao Han-dong. A novel assessment approach based on logical exploitation graph model for network security[D]. Changsha: Graduate School of National University of Defense Technology,2008.

[3] Ou Xin-ming. A scalable approach to attack graph generation [A]. Proceedings of the 13th ACM Conference on Computer and Communications Security[C]. Alexandria Virginia, USA: ACM,2006. 336 - 345.

[4] O Sheyner. Scenarios Graphs and Attack Graphs [D]. Pittsburgh, Pennsylvania, USA: Department of Computer Science, Carnegie Mellon University,2004.

[5] P Ammann, D Wijesekera, S Kaushik. Scalable, graph-based network vulnerability analysis [A]. Proceedings of the 9th ACM Conference on Computer and Communications Security [C]. Washington DC, USA: ACM,2002. 217 - 224.

[6] Li Wei. An approach to model network exploitations using exploitation graph[J]. SIMULATION,2006,82(8):523 - 541.

[7] L Swiler, C Philips, D Ellis, et al. Computer-attack graph generation tool[A]. DARPA Information Survivability Conference and Exposition Proceedings[C]. Anaheim, CA, USA: IEEE, 2002. 307 - 321.

[8] Lippmann R, K W Ingols. An Annotated Review of Past Papers on Attack Graphs[R]. Project Report IA-1, Lexington, Massachusetts: Lincoln Laboratory of Massachusetts Institute of Technology,2005.

[9] Wei Li. An Approach to Graph-Based Modeling of Network Exploitations[D]. Mississippi State: Mississippi State University,2005.

(下转第 70 页)

Kang Wei-xin. The test of pile foundation integrity based on wavelet analysis[J]. Journal of Electronic Measurement and Instrument, 2002, 16(2): 23 - 25. (in Chinese)

[3] kangweixin, pengxiyuan. Wavelet characteristic and experimental study of pile foundation fracture[J]. 7th International Conference on Electronic Measurement & Instruments (ICEMI). 2005, 6: 302 - 305.

[4] 康维新, 彭喜元. 桩基小波特征的研究[J]. 电子测量与仪器学报, 2005, 19(5): 25 - 27.
Kang Wei-xin, Peng Xi-yuan. Pile foundation wavelet characteristic[J]. Journal of Electronic Measurement and Instrument, 2005. 19(5): 25 - 27. (in Chinese)

[5] V N Vapnik. An overview of statistical learning theory[J]. IEEE Trans on Neural Networks, 1999, 10(5): 988 - 999.

[6] Cortes C, Vapnik V. Support vector networks[J]. Machine Learning, 1995, 20: 273 - 297.

[7] Scholkopf B, Sung K, Burges C, Girosi F, Niyogi P, Pogio T, Vapnik V. Comparing Support Vector Machines with Gaussian Kernels to Radial Basis Function Classifiers[R]. A. I. Memo1559, MIT, 1996.

[8] 张学工. 关于统计学习理论与支持向量机[J]. 自动化学报, 2000, (26)1: 32 - 42.
Zhang Xue-gong. Introduction to statistical learning theory and support vector machines[J]. Acta Automatica Sinica, 2000, 26(1): 32 - 42. (in Chinese)

作者简介:

康维新 男, 1963 年 4 月出生于黑龙江富锦, 哈尔滨工业大学自动化测试与控制系博士研究生, 主要从事自动测试与仿真、故障诊断和预测等研究工作.
E-mail: kangweixin@hrbeu.edu.cn.

彭喜元 男, 教授、博士生导师, 1961 年生于内蒙古四子王旗, 哈尔滨工业大学电气工程及自动化学院副院长, 主要研究方向为自动测试技术和智能故障诊断理论等.
E-mail: pxy@hit.edu.cn

(上接第 80 页)

[10] Russell, Stuart, Peter Norvig. 人工智能[M]. 北京: 人民邮电出版社, 2004.

[11] 宋泾舸, 查建中, 陆一平. 智能规划研究综述 ——一个面向应用的视角[J]. 智能系统学报, 2007, 2(2): 18 - 25.
Song Jian-ge, Cha Jian-zhong, Lu Yi-ping. Survey on AI planning research - an application - oriented perspective[J]. CAAI Transactions on Intelligent Systems, 2007, 2(2): 18 - 25.

[12] R M Jensen, M M Veloso, R E Bryant. Guided symbolic universal planning[A]. Proceedings of the 13th International Conference on Automated Planning and Scheduling[C]. Trento, Italy: IEEE, 2003. 123 - 132.