文章编号: 1001-0920 (2015) 01-0185-04 **DOI:** 10.13195/j.kzyjc.2013.1419

复杂系统脆性相对熵及其在分布式系统中的应用

冯丽媛[1,2], 姚绪梁[1], 曹 然[1], 邹艾利[1]

(1. 哈尔滨工程大学 自动化学院，哈尔滨 150001；2. 黑龙江科技大学 电子与信息工程学院，哈尔滨 150022)

摘 要: 分布式系统安全性和可靠性检测的难点在于缺乏对系统脆性的动态评估. 针对这一难点, 提出一种新的概念脆性相对熵来衡量系统的脆性, 并给出评估方法. 利用脆性相对熵可以动态地衡量当前概率分布与系统崩溃概率分布之间的相对距离, 有效地评估系统当前状态, 并对系统脆性的概率风险加以定量分析. 仿真结果表明, 脆性相对熵可以衡量系统的脆性特征, 且越接近系统脆性分布, 脆性相对熵越小.

关键词: 脆性相对熵；分布式系统；脆性条件相对熵；非负性；凸函数性

中图分类号: TP273 **文献标志码:** A

Relative entropy of complex system brittleness and its application in distributed systems

FENG Li-yuan[1,2], *YAO Xu-liang*[1], *CAO Ran*[1], *ZOU Ai-li*[1],

(1. College of Automation，Harbin Engineering University，Harbin 150001，China；2. College of Electronic and Information Engineering，Heilongjiang University of Science and Technology，Harbin 150022，China．Correspondent: FENG Li-yuan，E-mail：fengly1978@126.com)

Abstract: The difficulty of distributed system security and reliability testing lies in the lack of dynamic assessment in the system brittleness. Therefore, a new concept called brittle relative entropy is proposed to measure the system brittleness, and assessment methods are given. The brittle relative entropy can dynamically measure the relative distance between the current probability distribution and the collapse distribution, which can effectively assess the current state of the system and analyse the probabilistic risk of brittleness. The simulation results show that the brittle relative entropy can be used to measure the brittle characteristics of the system. When the brittle relative entropy is closer to the brittle distribution system, the brittle relative entropy is smaller.

Keywords: brittle relative entropy；distributed systems；brittle conditions relative entropy；non-negative；convex function

0 引 言

分布式控制应用的广泛使用和分布式系统结构的复杂程度使得人们对分布式系统的安全性和可靠性的要求日益增高. 在许多大型分布式系统中(如网络电视、文件共享、点播等应用中), 为了保证服务质量, 需要对其系统进行实时监控. 文献[1]研究了一种高度可扩展的分布式系统的监测网络, 可以有效地降低网络延迟并缓解网络压力. 但该研究方法侧重于网络的监控, 对于网络中出现故障的处理方法并没有讨论. 对于安全性要求较高的分布式系统(如航空、汽车、工业自动化等领域), 为了处理严重故障, 避免事故的发生, 往往对系统进行过度的资源配置. 文献[2]提出了一种动态的安全自适应技术和性能指标的评估框架, 具有较好的容错机制并减少对系统实时性和安全性的影响, 其不足之处在于缺乏对于系统严重故障的评估.

系统规模的不断扩大和各系统之间功能的不断完善使得复杂系统脆性问题日益凸显. 当某一系统崩溃后, 它对全局的影响是通过崩溃行为在子系统之间的传递和扩张实现的, 这种传递和扩张的过程称为脆性行为. 脆性理论是研究对象在内、外因素作用下, 其本身性能严重恶化, 以至于产生功能崩溃的理论. 文献[3]研究了由外部环境的不确定性和其结果的危害性 2 方面因素共同描述系统脆性的概率风险方法, 并定义脆性熵来对系统脆性的概率风险加以定量分析, 但并没有给出具体的应用范围. 文献[4]根据集对分析

收稿日期: 2013-10-14；**修回日期:** 2014-04-14.

基金项目: 国防科工局技术基础研究基金项目(Z192011B001).

作者简介: 冯丽媛(1978−), 女, 讲师, 博士生, 从事复杂系统的研究；姚绪梁(1969−), 男, 教授, 博士生导师, 从事电力电子及电力传动等研究.

理论, 定义了子系统间的脆性联系熵、脆性基元的概念, 并将非合作博弈的理论和方法应用于复杂系统脆性研究中, 但对于发生脆性的子系统对于其他子系统的影响并没有加以分析. 文献[5]以复杂子系统间的脆性联系为出发点, 定义了复杂系统的脆性基元、子系统间的脆性联系函数、脆性联系熵和脆性正交的概念, 但对于以上定义的概念并没有进行具体定量的分析.

相对熵的概念来源于信息论, 用来度量2种概率分布之间的差异性. 相对熵理论可以根据过去或当前的概率分布预测未来的概率分布, 或者衡量2个随机分布之间的差距. 文献[6]根据相对熵的最小相对熵理论, 将其应用于供应链中需求的预测, 说明相对熵理论可以用来预测概率分布. 文献[7]研究了网络在线异常检测系统, 根据相对熵确定网络流量的变化, 并根据流量的变化情况判断网络是否存在异常情况, 说明相对熵理论可以用来接近真实的概率分布. 文献[8]利用相对熵理论来检测相干风险, 但只给出了理论分析部分, 没有对具体的应用分析加以说明.

综上所述, 现有的复杂系统脆性分析过程只能对已经发生脆性的子系统进行定量分析, 缺乏对其他子系统的状态评估. 根据相对熵具有的可预测性、可检测性, 可以将其引入到复杂系统脆性研究中来评估发生脆性的子系统对其他子系统的动态影响. 基于上述考虑, 本文由复杂系统脆性熵的观点出发, 引出脆性相对熵和脆性条件相对熵的概念, 并给出复杂系统脆性相对熵的评估方法. 分布式系统仿真结果表明, 脆性相对熵可以用来度量复杂系统脆性, 并且能够动态地衡量当前概率分布与系统崩溃时概率分布的距离.

1 问题描述

由文献[3]可知, 假设在样本空间上, 系统 G 有 n 个可能事件 $I=\{I_1,I_2,\cdots,I_n\}$, 事件 I_i 发生的概率为 Q_i, 在事件 I_i 的作用下发生系统崩溃的概率为 q_i, $0\leqslant q_i\leqslant 1$. 如果事件 I_i 的脆性风险函数为 $R(q_i,Q_i)$, 则系统的脆性熵 $H=\sum\limits_{i=1}^{n}R(q_i,Q_i)$. 系统的脆性熵表示在某一时刻系统崩溃的概率风险, 但复杂系统通常由许多子系统构成, 子系统之间的联系也会导致系统发生脆性风险. 因此, 只知道系统的脆性熵对于分析系统脆性风险是不够的. 由文献[4-5]可知, 如果一个子系统 X 在干扰的情况下发生崩溃, 另外一个子系统 Y 的状态向量中至少有一个 $y_j(1<j<n)$ 与子系统 X 发生脆性同一熵 $H_a=-\sum\limits_{j=1}^{k}P_a\Big(\dfrac{y_j}{X}\Big)\ln P_a\Big(\dfrac{y_j}{X}\Big)$, 脆性对立熵为 $H_b=-\sum\limits_{j=1}^{k}P_b\Big(\dfrac{y_j}{X}\Big)\times\ln P_b\Big(\dfrac{y_j}{X}\Big)$, 脆性波动熵为 $H_c=-\sum\limits_{j=1}^{k}P_c\Big(\dfrac{y_j}{X}\Big)\ln P_c\Big(\dfrac{y_j}{X}\Big)$, 则子系统 X 崩溃时, 子系统 Y 也发生崩溃的脆性联系熵为

$$H_XY=\omega_aH_a+\omega_bH_b+\omega_cH_c.$$

系统的脆性联系熵表示子系统之间的脆性风险, 即一个子系统崩溃对另外的子系统的影响.

虽然脆性熵 H 和脆性联系熵 H_XY 分别给出了系统的脆性风险值和子系统之间的脆性风险值, 但无论是脆性熵 H 还是脆性联系熵 H_XY 的获得都是在已知 q_i、Q_i 和 $P(y_j/X)$ 概率条件下计算的, 即已知某个事件或子系统发生崩溃的概率或概率分布. 但在系统的运行过程中, 往往已知的概率分布与系统发生崩溃的概率分布不同, 要想判断系统的稳定性, 仅仅利用脆性熵和脆性联系熵是不够的.

2 复杂系统脆性相对熵

2.1 脆性相对熵定义

在复杂系统的运行过程中, 当某子系统发生脆性后, 通常更加关注其他子系统的稳定性和安全性. 实际系统在运行过程中是一个动态的过程, 而脆性熵与脆性联系熵都是计算静态条件下系统发生崩溃的风险. 如果要判断系统运行过程中某一子系统的脆性风险, 则需要引入新的概念和方法来计算系统运行过程中脆性的变化. 相对熵的概念来源于信息论, 是指2个随机分布之间距离的度量. 下面将相对熵的概念引入复杂系统, 定义脆性相对熵.

定义 1 若 p 和 q 分别表示当前分布和系统发生崩溃的分布, $p(x)$ 和 $q(x)$ 分别表示当前分布的概率密度函数和系统发生崩溃分布的概率密度函数, 则脆性相对熵为

$$D(p\|q)=\sum_{x\in X}p(x)\log\frac{p(x)}{q(x)}. \tag{1}$$

定义 2 在整个系统中, 若子系统 X 发生崩溃, 导致子系统 Y 也发生崩溃, 则脆性条件相对熵为

$$D\Big(p\Big(\frac{y}{x}\Big)\|q\Big(\frac{y}{x}\Big)\Big)=\sum_{x}p(x)\sum_{y}p\Big(\frac{y}{x}\Big)\log\frac{p\Big(\dfrac{y}{x}\Big)}{q\Big(\dfrac{y}{x}\Big)}, \tag{2}$$

其中 $p\Big(\dfrac{y}{x}\Big)$ 和 $q\Big(\dfrac{y}{x}\Big)$ 分别表示当前分布的条件概率密度函数和系统发生崩溃分布的条件概率密度函数.

定理 1 $D(p\|q)\geqslant 0$, 当且仅当 $p(x)=q(x)$ 时, 等号成立[10].

证明 设 $X'=\{x:p(x)>0\}$ 为 $p(x)$ 的支撑集, 则有

$$-D(p\|q)=-\sum_{x\in X'}p(x)\log\frac{p(x)}{q(x)}=\sum_{x\in X'}p(x)\log\frac{q(x)}{p(x)}\leqslant\log\sum_{x\in X'}p(x)\frac{q(x)}{p(x)}=\log\sum_{x\in X'}q(x)\leqslant\log\sum_{x\in X}q(x)=\log 1=0. \qquad\square$$

定理 2 $D(p\|q)$ 关于 (p,q) 是凸的[10].

证明　取 $0 \leqslant \lambda \leqslant 1$, 则有

$$\begin{aligned}&D(\lambda p_1+(1-\lambda)p_2\|\lambda q_1+(1-\lambda)q_2)=\\&\sum_{x\in X}(\lambda p_1(x)+(1-\lambda)p_2(x))\times\\&\log\frac{\lambda p_1(x)+(1-\lambda)p_2(x)}{\lambda q_1(x)+(1-\lambda)q_2(x)}\leqslant\\&\sum_{x\in X}\lambda p_1(x)\log\frac{\lambda p_1(x)}{\lambda q_1(x)}+\\&\sum_{x\in X}(1-\lambda)p_2(x)\log\frac{(1-\lambda)p_2(x)}{(1-\lambda)q_2(x)}=\\&\lambda\sum_{x\in X}p_1(x)\log\frac{p_1(x)}{q_1(x)}+\\&(1-\lambda)\sum_{x\in X}p_2(x)\log\frac{p_2(x)}{q_2(x)}=\\&\lambda D(p_1\|q_1)+(1-\lambda)D(p_2\|q_2),\end{aligned}$$

由此得证 $D(p\|q)$ 关于 (p,q) 是凸的. □

定理 3　相对熵随时间的增加将递减[10]. 将分布式系统视为马尔科夫链, 并设 p 和 q 分别为联合概率密度函数.

证明

$$\begin{aligned}&D(p(x_n,x_{n+1})\|q(x_n,x_{n+1}))=\\&D(p(x_n)\|q(x_n))+D(p(x_{n+1}|x_n)\|q(x_{n+1}|x_n))=\\&D(p(x_{n+1})\|q(x_{n+1}))+\\&D(p(x_n|x_{n+1})\|q(x_n|x_{n+1})).\end{aligned}$$

$$\because\ D(p(x_{n+1}|x_n)\|q(x_{n+1}|x_n))=0,$$

$$\begin{aligned}\therefore\ &D(p(x_n)\|q(x_n))=\\&D(p(x_{n+1})\|q(x_{n+1}))+(p(x_n|x_{n+1})\|q(x_n|x_{n+1})).\end{aligned}$$

又因为相对熵的非负性, 即

$$D(p(x_n|x_{n+1})\|q(x_n|x_{n+1}))\geqslant 0,$$

所以

$$D(p(x_n)\|q(x_n))\geqslant D(p(x_{n+1})\|q(x_{n+1})).$$

由此可知, 在马尔科夫链系统中, 2 个概率分布间的距离随时间增加而减小. □

综上所述, 由定义 1 和定义 2 可知, 脆性相对熵用以衡量整个系统的运行状态, 脆性相对条件熵用以描述某子系统对其他子系统稳定性的影响. 由定理 1 ∼ 定理 3 可知, 脆性相对熵可以利用已知的概率分布来预测未来的概率分布, 即根据当前状态推测与未知状态的距离. 由于已知概率分布是动态变化的, 相对熵也是动态变化的. 可以根据此特点来判断系统的运行情况, 用以评估复杂系统当前的运行状态.

2.2　脆性相对熵评估方法

若已知系统脆性熵 $H=\sum_{i=1}^{n}R(q_i,Q_i)$, 则对系统当前运行状态的评估方法如下:

Step 1: 根据当前概率分布 p_i 计算脆性相对熵. 若已知系统发生脆性时的概率为 q_i, 则根据当前概率分布 p_i 计算 i 时刻的脆性相对熵值 $D(p\|q)=\sum_{i=1}^{n}p_i(x)\log\frac{p_i(x)}{q_i(x)}$, 由于时刻 i 变化, 脆性相对熵值也发生动态变化.

由定理 1 可知, 脆性相对熵为正熵, 即脆性相对熵具有非负性. 当系统中某子系统发生崩溃后, 其他子系统的脆性情况可由脆性相对熵来描述. 当 2 个子系统概率分布相同时, 脆性相对熵为零; 当 2 个子系统概率分布不同时, 脆性相对熵大于零, 并随着分布距离的增大, 脆性相对熵也增大.

Step 2: 根据 Step 1 中的计算结果找出脆性相对熵的最小值. 由定理 2 可知, 当系统发生脆性后, 与其他子系统之间的脆性相对熵具有凸函数性, 即系统之间的脆性相对熵存在最小值. 这说明即使系统的崩溃导致其中某子系统发生脆性, 2 个子系统之间的脆性相对熵也不一定为零, 即不能以脆性相对熵是否为零来判断子系统是否发生脆性, 当子系统发生崩溃时, 脆性相对熵达到最小值.

Step 3: 根据已发生脆性子系统的特性, 寻找与其相似子系统. 由定理 3 可知, 若将分布式系统视为马尔科夫链, 则 2 个子系统之间的脆性相对熵随时间的增加递减. 当系统中的某子系统发生脆性后, 即使另一子系统的初始状态与发生脆性的子系统的初始状态不同, 在相同的运行条件下, 随着时间的推移, 2 个子系统也将趋于一致. 在分布式系统中, 若子系统 A 发生崩溃, 则可以根据脆性相对熵随时间增加而递减的特点, 找到运行条件相同的子系统 B, 提早作出预防措施, 防止子系统 B 发生崩溃, 即根据脆性相对熵可以预测系统发生脆性的行为.

3　仿真验证

以分布式系统为例, 采用文献[10]所提供的异常检测模型来验证脆性相对熵对于异常检测的准确性. 文献[10]只给出了接近于实际概率分布的检测方法和检测结果, 并没有分析 2 种结果之间的关系. 根据脆性相对熵评估方法中的步骤, 基于检测概率的不同计算脆性相对熵, 然后在计算的结果中找出最小值. 由 DoS 异常类型的数据结果可得, 实际发生概率为 $q_i=0.27$, 检测概率为 $p_i=0.31$. 由定理 1 可知, 脆性相对熵具有非负性, 由图 1 可以看出所有脆性相对熵的值均大于零; 由定理 2 可知, 脆性相对熵具有凸函数性, 由图 1 可以看出, 当概率 p_i 接近 0.3 时, 脆性相对熵值最小. 随着检测概率与实际异常概率差距的不断增加, 脆性相对熵的值也随之增大. 由此可以得出, 脆性相对熵的变化情况可以描述系统遭受到异常攻击后的实际分布与检测分布之间的相对距离, 即脆性相对熵可以用来衡量系统的脆性风险. 利用脆性相对熵可以接近实际分布, 并根据脆性相对熵的凸函数性, 说明检测分布与实际分布之间存在最小值, 即可以通

过脆性相对熵的计算来判断系统是否出现异常.

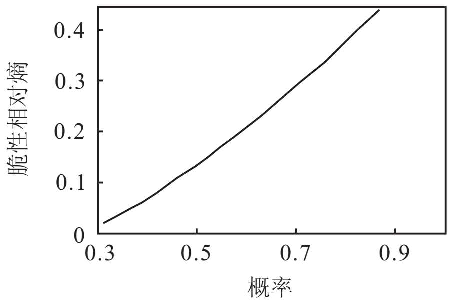

图 1 脆性相对熵与概率分布关系的一种检测方法

根据文献[11]中提供的网络异常检测方法及模型, 以 Probe 异常类型为例, 采用多种检测方法, 当检测方法不同时, 其概率分布也是不同的. 文献[11]只给出了不同检测方法检测出的不同概率分布, 以衡量不同方法之间的检测效率. 而本文是从系统脆性的角度, 利用其检测结果来分析脆性相对熵对于系统稳定性的影响. 根据 Probe 异常类型的数据结果, 检测概率分别为 $p_1 = 0.65$, $p_2 = 0.16$, $p_3 = 0.64$, $p_4 = 0.86$, $p_5 = 0.68$, 根据不同的 p_i 值, 计算脆性相对熵. 由图 2 可知, 不同的概率 p_i 值计算出的脆性相对熵值有较大的区别, 在概率 p_i 值由小变大的过程中, 脆性相对熵值整体呈下降趋势, 并存在最小值. 由此可以验证, 当采用多种方法对系统进行检测时, 脆性相对熵的理论依然成立. 脆性相对熵值的大小可以反映出当前系统运行的稳定情况: 当脆性相对熵达到最小值时, 系统处于不稳定状态, 系统发生脆性的概率较大; 当脆性相对熵值较大时, 表明系统处于相对稳定状态.

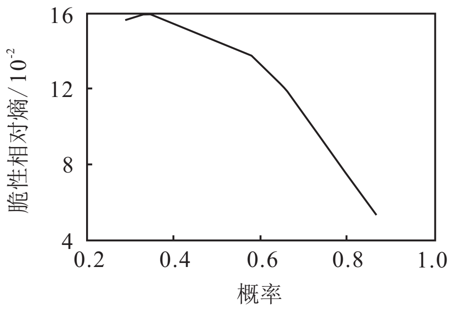

图 2 脆性相对熵与概率分布关系的多种检测方法

4 结 论

脆性是分布式系统的一种固有属性, 通常以脆性熵和脆性联系熵来度量系统的脆性风险. 本文定义脆性相对熵和脆性条件相对熵来对系统的脆性风险加以度量, 用以衡量系统当前分布与系统发生崩溃分布之间的相对距离. 经分布式系统网络异常类型攻击仿真, 验证了所提出的脆性相对熵的大小直接反映了当前分布与异常分布之间的差距. 脆性相对熵越大, 差距越大, 脆性相对熵越小, 差距越小. 根据脆性相对熵的变化特点, 可以判断和动态地监测系统当前的运行情况.

参考文献(References)

[1] Philip C H, Yuen S H, Gray Chan. Scalable real-time monitoring for distributed applications[J]. IEEE Trans on Parallel and Distributed Systems, 2012, 23(12): 2330-2337.

[2] Akshay Dabholkar, Abhishek Dubey, Aniruddha Gokhale, et al. Reliable distributed real-time and embedded systems through safe middleware adaptation[C]. The 31st Int Symposium on Reliable Distributed Systems. Irvine: IEEE Computer Society, 2012: 362-371.

[3] 李琦, 金鸿章, 林德明. 基于脆性熵的系统脆性研究[J]. 自动化技术与应用, 2004, 23(9): 16-18.
(Li Q, Jin H Z, Lin D M. Brittleness analysis based on the brittleness entropy[J]. Techniques of Automation and Applications, 2004, 23(9): 16-18.)

[4] 韦琦, 金鸿章, 郭健. 复杂系统崩溃的脆性致因的研究[J]. 系统工程, 2003, 21(4): 1-5.
(Wei Q, Jin H Z, Guo J. Research on the collapse of complex system based on brittle reason[J]. Systems Engineering, 2003, 21(4): 1-5.)

[5] 韦琦, 金鸿章, 郭健, 等. 基于脆性的复杂系统研究[J]. 系统工程学报, 2004, 19(3): 326-328.
(Wei Q, Jin H Z, Guo J, et al. Research on complex system based on brittleness[J]. J of Systems Engineering, 2004, 19(3): 326-328.)

[6] Suyan He. A weighted relative entropy method for forecasting demand[C]. 2011 Int Conf on Electric Information and Control Engineering(ICEICE). Wuhan: 2001: 130-133.

[7] Altyeb Altaher, Sureswaran Ramadass, Bhavani Thuraisingham, et al. On-line anomaly detection based on relative entropy[C]. The 4th IEEE Int Conf on Broadband Network and Multimedia Technology(IC-BNMT). Beijing: IEEE Press, 2011: 33-36.

[8] Ahmadi-Javid A. An information-theoretic approach to constructing coherent risk measures[C]. 2011 IEEE Int Symposium on Information Theory Proceedings. St.Petersburg: IEEE Press, 2011: 2125-2127.

[9] Tommas M Cover, Joy A Thomas. 信息论基础[M]. 北京: 机械工业出版社, 2005: 9-25.
(Tommas M Cover, Joy A Thomas. Elements of information theory[M]. Beijing: China Machine Press, 2005: 9-25.)

[10] Zhang Y L, Han Z G, Ren J X. A network anomaly detection method based on relative entropy theory[C]. The 2nd Int Symposium on Electronic Commerce and Security. Nanchang: IEEE Press, 2009: 231-235.

[11] Mahoney V M. A machine learning approach to detecting attacks by identifying anomalies in network traffic[D]. Melbourne: Florida Instrtute of Technology, 2003: 101-120.

(责任编辑: 闫 妍)