

文章编号: 1001-0920(2007)08-0951-05

基于粗糙集的网络信息系统安全评估模型研究

林梦泉^{1a,2}, 王强民^{1b}, 陈秀真^{1b}, 李建华¹

(1. 上海交通大学 a. 电子工程系, b. 信息安全工程学院, 上海 200030;

2. 教育部 学位与研究生教育发展研究中心, 北京 100083)

摘要: 从分析网络信息系统安全评估标准指标出发, 提出基于安全树的信息系统安全最佳节点基本属性模型, 并对相关评估指标进行优化; 在此基础上, 提出一种基于粗糙集的混合启发式约简算法, 进行指标属性约简和权重集构建, 进而建立融合的信息系统安全评估数学模型. 最后通过实例说明该安全评估模型建立方法的有效性及其实用性.

关键词: 网络信息系统; 粗糙集; 混合启发式约简; 安全评估模型

中图分类号: TP393.08

文献标识码: A

Study on network information system security assessment model based on rough set

LIN Meng-quan^{1a,2}, WANG Qiang-min^{1b}, CHEN Xiuzhen^{1b}, LI Jian-hua¹

(1a. Department of Electronic Engineering, 1b. School of Information Security Engineering, Shanghai Jiaotong University, Shanghai 200030, China; 2. Center of Degree and Graduate Student Education Development, Ministry of Education, Beijing 110083, China. Correspondent: LIN Meng-quan, E-mail: linmq@cdgdc.edu.cn)

Abstract: Through analyzing the concept of network information system security from multi-criterion factors, an information system security basic attribute model is proposed and the relevant assessment criteria are optimized. Then a heuristic rough set algorithm is proposed to reduce the attributes and build weight set. In addition, an information system security model is established. The examples show the effectiveness and the practical value of the method.

Key words: Information system; Rough set; Mixed heuristic reduction algorithm; Security assessment model

1 引言

随着各类新型网络信息系统的不断涌现, 网络应用已成为政府、企事业单位、科技、教育、金融甚至社区服务不可缺少的管理手段. 网络安全问题已受到广泛关注. 随着人们对安全问题危害性认识的不断深入, 信息安全问题也从被动解决问题、技术防范等发展到管理防范的阶段, 信息系统安全管理问题已成为该领域研究的热点之一. 要安全、有效地运营和管理网络信息系统, 对其网络信息系统安全性进行评估是必不可少的.

目前, 许多学者在信息安全评估中应用有型资产评估理论, 研究信息系统安全的风险评估, 并取得了一些研究成果^[1,2]. 但风险评估方法一般需要一些先验知识, 如威胁出现的概率、无形资产的赋值等, 而要准确获得这些数据在实际中存在一定的困

难. 有人采用模糊、神经网络、灰色理论等方法建立信息安全评估模型, 但大多侧重于对局部系统的评估, 仅局限于技术层面, 且多见于理论研究. 本文从技术、管理、安全意识等更加宏观的层面审视信息安全及其评估问题, 认为基于安全因素的树型结构安全模型是描述信息安全更有效的模型, 提出了树型结构最佳节点基本模型的概念. 在此基础上, 应用粗糙集理论对系统进行约简优化并确定安全属性重要性权集, 进而获得更具有实际意义且优化的信息系统安全评估解决方案.

2 信息系统安全评估最佳节点基本模型

本文讨论的基于粗糙集理论的信息系统安全评估模型, 是以信息系统安全树型结构的安全模型为理论基础, 如图 1 所示. 依据系统中各安全因素对系统整体安全的影响以及影响程度来度量系统整体安

收稿日期: 2007-02-06; 修回日期: 2007-05-09.

基金项目: 国家自然科学基金项目(60605019/F030509); 教育部委托学位与研究生教育学会“十一·五”重大课题项目(06W0100a).

作者简介: 林梦泉(1959—), 男, 福建仙游人, 副研究员, 博士生, 从事网络信息系统安全评估、教育评估等研究; 李建华(1965—), 男, 江西九江人, 教授, 博士生导师, 从事网络安全综合管理、信息系统安全评估等研究.

全性,该评估模型具有许多优点^[3,4].但信息系统安全因素涵盖系统的各个层面,按目前国内外公认的CC和BS7799的安全准则,约有350余个安全因素,模型指标数量庞大.在评估整个信息系统安全状况时,全面地按最底层的安全因素进行测评,对庞大的末级控制点与通过多级权重折算的权重集进行加权综合来评价整体安全,所产生的积累误差容易造成总体安全的测量偏差,甚至出现错误的结论.另外,树型结构的评估模型权重集的构造也是个难题,目前多采用AHP和Delphi等方法构造,而这些方法需要大量的样本或进行问卷调查.当指标维数较大时,这些方法的算法应用和结果可用性还存在不少问题.

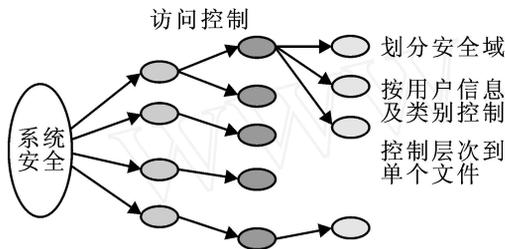


图1 信息系统树型安全模型

2.1 信息系统安全指标优化的基本问题

基于树型结构信息安全评估模型的安全指标(安全因素)通常具有相关性.采用相关性理论进行分析,去除相关性大的安全指标,可以简化模型,降低模型维数,但相关性分析需要确定性的数据才能实现.应用粗糙集理论,可在积累一定的信息系统评估数据的基础上,利用约简原理得到更加简洁、易于实施的安全评估模型.

应用粗糙集理论对模型进行优化时,一般不需要提供求解问题时所需处理的数据集合之外的任何先验知识,仅对实测数据本身进行分类处理即可挖掘隐含知识,揭示潜在于数据内部的规律;能在保留关键信息的前提下对有关数据进行化简并求出知识的最小表达;能从经验数据中获取易于验证的分类规则.

人们总是希望约简中的属性尽量的少,从而降低用简化模型对信息系统进行安全评估的成本.但根据粗糙集基本原理对信息系统相应的数据库进行知识获取并约简时,可能产生多个约简结果,约简后属性的个数将直接影响粗糙集理论导出规则的多少.信息系统或决策表的最小约简过程实际上是一个迭代过程.Wong和Ziarko^[5]早在1985年已证明,找出最小约简的过程是个NP问题.

2.2 信息系统安全最佳节点基本模型的建立

根据以上分析可知,所建指标项越少,对粗糙集

约简算法的实现越有利.因此,本文提出了根据评估经验和信息安全专家知识,对信息系统树型结构的原始安全指标集进行分析和分类,选择树型模型上合适的节点构建安全评估模型,实现模型初步简化的思想.图1中的第3层次安全要素包含“重要信息划分系统安全域”等80多个指标,第2层指标可归纳“访问控制”等30余个指标,每个2级一般包含若干个3级指标.在进行系统安全评估时,只需对第2层指标进行评价,因此,第2层指标构成的安全评估模型称为最佳节点基本评估模型.基本模型既降低了粗糙集约简需要处理的维度,减少了系统评估所需信息的冗余,又使得评估实施快捷有效.

3 混合启发式粗糙集约简评估模型

应用粗糙集理论可对不同层次指标的评估数据进行约简,优化评估模型.这里探讨基于粗糙集的信息系统安全模型描述、约简过程及算法特征,同时研究基于属性权重集的混合启发式约简算法,以使约简更快捷,约简的模型更加合理.

3.1 基于粗糙集的信息系统安全模型描述

作为一个安全评估原始信息系统,在粗糙集理论中可用一个4元组来表示和处理知识,即

$$S = (U, A, V, f). \quad (1)$$

其中: U 为论域,信息系统中研究对象的非空有限集合,界定为多个同类网络信息系统采集到的大量网络安全相关信息对对象集,即信息表中的元组(样本), $U = \{x_1, x_2, \dots, x_N\}$, x_i 为元组, $i = 1, 2, \dots, N$; A 为对象属性非空有限集合, $A = \{a_1, a_2, \dots, a_M\}$, a_j 为对象属性, $j = 1, 2, \dots, M$, $A = C \cup D$, C

$D = \dots$, C 称为条件属性集合,是采集到信息经分析整理后得到网络信息系统的安全要素, D 称为决策属性集(即评估结果集 R),表示安全度量,具有条件属性和决策属性的信息系统称为决策表; V 为属性值的非空有限集,是属性值域集, $V = \{v_1, v_2, \dots, v_M\}$, v_j 为属性 a_j 的值域, $j = 1, 2, \dots, M$; f 为信息函数, $f: U \times A \rightarrow V$, $f(x_i, a_j) = v_j$ 是元组 x_i 在属性 a_j 处的取值, $i = 1, 2, \dots, N$, $j = 1, 2, \dots, M$.

式(1)表示的安全评估原始信息系统可能存在属性依赖性、决策规则重复性和冗余属性.运用粗糙集理论对式(1)表示的安全评估原始信息系统进行属性约简,得到等价的约简信息系统

$$S^0 = (U^0, A^0, V^0, f^0). \quad (2)$$

其中:原始论域与约简论域关系为 $U^0 = \{x_1^0, x_2^0, \dots, x_n^0\} \subseteq U = \{x_1, x_2, \dots, x_N\}$, $n \leq N$;原始属性与约简属性关系为 $A^0 = \{a_1^0, a_2^0, \dots, a_m^0\} \subseteq A = \{a_1, a_2, \dots, a_M\}$, $m \leq M$;条件属性关系为 $C^0 \subseteq C$;决策属性关系为 $D^0 \subseteq D$.

建立信息系统安全决策表是进行粗糙集约简的基础。根据 n 个同类网络信息系统评估数据, 建立如式 (1) 所示的原始信息系统安全评估信息决策表, 见表 1。在评估信息决策表的基础上, 充分利用粗糙集的属性约简能力来度量安全要素的重要性, 删除对安全评估结果无影响或影响很小的安全因素 (即重要性为 0 或很小的安全因素)。

表 1 信息系统安全评估原始决策表

$S = (U, A, V, f)$		属性 $A = C, D$, 条件属性 C , 决策属性 D		
		a_1	...	a_M
对象	x_1	v_{11}	...	v_{1M}
	x_2	v_{21}	...	v_{2M}

U	x_N	v_{N1}	...	v_{NM}

3.2 信息系统约简特征分析

根据粗糙集理论和方法, 约简与决策表一致性有关, 因此首先需要进行一致性分析。一致性决策表约简和不一致性决策表约简的逻辑关系如图 2 所示。

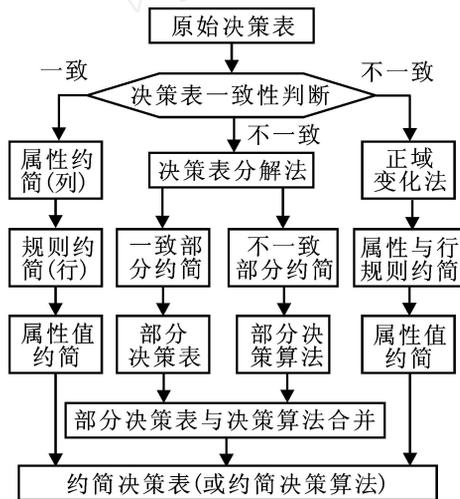


图 2 粗糙集约简全过程

目前采用粗糙集理论进行约简, 一般是将决策表看成一致性的, 而实际上系统决策表存在非一致性情况。

当决策表中的决策属性集全部依赖于条件属性集时, 即 $C \Rightarrow D$ 时, 决策表 $T = (U, A, C, D)$ 是一致的; 否则, 决策表是不一致的。根据粗糙集理论, 决策表的一致性决定所用的约简方法和算法。通过计算条件属性与决策属性之间的依赖程度可以判断决策表的一致性。属性间依赖度用 k 表示, 并定义为

$$k = (\text{card}(\text{POS}(C, D)) / \text{card}(C, D)). \quad (3)$$

当依赖程度等于 1 时, 决策表是一致的; 否则不一致。

决策表一致性还可通过计算决策属性集合 D 下近似 $C_*(D)$ 、正域 $\text{POS}_C(D)$ 和论域 U 之间的关系来判断。如果 3 者关系满足下式:

$$\text{POS}_C(D) = C_*(D) = U, \quad (4)$$

则决策表是一致的; 否则不一致。

约简算法运行之前, 需进行以上判断, 再选择相应的约简方法。

4 安全模型重要性启发式约简

对于决策表一致性和不一致的情况, 其约简方法是不同的。本文以最重要的一致性条件下约简为重点, 提出混合启发式约简的新方法。

4.1 条件属性基本约简方法

运用粗糙集理论和方法对决策表进行约简。首先删除对象属性中依赖于其他属性的非独立属性; 然后合并条件属性和决策属性都相同的对象; 最后消除决策规则中不必要的条件属性, 得到式 (2) 表示的约简的信息系统安全模型。设信息系统 $S = (U, A, V, f)$ 的分明矩阵为 $M(S) = [c_{ij}]_{N \times N}$, 矩阵项的定义为

$$c_{ij} = \{a \in A \mid a(x_i) = a(x_j), i, j = 1, 2, \dots, N\}. \quad (5)$$

其中 c_{ij} 是对象 x_i 和 x_j 有区别的所有属性的集合, 分明矩阵具有对称性, 可用 $M(S)$ 的下三角表示 $M(S)$ 。分明矩阵对应的唯一分明函数 $f_{M(S)}$ 是一个含有变元 $a_i (a_i \in A, i = 1, 2, \dots, M)$ 的布尔函数, 它是 c_{ij} 的合取 (交), c_{ij} 是矩阵项 c_{ij} 中各元素的析取 (并), $1 \leq j < i \leq N$ 且 c_{ij} 。

根据分明函数与约简的对应关系, Skowron^[6] 提出了信息系统的约简方法:

- 1) 计算信息系统的分明矩阵 $M(S)$;
- 2) 计算与分明矩阵对应的分明函数 $f_{M(S)}$;
- 3) 计算分明函数 $f_{M(S)}$ 的最小析取范式, 其中每个析取分量对应一个约简。

该方法可求出所有的约简, 但当对象和属性的规模较大时, 矩阵将占用大量的存储空间, 因此, 只适用于非常小的数据集。当数据量较大时, 需要寻求一种改进方法处理求解问题。

4.2 混合重要性启发式属性约简方法

粗糙集约简计算是 NP-hard 问题, 且约简有多个理论计算结果, 不便于实际应用。为使约简结果更符合实际, 并融合专家知识和经验, 本文应用安全系统属性的重要性作为约束条件, 并作为启发规则应用于约简过程。启发式约简使用核作为计算约简的基点, 按照属性的重要度从大到小逐个加入属性, 直到该集合是一个约简为止, 从而得到一个较优或满足用户要求的次优约简。

信息系统安全情况复杂, 安全要素较多, 特别是在计算机网络系统迅速发展的今天, 网络信息系统建设剧增, 系统结构繁杂, 如教育科研、金融系统、

敏感系统、水电系统、社会服务系统等。这些系统对于安全需求及需求的侧重面不同,根据专家知识及用户经验获得的属性重要性系数,具有重要的实际价值。本文将由实际经验获得的经验重要性权集和约简重要性综合,如加权平均,作为最终的启发规则,使约简的结果更加切合实际,更优化。

4.2.1 属性重要性的定义

根据依赖度的变化,设 S 为一决策表, C 和 D 分别为条件属性集和决策属性集。 $R \subset C$, 对于任意属性 $a \in C - R$ 的重要性定义为

$$\text{SGF}(a, R, D) = k(R \cup \{a\}, D) - k(R, D), \quad (6)$$

其中

$$k(R, D) = \text{card}(\text{POS}_R(D)) / \text{card}(\text{POS}_C(D)).$$

重要性还可定义为

$$\text{SGF}(a, R, D) = r_{R \cup \{a\}} - r_R, \quad (7)$$

其中

$$r_R = \text{card}(\text{POS}_R(D)) / \text{card}(U).$$

根据信息熵,设 $H(D/R)$ 为 D 相对于 R 的条件熵,属性 a 的重要性定义为

$$\text{SGF}(a, R, D) = H(D/R) - H(D/R \cup \{a\}). \quad (8)$$

根据分明矩阵中出现的频率,设 $M(S)$ 为分明矩阵, $p(a)$ 为 $M(S)$ 中属性 a 的属性频率函数,它定义为 a 在 $M(S)$ 中出现的次数,则属性重要性定义为

$$\text{SGF}(a, R, D) = p(a). \quad (9)$$

属性的专家经验重要性权集可采用问卷调查法,再用 Delphi 方法^[7] 进行处理后构造权重集,并建立属性的经验重要性权集知识库,供不同类型信息系统约简算法使用。

4.2.2 混合启发式约简算法

根据粗糙集对信息系统描述的定义,构建信息系统决策表。通过决策表分析,计算条件属性的重要性。再根据重要性来判断条件属性相对于决策属性的必要性,进而决定属性的约简。本文提出了将专家经验权重和条件属性固有重要性权重混合,作为约简启发式因子,优化约简算法称为混合启发式粗糙集约简算法。应用此算法找出最优或次优约简,构建信息系统安全评估优化模型。具体算法如下:

1) 计算条件属性集 C 和决策属性 d 的不可分辨等价类,表示为 $\text{IND}(C)$ 和 $\text{IND}(d)$ 。对每个属性子集 B ,不可分辨等价类为

$$\text{IND}_{\text{DS}}(B) = \{(x_i, x_j) \in U \times U \mid \forall a \in B, a(x_i) = a(x_j), i, j = 1, 2, \dots, m\}.$$

2) 计算下近似集 $C \cdot (d)$, 判断信息决策系统

DS的一致性。若 $\text{POS}_C(d) = C \cdot (d) = U$, 说明论域 U 是 C 上相对于 d 一致的,即决策表是一致的。若关系不满足,则说明决策表是不一致的,应按不一致决策表约简方法处理。方法 1 是考虑正域的变化;方法 2 是分成一致和不一致两个子表。

3) 依次计算条件属性 $c_i (i = 1, 2, \dots, m)$ 的不可分辨等价类 $\text{IND}(C \setminus \{c_i\})$, 进而得到 $\text{POS}_{C \setminus \{c_i\}}(d)$ 。

4) 依次计算 $C \setminus \{c_i\}$ 对 d 近似分类的质量,计算公式为

$$r_{C \setminus \{c_i\}}(d) = \text{card}(\text{POS}_{C \setminus \{c_i\}}(d)) / \text{card}(U).$$

5) 计算条件属性 $c_i (i = 1, 2, \dots, m)$ 的重要性

$$r_C(d) = \text{card}(\text{POS}_C(d)) / \text{card}(U),$$

$$k(c_i) = r_C(d) - r_{C \setminus \{c_i\}}(d).$$

6) 根据设定的迭代分支数 N , 每步依次从前 N 个重要性较大的属性中选择一个属性,转 3) 继续进行迭代运算,直到该分支最后选取的属性重要性为 1 (选取此属性后,剩下未选取属性的重要性均为零),得到一个约简。每步每次选取一个属性,最多 N 个迭代分支。如果某步前 N 个属性重要性均相等,则该步有 N 个迭代分支;如果前 N 个属性重要性不相等,则与最大重要性值差小于设定值(如 5%) 的属性数为该步的迭代分支数。

迭代计算过程表明,约简属性选择顺序与属性在各约简中出现的频次具有一致性,即频次高的属性在各约简中重要性较大,因此优先选择为约简迭代属性。

通过以上约简算法可求出全部等价约简,在应用属性固有重要性权启发式优化方法的前提下,约简模型一般不是唯一的,但都包含了重要的属性。而混合启发式约简通常是唯一的,其约简模型包含了专家的知识。

7) 知识融合模型。在实际应用中,根据专家知识和各类系统用户的经验可确定部分信息系统重要的安全因素。为使约简评估模型更有代表性并符合实际应用情况,将固有重要性启发约简与包含专家对属性重要性知识的约简进行融合,获得比较优化的、更加全面的评估数学模型。

4.2.3 混合启发式约简算法的运行

寻找决策表最小约简子集,一般算法的复杂度为 $O(N^2 * M)$, 最严重情况下约简算法过程重复 2^M 次,对应的复杂度为 $O(2^M * N^2 * M)$, 约简问题属于 NP-Hard 问题。本文提出的混合启发式约简算法可大大降低算法的复杂度,提高运行效率,如表 2 所示。运行环境为 PC/CPU1.3G/RAM512M/Windows XP, 属性数为 32, 样本数为 24。

表 2 混合启发式约简算法的运行

迭代分支数	内存占用 / M	运行时间 / s	迭代次数 / 次	约简集个数 / 个	约简集平均属性 / 个
1	4.40	6	6	1	6
2	4.45	33	22	16	5.5
3	4.55	37	24	29	5.5

4.3 约简实例分析

本文提出在基本模型的基础上进行约简,可部分地解决复杂度问题,与原始安全模型直接约简相比具有明显的优点,在约简算法上应用混合启发式算法可获得优化的约简结果.下面根据评估经验提炼出的敏感信息系统的最优节点基本模型,给出一个粗糙集约简的实例.敏感信息系统基本模型包含物理隔离、访问控制、信息加密及人员管理等 30 余项测评指标.应用基本模型进行人工评估,得到 20 余个案例真实数据,将其作为约简样本,实际测评数据如表 3 所示.

表 3 信息系统评估信息表

样本序号	物理隔离	最高密级防护	身份鉴别	...	人员培训	测评结论
1	基本合格	基本合格	基本合格		基本合格	合格
2	基本合格	基本合格	合格		合格	合格
...						
n	合格	合格	不合格		合格	不合格

以表 3 数据作为样本,通过启发式粗糙集方法约简,融合专家经验模型,得到最终的约简结果包含 15 个安全属性,其中包含的安全指标有物理隔离、身份鉴别等,IC 卡物理保护也在其中.约简指标及同时获得重要性权集如表 4 所示.

表 4 信息系统约简决策表

项目	编 号						
	1	2	...	9	10	...	15
安全指标	物理隔离	身份鉴别		病毒防护	IC 卡物理保护		设备安全
重要性权	0.135	0.134		0.024	0.018		0.006

从约简的结果看,所获得的模型是有效的且符合实际.约简结果包含了敏感信息系统安全要求公认的、必须满足的物理隔离、访问控制、身份鉴别等主要指标,重要性权也较高.约简结果还包含了病毒防护和 IC 卡管理等指标.病毒攻击在目前信息安全方面具有较大的危害,对其预测较为困难;IC 卡是信息系统人员管理和控制主观危害的重要手段.

另外注意到,基本模型约二分之一的指标被约简,使优化模型更为简化,其主要原因是敏感系统对约简结果中几个权值高的指标要求明确,在应用基本模型对信息系统进行评估时,系统整体安全性主

要取决于这些安全指标.从而表明知识融合约简结果是有效且合理的.对于其他信息系统,如教育、科技等,对物理隔离等指标没有特别的要求,约简结果模型包含的指标可能不如敏感系统那么集中,指标数也会较多.

约简后模型对应的决策表与约简前的原始决策表具有相同的功能,即从决策或判断的角度来看,约简后的模型与原始模型对信息系统安全评估的功能是等价的.采用约简模型对新的信息系统进行安全评估,能抓住主要矛盾,提高评估的效率和效益.

5 结 语

本文从信息系统安全评估的宏观层面,基于专家经验和粗糙集理论与方法相结合的新思想,提出了信息系统安全评估基本模型的概念和界定方法.在此基础上,提出基于粗糙集方法和专家经验的安全属性约简算法,将专家经验转化为属性重要性权值,并利用混合权值作为约简的启发式信息,得到更为合理和实用的包含专家知识的约简结果,使信息系统安全评估结果整体上更加客观和优化.根据粗糙集约简的基本原理,基于专家和评测人员现场评测的信息系统安全信息样本数据,约简结果集中体现了被评估信息系统类型的样本数据的主要特征,因此,用约简的安全评估模型评估相应类型的信息系统最有效.对于其他类型有安全性要求的信息系统评估,可应用同类型的评估数据,采用本文提出的启发式约简算法进行约简,得到相应类型信息系统的安全评估模型.

参考文献(References)

[1] 魏大宽. 不完备模糊目标信息系统粗糙集模型与知识约简[J]. 计算机工程, 2006, 32(8): 48-51.
(Wei Da-kuan. Rough set model and precision reduction in incomplete and fuzzy decision information systems [J]. Computer Engineering, 2006, 32(8): 48-51.)

[2] 陈淑珍. 基于粗糙集的几种约简算法分析[J]. 武汉工业学院学报, 2005, 24(3): 118-120.
(Chen Shu-zhen. Analysis of attribute reduced algorithm based on rough set theory[J]. J of Wuhan Polytechnic University, 2005, 24(3): 118-120.)

[3] Lin Meng-quan, Zhu Yun, Li Jian-hua. Research on assessment model of information system security based on various security factors[J]. To be Appeared in J of Shanghai Jiaotong University, 2007, 12(3): 262-268.

[4] 史忠植. 高级人工智能[M]. 第 2 版. 北京:科学出版社, 2006.
(Shi Zhong-zhi. Advanced artificial intelligence [M]. 2ed. Beijing: Science Press, 2006.)

(下转第 960 页)



$$t_{m+1} - t_m = 0.1 \times \text{rand}, m = 0, 1, \dots;$$

其中 $0 < \text{rand} < 1$ 为一随机数. 分别在时间区间 $[0.8 \text{ s} \sim 1.2 \text{ s}]$ 和 $[2.8 \text{ s} \sim 3.2 \text{ s}]$ 上加外部干扰 $u = [4, 4]^T$. 仿真结果如图 1 和图 2 所示, 它们分别是系统 (9) 在两个不同切换路径 $\alpha_1(t)$ 和 $\alpha_2(t)$ 下的状态 x 的响应曲线.

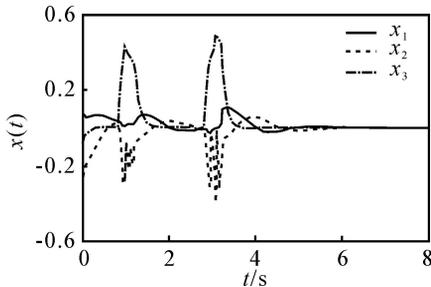


图 1 在路径 α_1 下的状态 x 曲线

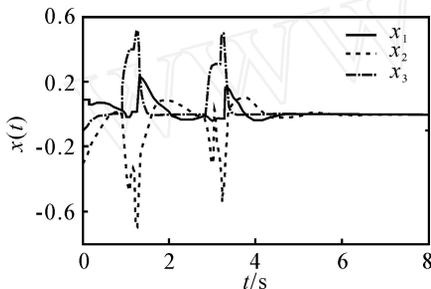


图 2 在路径 α_2 下的状态 x 曲线

从图 1 和图 2 可以看出, 在切换路径 $\alpha_1(t)$ 和 $\alpha_2(t)$ 下, 闭环系统很快收敛到零平衡点. 由此可知, 鲁棒控制器 (10) 可以很好地镇定系统 (9). 仿真结果验证了定理 1 的正确性和有效性.

6 结 论

本文研究含有无穷多个子模型的混杂切换 Hamilton 系统在(任意)切换路径下的控制设计问题, 设计了一种 H_∞ 鲁棒控制方案. 将得到的结果运用到一般非线性混杂切换系统中, 设计了相应的鲁棒控制器. 数值仿真验证了本文结果的正确性和有效性.

参考文献 (References)

[1] Wang Y, Feng G, Cheng D, et al. Adaptive L_2

disturbance attenuation control of multimachine power systems with SMES units [J]. Automatica, 2006, 42 (7): 1121-1132.

[2] Wang Y, Cheng D, Li C, et al. Dissipative Hamiltonian realization and energy-based L_2 -disturbance attenuation control of multimachine power systems[J]. IEEE Trans on Automatic Control, 2003, 48(8): 1428-1433.

[3] Wang Y, Li C, Cheng D. Generalized Hamiltonian realization of time-invariant nonlinear systems [J]. Automatica, 2003, 39(8): 1437-1443.

[4] Escobar G, Van der Schaft A J, Ortega R. A Hamiltonian Viewpoint in the modeling of switching power converters[J]. Automatica, 1999, 35 (3): 445-452.

[5] Haddad W M, Nersesov S G, Chellaboina V S. Energy-based control for hybrid port-controlled Hamiltonian systems[J]. Automatica, 2003, 39(8): 1425-1435.

[6] Dayawansa W P, Martin C F. A converse Lyapunov theorem for a class of dynamical systems which undergo switching[J]. IEEE Trans on Automatic Control, 1999, 44(4): 751-760.

[7] Cheng D, Lin Y, Guo L, et al. Stabilization of switched linear systems[J]. IEEE Trans on Automatic Control, 2005, 50(5): 661-666

[8] Branicky M S. Multiple Lyapunov functions and other analysis tools for switched and hybrid systems[J]. IEEE Trans on Automatic Control, 1998, 43(4): 475-482.

[9] Zhao J, Dimirovski G M. Quadratic stability of a class of switched nonlinear systems [J]. IEEE Trans on Automatic Control, 2004, 49(4): 574-578.

[10] Sun Z, Ge S S. Switched linear systems: Control and design[M]. Berlin: Springer-Verlag, 2005.

[11] Zhu L, Wang Y. Stability of hybrid dissipative Hamiltonian systems[C]. Proc of the 25th Chinese Control Conf. Harbin, 2006: 1060-1065.

[12] 朱礼营, 王玉振. 切换耗散 Hamilton 系统的稳定性研究[J]. 中国科学(E辑), 2006, 36(6): 617-630. (Zhu Li-ying, Wang Yu-zhen. Study on the stability of switched dissipative Hamiltonian systems[J]. Science in China(Series E), 2006, 36(6): 617-630.)

(上接第 955 页)

[5] Wong S K M, Ziarko. Optimal decision rules in decision table[J]. Bulletin of the Polish Academy of Sciences, 1985, 33(11/12): 693-696.

[6] Skowron A, Rauszer C. The discernibility matrices and functions in information systems [C]. Intelligent Decision Support - Handbook of Applications and

Advances of the Rough Sets Theory. Netherlands: Kluwer Academic Publishers, 1992: 331-362.

[7] Lin Meng-quan, Wang Qiang-min, Li Jian-hua. Methodology of quantitative risk assessment for information system security[C]. Proc of Lecture Notes in Artificial Intelligence 3802. Berlin: Springer, 2005: 526-531.