

# 云计算系统认知生存模型及量化分析

赵国生<sup>1</sup>, 李光程<sup>1</sup>, 王 健<sup>2</sup>

(1. 哈尔滨师范大学计算机科学与信息工程学院 哈尔滨 150025; 2. 哈尔滨理工大学计算机科学与技术学院 哈尔滨 150001)

**【摘要】**从云计算演变而来的云安全已成为网络安全领域新的研究热点, 而云安全中的可生存性研究尤为重要。首先分析了云计算系统可生存性的研究现状; 然后基于认知计算技术提出云计算系统的认知生存性定义, 讨论了云计算系统的认知生存能力; 最后使用半马尔科夫性能进程代数(SM-PEPA)对认知生存模型建模, 并对其进行了量化评估。仿真试验以认知生存指数作为评估指标, 对生存性威胁的构成、抵抗攻击的能力、策略库的知识丰富度以及生存性威胁检测率等参数的取值结合实例模拟对云计算系统认知生存性的影响, 通过求解模型的首次通过时间概率密度函数, 验证模型对认知生存能力评估的合理性和有效性。

**关键词** 云计算; 云安全; 认知生存性; 量化分析

**中图分类号** TP393.8 **文献标志码** A **doi**:10.3969/j.issn.1001-0548.2017.05.012

## Cognitive Survival Model and Quantitative Analysis for Cloud Computing Systems

ZHAO Guo-sheng<sup>1</sup>, LI Guang-cheng<sup>1</sup>, and WANG Jian<sup>2</sup>

(1. College of Computer Science and Information Engineering, Harbin Normal University Harbin 150025;

2. School of Computer Science and Technology, Harbin University of Science and Technology Harbin 150001)

**Abstract** The cloud security evolved from cloud computing has become a research hotspot in network security field, and the survivability of cloud security is particularly important. The current research status of survivability is analyzed firstly. Then the definition of cognitive survivability based on cognitive computing is proposed, and the ability of cognitive survivability is discussed. Finally, the cognitive survival model based on semi-Markov performance evaluation process algebra (SM-PEPA) is formalized and the solution of the quantitative assessment is described. The simulation experiment uses the cognitive survival index as evaluation parameters, such as survival threats, the ability to resist attacks and the richness of strategies. The proposed model is validated by solving the first passage time probability density function.

**Key words** cloud computing; cloud security; cognitive survivability; quantitative analysis

云计算是一种具有跨时代意义的新型互联网络服务计算模式<sup>[1]</sup>。云计算系统以提供各种可信关键服务的形式存在, 其服务提供者的特点使它成为可生存性<sup>[2-3]</sup>研究最具有代表性的平台。而云安全中的可生存性研究尤为重要, 目前对于它的研究还刚刚起步<sup>[4]</sup>。文献[5]提出了一种以可生存性为中心的云计算支持的应急响应和管理系统。文献[6]提出了云环境下的轻量级软件容错系统, 提高软件的可生存性。文献[7]提出了一种提高虚拟化数据中心可生存能力的服务感知方法。文献[8]基于混合线性规划的启发式算法解决了面向云数据中心虚拟多播服务的可生存性配置策略。文献[9]介绍了安全云基础设施的防护原则、漏洞威胁和安全机制等业务需求。文

献[10]研究了云计算平台的生存性需求和存活机制。文献[11]提出了服务质量(quality of service, QoS)的计算方法及分布式系统可生存性的量化评估方法。文献[12]针对云计算中心性能分析问题, 提出基于排队系统的云计算中心分析模型。

云计算系统下可生存性研究正如火如荼展开, 但是现有研究大都从如何增强虚拟机的安全角度来提高云计算系统的服务生存能力或者通过单一度量服务可用性来评估云计算系统的可生存性。本文基于认知计算技术, 提出以认知生存指数作为云计算系统健康度与可信性的评估指标, 对认知生存模型进行了形式化描述并结合实例分析了模型参数对认知生存性的影响。

收稿日期: 2015-11-27; 修回日期: 2016-12-02

基金项目: 国家自然科学基金(61202458, 61403109)

作者简介: 赵国生(1977-), 男, 博士, 教授, 主要从事可生存性技术、认知网络、可信计算方面的研究。

# 1 云计算系统的生存性建模

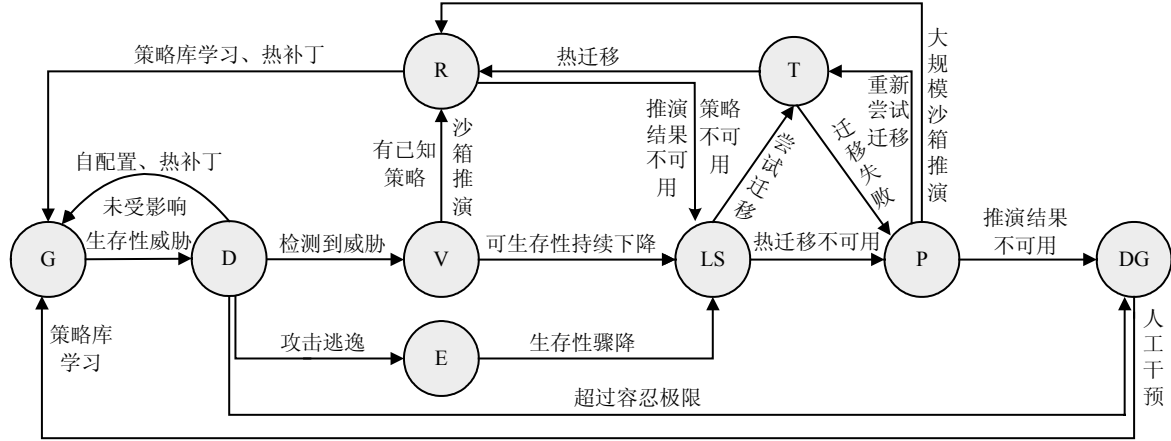
云计算系统应该是一个智能的、自我管理、有认知能力和自律特性的智能决策分析系统,具有高度自主认知的可生存能力<sup>[13-15]</sup>。

## 1.1 认知生存性的定义

**定义 1** 云计算系统的可生存性是指当云计算

系统的某个云节点、服务或系统本身遭受攻击、意外失效等威胁时,系统仍能持续完成任务或对外提供关键服务且能够及时修复被损坏服务的能力。

**定义 2** 认知生存性是指系统在自主认知内外生存环境变化,导致系统生存性下降到一定阈值时,采取自配置、自优化等高生存策略而使系统可生存性得以保持和增长的手段与能力。



General (G)正常态 Vulnerable(V)脆弱态 Detection(D)检测态 DeGradation(DG)降级服务态 Escape(E)逃逸态  
Recovery(R)自恢复态 Transfer(T)迁移态 LowSurvivability(LS)低可生存性态 Pressing(P)紧急态

图1 云计算系统认知生存状态转移模型

对于云计算系统,导致其生存性能下降有诸多因素,本文将其划分为人为恶意攻击(attack)、硬件故障失效(failure)及意外事故(accident)3种情况。云计算系统将认知生存能力分级应对各种使可生存性降低的威胁,按图1所示的状态转移模型能够很好地刻画可生存性的演化过程。

## 1.2 认知生存性的形式化描述

PEPA<sup>[16-17]</sup>是一种典型的进程代数,具有的优点<sup>[18]</sup>和语法<sup>[19-20]</sup>略。基于SM-PEPA对云计算系统进行形式化建模如下:

```
Intruder:=(searching,h).Attack;
Attack:=(start_attack,Lp).(attack,k).Attack+(start_attack,Lg).Intruder;
Failure:=(start_failing,i).Failure0;
Failure0:=(failing,q1).Failure;
Accident:=(start_error,j).Accident0;
Accident0:=(error,q2).Accident;
General:=(attack,z1).Detection+(failing,z2).Detection+
(error,z3).Detection;
Detection:=(start_detect,L1).Escape+(start_detect,
L2).DeGradation+(start_detect,L3).Vulnerable+(start_
detect,L4).(mask,w1).General;
```

```
Vulnerable:=(search_policy,L5).(searched,w2).Recovery||
(sandbox_derive,w3).Recovery+(drop,w4).LowSurvivability;
```

```
LowSurvivability:=(intend_transfer,w5).Transfer+
(forbid_transfer,L6).Pressing;
```

```
Transfer:=(transferring,w6).Recovery+(failed_transfer,
L7).Pressing;
```

```
Pressing:=(intend_transfer,w7).Transfer||
(largescale_sandbox_derive,w8).Recovery+(disable,L8).DeGradation;
```

```
Recovery:=(failed_recovery,L9).LowSurvivability+
(recover,w9).General;
```

```
DeGradation:=(qm_intervention,w10).General;
```

```
Escape:=(plummet,w11).LowSurvivability;
```

```
(Attack[m]▷◁ Failure[n]▷◁ Accident[I])||
(attack,failing,erro)General
```

各参数代表的含义如表1所示。需要指出的是,如果某个action的变迁速率服从指数分布时,动作变迁导致不同的结果,如 $P=(action,\lambda_1).P_1+(action,\lambda_2).P_2$ ,那么P到P<sub>1</sub>的概率(likelihood)为 $\lambda_1 / (\lambda_1 + \lambda_2)$ 。以此类推,对有限多情况,  $likelihood_i = \lambda_i / \sum_i \lambda_i$ ,  $i = 1, 2, 3, \dots$ 。为方便计算,直接令P到P<sub>i</sub>的变迁速率

为  $L_i = \text{likelihood}_i (0 < L_i < 1)$ ,  $\sum_i L_i(\text{action}) = 1$ 。

表1 各参数代表的含义

| 参数       | 含义                     |
|----------|------------------------|
| $h$      | 发现漏洞的变迁速率              |
| $L_p$    | 持续攻击的概率                |
| $k$      | 入侵动作的变迁速率              |
| $L_g$    | 入侵者放弃攻击的概率             |
| $i$      | 随机故障转化为可使生存性降低的威胁的变迁速率 |
| $q_1$    | 故障失效的变迁速率              |
| $j$      | 误操作转化为生存性威胁的变迁速率       |
| $q_2$    | 误操作的变迁速率               |
| $z_1$    | 入侵攻击进入检测态的变迁速率         |
| $z_2$    | 故障失效进入检测态的变迁速率         |
| $z_3$    | 意外事故进入检测态的变迁速率         |
| $L_1$    | 攻击逃逸的概率                |
| $L_2$    | 受到超出容忍极限的攻击的概率         |
| $L_3$    | 生存性下降的概率               |
| $w_1$    | 屏蔽漏洞的变迁速率              |
| $L_4$    | 生存性未下降的概率              |
| $L_5$    | 策略库有策略的概率              |
| $w_2$    | 策略库搜索的速率               |
| $w_3$    | 沙箱推演的速率                |
| $w_4$    | 脆弱态至低生存性态的变迁速率         |
| $w_5$    | 低生存性态转移到迁移态的变迁速率       |
| $L_6$    | 迁移不可用的概率               |
| $w_6$    | 迁移态到自恢复态的变迁速率          |
| $L_7$    | 迁移失败的概率                |
| $w_7$    | 由紧急态进入迁移态的变迁速率         |
| $w_8$    | 由紧急态进入自恢复态的变迁速率        |
| $L_8$    | 紧急态进入降级服务态的概率          |
| $L_9$    | 自恢复失败的概率               |
| $w_9$    | 自恢复态进入正常态的变迁速率         |
| $w_{10}$ | 降级服务态进入正常态的变迁速率        |
| $w_{11}$ | 逃逸态进入低生存形态的变迁速率        |

模型中, Attack[ $m$ ]、Failure[ $n$ ]与Accident[ $l$ ]分别表示入侵攻击、故障失效与意外事故3类威胁的序列,  $m$ 、 $n$ 、 $l$ 表示序列中元素的个数。

### 2 模型的求解与量化分析

因为SM-PEPA可转化为半马尔可夫过程(semi Markov process, SMP), 所以可求解对应SMP各状态的稳态概率来分析SM-PEPA, 稳态概率向量的求解过程可参考文献[19-21]。通过求解获得SM-PEPA模型中各状态的稳态概率。

本文使用爱丁堡大学计算机科学基础实验室的Version v25 of the PEPA Eclipse Plugin<sup>[22]</sup>工具对模型进行辅助求解, 其运行界面如图2所示。

本文借鉴认知计算与系统可生存性的量化方法, 参考文献[23]的自律可信指数定义, 从稳态概率分析的角度对认知生存性进行量化评估, 用认知生存指数表征系统的认知生存性。

将SM-PEPA模型的状态空间分为两部分: 认知状态集 $X_1$ 和非认知状态集 $X_2$ 。同理, 稳态概率集合  $\pi = \{\pi_1, \pi_2, \dots, \pi_s\}$ , 也可分为两部分, 对应 $X_1$ 的子集记为 $C_D$ , 另一子集记为 $C_{UD}$ 。

定义 3 设  $\pi_1, \pi_2, \dots, \pi_s$  分别为认知生存状态的稳态概率, 认知生存指数  $\Gamma_{AD} \in (0,1)$  满足:

$$\Gamma_{AD} = \sum_{\pi_i \in C_D} \pi_i \tag{1}$$

即系统处于认知生存状态的稳态概率之和。

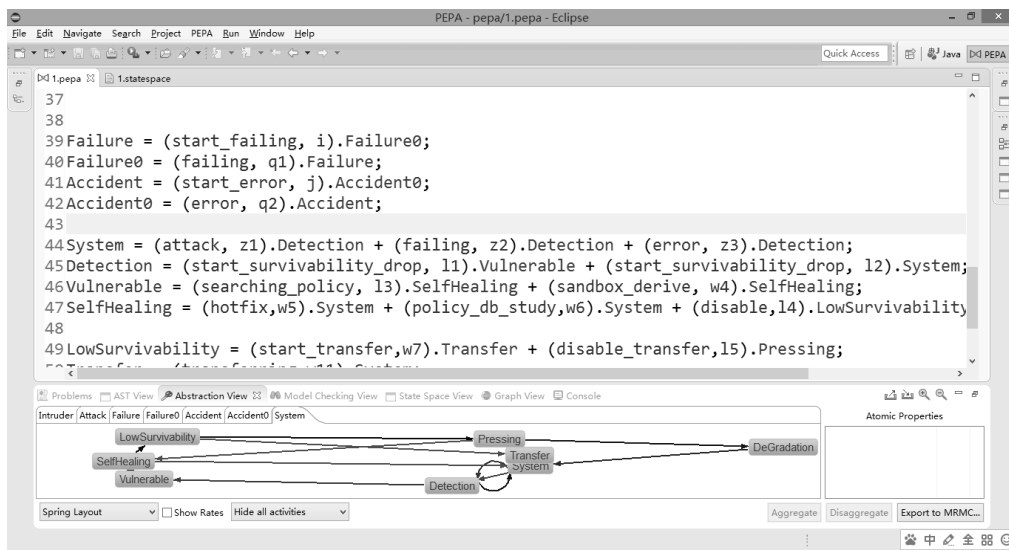


图2 the PEPA Eclipse Plugin运行界面

结合一个实例对  $\Gamma_{AD}$  进行说明, 为了将问题简化, 方便计算与分析, 假设云计算系统对应的认知

生存模型中  $m=n=l=1$ , 并简化模型中所有的动作均服从指数分布, 模型中各参数的取值如表2所示。将

表2中数据代入模型中,计算其对应的SMP,得到88个状态,然后解得隐含SMP的各个状态的稳态概率

如表3所示。将表3中的稳态概率代入到式(1)中即可求得该实例的认知生存指数为0.998 14。

表2 模型的参数取值

| 参数    | 取值      | 参数       | 取值              | 参数       | 取值    |
|-------|---------|----------|-----------------|----------|-------|
| $h$   | 0.001 8 | $L_1$    | 0.01            | $w_5$    | 0.8   |
| $k$   | 0.3     | $L_2$    | 0.005           | $L_6$    | 0.05  |
| $i$   | 0.3     | $L_3$    | 0.75            | $w_6$    | 0.3   |
| $j$   | 0.9     | $w_1$    | 1.0             | $L_7$    | 0.01  |
| $w_1$ | 1.0     | $w_{10}$ | 0.1             | $w_7$    | 0.8   |
| $q_1$ | 0.2     | $L_4$    | $1-L_1-L_2-L_3$ | $w_8$    | 0.4   |
| $q_2$ | 0.3     | $L_5$    | 0.5             | $L_8$    | 0.05  |
| $z_1$ | 0.7     | $w_2$    | 0.7             | $L_9$    | 0.007 |
| $z_2$ | 0.3     | $w_3$    | 0.3             | $w_9$    | 0.8   |
| $z_3$ | 0.9     | $w_4$    | 0.3             | $w_{11}$ | 1.0   |

表3 模型的稳态概率

| NO. | 状态  | $\pi_i$                                       |
|-----|---|---|
| 1   | {General,Attack,Attack,Failure,Accident}        | $2.137\ 631\ 469\ 423\ 467\ 4 \times 10^{-7}$ |
| 2   | {Detection,Attack,Attack,Failure,Accident}      | $2.137\ 631\ 469\ 423\ 465\ 8 \times 10^{-7}$ |
| 3   | {General,Attack,Intruder,Failure,Accident}      | $1.187\ 573\ 038\ 568\ 590\ 3 \times 10^{-4}$ |
| 4   | {General,Attack,Attack,Failure0,Accident}       | $3.206\ 447\ 204\ 135\ 207\ 0 \times 10^{-7}$ |
| 5   | {General,Attack,Attack,Failure,Accident0}       | $6.412\ 894\ 408\ 270\ 411\ 0 \times 10^{-7}$ |
| 6   | {Escape,Attack,Attack,Failure,Accident}         | $2.137\ 631\ 469\ 423\ 463\ 6 \times 10^{-8}$ |
| 7   | {DeGradation,Attack,Attack,Failure,Accident}    | $2.794\ 589\ 757\ 827\ 866\ 0 \times 10^{-7}$ |
| 8   | {Vulnerable,Attack,Attack,Failure,Accident}     | $1.233\ 248\ 924\ 667\ 382\ 2 \times 10^{-7}$ |
| 9   | {Detection,Attack,Intruder,Failure,Accident}    | $1.187\ 573\ 038\ 568\ 589\ 2 \times 10^{-4}$ |
| 10  | {Detection,Attack,Attack,Failure0,Accident}     | $3.206\ 447\ 204\ 135\ 202\ 3 \times 10^{-7}$ |
| ⋮   | ⋮   | ⋮   |
| 86  | {Recovery,Intruder,Intruder,Failure0,Accident0} | 0.071 371 933 450 448 330                     |
| 87  | {Transfer,Intruder,Intruder,Failure0,Accident0} | 0.048 262 073 844 649 506                     |
| 88  | {Pressing,Intruder,Intruder,Failure0,Accident0} | 0.011 984 541 827 194 816                     |

### 3 仿真分析

#### 3.1 生存性威胁构成的分析

生存性威胁的构成与数量是表征系统受安全威胁程度的重要参数,假设威胁序列threats中的每类威胁的效用时间服从相同分布,通过改变模型中 $m$ 、 $n$ 、 $l$ 的取值可求解不同取值对认知生存性的影响。实验结果如表4所示,表中可以看出随着参数取值的变化,认知生存性均维持于较高的水平,且样本的总体方差为 $1.365\ 21 \times 10^{-6}$ ,这说明生存性威胁的构成与数量的改变对系统的认知生存性影响较小,云计算系统的生存稳定性较高。

表4 威胁构成与数量对认知生存性的影响

| $m$ | $n$ | $l$ | 状态空间数量 | 认知生存指数   |
|-----|-----|-----|--------|----------|
| 1   | -   | -   | 22     | 0.999 42 |
| -   | 1   | -   | 22     | 0.999 77 |
| -   | -   | 1   | 22     | 0.999 56 |
| 1   | 1   | -   | 44     | 0.998 81 |
| 1   | -   | 1   | 44     | 0.998 78 |
| -   | 1   | 1   | 44     | 0.998 94 |
| 1   | 1   | 1   | 88     | 0.998 14 |
| 10  | -   | -   | 121    | 0.996 32 |
| -   | 10  | -   | 121    | 0.996 96 |
| -   | -   | 10  | 121    | 0.997 01 |
| 5   | 5   | 5   | 2 376  | 0.996 98 |

#### 3.2 生存性威胁检测率的分析

下面就生存性威胁检测率  $\text{likelihood}_{\text{Detection}} = 1-L_1$ 对认知生存指数的影响进行量化分析。通过改变表2中 $L_1$ 与 $L_4$ 的值而改变  $\text{likelihood}_{\text{Detection}}$  的取值,求解每次实验的  $\Gamma_{AD}$ ,得到  $\text{likelihood}_{\text{Detection}}$  与  $\Gamma_{AD}$  的关系如图3所示。

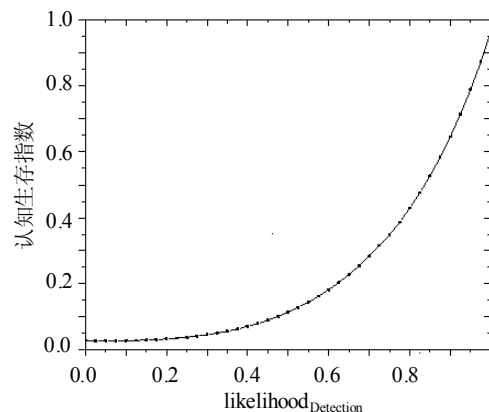


图3 威胁检测率对认知生存性的影响

由图3可以看出,系统认知生存指数随威胁的检测率提高而迅速上升。当  $\text{likelihood}_{\text{Detection}} \rightarrow 0$  时,  $\Gamma_{AD} \rightarrow 0$ ,这是因为当威胁检测率较低时,大量未检测的威胁会令系统的认知生存指数下降。随着威

胁检测率的升高, 认知生存指数呈上凹趋势, 即  $\frac{d^2 \Gamma_{AD}}{d(\text{likelihood}_{\text{Detection}})^2} > 0$ , 当  $\text{likelihood}_{\text{Detection}} \rightarrow 1$  时,  $\Gamma_{AD} \rightarrow 0$ 。这主要是因为检测到生存性威胁后被认知生存模型中的各认知层分级优化自配置处理, 使得系统的认知生存能力得以提高。

### 3.3 入侵防御能力的分析

参数  $h$  表示入侵者能够检测到系统漏洞的概率, 该参数间接反映了系统对入侵攻击的防御能力。  $h$  越小, 系统对入侵的抵抗能力越强。

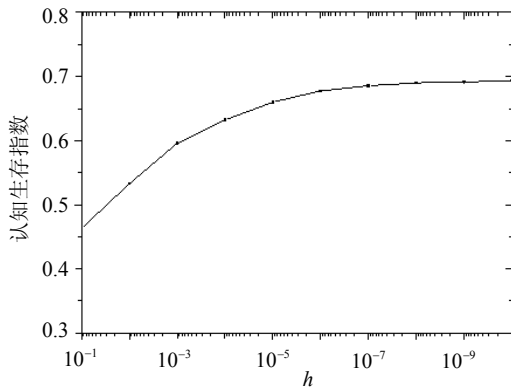


图4  $h$ 对认知生存性的影响

对表2中参数  $h$  取不同的值并计算每次实验的  $\Gamma_{AD}$ , 实验结果如图4所示。认知生存指数随  $h$  值的减小而增加, 当  $h \rightarrow 1 \times 10^{-9}$ , 系统的认知生存指数趋近于0.8, 在此之后生存性指数的增长率迅速降低, 曲线趋于稳定。因此, 适度提高抗攻击能力对提升云计算系统认知生存性是重要的生存措施。

### 3.4 策略库知识丰富度的分析

通过改变  $L_5$  的取值模拟改变策略库的知识丰富度, 并通过计算每次实验  $\Gamma_{AD}$  的值来分析策略库知识丰富度对认知生存性的影响, 实验结果如图5所

示。认知生存能力随策略库知识丰富度增加而提高。云计算系统基于策略库指定最优动作能够快速执行最优方案解, 从而减少状态转移次数和动作延迟, 降低系统处于低生存性状态的时间和概率。采用更加高效的聚类算法对样本进行训练, 提高系统认知策略库的自学习能力是今后研究的方向。

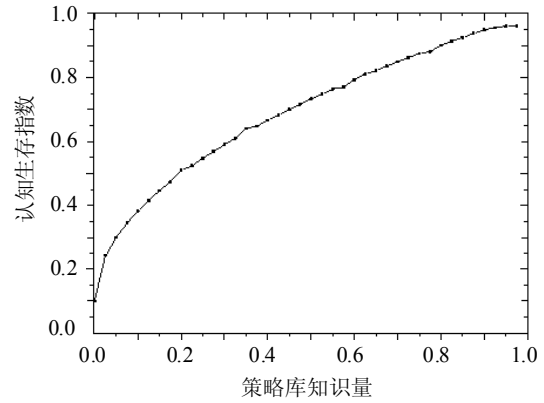


图5  $L_5$ 对认知生存性的影响

### 3.5 首次通过时间概率密度函数

首次通过时间(first passage time)是分析Markov过程的一个重要参数<sup>[24]</sup>。下面通过求解从生存性威胁出现至系统从威胁中恢复的首次通过时间概率密度函数(probability density function, PDF)与积累分布函数(cumulative distribution function, CDF)分析云计算系统的可生存性变化。

通过图6与图7可以看出, 在100个时间单位内PDF与CDF都维持在较小的数值变化范围内, PDF从第3个时间单位之后都处于下降趋势, CDF在32时间单位达到1.0之后基本不再增长, 可以在一定程度上印证本文的云计算系统认知生存模型在保持合理性和稳定性的同时, 极大地降低了系统进入低生存状态的可能性。

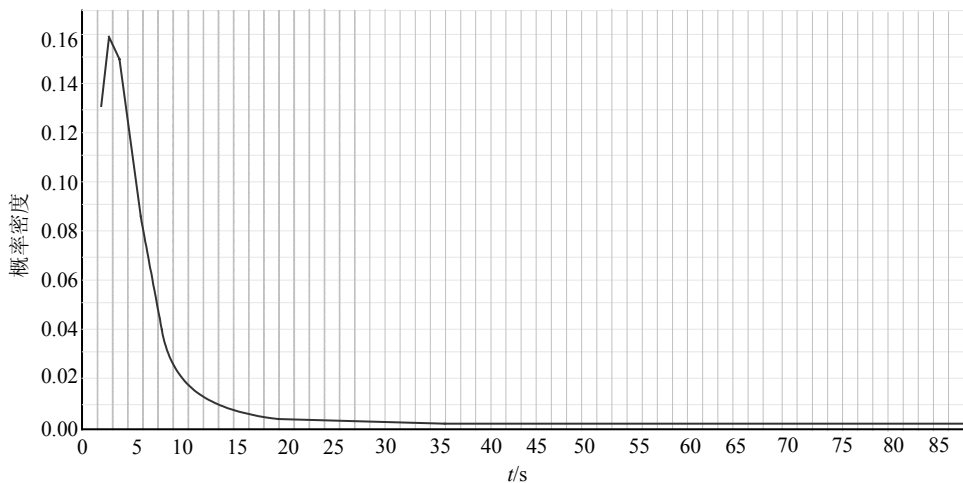


图6 首次通过时间概率密度函数

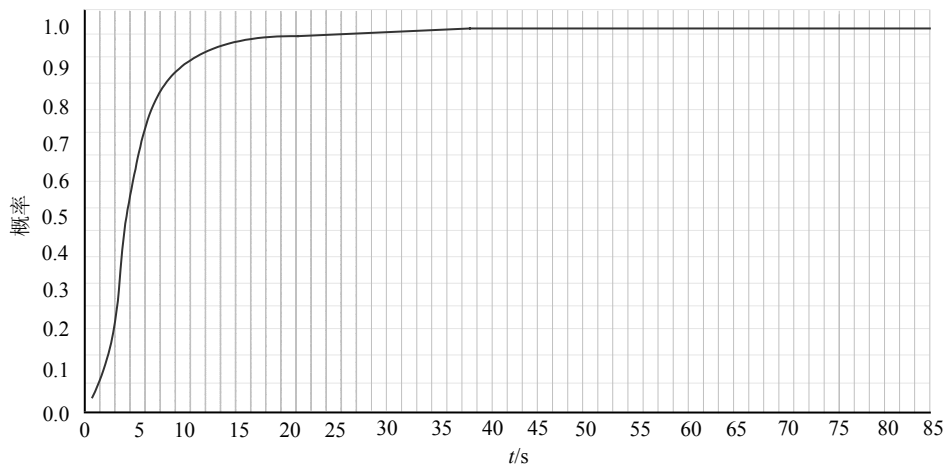


图7 首次通过时间积累分布函数

## 4 结束语

受认知计算的启发,提出了一种云计算系统的认知生存模型,使用SM-PEPA语言对模型进行了形式化描述,以认知生存指数为指标分析了部分模型参数对云计算系统认知生存性的影响。下一步的研究工作是建立实际的云安全应用场景,对认知生存能力的评估体系和评估参数的合理性、可行性做进一步测试研究。另外,由于现有SM-PEPA求解工具都存在自动化程度低的缺点,因此需要编写更加高效的分析求解工具。

本文的研究工作得到了哈尔滨市科技创新人才研究专项资金(2016RAQXJ036)的资助,在此表示感谢!

### 参 考 文 献

- [1] MELL P, GRAMCE T. The NIST definition of cloud computing[J]. *Communications of the Acm*, 2011, 53(6): 50-50.
- [2] WESTMARK V R. A definition for information system survivability[C]//*Proceedings of the 37th Hawaii Internal Conference on System Sciences*. Washington: IEEE Computer Society Press, 2004: 2086-2096.
- [3] ELLISON R, LINGER R, LONGSTAFF T. Survivability network system analysis: a case study[J]. *IEEE Software*, 1999(4): 70-77.
- [4] 吴吉义, 沈千里, 章剑林. 云计算: 从云安全到可信云[J]. *计算机研究与发展*, 2010, 48(z1): 229-233.  
WU Ji-yi, SHEN Qian-li, ZHANG Jian-lin. Cloud computing: Cloud security to trusted cloud[J]. *Journal of Computer Research and Development*, 2010, 48(z1): 229-233.
- [5] MA Z S, LIEXUN Y, RONALD P N, et al. A survivability-centered research agenda for cloud computing supported emergency response and management systems[C]//*Proceedings of IEEE Aerospace Conference*. Big Sky, MT, USA: IEEE Computer Society Press, 2014: 1-17.
- [6] CHEN G, JIN H, ZOU D Q, et al. A lightweight software fault-tolerance system in the cloud environment[J]. *Concurrency Computation*, 2015, 27(12): 2982-2998.
- [7] XU J L, TANG J, KWIAT K, et al. Enhancing survivability in virtualized data centers: a service-aware approach[J]. *IEEE Journal on Selected Areas in Communications*, 2013, 31(12): 2610-2619.
- [8] LIAO D, SUN G, ANAND V, et al. Survivable provisioning for multicast service oriented virtual network requests in cloud-based data centers[J]. *Optical Switching and Networking*, 2014, 44(3): 260-273.
- [9] MEDHIOUB M, HAMDY M, KIM T H. Requirements capture and comparative analysis of cloud security techniques[J]. *International Journal of Grid and Distributed Computing*, 2015, 8(2): 285-308.
- [10] 赵淦森, 王维栋, 孙伟. 云计算平台生存性研究[J]. *电信科学*, 2011, 27(9): 52-59.  
ZHAO Gan-sen, WANG Wei-dong, SUN Wei. Research of cloud survivability[J]. *Telecommunications Science*, 2011, 27(9): 52-59.
- [11] 张勇实, 张乐君, 张健沛, 等. 基于QoS关联分析的分布式系统可生存性评估[J]. *电子科技大学学报*, 2013, 42(1): 109-114.  
ZHANG Yong-shi, ZHANG Le-jun, ZHANG Jian-pei. Distributed system survivability evaluation based on the correlations analysis of QoS[J]. *Journal of University of Electronic Science and Technology of China*, 2013, 42(1): 109-114.
- [12] 何怀文, 傅瑜. 批量到达下的IaaS云计算中心服务性能评价[J]. *电子科技大学学报*, 2015, 44(3): 445-450.  
HE Huai-wen, FU Yu. Service performance evaluation of IaaS cloud computing center under batch arrivals[J]. *Journal of University of Electronic Science and Technology of China*, 2015, 44(3): 445-450.
- [13] 王慧强, 徐俊波, 冯光升, 等. 认知网络体系结构研究新进展[J]. *计算机科学*, 2011, 38(8): 9-16, 24.  
WANG Hui-qiang, XU Jun-bo, FENG Guang-sheng, et al.

- Review of architectures of cognitive network[J]. Computer Science, 2011, 38(8): 9-16, 24.
- [14] 董超, 毕晓君. 认知计算的发展综述[J]. 电子世界, 2014(15): 200-201.  
DONG Cao, BI Xiao-jun. Survey on cognitive computing[J]. Electronics World, 2014(15): 200-201.
- [15] 林俊宇, 王慧强, 马春光, 等. 一种基于DAG动态重构的认知网络服务迁移方法[J]. 软件学报, 2014(10): 2373-2384.  
LIN Jun-yu, WANG Hui-qiang, MA Chun-guang, et al. Service migration method for cognitive network based on DAG dynamic reconstruction[J]. Journal of Software, 2014(10): 200-201.
- [16] HILLSTON J. Tuning systems: from composition to performance[J]. Computer Journal, 2005, 48(4): 385-400.
- [17] 严博, 吴晓平, 廖巍, 等. 基于随机进程代数的P2P网络蠕虫对抗传播特性分析[J]. 电子学报, 2012, 40(2): 293-299.  
YAN Bo, WU Xiao-ping, LIAO Wei, et al. Propagation characteristics analysis of worm-anti-worm in P2P network based on stochastic process algebra[J]. Acta Electronica Sinica, 2012, 40(2): 293-299.
- [18] 郭辉. 进程代数及其在性能评价中的应用综述[J]. 微计算机应用, 2007, 28(9): 901-905.  
GUO Hui. Process algebra and application of it in performance evaluation[J]. Micorocomputer Applications, 2007, 28(9): 901-905.
- [19] BRADLEY J T. Semi-Markov PEPA: Modelling with generally distributed actions[J]. International Journal of Simulation, 2005, 6(3): 43-51.
- [20] BRADLEY J T. Semi-Markov PEPA: Compositional modelling and analysis with generally distributed actions[D]. Bradford: University of Bradford, 2004.
- [21] 王健, 赵国生. 基于SM-PEPA可生存系统认知模型及量化分析[J]. 华中科技大学学报(自然科学版), 2015, 43(5): 99-103.  
WANG Jian, ZHAO Guo-sheng. Cognitive model and quantitative analysis for survivable system based on SM-PEPA[J]. Journal of Huazhong University of Science and Technology (Nature Science Edition), 2015, 43(5): 99-103.
- [22] Laboratory for Foundations of Computer Science, the University of Edinburgh. Version v25 of the PEPA eclipse plugin[EB/OL]. (2011-6-8)[2015-02-10]. <http://www.dcs.ed.ac.uk/pepa/downloads>.
- [23] 王慧强, 吕宏武, 赵倩, 等. 一种关键任务系统自律可信性模型与量化分析[J]. 软件学报, 2010, 21(2): 344-358.  
WANG Hui-qiang, LÜ Hong-wu, ZHAO Qian, et al. Model and quantification of autonomic dependability of mission-critical systems[J]. Journal of Software, 2010, 21(2): 344-358.
- [24] BRADLEY J T, DINGLE N J, HARRISON P G, et al. Distributed computation of transient state distributions and passage time quantiles in large semi-Markov models[J]. Future Generation Computer Systems, 2006, 22(7): 828-837.

编辑 漆蓉