基于平行控制的信息安全管理措施仿真与优化

王 鹏 [1] 陈 森 [1]

摘 要 为了有效提高信息安全管理措施的有效性, 采用平行控制方法来研究信息安全管理措施的优化问题. 采用仿真软件 Extend 来构建信息安全管理系统的人工系统, 基于人工系统来评估信息安全管理措施的效果; 使用平行控制系统实现真实系统和人工系统之间的交互, 尽可能地使真实系统和人工系统之间的差异最小化; 采用计算实验方法来不断调整信息安全管理措施, 最终得到一套有效的信息安全管理措施. 以互联网管理为例, 证明本方法能够实现信息安全管理措施的实时仿真、评估和优化.

关键词 决策理论, 管理措施, 平行控制, 仿真

DOI 10.3724/SP.J.1004.2011.01351

A Parallel Control Approach to Optimization of Information Security Management Measures

WANG Peng[1] CHEN Sen[1]

Abstract A parallel control method is proposed for optimization of information security management measures. The information security management measure is evaluated using the artificial system, which is built by the simulation software. A parallel control system is used to obtain the interaction between the actual system and the artificial system to minimize their difference. The computational experiment method is used to continuously adjust the information security management measure, and obtain the satisfying information security management measure. An internet management as example indicates that this method can achieve the real-time simulation, evaluation and optimization of information security management measures.

Key words Decision theory, management measure, parallel control, simulation

以互联网为代表的计算机网络在全球迅速普及, 使国家政治、经济、军事及整个社会对基于网络的信息系统的依赖越来越大. 与此同时, 信息系统的脆弱性将会对国家关键基础设施构成直接威胁, 信息系统和信息安全已成为国家安全的基础之一; 信息系统和信息安全关系着国家安全、民族兴衰和战争胜负; 信息系统和信息安全对一个国家和民族的战略重要性已成为不争的事实.

针对电力系统信息安全的现状, 刘利成[1] 从技术和管理两个方面给出了解决电力信息安全的措施, 技术措施主要包括物理隔离、入侵检测、隐患扫描、查杀毒、数据加密、数据备份等手段, 而管理措施强调了信息安全教育及人员、密码、技术、数据等方面的管理内容, 并阐述了电力信息安全的实施要点. 付钰等[2] 借助模糊集合理论, 对信息系统所涉及的风险因素分别从资产影响、威胁频度、脆弱性严重程度这三个方面进行分析, 对信息系统安全风险等级进行综合评价, 进而给出改进措施.

不难看出, 现有信息安全管理措施的研究, 基本上都是一些经验措施或定性方法. 为有效提高信息安全管理措施的有效性, 本文尝试采用平行控制方法来研究信息安全管理措施的仿真、评估和优化问题.

本文的科学问题可概括为: 采用先进的计算机技术, 对信息安全管理系统进行仿真; 基于信息安全管理仿真系统来验证信息安全管理措施的有效性; 采用计算实验方法来不断调整信息安全管理措施, 最终得到一套有效的信息安全管理措施.

1 理论基础

为有效解决复杂社会系统的实验问题, 王飞跃等[3−5] 认为可利用人工社会中计算实验的可设计性和可重复性, 对人工系统设计不同实验方案, 按不同指标体系对复杂系统进行量化实验分析. 同时可通过人工系统与实际系统的相互对比和参照, 完成对相关行为和决策的实验与评估, 实现对实际系统的管理与控制. 计算实验方法的提出, 弥补了复杂社会系统难以进行全面和综合实验的不足, 也为综合集成研讨厅体系提供了一种经济快速、虚实结合地进行复杂系统实验的有效途径.

收稿日期 2011-01-20 录用日期 2011-05-25
Manuscript received January 20, 2011; accepted May 25, 2011
国家自然科学基金 (70971131) 资助
Supported by National Natural Science Foundation of China (70971131)
1. 国防科学技术大学信息系统与管理学院 长沙 410073
1. School of Information System and Management, National University of Defense Technology, Changsha 410073

社会计算的应用近年来取得了长足的发展. 首先, 社会计算是对国家和公共安全进行有效分析、预测和控制的关键信息技术手段. 中国科学院自动化研究所情报与安全信息学研究团队构建的天网工程, 以开源情报的获取和处理为基础, 对社会媒体和舆情信息进行实时监控, 实现了面向多领域的关键信息提取和辅助决策支持. 由于万维社会媒体能够充分体现人们的价值取向和真实意愿, 往往做出比传统媒体更为迅速、灵敏、准确的反应, 开源信息在辅助应急预警中也发挥了重要的作用[6]. 此外, 利用计算技术来研究文化冲突和变迁, 分析不同文化国家或组织的决策过程, 探寻其行为所依赖的文化因素的社会文化建模方法已开始应用于安全和反恐决策预警中[7−9].

采用社会计算方法探索金融风险和危机的动态规律和管理方式的研究思路逐渐显现出其在方法论和研究工具方面的优势. 许多发达国家都在政府资助下启动了研究项目, 如美国 Sandia 国家实验室的 ASPEN、欧盟的 EURACE、英国的 E-Lab, 都是政府资助的大型多市场金融经济社会计算模型, 并在国家宏观经济政策制定中起到日益重要的作用. 国内天津大学张维等[10−11] 在自然科学基金资助下较早开展了计算实验金融学研究, 建立了基于我国市场特征的单市场社会计算模型, 对市场波动规律及微观成因、智能体竞争策略生存性等开展了研究.

工程应用领域的一个核心的问题就是如何尽可能避免事故隐患, 实现安全节能有效的长周期生产. 由于人和生产组织结构对安全生产过程具有重要影响和制约, 如何在企业安全生产管理中加入社会计算模型, 成为目前工程领域应用研究的一个关键问题.

在军事领域, 近年来发达国家纷纷投巨资加速军事信息化的发展. 如何把先进的计算技术应用到国防事业中, 是信息技术在军事领域应用的主要源动力. 军事科学院采用综合集成方法, 建立了人工军事模型系统, 对现代军事尤其是信息化战争形态进行了系统分析.

2 本文方法

基于平行控制的信息安全管理措施仿真与优化的基本流程图如图 1 所示. 不难看出, 本方法主要包含三个步骤: 1) 构建人工系统, 采用仿真软件 Extend 构建信息安全管理系统的仿真系统; 2) 构建平行执行系统, 其主要负责真实系统和仿真系统之间的管理与交互, 尽可能地使真实系统和仿真系统之间的差异最小化; 3) 基于仿真的计算实验, 该模块通过不断调整信息安全管理措施, 基于人工系统评估信息安全管理措施的效果, 最终得到一套有效的信息安全管理措施.

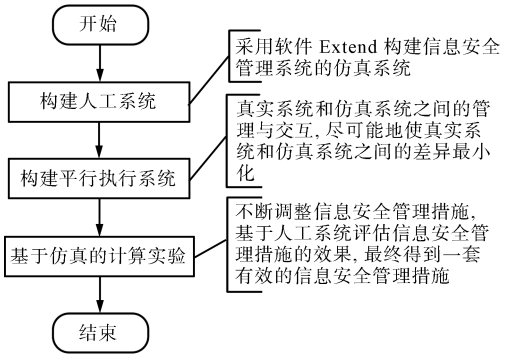


图 1 本文方法的基本流程图

Fig. 1 Basic procedure used in the paper

2.1 构建人工系统

采用仿真软件 Extend 构建信息安全管理仿真系统的基本步骤如下:

步骤 1. 信息安全管理系统的描述. 由熟悉情况的决策者或分析师来描述待研究信息安全管理系统内的实体、资源、活动及控制关系等.

步骤 2. 设置仿真研究的目标. 通过明确仿真研究的目标可使未来进行系统调研和建模时抓住重点[13].

步骤 3. 收集数据, 建立概念模型. 研究现有系统, 收集相关数据, 理解系统运作流程, 在此基础上, 建立系统的概念模型. 概念模型通常以图形表示系统运作流程, 便于理解和交流[13].

步骤 4. 建立计算机仿真模型. 一旦概念模型通过审核, 就可利用仿真软件根据概念模型建立计算机仿真模型[13].

步骤 5. 模型校核与验证. 模型校核是指考察计算机仿真模型是否按照预先设想的情况运行, 找出模型中的各种语法及逻辑错误. 模型验证是指考察仿真模型是否符合实际情况, 如模型的输入分布与实际观察结果是否一致, 模型的输出性能指标与实际情况是否一致[13].

步骤 6. 实验运行和结果分析. 运行仿真实验, 得出输出数据并进行结果分析: 包括仿真实验方案的设计、通过实验运行得到输出性能指标的统计、根据实验结果比较不同方案、进行敏感性分析及最优化分析等[13].

2.2 构建平行执行系统

平行执行系统主要负责真实系统和人工系统之间的管理与交互: 对真实系统和人工系统之间的行为进行对比和分析, 对各自的未来状况进行 “借鉴” 和 “预估”, 执行相应的管理与控制方式, 尽可能地使真实系统和仿真系统之间的差异最小化, 达到实

施有效解决方案及学习和培训等目的[14−15]. 平行执行系统的基本框架如图 2 所示.

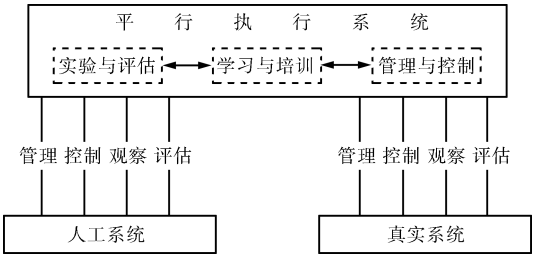


图 2　平行执行系统的基本框架

Fig. 2　Fundamental framework of parallel execution systems

1) 实验与评估. 通过计算实验分析人工系统的行为和反应, 对不同解决方案的效果进行评估, 为选择和支持管理与控制决策提供依据.

2) 学习与培训. 通过对实际系统与人工系统的连接组合, 使有关人员能迅速地掌握实际系统的各种状况及行为. 人工系统的管理与控制系统也可作为实际系统的备用系统, 增加其运行的可靠性和应变能力.

3) 管理与控制. 采用人工系统尽可能模拟实际系统, 对其行为进行预估, 为寻找对实际系统有效的解决方案或对当前方案进行改进提供依据. 通过观察真实系统与人工系统评估的状态之间的不同, 产生误差反馈信号, 对人工系统的评估方式或参数进行修正, 尽可能地使真实系统和仿真系统之间的差异最小化.

2.3　基于仿真的计算实验

针对人工系统设计多种 “实验” 方案, 并进行多次重复仿真, 可全面、准确和及时地对复杂系统的解决方案进行分析和评估. 利用人工系统 “计算实验” 的可设计性及可反复进行的特点, 还可对实际系统的解决方案进行各种关于性能可靠性和质量等的 “加速” 实验、“压力” 实验及 “极限” 实验等.

3　应用实例

为了进一步加强信息安全管理工作, 很多科研单位都通过设置网吧来加强互联网管理 — 将所有互联网机器集中在网吧内管理, 而网吧以外的其他工作机器均与互联网采取物理隔离. 客户只能通过网吧计算机来访问互联网, 同时采用光盘刻录方式将需要的数据拷贝出来. 笔者以 XX 单位的实际情况为基础, 构建 “互联网管理” 典型应用的仿真系统. 主要考虑以下因素: 有上网需求的客户、上网机和信息传递途径.

XX 单位共有客户 100 余人, 假设客户按均值为 3 分钟的泊松分布进入网吧上网. 对于进入网吧的客户, 假设 60 % 的客户有刻录需求 (既查阅资料, 又需要刻录), 40 % 的客户没有刻录需求 (只查阅资料). XX 单位共有 5 台上网机, 其中 2 台可以进行刻录, 3 台不能进行刻录.

对于有刻录服务的客户, 上网时间服从均值为 30 分钟, 方差为 10 分钟的正态分布. 如果排队等到空闲的可刻录上网机, 则正常在该机器上查询并刻录出来所需资料; 如果排队等到空闲的没有刻录服务的上网机, 则在该机器上查询资料, 并以违规方式将数据拷贝出来.

对于没有刻录服务的客户, 可选择任何一台空闲的上网机进行上网, 假设上网时间服从均值为 20 分钟, 方差为 10 分钟的正态分布. 采用仿真软件 Extend 构建的 “互联网上网机管理” 典型应用的仿真系统如图 3 所示.

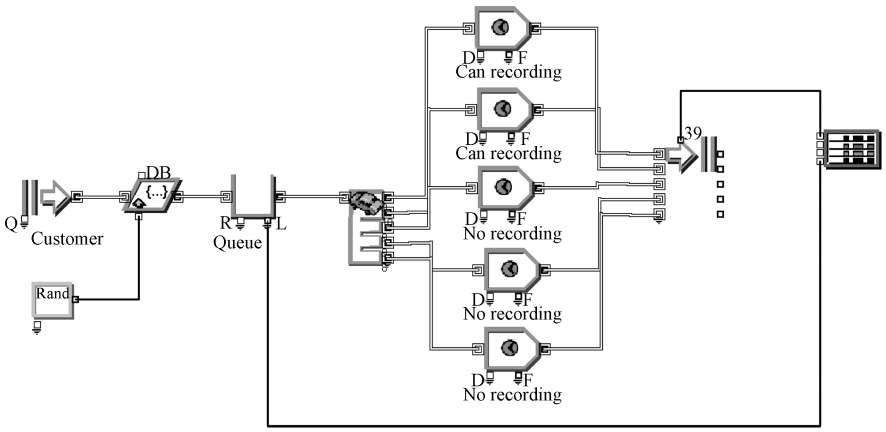


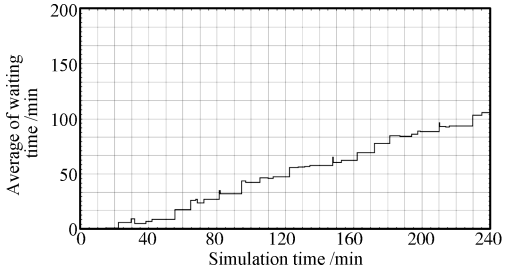
图 3　“互联网管理” 典型应用的仿真系统

Fig. 3　Simulation system of “internet management” application

本文拟从以下指标来评价当前安全管理措施的效果: 1) 平均等待时间, 即所有客户在网吧内等待上网机所耗费的平均等待时间; 2) 服务人数, 即在固定时段内获得上网服务的总人数; 3) 发生违规操作的概率, 即违规操作人数与服务人数的比值; 4) 管理措施所带来的成本, 即因为调整管理措施而带来的额外成本.

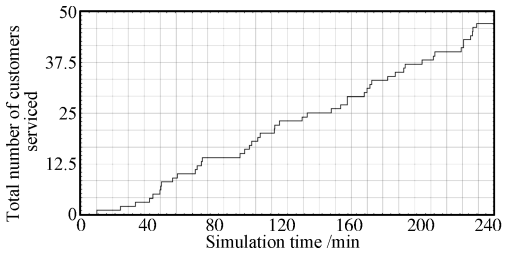
在本研究中, 假设所有技术措施都是成熟的, 笔者主要从管理措施着手, 研究如何最大程度地提高信息安全管理措施的有效性. 在 "互联网管理" 典型应用中, XX 单位的管理措施可概括为: 在上网机的配置上, 有 2 台可刻录的上网机和 3 台不能刻录的上网机; 在上网时间上, 有刻录服务的客户上网时间服从均值为 30 分钟、方差为 10 分钟的正态分布, 无刻录服务的客户上网时间服从均值为 20 分钟、方差为 10 分钟的正态分布. "互联网管理" 现有管理措施的评价结果如图 4 所示. 从图 4 (a) 中可以看出, 随着仿真时间的推进, 平均等待时间越来越大, 最终达到 100 多分钟; 从图 4 (b) 中可以看出, 随着仿真时间的推进, 服务人数越来越多, 在 4 小时内可服务 45 人左右; 从图 4 (c) 中可以看出, 整个服务系统内约有 30 % 的客户在进行违规操作.

从图 4 的评价结果中不难看出, "互联网管理" 的现有管理措施还需要进一步调整和优化. 鉴于此, 笔者拟从两个方面来调整管理措施: 从上网机配置方面入手, 可考虑: 1) 将现有机器全部升级为可刻录上网机 (按每台刻录机 200 元估算, 增加 3 个刻录机需 600 元); 2) 将现有机器升级为 10 台可刻录上网机 (按每台可刻录上网机 3 000 元估算, 增加 5 台可刻录上网机需 1.5 万); 3) 从上网时间入手, 可考虑将上网时间分别设置为固定的 10 分钟、20 分钟和 30 分钟. 不同管理措施及其评价结果如表 1 所示.



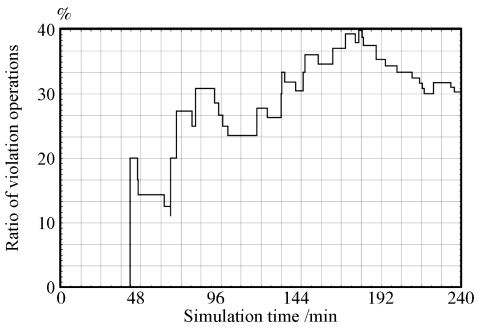
(a) 平均等待时间

(a) Average waiting time



(b) 服务人数

(b) Number of service



(c) 发生违规操作的概率

(c) Probability of violation operations

图 4 "互联网上网机" 现有管理措施的评价结果

Fig. 4 Evaluation result of management prescription of "computers on internet"

表 1 不同管理措施及其评价结果

Table 1 Different management prescriptions and evaluation results

服务台	评价指标	服务时间		
		固定时间 10 分钟	固定时间 20 分钟	固定时间 30 分钟
2 台可刻录上网机 + 3 台无刻录上网机	最大等待时间 (分钟)	1	71	133
	最大服务人数 (个)	81	56	36
	发生违规操作的最大概率 (%)	45	56	40
	管理措施所带来的成本 (万)	0	0	0
5 台可刻录上网机	最大等待时间 (分钟)	2	68	130
	最大服务人数 (个)	79	58	38
	发生违规操作的最大概率 (%)	0	0	0
	管理措施所带来的成本 (万)	0.06	0.06	0.06
10 台可刻录上网机	最大等待时间 (分钟)	0	3	11
	最大服务人数 (个)	86	78	72
	发生违规操作的最大概率 (%)	0	0	0
	管理措施所带来的成本 (万)	1.56	1.56	1.56

从表 1 的结果中可以看出, “互联网管理” 的较为满意的管理措施为: 将现有机器全部升级为可刻录上网机; 将上网时间分别设置为固定的 10 分钟.

4 结论

本文的主要创新点: 采用平行控制方法研究信息安全管理措施的仿真与优化问题; 以互联网管理为例, 说明本方法能实现信息安全管理措施的仿真、评估和优化.

References

1 Liu Li-Cheng. The solution of technology and management for the power information security. *Electric Safety Technology*, 2006, **8**(2): 8−10
(刘利成. 解决电力信息安全的技术措施和管理措施. 电力安全技术, 2006, **8**(2): 8−10)

2 Fu Yu, Wu Xiao-Ping, Ye Qing, Peng Xi. An approach for information systems security risk assessment on fuzzy set and entropy-weight. *Acta Electronica Sinica*, 2010, **38**(7): 1489−1494
(付钰, 吴晓平, 叶清, 彭熙. 基于模糊集与熵权理论的信息系统安全风险评估研究. 电子学报, 2010, **38**(7): 1489−1494)

3 Wang Fei-Yue, Qiu Xiao-Gang, Zeng Da-Jun, Cao Zhi-Dong, Fan Zong-Chen. A computational experimental platform for emergency response based on parallel systems. *Complex Systems and Complexity Science*, 2010, **7**(4): 1−10
(王飞跃, 邱晓刚, 曾大军, 曹志冬, 樊宗臣. 基于平行系统的非常规突发事件计算实验平台研究. 复杂系统与复杂性科学, 2010, **7**(4): 1−10)

4 Wang Fei-Yue. Parallel system methods for management and control of complex systems. *Control and Decision*, 2004, **19**(5): 485−489
(王飞跃. 平行系统方法与复杂系统的管理和控制. 控制与决策, 2004, **19**(5): 485−489)

5 Wang Fei-Yue. Fundamental issues in research of computing with words and linguistic dynamic systems. *Acta Automatica Sinica*, 2005, **31**(6): 844−852
(王飞跃. 词计算和语言动力学系统的基本问题和研究. 自动化学报, 2005, **31**(6): 844−852)

6 Zeng Da-Jun, Wang Fei-Yue, Cao Zhi-Dong. Open source information in emergency response. *Science and Technology Review*, 2008, **26**(16): 33−35
(曾大军, 王飞跃, 曹志冬. 开源信息在突发事件应急管理中的应用. 科技导报, 2008, **26**(16): 33−35)

7 Subrahmanian V S, Albanese M, Martinez M V, Nau D, Reforgiato D, Simari G I, Sliva A, Wilkenfeld J, Udrea O. CARA: a cultural-reasoning architecture. *IEEE Intelligent Systems*, 2007, **22**(2): 12−16

8 Subrahmanian V S. Computer science: cultural modeling in real time. *Science*, 2007, **317**(5844): 1509−1510

9 Martinez V, Simari G I, Sliva A, Subrahmanian V S. CONVEX: similarity-based algorithms for forecasting group behavior. *IEEE Intelligent Systems*, 2008, **23**(4): 51−57

10 Zhang W, Zhang Y, Xiong X, Jin X. BSV investors versus rational investors: an agent-based computational finance model. *International Journal of Information Technology and Decision Making*, 2006, **5**(3): 455−466

11 Zhang Y, Zhang W. Can irrational investor survive? A social-computing perspective. *IEEE Intelligent Systems*, 2007, **22**(5): 58−64

12 Qin Tian-Bao, Wang Yan-Feng. *Application Oriented Simulation Modeling and Analysis with ExtendSim*. Beijing: Tsinghua University Press, 2009
(秦天保, 王岩峰. 面向应用的仿真建模与分析: 使用 ExtendSim. 北京: 清华大学出版社, 2009)

13 Cheng Chang-Jian, Cui Feng, Li Le-Fei, Xiong Gang, Zou Yu-Min, Liao Chang-Yong. Parallel management systems for complex productions systems: methods and cases. *Complex Systems and Complexity Science*, 2010, **7**(1): 24−32
(程长建, 崔峰, 李乐飞, 熊刚, 邹余敏, 廖昌勇. 复杂生产系统的平行管理方法与案例. 复杂系统与复杂性科学, 2010, **7**(1): 24−32)

14 Du Jun-Ping, Zhou Yi-Peng. Study on data-based tourism management decision support system. *Acta Automatica Sinica*, 2009, **35**(6): 834−840
(杜军平, 周亦鹏. 基于数据的旅游管理决策支持系统研究. 自动化学报, 2009, **35**(6): 834−840)

15 Zhen Zi-Yang, Wang Zhi-Sheng, Wang Dao-Bo. Information fusion estimation based preview control for discrete linear system. *Acta Automatica Sinica*, 2010, **36**(2): 347−352
(甄子洋, 王志胜, 王道波. 基于信息融合估计的离散线性系统预见控制. 自动化学报, 2010, **36**(2): 347−352)

王 鹏 国防科学技术大学信息系统与管理学院管理系博士研究生. 主要研究方向为系统规划与管理决策技术. 本文通信作者. E-mail: phd2999@gmail.com
(**WANG Peng** Ph. D. candidate at the School of Information System and Management, National University of Defense Technology. His research interest covers system planning and management and decision technology. Corresponding author of this paper.)

陈 森 国防科学技术大学信息系统与管理学院管理系博士研究生. 主要研究方向为科技与教育管理.
E-mail: csen0636@sina.com
(**CHEN Sen** Ph. D. candidate at the School of Information System and Management, National University of Defense Technology. His research interest covers management of technology and education.)