基于博弈论的信息系统生存性提升方法研究

王志文 卢 柯 王晓飞

(西安交通大学电子与信息工程学院 西安 710049)

摘 要 当前对信息系统生存性的研究主要集中在静态环境下生存性定量分析及保障的技术实现,但生存性在不同技术和动态环境下的能力是不一样的,根据生存性能力高低可以将其划分成若干等级。用户在向信息系统提交业务时需要根据生存性等级来支付费用,而经营者为达到相应的生存性等级必须付诸一定的投资,因此,经营者迫切希望能够找到一种提升方法,以自身的收益来决定信息系统应该具备的生存性等级。通过对信息系统经营者和用户之间的博弈行为及收益分析,构建了博弈模型,并对混合策略下的纳什均衡进行了求解,并根据收益最大化原则设计了经营者是否提升信息系统生存性等级的控制策略。最后在一个生存性被划分为5个等级的信息系统上进行了仿真实验,计算结果表明所提出的博弈模型及生存性提升方法是合理、可行的。

关键词 信息系统,生存性提升,博弈论

中图法分类号 TP393 **文献标识码** A

Approach on Promoting Survivability for Information System Based on Game-theory

WANG Zhi-wen LU Ke WANG Xiao-fei

(School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract The current study of survivability of information system is focused on the technique realization of quantitatively analysis and guarantee of survivability in static environments. The survivability is different with various techniques in dynamic work conditions, which can be classified into multiple grades according to corresponding capability. Custom needs to pay different service fee at different survivability grade in an information system. At the same time provider must invest considerable money so as to keep a particular survivability grade. An approach has to be proposed urgently, with which the provider can decide whether to promote the survivability grade by his income. A game-theory based model was constructed in this paper by analyzing the action and income of customer and provider who act as the two players. The mixed strategy Nash equilibrium were derived from the model and the strategy for promoting survivability grade was devised, with which the income of provider can be maximized. An experiment was carried out in an information system simulated by 5 survivability grades and the results show that the game-theory based approach presented in the paper is correct and reasonable.

Keywords Information system, Survivability promotion, Game-theory

1 引言

信息系统的生存性是指系统在遭受攻击、软硬件故障等事故时,能够实时地为用户提供基本服务的能力[1],是可信系统中的重要组成内容。信息系统的生存性不同于常规的安全需求,它关注的是将系统作为一个整体对外提供服务的全局性能力,是在传统安全基础之上的更高一层考虑,综合了网络安全、可靠性以及容错机制等领域研究成果。

业界对信息系统生存性的研究主要集中在生存性度量分析以及保障两个领域。所提出的生存性度量分析模型可分为基于系统结构和基于系统服务这两种类型,基于系统结构的模型一般是从信息系统的物理结构上来考虑的,它利用图作为表示方式来反应网络节点之间的连接信息或者其它特定的网络性能参数[2];基于系统服务的模型从网络系统提供的服务出发,将服务涉及到的系统组件组织在一起从而达到简化系统结构的目的[3]。生存性保障研究主要是针对系统的关键服务设计冗余资源分配算法以保证持续的服务能力。Tun Lu根据面向服务计算(SOC)的生存性需求,提出了基于服务依赖性的配置算法以提升服务的生存性[4]。文献[5]针对应急反应的需求,以恢复时间和服务中止作为限制条件,设计了紧急服务的生存性保障算法。上述研究关注的都是静态环境下信息系统生存性的分析及保障,均侧重于技术实现,尽管这些技术使得信息系统具备生存性,但各自获得的生存性能力存在差异,根据生存性能力高低可以将其划分成不同的等级。

到稿日期:2009-10-28 返修日期:2010-02-01 本文受国家自然科学基金面上项目(60970121),国家科技人员服务企业行动项目(2009GJG00025),西安交通大学科研基金项目(XJ20090511)资助。

王志文(1973-),男,博士,副教授,CCF高级会员,主要研究方向为网络安全与管理、高性能通信网络,E-mail:wzw@mail.xjtu.edu.cn;卢 柯(1986-),男,硕士生,主要研究方向为网络安全;王晓飞(1984-),男,硕士生,主要研究方向为网络安全。

不同技术使得同一信息系统具备不同的生存性等级，同一技术作用于不同工作环境下的同一信息系统也会导致不同的生存性等级。

信息系统在不同生存性等级下能够提供不一样的生存性能力，相应地，用户在不同生存性等级下提交同一业务请求所需要支付的成本也不一样，经营者为达到并维持特定生存性等级所付诸的投资也不一样。因此，经营者迫切希望能够找到一种控制策略，以自身的收益状况来决定信息系统应该具备的合理生存性等级，进而保障信息系统的可持续运营。

本文将基于博弈理论构建信息系统经营者和用户这对博弈方的博弈模型，并以经营者的收益为目标提出一种信息系统生存性提升的控制策略。借助该策略，经营者可以根据用户的业务提交概率做出是否提升生存性等级的合理抉择。

2 基于收益的生存性等级提升

影响信息系统生存性的关键因素包括内因和外因两个方面，内因主要由系统的配置、部署以及工作人员业务水平能力等构成，外因是专指信息系统需要处理的各种用户业务。从运营角度看，信息系统的有效性实质上是受内、外因交互所产生的收益决定的；如果外因过强，即业务负载过大会导致信息系统的生存性下降并使得经营者的收益减少，当生存性降至某一警界程度时，信息系统则会失去其继续存在的意义；反之，如果内因过强，即信息系统提供有强大的服务能力又会因为业务负载欠缺导致经营者的投资回报不足，影响到信息系统长时间的可持续运行。

基于上述分析，有必要为经营者设计一种信息系统生存性控制机制，使信息系统的生存性与其处理的用户业务相匹配。匹配的衡量标准就是经营者收益，如果能够保证经营者在提供不同信息系统生存性等级时都能够获得一定的合理收益，则认为是匹配的，能够保障信息系统的顺利运行。在信息系统运行中，用户是否提交业务的根本点在于其获得的收益是否大于提交成本，而业务收益与提交成本又与信息系统的生存性等级紧密相关；对于经营者而言，由于用户是否提交业务是不确定的，相应地，是否提升信息系统生存性等级也不是确定的，需要取决于用户业务的提交程度，因此如果用户提交的业务使得经营者在提升生存性等级后能够获取收益，则经营者的理性选择是提升，否则，应该放弃提升。

博弈理论在网络安全领域已经得到了较为广泛的应用。田立勤等构建了博弈模型用于用户网络行为的信任控[6]，Bell 利用博弈论对随机网络的脆弱性进行了测量[7]。本文拟利用博弈论来分析信息系统中经营者与用户这对博弈双方行为的不确定性，并给出了经营者对信息系统生存性等级的提升策略。

3 符号定义

在构建博弈模型之前，先给出如下符号定义。

l：表示信息系统当前的生存性等级划分，$l\in\{1,2,3,\cdots,L\}$。信息系统所处的级别越高，表明其生存性越强，级别 1 具有最完备的生存性，级别 L 的生存性最低；除级别 1 外，其他级别都可以根据需要进行相应的提升。

$P_{in}(l)$：表示经营者在信息系统生存性级别为 l 时接受用户提交业务能够获取的平均收益，生存性级别越高，其对应的收益越大。

$P_{pro}(l)$：表示经营者为将信息系统的当前生存性级别 l 提升到级别 $l-1$ 所需要的开销，如购置相关的安全工具，对信息系统执行安全规划和配置以及对系统操作人员进行安全培训等。信息系统的生存性级别越高，其提升的开销则越大；为了简化博弈模型，本文假定生存性级别的提升是逐级进行的，不支持越级提升。

$C_{in}(l)$：表示用户向生存性级别为 l 的信息系统提交业务所能够获取的平均收益，信息系统的生存性级别越高，则用户获得的收益越大。

$C_{pro}(l)$：表示用户因信息系统生存性由级别 l 提升到 $l-1$ 而需要额外支付的开销，信息系统的生存性级别越高，用户因提升而需支付的开销则越大。

4 博弈模型

4.1 支付矩阵

信息系统具有不同的生存性等级，相应地，博弈双方的支付矩阵也会因生存性等级的不同而存在差异。根据之前对信息系统定义的生存性等级，设信息系统当前的生存性等级为 l，定义经营者和用户的支付矩阵分别为：

$$M_p(l)=\begin{pmatrix}P_{in}(l-1)-P_{pro}(l) & -P_{pro}(l)\\ P_{in}(l) & 0\end{pmatrix},l=2,3,\cdots,L$$

$$M_c(l)=\begin{pmatrix}C_{in}(l-1)-C_{pro}(l) & 0\\ C_{in}(l) & 0\end{pmatrix},l=2,3,\cdots,L$$

在上述支付矩阵中，第 1 行和第 2 行分别表示生存性等级提升后与提升前经营者与用户的收益情况，第 1 列和第 2 列分别表示用户向信息系统提交与不提交业务情形下经营者与用户的收益情况，如矩阵元素 $P_{in}(l-1)-P_{pro}(l)$ 表示经营者在生存性等级提升后且用户提交业务时的收益，而矩阵元素 $C_{in}(l-1)-C_{pro}(l)$ 则表示用户在经营者提升了生存性等级时所提交业务的收益。

4.2 纳什均衡

通过简单的划线方法可以判定该博弈模型不存在纯策略均衡[7]，其原因在于：如果经营者提升当前的信息系统生存性等级，则用户的理性选择就是提交业务；如果用户选择提交业务，则经营者的最优策略就是保持当前生存性等级不变以降低经营成本；如果经营者保持当前生存性等级不变，则用户提交业务的概率势必要降低；如果用户提交业务概率降低，则经营者必须提升当前的生存性等级以吸引更多的用户提交业务。

尽管没有一种策略组合能够组成纯纳什均衡，但我们可以求解混合策略下的纳什均衡。假定经营者以概率 x 选择对提升信息系统当前的生存性等级，以 $1-x$ 的概率保持原有生存性等级不变，即经营者的混合策略为 $\rho_p=(x,1-x)$；同样，假定用户以概率 y 选择向信息系统提交业务，以 $1-y$ 的概率不提交业务，则用户的混合策略为 $\rho_c=(y,1-y)$。

由支付矩阵以及经营者和用户的混合策略可知，经营者和用户在信息系统生存性等级 l 下的预期支付函数 $E_p(l)$ 和 $E_c(l)$ 分别为：

$$\begin{aligned}E_c(l)&=\rho_c\times M_c(l)^T\times\rho_p^T\\&=(y,1-y)\begin{pmatrix}C_{in}(l-1)-C_{pro}(l) & C_{in}(l)\\ 0 & 0\end{pmatrix}\begin{pmatrix}x\\1-x\end{pmatrix}\end{aligned}$$

$$=y(xC_{in}(l-1)-xC_{pro}(l)+C_{in}(l)-xC_{in}(l)) \quad (1)$$

$$E_P(l)=\rho_p\times M_p(l)\times\rho_c^T$$

$$=(x,1-x)\begin{pmatrix}P_{in}(l-1)-P_{pro}(l) & -P_{pro}(l)\\ P_{in}(l) & 0\end{pmatrix}\begin{pmatrix}y\\1-y\end{pmatrix}$$

$$=xy(P_{in}(l-1)-P_{in}(l))-xP_{pro}(l)+yP_{in}(l) \quad (2)$$

对式(1)关于 y 求偏导,可得经营者最优化的一阶条件为:

$$\frac{\partial E_c(l)}{\partial y}=xC_{in}(l-1)-xC_{pro}(l)+C_{in}(l)-xC_{in}(l)=0$$

解得

$$x^*=C_{in}(l)/(C_{in}(l)-C_{in}(l-1)+C_{pro}(l)) \quad (3)$$

同样,对式(2)关于 x 求偏导,可得用户最优化的一阶条件为:

$$\frac{\partial E_p(l)}{\partial x}=y(P_{in}(l-1)-P_{in}(l))-P_{pro}(l)=0$$

解得

$$y^*=P_{pro}(l)/(P_{in}(l-1)-P_{in}(l)) \quad (4)$$

5 生存性等级提升策略

博弈模型得出了信息系统经营者和用户的混合纳什均衡策略,即解决了经营者和用户在信息系统中分别执行生存性等级提升和业务提交的概率问题。但对于一个具体的信息系统而言,经营者究竟是否应该提升其生存性等级还不能明确确定,它必须依赖于用户在不同生存性等级下提交业务的概率,即博弈决策不是由单方面策略决定的,还必须受制于博弈对方的决策策略。根据已定义的博弈模型,可以求出经营者提升信息系统生存性等级所要求的先决条件。

如果信息系统经营者需要提升当前的生存性等级 i,必须满足条件:

$$y(i-1)^*P_{in}(i-1)-y(i)^*P_{in}(i)-P_{pro}(i)>0 \quad (5)$$

式中,$y(i)^*$ 和 $y(i-1)^*$ 是信息系统在生存性等级 i 提升前和提升后的用户纳什均衡的提交业务概率,$P_{in}(i)$ 和 $P_{in}(i-1)$是经营者在信息系统生存性等级 i 提升前和提升后的平均收益,$P_{pro}(i)$是提升信息系统生存性等级 i 的开销。

解释过程如下:由于博弈的本质就是选择能够使己方收益最大化的决策过程,根据这一原则,可以认为经营者是否提升信息系统生存性等级取决于提升前、后的收益大小,如果提升后的收益大于提升前的收益,则选择提升策略;否则就没有必要进行提升。

根据式(2)给出的经营者预期支付函数可知,如果经营者选择提升信息系统的生存性等级 i,则提升概率 x 等于 1,用户业务提交概率也因生存性等级得到提升而变成 $y(i-1)^*$,该情形下的经营者收益为:

$$E_p^{pro}(i)=y(i-1)^*P_{in}(i-1)-P_{pro}(i)$$

与之相对应的是,如果经营者保持信息系统现有生存性等级不变,则提升概率 x 变成 0,用户业务提交概率为 $y(i)^*$,经营者收益为:

$$E_p^{no\_pro}(i)=y(i)^*P_{in}(i)$$

经营者要想提升信息系统的生存性等级,必须满足生存性等级提升后的收益大于提升前的收益,即:

$$E_p^{pro}(i)-E_p^{no\_pro}(i)>0\Rightarrow y(i-1)^*P_{in}(i-1)-P_{pro}(i)-y(i)^*P_{in}(i)>0$$

6 实验分析

假设有一个信息系统,其生存性级别被划分为 5 个等级,其中的等级 1 和等级 5 分别对应于生存性的最高和最低等级。表 1 的第 2,3,4 和 5 列给出了博弈双方的收益参数初值,其中的 $P_{in}(l)$表示经营者在等级 l 的收益,$P_{pro}(l)$表示提升等级 l 需要的开销,$C_{in}(l)$表示用户在等级 l 下可获得的业务收益,$C_{pro}(l)$表示用户因等级 l 得到提升而需支付的开销;将上述参数值代入式(3)可求得信息系统经营者对生存性等级 l 的混合纳什均衡提升概率 $x(l)^*$,代入式(4)可求得用户在生存性等级 l 下混合纳什均衡的业务提交概率 $y(l)^*$,具体博弈结果见表 1 的第 6,7 列。根据本文建立的博弈分析模型要求,等级 1 是不可提升的,所以表中与等级 1 相对应的参数 $P_{pro}(l)$,$C_{pro}(l)$,$x(l)^*$ 和 $y(l)^*$ 没有实际意义,以"×"标识。有了 $P_{in}(l)$,$P_{pro}(l)$以及计算得到的用户提交业务概率 $y(l)^*$,就可以利用式(5)计算信息系统经营者可获得的效益,并以此为依据进行生存性提升决策控制,如果计算结果大于 0,则接受生存性等级提升策略,否则就拒绝提升。

表 1 博弈模型参数初值和计算结果值

l	$P_{in}(l)$	$P_{pro}(l)$	$C_{in}(l)$	$C_{pro}(l)$	$x(l)^*$	$y(l)^*$
1	114	×	121.5	×	×	×
2	95	16.8	115.7	145.4	0.823	0.888
3	79.2	11.2	110.2	133.1	0.864	0.71
4	66	7.5	105	121	0.907	0.568
5	55	5	100	110	0.952	0.455

图 1 给出了信息系统经营者在不同生存性等级下所获得的收益情况,图中的等级收益表示在生存性等级 l 下的经营者收益,即 $y(l)^*P_{in}(l)$;超额收益是指生存性等级 l 提升后与提升前的收益差值,即 $y(l-1)^*P_{in}(l-1)-y(l)^*P_{in}(l)$;提升成本是指经营者为提升生存性等级 l 而需要的开销,即 $P_{pro}(l)$;由于等级 1 不可提升,我们假定在等级 1 下的提升成本为 0,超额收益为 0,用户提交业务概率为 1。根据生存性提升策略可知,只要生存性等级 l 的提升成本小于超额收益,则经营者实施等级提升就可以获得更多的收益,从图 1 可以看出,生存性等级 2~5 的提升成本均小于其超额收益,表明经营者在各个等级下实施生存性等级提升都是合理的。

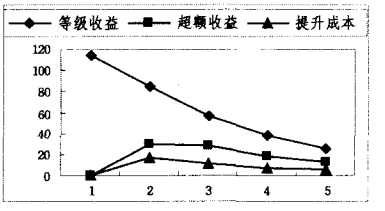

图 1 生存性等级提升收益

结束语 信息系统按其生存性能力高低可划分为不同的等级,用户根据生存性等级支付其业务的提交成本,经营者为达到一定的生存性等级必须付诸相应的投资,因此经营者希望能够找到一种控制策略,以自身的收益状况来决定信息系统应该具备的生存性等级。

论文通过对信息系统经营者和用户双方的博弈行为及收益分析,构建了博弈模型的支付矩阵,对混合策略下的纳什均衡进行了求解,并根据收益最大化原则设计了经营者是否提升信息系统生存性等级的控制策略,最后在一个划分为 5 个生存性等级的信息系统上进行了仿真实验,计算结果表明了本文提出的博弈模型及生存性提升策略是正确的。本文对于实际的信息系统生存性分析与控制有着重要的指导意义与参

考价值。

参 考 文 献

[1] Ellison R J, Fisher D A, Lingers R C, et al. Survivable Network System: An Emerging Discipline [R]. CMU/SEI-97-TR-013. Carnegie Mellon University, 1997

[2] Moitra Soumyo D, Konda Suresh L. A Simulation Model for Managing Survivability of Networked Information Systems[R]. CMU/SEI-2000-TR-020. 2005

[3] Gao Zhi-xing, Ong Chen-hui, Tan Woon-kiong. Survivability Assessment: Modelling Dependencies in Information Systems[C]// The 4th IEEE/CMU/SEI Information Survivability Workshop (ISW-2001/2002). Vancouver, BC Canada, October 2001

[4] Lu Tun, Gu Ning. Survivability-Aware Configuration Management of Service-Oriented System Based on Service Dependency [C]// IEEE/IFIP Symposium on Theoretical Aspects of Software Engineering(TASE'07). 2007

[5] Wang Jian, Wang Hui-qiang, Zhao Guo-sheng. ERAS— an Emergency Response Algorithm for Survivability of Critical Services[C]// Proceedings of the First International Multi-Symposiums on Computer and Computational Sciences(IMSCCS'06). 2006

[6] 田立勤,林闯. 可行网络中一种基于行为信任预测的博弈控制机制[J]. 计算机学报,2007,30(11):1030-1938

[7] Bell M. The use of game theory to measure the vulnerability of stochastic networks[J]. IEEE Transaction on Reliability, 2003, 52(1):63-68

(上接第 47 页)

间延迟的对比情况。由表 3 可见,不同消息传输方式中,传输路径上站点对转发消息的响应时间之和与消息传输时间延迟有一定的差值,且随着转发次数的增多,差值逐渐增大。这是由于随着转发次数的增多,消息在空间传播的时间也逐渐加长。此外,天线发送消息、消息在站点内部的处理也需花费时间。

表 3 时间延迟抖动数据特征值(单位:秒)

消息传输方式	站点对转发消息的响应时间					响应时间之和	消息时间延迟	差值
	A_1	E_1	E_2	E_3	E_4			
1	3.36	▲	▲	▲	▲	3.36	3.59	0.23
2	3.36	0.84	▲	▲	▲	4.20	4.53	0.33
3	3.36	7.17	▲	0.56	▲	11.09	11.51	0.42
4	3.36	7.17	3.18	▲	0.57	14.28	15.55	1.27

注:表 3 中▲表示该消息传输方式中,消息不需对应的站点转发。

4.4 消息时间延迟抖动

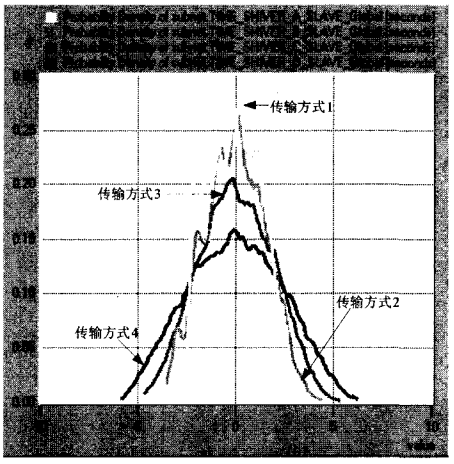

图 8 不同消息传输方式下的时间延迟抖动概率密度曲线比较

消息时间延迟抖动是指:对于某一特定站点发送的消息,其它站点收到的该消息的时间延迟与该站点消息时间延迟均值的差值。过大的时间延迟抖动不利于时间延迟误差的精确补偿,因此要求站点消息的时间延迟抖动必须较小且集中于某一数值。4 种消息传输方式的时间延迟抖动概率密度曲线比较如图 8 所示。由图可见,消息以传输方式 1,2,3,4 传输到子网 A,B,C,D 从属站的时间延迟抖动数据越来越分散。这是由于不同传输方式的格式转换次数不同,消息转发次数也有差别,每一次格式转换和消息转发都会造成附加时间延迟,其大小受转发站转发策略、格式转换能力等众多因素的影响,有一定的随机性。随着格式转换和消息转发次数的增多,这种随机性也被逐步放大,造成时间延迟抖动数据分布越来越分散。

结束语 本文分析了数据链消息传输过程,设计了 TDL_DSAP原型系统并实现了部分功能,以多网数据链为背景分析了其消息传输时间延迟。结果表明多网数据链中,消息以不同方式传输到目的站时,消息转发次数、站点转发消息时的角色、消息格式转换等因素对消息时间延迟、站点响应时间、时间延迟抖动等指标有重要影响。

消息时间延迟过大,会影响基于这些消息的特定应用。以现代空战为例,飞机飞行速度达到音速或亚音速时,如作战单元之间传输定位消息的时间延迟为 1s,则由此引起的定位误差可能达到数百米。虽然消息传输方式 1 的各项指标最好,但由于装备的限制,作战单元之间可能不得不使用其它消息传输方式。由于需转发消息的重要性较高,为了获得较小的时间延迟,应尽量减少消息的转发次数,同时转发站应将转发消息设置为高优先级,减小消息在转发站的附加时间延迟,使消息具有较好的时效性。

参 考 文 献

[1] 任培,周经伦,罗鹏程,等. 美军数据链发展概况与启示[J]. 装备指挥技术学院学报,2008,19(1):43-47

[2] 王文政,周经伦,罗鹏程,等. 战术数据链仿真综述[J]. 系统仿真学报,2008,20(14):3623-3627

[3] 孙义明,杨丽萍. 信息化战争中的战术数据链[M]. 北京:北京邮电大学出版社,2005

[4] 梅文华,蔡善法. JTIDS/Link16 数据链[M]. 北京:国防工业出版社,2007

[5] Charlie I, Cruz M. Netwars Based Study of a Joint Stars Link-16 Network[R]. Rand, 2004

[6] 邢智,戴浩. 基于 OPNET 的 Link-16 数据链建模与仿真[J]. 军事运筹与系统工程,2005,19(1):62-66

[7] 任培. 战术数据链传输时延及其作战效果影响分析方法研究[D]. 长沙:国防科技大学,2008

[8] 崔昊,匡镜明,何遵文. Link16 与 VHF 数据链互连建模与仿真研究[J]. 计算机工程与设计,2007,28(5):1119-1122

[9] 田斌鹏. 战术数据链实时性研究[D]. 成都:西南交通大学,2007