·情报理论与前瞻观点·

智慧城市信息安全监管策略的演化博弈分析

邹 凯 万 震* 曹 丹 张东东
（湘潭大学公共管理学院，湖南 湘潭 411105）

摘 要：［目的/意义］在智慧城市环境下针对信息安全监管策略进行演化博弈分析，有利于为智慧城市相关主体有效应对信息风险和漏洞带来的信息安全危机，加强多方位的信息安全监管提供一定参考。［方法/过程］围绕智慧城市信息安全监管中存在的信息安全问题，以智慧城市运营方和信息安全监管方为博弈主体，构建了收益矩阵，通过计算得出 6 种策略下博弈主体行为稳定的条件，并运用计算机仿真，分析了不同情况下智慧城市信息安全监管双方的博弈行为以及各关键变量对博弈主体策略选择的方向性及程度性影响。［结果/结论］研究发现，当加强信息安全管理的成本低于发生信息安全事件的期望损失时，其双方博弈结果达到理想状态，且智慧城市监管方对运营方处以较重的处罚时，会加快这一过程的收敛。

关键词：智慧城市；信息安全监管；演化博弈
DOI: 10.3969/j.issn.1008-0821.2021.03.001
〔中图分类号〕G203 〔文献标识码〕A 〔文章编号〕1008-0821（2021）03-0003-12

Evolutionary Game Analysis of Information Security Regulatory Strategy in Smart City

Zou Kai Wan Zhen* Cao Dan Zhang Dongdong
（School of Public Administration，Xiangtan University，Xiangtan 411105，China）

Abstract：［Purpose/Significance］In the smart city environment，evolutionary game analysis of information security regulatory strategy is conducive to effectively deal with the information security crisis caused by information risks and loopholes，and provide certain reference for strengthening multi-dimensional information security supervision.［Method/Process］Around wisdom city of information security problems in information security regulation，urban operators with wisdom and information safety regulators as the main body in the game，to build the pay-off matrix，calculated the six main strategy game behavior and stable conditions，and using the computer simulation，analyzed the wisdom city information security regulation under different conditions on both sides of the main game behavior as well as the key variables for game strategy choice of direction and degree of influence.［Result/Conclusion］It is found that when the cost of strengthening information security management is lower than the expected loss of information security incidents，the game results of both sides reach an ideal state，and the smart city regulators impose heavier penalties on operators，which will accelerate the convergence of this process.

Key words：smart city；information security supervision；evolution game

智慧城市是以海量信息与创新概念为特征，以实现城市治理的精确化和高效化为目的[1]，以大数据、互联网等前沿信息技术为支撑的城市发展新模式[2]。智慧城市以新一代信息技术为依托，极大地助力了城市治理精确化和高效化进程，但信息技术的广泛应用也使得智慧城市较传统城市而言面

收稿日期：2020-10-30
基金项目：国家社会科学基金项目“大数据环境下智慧城市信息安全困境及应对策略研究”（项目编号：18BTQ055）；湖南省社会科学基金项目“智慧城市信息安全风险评估指标体系研究”（项目编号：18YBA398）。
作者简介：邹凯（1965-），男，教授，博士，研究方向：智慧城市，公共信息资源管理等。曹丹（1996-），女，硕士研究生，研究方向：智慧城市信息服务。张东东（1995-），男，硕士研究生，研究方向：智慧城市信息安全。
通讯作者：万震（1995-），男，硕士研究生，研究方向：智慧城市与信息服务。

临更为复杂的信息安全风险。2020 年，国家标准化管理委员会发布了《信息安全技术——智慧城市建设信息安全保障指南》，从网络通信等 5 个不同层次分析了智慧城市建设所面临的信息安全风险，并着重强调了针对智慧城市运营者等智慧城市建设主要角色开展信息安全监管的必要性[3]。智慧城市信息安全监管是一个动态的过程，涉及多个参与主体，且各参与主体的策略及行为均可在一定程度上对其他主体产生影响，其博弈过程中的行为决策均具有不完全理性的特点，且往往是动态变化的。基于此，本文基于演化博弈的方法，构建了智慧城市运营方和监管方信息安全的成本收益矩阵，探究不同条件下双方的博弈平衡状态，并对信息安全监管方和智慧城市运营方投入行为的演化路径和稳定策略进行了分析，以期为智慧城市信息安全监管工作的改善提供参考和借鉴。

1 相关研究综述

1.1 智慧城市信息安全研究

Elmaghraby A S 等[4]认为，用户在信息的产生、传播、存储和使用的各个阶段都会面临信息安全风险，完善法律条例和推广信息安全教育等将会有效改善智慧城市信息安全问题；Li X 等[5]将模糊集理论和灰色关联应用到对智慧城市信息安全的研究中，利用相关理论对智慧城市信息安全进行了风险评估，并对智慧城市信息系统的脆弱性指数进行了预判；向尚等[6]在改进现有智慧城市信息安全风险指标体系的基础上，运用随机森林算法建立了其预测模型，并与传统模型预测结果做了对比；邹凯等[7]基于环境、逻辑、组织 3 个维度，构建了智慧城市信息安全风险影响因素三维结构框架，并运用 DEMATEL 方法对智慧城市信息安全风险影响因素进行了识别；毛子骏等[8]摘选了我国 20 个智慧城市试点地区，并基于贝叶斯网络对各试点的信息安全风险进行量化评估，发现我国各智慧城市试点间有较大差距的信息安全风险水平；张艳丰等[9]基于扎根理论，构建了智慧城市信息安全影响因素框架模型，阐明用户自身、数据服务、人员管理、外部环境 4 大因素对智慧城市信息安全的影响及其相互之间的作用关系。

1.2 信息安全监管策略研究

Rostami E 等[10]将现有的信息安全监管策略研究总结为 14 个需求主题，并基于 28 个用户案例为信息安全管理人员信息安全策略的设计提供了支持。Guan B W 等[11]采用结构方程模型对企业信息安全监管策略的影响因素进行研究，研究结果发现，滥用监督对员工的情感承诺、规范承诺和持续承诺具有显著的负向影响，而员工制裁的感知确定性对信息安全监管策略起到了正向的调节作用。韩欣毅[12]以对上海网络信息安全监管工作的研究为基础，建立了网站信息安全评估模型并对其信息安全监管提出了相应对策，随后通过网站安全评估对其对策的有效性进行了验证。张磊等[13]以国家知识产权局安全监管实践为研究实例，在私有云模式的基础上提出了信息安全监管的改进策略，以此提高对云计算平台自身的安全性。危怀安等[14]对第三方网上支付信息安全监管的影响因素进行了分析，讨论了监管部门对第三方支付机构监管的必要性和对策，为制定和完善信息安全监管及措施提供理论支持。

1.3 演化博弈下的监管策略研究

He N 等[15]以网络团购市场制定有效的监管策略为目标，构建了网络团购的三方演化博弈模型，并通过系统动力学对演绎模型进行了整体仿真。Shu-Huan F U 等[16]通过博弈论的方法，研究了网络汽车代驾行为的影响因素、监管以及网络代驾平台的选择，提出了第三方监管对网络汽车行业的指导和监管作用。陈福集等[17]采用演化博弈理论对微博运营商、网民和政府微博 3 个监管主体进行分析，并建立三方演化博弈模型，进而从政府的层面提出相应的监管策略。杜杨[18]以动态演化博弈为方法基础，构建出互联网金融创新的路径选择并提出有效的监管策略。赵静娴[19]利用演化博弈方法建立伪舆情相关干系方的三方演化博弈模型，并从制定专项法律法规和加大理论及算法研究两方面提出了针对网络伪舆情治理的具体监管建议。尹珏力等[20]建立了一种网络舆情传播的三方演化博弈模型，进行仿真实验后根据分析结果提出政府监管在线社交网络中负面舆情传播的 3 个关键点及应对策略。

综上所述，智慧城市信息安全研究主要集中在影响因素分析和风险预测评估方面，信息安全监管

策略的制定和有效性分析逐渐成为研究热点，演化博弈下的企业运作和政府舆情的监管策略研究也取得了一定成果，但现阶段鲜有研究将演化博弈理论与智慧城市信息安全相结合，演化博弈视角下的智慧城市信息安全监管策略研究更是有待进一步推进。基于此，本文从智慧城市信息安全监管的利益主体出发，构建出了智慧城市信息安全监管演化博弈模型，通过 MATLAB 仿真分析，探讨了各情形下智慧城市运营方和信息安全监管部门的监管策略，并在此基础上对智慧城市信息安全监管工作的改善提出了相应的建议，以期对智慧城市信息安全监管工作的完善起到一定借鉴作用。

2 演化博弈模型的构建

2.1 模型背景与适用性分析

在智慧城市信息安全监管的过程中，必然会涉及政府机关、民众、高新技术公司等不同群体。对于智慧城市本身而言，信息安全方面的建设与管理涉及的利益群体之间的划分必须是明确且科学合理的，只有针对智慧城市信息安全的利益相关者的不同利益诉求，才能进行具有现实意义的应对。通过分析智慧城市信息安全监管，得出智慧城市信息安全监管的博弈双方角色，如表 1 所示。

表 1 智慧城市信息安全监管博弈双方

涉及层面	具体部门
智慧城市运营方	城市公民、信息基础设施提供商、云服务提供商、IT 和互联网公司、相关运营公司等
信息安全监管部门	网络监控中心、密钥监管中心、电子交易安全证书授权中心、计算机病毒防治中心、网络安全应急响应中心、关键网络系统灾难恢复中心等

在智慧城市运营过程中，智慧城市运营方是以经济利益最大化来进行生产和运营活动的，因此其信息安全建设方案和管理措施更加符合现实情况，也更注重运营成本的高低。当智慧城市运营方按照信息安全监管部门的相关政策规定进行信息安全风险管理的同时，会考虑进行信息安全风险管理所投入的成本和违反国家标准而受到的处罚成本之间的权衡。这就导致了信息安全监管部门与智慧城市建设方的冲突，前者通过进行监管和奖惩措施来对智慧城市信息安全进行管理与决策，后者则更加重视智慧城市建设本身的经济效益，这样就构成了信息安全监管部门与智慧城市建设方在各自决策中的博弈。

通过对智慧城市信息安全利益主体博弈关系进行分析，可以发现在信息安全监管部门对智慧城市运营方进行监管的过程中，二者的策略选择具有较大的不确定性因素，他们的行为策略选择还会彼此影响、相互制约，再加上信息安全监管部门和智慧城市运营方获取的信息不够全面等因素，都会导致智慧城市信息安全监管的双方在策略选择时都不是完全理性的，没有办法使得在博弈的起点就找到对各自最为有利的策略。因此，信息安全监管机构和智慧城市运营方需要在博弈中不断根据对方的博弈策略和群体内部的博弈选择，调整自身的博弈行为。另外，在智慧城市运营方的群体之中，他们的行为策略具有一定的传播性，如果某一信息服务提供商或基础设施建设者为了本身的利益成本，罔顾信息安全管理，发生了信息安全事件而没有得到有效的处罚，会使得这种监管不力的行为持续下去，从而影响到更多的智慧城市运营方；相反，如果加强信息安全管理的智慧城市相关企业所得到的奖励措施或其收益大于不进行信息安全管理的企业，其他智慧城市运营方也会争相模仿。这样的解释也同样适用于智慧城市中信息安全监管机构的行为策略分析。因此，演化博弈理论对于智慧城市信息安全监管具有一定的适用性。

2.2 基本假设与模型构建

在智慧城市建设的相关政策文件和标准指南下达之后，对于信息安全的整体要求会使得智慧城市运营方采取一系列的措施，如加强信息产品质量管理，规范信息服务人员行为，构筑安全可行的信息网络和信息系统等，使其通过信息安全监管部门的评估，达到相关标准和规范的具体要求。因此，针对与具体信息安全事件有关的行为策略，信息安全监管部门可以采取的行动是监管和不监管，而企业可以采取的行动是加强信息安全管理和不加强信息安全管理。

在查找相关文献和询问有关专家的基础之上，对信息安全事件的具体监管措施和信息安全管理措施的具体影响进行分析，发现主要可以从成本和收

益的角度对博弈过程进行分析，因此，对智慧城市信息安全监管演化模型提出了下列基本假设:

1) 信息安全监管部门和智慧城市运营方都是追求各自利益的最大化，并在此基础上开展行为策略的选择。

2) 假设以下参数的设定皆为正数:

①将信息安全监管部门对某类信息安全事件监管的概率设为 x，不监管的概率设为 $1-x$。

②将智慧城市运营方为了防范该类信息安全事件的发生加强信息安全管理的概率设为 y，不加强信息安全管理的概率设为 $1-y$。

③将智慧城市运营方不加强信息安全管理引发的该类信息安全事件发生概率设为 p，事件发生时智慧城市运营方所要承担的此类相应损失为 L（包括对因信息安全事件发生损失的单位和个人的赔偿 L_1，智慧城市运营方本身因发生信息安全事件时的直接损失 L_2，带来的信誉、口碑等间接损失 L_3 等）。

④将对于该类信息安全事件，信息安全监管部门所投入的监管成本设为 C（包括投入的监管技术成本 C_1 和其他管理成本 C_2 等）。

⑤将智慧城市运营方为了防范该类信息安全事件的发生在加强信息安全管理的情况下投入的额外成本设为 A（包括技术成本 A_1 和管理成本 A_2 等）。

⑥将智慧城市运营方不发生该类信息安全事件时所获得的正常收益设为 R。

⑦将发生该类信息安全事件时，信息安全监管部门产生的损失设为 k。

⑧针对该类信息安全事件，信息安全监管部门对智慧城市运营方不加强信息安全管理行为的处罚金额设为 T。

在上述假设和参数设置的基础上，可以分析信息安全监管部门和智慧城市运营方不同行为策略下的收益，具体情况如表 2 所示。

表 2 监管部门和运营方博弈的收益矩阵

智慧城市运营方	信息安全监管部门	
	监管(x)	不监管($1-x$)
加强信息安全管理(y)	$R-A,0$	$R-A,C$
不加强信息安全管理($1-y$)	$R-pL-T,T$	$R-pL,C-pk$

2.3 演化博弈模型的建立

1) 信息安全监管部门的角度:

由表 2 可知，在监管的情况下，智慧城市运营方选择加强信息安全管理或者不加强信息安全管理时，信息安全监管部门的收益分别为 0 和 T；而在不监管的情况下，智慧城市运营方选择加强信息安全管理或者不加强信息安全管理时，信息安全监管部门的收益分别为 C 和 $C-pk$。由于信息安全监管部门和智慧城市建设方各有一定的概率来选择相应的策略，所以信息安全监管部门的期望收益算式如下:

$$E_G(x,y)=yT(1-x)+(1-y)[C-(1-x)pk] \quad (1)$$

当政府部门完全监管时 $x=1$，政府部门收益为:

$$E_G(1,y)=0+(1-y)T=T(1-y) \quad (2)$$

当政府部门完全不监管时 $x=0$，政府部门收益为:

$$E_G(0,y)=yC+(1-y)(C-pk)=C-(1-y)pk \quad (3)$$

因此，信息安全监管部门的复制动态方程用以下公式表示:

$$E_{gt}=\frac{dx}{dt}=F(x)=x[E_G(1,y)-E_G(x,y)]=x(1-x)[T+pk-C-y(T+pk)] \quad (4)$$

2) 智慧城市运营方的角度

由表 2 可知，在加强信息安全管理的情况下，信息安全监管部门选择监管或者不监管时，智慧城市运营方的收益分别为 $R-A$ 和 $R-pL-T$；而在加强信息安全管理的情况下，信息安全监管部门选择监管或者不监管时，智慧城市运营方的收益分别为 $R-A$ 和 $R-pL$。因此可得到智慧城市运营方的期望收益算式如下:

$$E_B(x,y)=y(R-A)+(1-y)(R-pL-Tx)=(R-pL-Tx)+y(Tx+pL-A) \quad (5)$$

当运营方加强信息安全管理时 $y=1$，建设方的收益为:

$$E_B(x,1)=x(R-A)+(1-x)(R-A)=R-A \quad (6)$$

当运营方不加强信息安全管理时 $y=0$，建设方的收益为:

$$E_B(x,0)=x(R-pL-T)+(1-x)(R-pL)=R-pL-Tx \quad (7)$$

因此，智慧城市运营方选择加强信息安全管理

时，复制动态方程用以下公式表示:

$$E_{bt}=\frac{dy}{dt}=F(y)=y[E_B(x,1)-E_B(x,y)]=y(1-y)(Tx+pL-A) \quad (8)$$

首先，需要联立信息安全监管部门的复制动态方程式（4）和智慧城市运营方的复制动态方程式（8），构成智慧城市运营方与信息安全监管部门的博弈进化系统，结果如下所示:

$$\begin{cases}\frac{dx}{dt}=x(1-x)[T+pk-C)-y(T+pk)] \\ \frac{dy}{dt}=y(1-y)(Tx+pL-A)\end{cases} \quad (9)$$

即智慧城市运营方与信息安全监管部门的演化博弈系统可以用式（9）描述。该系统有 5 个均衡点，分别是:（0,0）、（0,1）、（1,1）、（0,1）、$\left(\frac{T+pk-C}{T+pk},\frac{A-pL}{T}\right)$。

分别对式(9)中的信息安全监管概率 x 和智慧城市运营方加强信息安全管理概率 y 求导，可以得到智慧城市信息安全监管稳定策略的雅克比矩阵为:

$$J=\begin{bmatrix}(1-2x)[T+pk-C-y(T+pk)] & -x(1-x)(T+pk) \\ Ty(1-y) & (1-2y)(pL+Tx-A)\end{bmatrix} \quad (10)$$

其行列式为:

$$detJ=(1-2x)[T+pk-C-y(T+pk)](1-2y)(pL+Tx-A)+Ty(1-y)x(1-x)(T+pk) \quad (11)$$

其迹为:

$$trJ=(1-2x)[T+pk-C-y(T+pk)]+(1-2y)(pL+Tx-A) \quad (12)$$

2.4 信息安全监管博弈双方演化稳定分析

根据演化稳定策略的性质及微分方程的稳定性定理，当上述求解的雅克比矩阵行列式（11）和迹（12）不同正负号时，即为智慧城市信息安全监管博弈系统中各自的演化稳定策略。通过分析信息安全监管部门和智慧城市运营方执行各自行为策略时的成本，得出在以下 6 种情况下智慧城市信息安全监管的博弈行为策略选择，并作出相应稳定性分析和仿真分析。

1）监管高成本、管理低成本的博弈行为

在监管高成本、管理低成本即 $A<pL$ 并且 $C>T+pk$ 时，求解智慧城市运营方与信息安全监管部门的博弈进化系统可得，平衡点分别为(0,0)、(1,0)、(1,1)、(0,1)，演化稳定分析如表 3 所示。此时模型仿真结果如图 1 所示。

表 3 监管高成本、管理低成本时演化稳定分析

平衡点	$detJ$	符号	trJ	符号	局部稳定性
(0,0)	$(T+pk-C)(pL-A)$	<0	$T+pk-C+pL-A$		鞍点
(0,1)	$C(pL-A)$	>0	$-(pL-A)-C$	<0	ESS
(1,1)	$-C(pL+T-A)$	<0	$-(pL+T-A)+C$		鞍点
(1,0)	$-(pL+T-A)(T+pk-C)$	>0	$(pL+T-A)-(T+pk-C)$	>0	不稳定点

依据上述条件，将博弈模型取值设置为 $A=0.5$、$p=0.2$、$L=5$、$C=2$、$T=1$、$k=2$。以概率为纵轴，时间为横轴，经过演化稳定分析得到图 1，可以看出随着时间的推移，信息安全监管部门的监管概率逐渐收敛为 0，智慧城市运营方加强信息安全管理的概率逐渐收敛为 1，即智慧城市信息安全监管演化模型在该情况下的稳定点是(0,1)。该情形表明: 当智慧城市运营方加强信息安全管理的成本小于发生信息安全管理事件的期望损失时，智慧城市运营方选择加强信息安全管理; 此时，在信息安全监管机构高监管成本的情况下，信息安全监管部门选择不监管的行为策略，来避免支付高额的监管费用。相对应的仿真图 1 中，无论信息安全监管的起始概率是多少，最终都会收敛于 $x=0$，加强信息安全监管概率则会收敛于 $y=1$，同样印证了雅克比行列式的分析结果。

2）双方低成本的博弈行为

在双方低成本的博弈行为即 $A<pL$ 并且 $C<T+pk$ 时，求解智慧城市运营方与信息安全监管部门的博弈进化系统可得，平衡点分别为(0,0)、(1,0)、(1,1)、(0,1)，演化稳定分析如表 4 所示。此时模型仿真结果如图 2 所示。

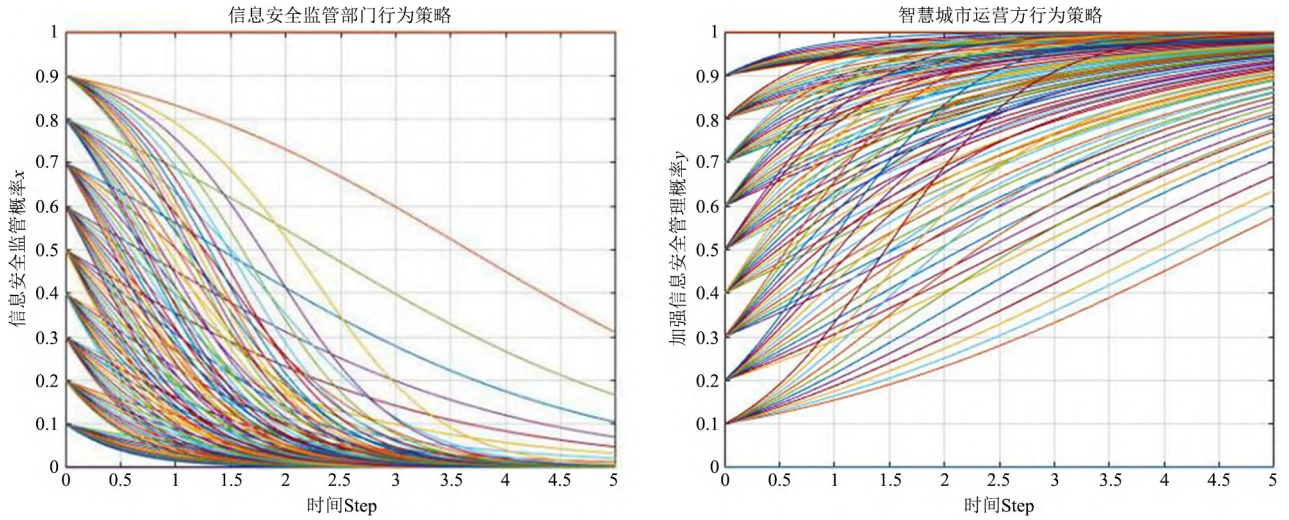

图 1　监管高成本、管理低成本时仿真分析

表 4　双方低成本时演化稳定分析

平衡点	*detJ*	符号	*trJ*	符号	局部稳定性
(0,0)	$(T+pk-C)(pL-A)$	>0	$T+pk-C+pL-A$	>0	**不稳定点**
(0,1)	$C(pL-A)$	>0	$-(pL-A)-C$	<0	EES
(1,1)	$-C(pL+T-A)$	<0	$-(pL+T-A)+C$		**鞍点**
(1,0)	$-(pL+T-A)(T+pk-C)$	<0	$(pL+T-A)-(T+pk-C)$		**鞍点**

依据上述条件，将博弈模型取值设置为 $A=0.8$、$p=0.2$、$L=5$、$C=1$、$T=1$、$k=2$。**以概率为纵轴，时间为横轴，经过演化稳定分析得到图 2，可以看出随着时间的推移，信息安全监管部门的监管概率逐渐收敛为 0，而智慧城市运营方加强信息安全管理概率逐渐收敛为 1，即智慧城市信息安全监管系统模型在该情形下的稳定点是(0,1)。该情形说明：智慧城市运营方选择加强信息安全管理，而信息安全监管机构选择不监管。在该演化稳定策略中，可能由于信息安全监管部门长时间不对智慧城市运营方进行监管，造成智慧城市运营方为了能从不加强信息安全监管的行为策略中获得较多的利益，而选择不加强信息安全管理，进而可能造成更多信息安全事件的发生。相对应的仿真图 2 中，无论信息安全监管的起始概率是多少，最终都会收敛于** $x=0$，**加强信息安全监管概率则会收敛于** $y=1$，**同样印证了雅克比行列式的分析结果。**

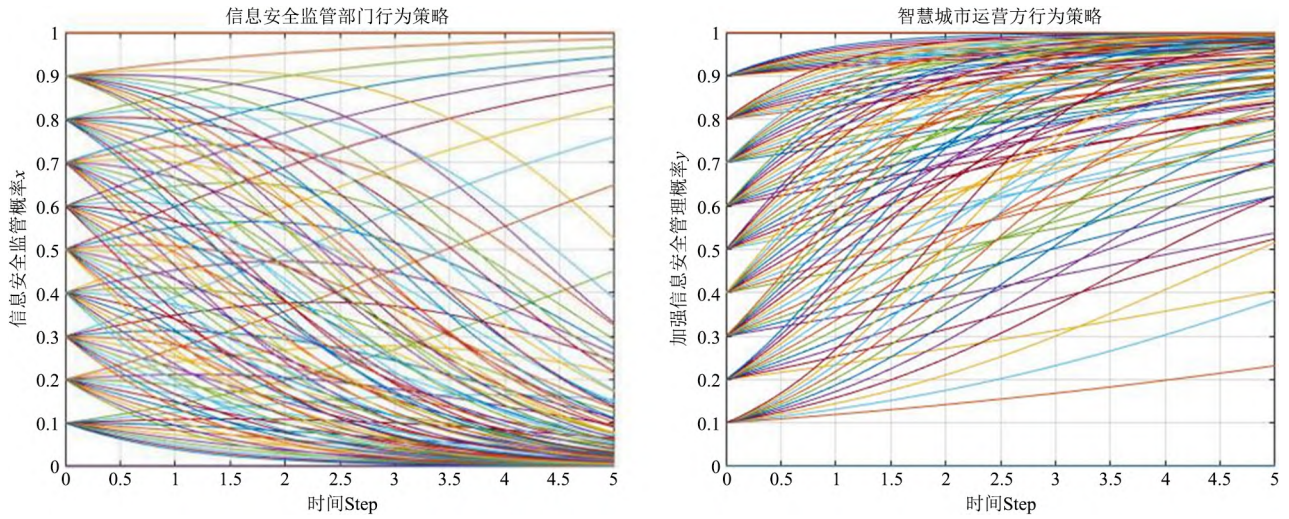

图 2　双方低成本时仿真分析

3) 监管低成本、管理高成本的博弈行为

在监管低成本、管理高成本即 $A>pL+T$ 且 $C<T+pk$ 时，求解智慧城市运营方与信息安全监管部门的博弈进化系统可得，平衡点分别为(0,0)、(1,0)、(1,1)、(0,1)，演化稳定分析如表 5 所示。此时模型仿真结果如图 3 所示。

表 5 监管低成本、管理高成本时演化稳定分析

平衡点	$detJ$	符号	trJ	符号	局部稳定性
(0,0)	$(T+pk-C)(pL-A)$	<0	$T+pk-C+pL-A$		鞍点
(0,1)	$C(pL-A)$	<0	$-(pL-A)-C$		鞍点
(1,1)	$-C(pL+T-A)$	>0	$-(pL+T-A)+C$	>0	不稳定点
(1,0)	$-(pL+T-A)(T+pk-C)$	>0	$(pL+T-A)-(T+pk-C)$	<0	EES

依据上述条件，将博弈模型取值设置为 $A=2.4$、$p=0.2$、$L=5$、$C=1.2$、$T=1$、$k=2$，以概率为纵轴，时间为横轴，经过演化稳定分析可以得到图 3，可以看出随着时间的推移，信息安全监管部门的监管概率逐渐收敛为 1，而智慧城市运营方加强信息安全管理的概率逐渐收敛为 0，即智慧城市信息安全监管系统模型在该情形下的稳定点是(1,0)。该情形表明：当智慧城市运营方加强信息安全管理属于高成本、信息安全监管属于低成本时，运营方选择不加强信息安全管理，监管机构选择进行信息安全监管策略。该情形说明：当 $C<T+pk$ 并且 $A>pL+T$，即当智慧城市运营方加强信息安全管理的成本，大于其不加强信息安全管理所缴纳罚金与发生信息安全事件时的期望损失之和时，智慧城市运营方会选择铤而走险，不加强信息安全管理来获得更高的收益；而由于信息安全监管机构监管低成本，并且监管能够为信息安全监管机构带来更高的收益效果，因此信息安全监管机构将选择执行监管的行为策略。长此以往，该类信息安全事件处罚力度不够，收效甚微，相关事件的发生屡禁不止。相对应的仿真图 3 中无论信息安全监管的起始概率是多少，最终都会收敛于 $x=0$，加强信息安全监管概率则会收敛于 $y=0$，同样印证了雅克比行列式的分析结果。

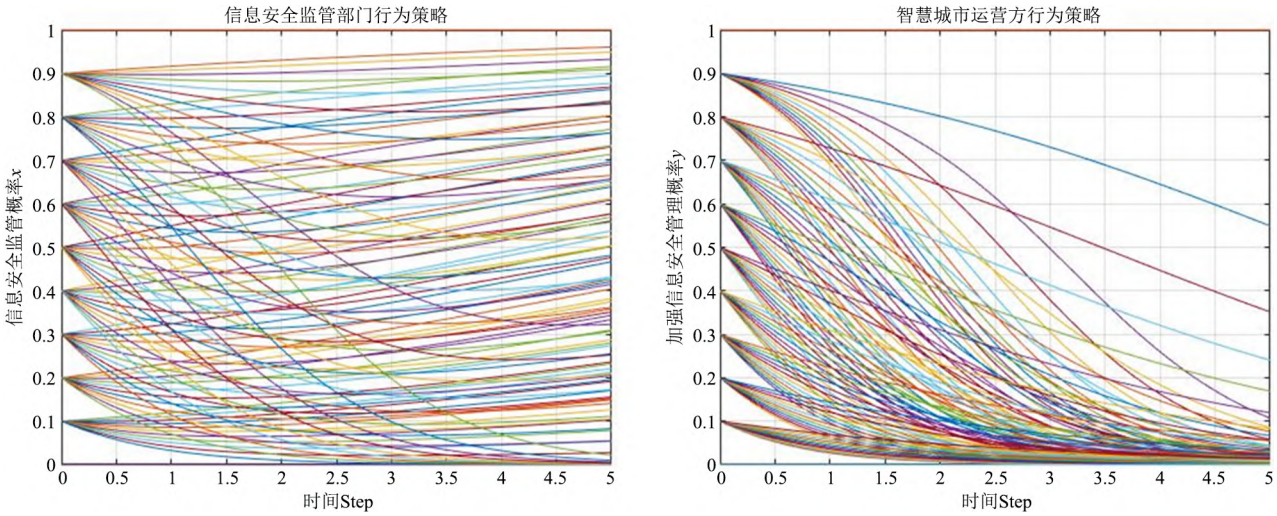

图 3 监管低成本、管理高成本时仿真分析

4) 双方高成本的博弈行为

在双方高成本即 $A>pL+T$ 且 $C>T+pk$ 时，求解智慧城市运营方与信息安全监管部门的博弈进化系统可得，平衡点分别为(0,0)、(1,0)、(1,1)、(0,1)，演化稳定分析如表 6 所示。此时模型仿真结果如图 4 所示。

表 6 双方高成本时演化稳定分析

平衡点	*detJ*	符号	*trJ*	符号	局部稳定性
(0,0)	$(T+pk-C)(pL-A)$	>0	$T+pk-C+pL-A$	<0	EES
(0,1)	$C(pL-A)$	<0	$-(pL-A)-C$	0	鞍点
(1,1)	$-C(pL+T-A)$	>0	$-(pL+T-A)+C$	>0	不稳定点
(1,0)	$-(pL+T-A)(T+pk-C)$	<0	$(pL+T-A)-(T+pk-C)$		鞍点

依据上述条件，将博弈模型取值设置为 $A=2.4$、$p=0.2$、$L=5$、$C=2$、$T=1$、$k=2$。以概率为纵轴，时间为横轴，经过演化稳定分析得到图 4，可以看出随着时间的推移，信息安全监管部门的监管概率和智慧城市运营方加强信息安全管理的概率都逐渐收敛为 0，即智慧城市信息安全监管系统模型在该情形下的稳定点是(0,0)。该情形表明：当信息安全监管机构监管成本大于对不加强信息安全管理智慧城市运营方所收罚款，与其不选择监管策略发生信息安全事件而所受期望损失之和时，信息安全机构会选择不监管的行为策略；而智慧城市运营方加强信息安全管理的成本，大于其不加强信息安全管理而所缴纳罚金与发生信息安全事件的期望损失之和时，智慧城市运营方会选择不安全行为策略。相对应的仿真图 4 中无论信息安全监管的起始概率是多少，最终都会收敛于 $x=0$，加强信息安全监管概率则会收敛于 $y=0$，同样印证了雅克比行列式的分析结果。

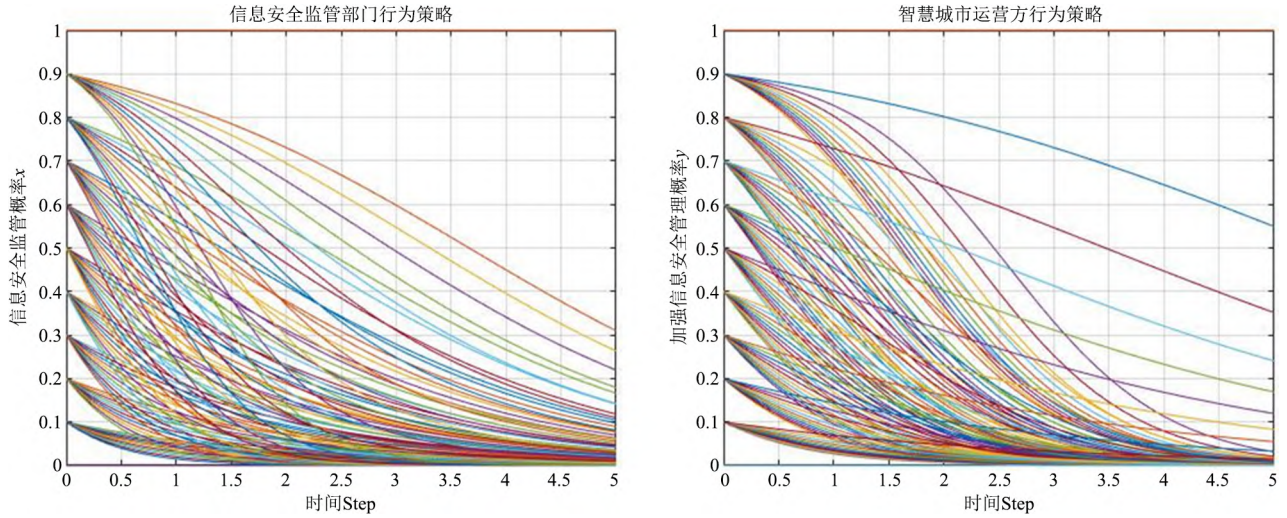

图 4 双方高成本时仿真分析

5) 监管高成本、管理中间成本的博弈行为

当监管高成本、管理中间成本即 $C>T+pk$ 时，求解智慧城市运营方与信息安全监管部门的博弈进化系统可得，平衡点分别为(0,0)、(1,0)、(1,1)、(0,1)，演化稳定分析如表 7 所示。此时模型仿真结果如图 5 所示。

表 7 监管高成本、管理中间成本时演化稳定分析

平衡点	*detJ*	符号	*trJ*	符号	局部稳定性
(0,0)	$(T+pk-C)(pL-A)$	>0	$T+pk-C+pL-A$	<0	EES
(0,1)	$C(pL-A)$	<0	$-(pL-A)-C$		不稳定点
(1,1)	$-C(pL+T-A)$	>0	$-(pL+T-A)+C$	>0	鞍点
(1,0)	$-(pL+T-A)(T+pk-C)$	<0	$(pL+T-A)-(T+pk-C)$		鞍点

依据上述条件，将博弈模型取值设置为 $A=1.5$、$p=0.2$、$L=5$、$C=2$、$T=1$、$k=2$。以概率为纵轴，时间为横轴，经过演化稳定分析得到图 5，可以看出随着时间的推移，信息安全监管部门的监管概率和智慧城市运营方加强信息安全管理的概率都逐渐收敛为 0，即智慧城市信息安全监管系统模型在该情形下的稳定点是(0,0)。该情形说明：信息安全监管机构由于较高的监管成本，选择不监管的行为策略；当智慧城市加强信息安全监管的成本小于不加强信息安全管理所缴纳罚金与信息安全事件发生的期望损失之和，而又大于信息安全事件发生的期望损失时，智慧城市运营方的行为策略选择则会呈现为混合状态，既可能选择加强信息安全管理，亦可能选择不加强信息安全管理，但最终智慧城市运营方都会向不加强信息安全管理演化。相对应的仿真图 5 中无论信息安全监管的起始概率是多少，最终都会收敛于 $x=0$，加强信息安全监管概率则会收敛于 $y=0$，同样印证了雅克比行列式的分析结果。

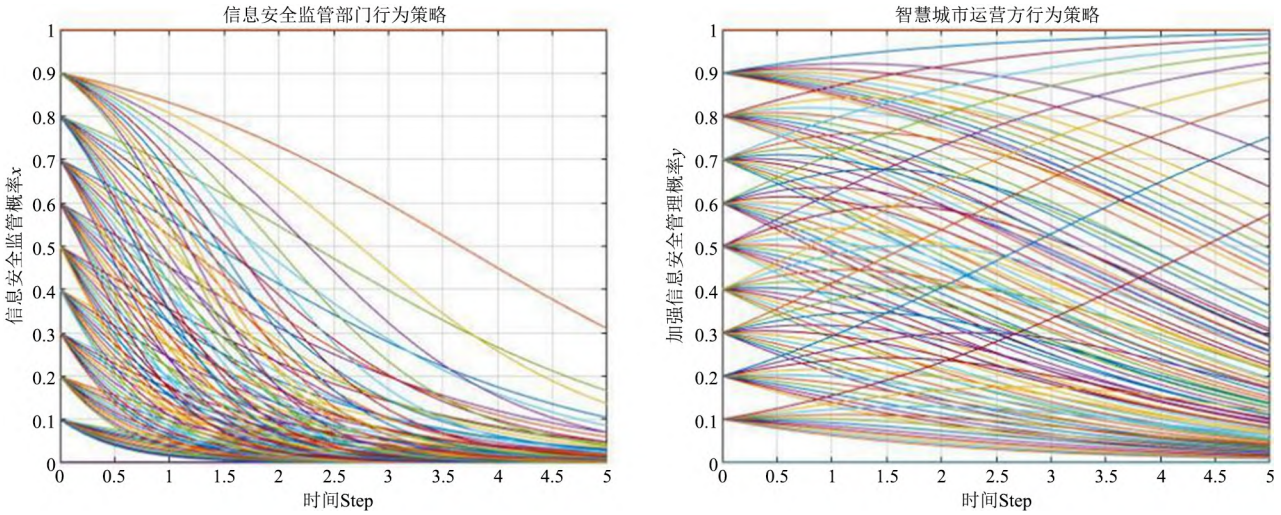

图 5 监管高成本、管理中间成本时仿真分析

6) 监管低成本、管理中间成本的博弈行为

当监管低成本、管理中间成本即 $C<T+pk$ 时，求解智慧城市运营方与信息安全监管部门的博弈进化系统可得，平衡点分别为(0,0)、(1,0)、(1,1)、(0,1)，演化稳定分析如表 8 所示。此时模型仿真结果如图 6 所示。

表 8 监管低成本、管理中间成本时演化稳定分析

平衡点	$detJ$	符号	trJ	符号	局部稳定性
(0,0)	$(T+pk-C)(pL-A)$	<0	$T+pk-C+pL-A$		鞍点
(0,1)	$C(pL-A)$	<0	$-(pL-A)-C$		鞍点
(1,1)	$-C(pL+T-A)$	>0	$-(pL+T-A)+C$	>0	不稳定点
(1,0)	$-(pL+T-A)(T+pk-C)$	<0	$(pL+T-A)-(T+pk-C)$		鞍点
(x_0,y_0)	$x_0(1-x_0)y_0(1-y_0)T(T+pk)$	>0	0		中点

依据上述条件，将博弈模型取值设置为 $A=1.5$、$p=0.2$、$L=5$、$C=1.2$、$T=1$、$k=2$。从表 8 中可以看出点(x_0,y_0)的迹值为 0，所以点(x_0,y_0)是中心点。这种情况说明：当信息安全监管成本较低，加强信息安全管理成本属于中间成本时，智慧城市运营方可能选择加强也可能选择不加强信息安全管理的行为策略，信息安全监管机构员可能选择监管策略，也可能选择不监管策略。相对应的仿真图 6 中信息安全监管的起始概率和加强信息安全监管概率仿真结果都没有明显收敛于 0 或 1，同样印证了雅克比行列式的分析结果。

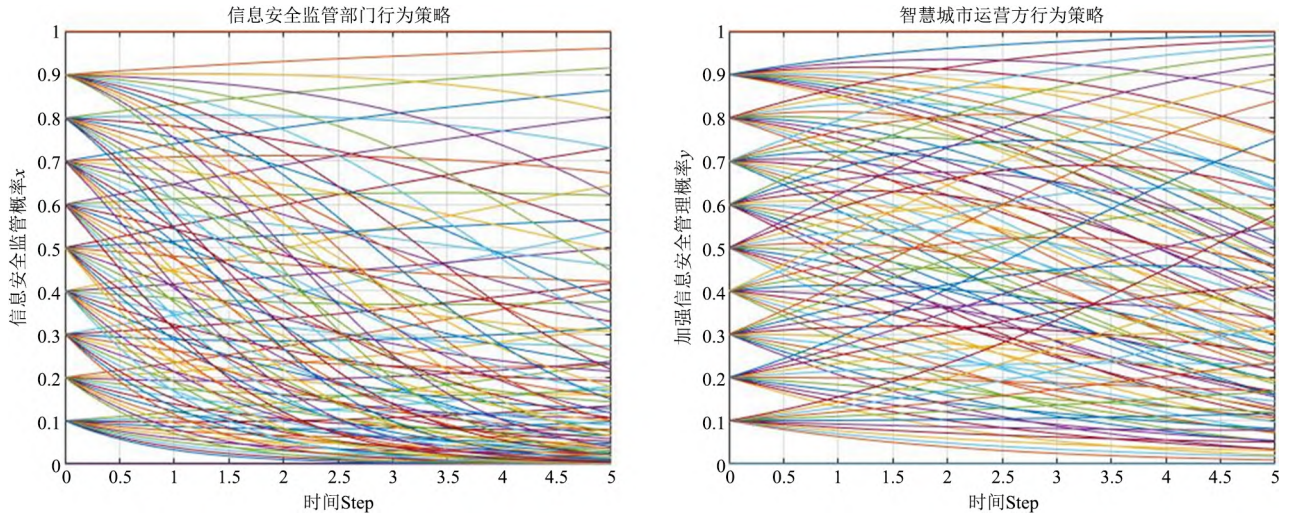

图 6 监管低成本、管理中间成本时仿真分析

综上所述，根据上述演化稳定分析和仿真分析结果，确定了信息安全监管机构和智慧城市运营方的演化稳定策略，具体如表 9 所示。

表 9 智慧城市信息安全监管演化稳定策略表

演化博弈的初始条件	演化稳定策略	信息安全监管策略	加强信息安全管理概率	平衡状态
$A<pL$ and $C>T+pk$	(0,1)	不监管	加强	(1)
$A<pL$ and $C<T+pk$	(0,1)	不监管	加强	(2)
$A>pL+T$ and $C<T+pk$	(1,0)	监管	不加强	(3)
$A>pL+T$ and $C>T+pk$	(0,0)	不监管	不加强	(4)
and $C>T+pk$	(0,0)	不监管	不加强	(5)
and $C<T+pk$	无	混合策略	混合策略	(6)

3 信息安全监管机构行为演化结果分析

信息安全监管机构的目标就是通过行使权力和监督职能保障智慧城市信息安全，促进智慧城市运营方的合理合法竞争。其本身更倾向于不监管或者少监管，在降低监管成本的同时对智慧城市运营方的行为进行管理，约束其不断加强信息安全管理，保障智慧城市各个业务系统的信息安全。因此，根据智慧城市信息安全监管演化稳定策略如表 9 所示，平衡（1）和平衡（2）的最终演化结果都属于理想状态，而平衡（1）由于监管成本较低，在博弈过程中更容易达到共赢。根据达到平衡（1）和平衡（2）所需要满足的条件可知，当 $A<pL$ 时，即加强信息安全管理的成本低于发生信息安全事件的期望损失时，无论信息安全监管部门监管概率的高低，其智慧城市运营方演化的最终结果都将收敛于 1，即采取加强信息安全管理的策略，而较高的信息安全监管概率和较重的处罚政策会加快这一过程的收敛。所以，对于信息安全监管机构，可以给出以下策略建议:

1）针对 $A<pL$ 的信息安全管理措施，要考虑到发生信息安全事件时产生的社会影响和经济影响。对于社会影响和经济影响较大的某一项信息安全管理措施，要采取积极监管的态度，增加被监管部门接受监管的概率，加快智慧城市运营方的演化稳定，引导其加强信息安全管理。对于社会影响和经济影响较小的某项信息安全管理措施，可采取被动监管的态度，在发生信息安全事件时收缴一定的罚金，促使智慧城市运营方改善自身的信息安全技

术和管理条件，加强此项信息安全管理措施。信息安全监管机构也要考虑到自身的成本投入，通过改善人员配置和优化监管技术等措施，降低监管过程中的成本，促使演化博弈过程向着平衡（2）转化，实现双方的共赢。

2）针对 $A>pL$ 的信息安全管理措施，为了督促智慧城市运营方采取积极的管理措施，要加入合理的奖惩制度。通过设置合适的罚金，使其收益受到监管部门监管概率和罚金的影响，促使其向平衡（5）和平衡（6）的转化，采取混合策略，并最终通过改善自身的信息安全技术和管理条件，减轻加强信息安全管理时的成本投入，促使其加强信息安全管理的成本低于发生信息安全事件的期望损失，即 $A<pL$，使之向平衡（1）和平衡（2）转化。因此在此过程中罚金的大小将成为关键因素，要使 $pL+T\geqslant A\geqslant pL$，即智慧城市运营方加强信息安全管理的成本要小于发生信息安全事件时的期望损失和罚金之和。

3）由上述演化博弈分析过程可知，信息安全监管部门应该对智慧城市中的信息安全管理措施实现分类分级监管，针对不同演化博弈的初始条件，设置不同的监管概率，采取对应的监管措施，这样能够有效降低监管成本。此外，监管机构还可通过厘定信息安全监管主体责任，加强监管队伍建设和实现监管技术突破等手段，有效降低监管机构监管成本，提高信息安全监管工作的可控性和可操作性。

4 智慧城市运营方行为演化结果分析

智慧城市运营方虽然主要以自身的盈利为目的，在参与到智慧城市信息安全建设的过程中时，不应只以短期利益为主要着眼点，应该兼顾信息安全管理措施本身的经济效应和社会效应。作为成功的智慧城市运营方，不仅仅是获得较高水平的经济利益，也应该以市场和人民群众的信息安全需求为导向，形成良好的口碑和示范效应。因此，根据如表 9 所示的智慧城市信息安全监管演化稳定策略，针对智慧城市运营方的演化博弈行为，笔者给出以下几点建议。

1）考虑到加强信息安全管理的成本 A 的影响，应该建立起智慧信息安全技术体系。建议根据《计算机信息系统安全保护等级划分准则》，采用分等级保护的思想，将智慧城市信息安全保护分为 5 个等级[21]。针对智慧城市内相关信息的重要程度和社会影响等不同，权衡进行信息安全保护应付出的相应的代价，对关系到智慧城市建设和运营的关键信息与城市居民隐私实施重点保护，对相对不太重要的信息给予适当保护。另外，在智慧城市信息安全技术体系的构建过程中，也要根据信息安全理论、方法和技术，不断提升体系的科学性和合理性，在达到信息安全标准和要求的同时，降低加强信息安全管理的经济成本。

2）考虑到发生信息安全事件时的期望损失 pL 的影响，应该建立起科学可行的智慧城市信息安全风险评估流程和应急响应机制。在信息安全风险评估流程建立过程中，应该运用人工智能、云计算等技术建立风险评估模型，对风险的特征数据进行分析，得出信息安全风险的威胁指数和等级划分，预测风险发生的可能性和可能造成的经济影响和社会影响，给出从制度、技术和管理上解决信息安全风险的处理措施。此外，还需建立一套应对智慧城市系统中各种信息安全事件发生的应急响应机制，以有效降低发生信息安全事件时产生的损失，保障智慧城市运营方的经济利益。

3）另外，根据不同主体用户信息安全保障需求以及问题反馈，相关研究机构和运营公司应采取差异化和个性化管理，实施具有针对性和现实意义的智慧城市信息安全管理和改进方案，降低自身加强信息安全管理措施时的成本。在发挥自身服务优势的同时，平衡多方利益，整合各方服务，从传统的项目型公司转变为面向政府、市民和其他企业的服务型公司，在确保智慧城市产业链之间数据共享安全的同时，形成良好的业界口碑和品牌效应。

5 结束语

基于演化博弈的方法，构建了智慧城市运营方与监管方博弈的收益矩阵，并基于此建立了双方主体的演化博弈模型，针对不同信息监管成本和信息管理成本组合的情况，运用 MATLAB 以及计算机仿真的方式，进行了信息安全监管博弈双方演化稳

定分析，得出了不同境况下监管方与运营方博弈的平衡状态。研究发现，当加强信息安全管理的成本低于发生信息安全事件的期望损失时，其双方博弈结果达到理想状态，且较重的处罚政策，会加快这一过程的收敛。

在理论层面，本研究运用演化博弈对智慧城市信息安全监管问题进行了探讨，通过计算机仿真模拟，探讨了不同情况下博弈双方的平衡条件，并依据平衡条件提出了相关对策建议，为智慧城市信息安全监管问题的研究提供了新的视角。在实践层面，本研究找到了智慧城市信息安全监管方和运营方博弈的理想平衡状态，有利于智慧城市信息安全监管部门改善管理制度以及明确技术改进方向，提升智慧城市信息安全风险应对能力，优化后续智慧城市信息安全监管工作提供一定的参考。

最后，本文还具有可以改进之处：①在仿真数据方面，缺少基于真实案例的实际数据进行仿真。下一步拟找到基于真实案例的实际数据进行仿真，使得研究结论更加可靠。②本文变量设计建立在场景假设的基础上，现实中难免有其他变量的存在而未纳入考虑，今后将在研究中纳入更多变量。③智慧城市信息安全监管过程中除运营和监管双方外，还会涉及到部分社会公众的利益问题，后续研究将对智慧城市信息安全监管过程进行三方博弈分析，从而针对智慧城市信息安全监管的博弈过程进行更系统更全面地分析。

参 考 文 献

[1] 郭骅，苏新宁. 智慧城市信息安全管理的环境、挑战与模式研究 [J]. 图书情报工作，2016，60 (19)：49-58.

[2] 佟大柱. 基于信息安全视角下的智慧城市建设研究 [J]. 网络空间安全，2019，10 (2)：1-4.

[3] 全国标准信息公共服务平台. 信息安全技术—智慧城市建设信息安全保障指南 [EB/OL]. http://std.samr.gov.cn/gb/search/gbDetailed?id=A47A713B75D 614ABE05397BE0A0ABB25_.html_.htm，2020-04-28.

[4] Elmaghraby A S，Losavio M M. Cyber Security Challenges in Smart Cities：Safety，Security and Privacy [J]. Journal of Advanced Research，2014，5 (4)：491-497.

[5] Li X，Li H，Sun B，et al. Assessing Information Security Risk for an Evolving Smart City Based on Fuzzy and Grey FMEA [J]. Journal of Intelligent & Fuzzy Systems，2018，34 (4)：2491-2501.

[6] 向尚，邹凯，蒋知义，等. 基于随机森林的智慧城市信息安全风险预测 [J]. 中国管理科学，2016，24 (S1)：266-270.

[7] 邹凯，侯岚，蒋知义，等. 智慧城市信息安全风险影响因素的三维结构框架与识别研究 [J]. 现代情报，2019，39 (10)：15-23.

[8] 毛子骏，梅宏，肖一鸣，等. 基于贝叶斯网络的智慧城市信息安全风险评估研究 [J]. 现代情报，2020，40 (5)：19-26，40.

[9] 张艳丰，王羽西，邹凯，等. 智慧城市信息安全影响因素与关联路径研究——基于扎根理论的探索性分析 [J/OL]. 情报科学：1-7 [2020-10-10].

[10] Rostami E，Karlsson F，Gao S. Requirements for Computerized Tools to Design Information Security Policies. [J]. Computers Security，2020，99.

[11] Guan B W，Hsu C R. The Role of Abusive Supervision and Organizational Commitment on Employees´Information Security Policy Noncompliance Intention [J]. Internet Research，2020，30 (5)：1383-1405.

[12] 韩欣毅. 特大型城市网络信息安全监管研究 [J]. 信息网络安全，2016，(6)：74-80.

[13] 张磊，于东升，杨军，等. 基于私有云模式的信息安全监管策略研究 [J]. 信息网络安全，2017，(10)：86-89.

[14] 危怀安，李松涛. 第三方支付信息安全监管影响因素及决策分析 [J]. 统计与决策，2018，34 (8)：59-63.

[15] He N，Ip W H，Jiang Z Z，et al. Evolutionary Game Analysis and Regulatory Strategies for Online Group-buying Based on System Dynamics [J]. Enterprise Information Systems，2018，12 (6-10)：695-713.

[16] Shu-Huan F U，Kui-Ran S，Finance S O，et al. Evolutionary Game Analysis of Regulatory Dilemma in Online Car-hailing and Optimizing Policy [J]. On Economic Problems，2019.

[17] 陈福集，王澍贤. 基于演化博弈理论的微博监管策略研究 [J]. 情报杂志，2015，34 (8)：110-114，47.

[18] 杜杨. 基于动态演化博弈的互联网金融创新路径与监管策略 [J]. 统计与决策，2015，(17)：37-41.

[19] 赵静娴. 演化博弈视角下的网络伪舆情监管对策研究 [J]. 情报科学，2016，34 (6)：143-146，169.

[20] 尹珏力，陈会英，王家坤. 在线社交网络中的负面舆情信息传播机制及演化博弈分析 [J]. 情报科学，2020，38 (4)：153-162.

[21] GB 17859-1999，计算机信息系统安全保护等级划分准则 [S].

(责任编辑：郭沫含)