服务自组织途径的信息系统生存性增强

张乐君[1]，李子平[2]，国 林[1]，张健沛[1]，杨永田[1]

(1. 哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001；2. 北京青年政治学院计算机系 北京 朝阳区 100102)

【摘要】在组件冗余备份的前提条件下，提出一种基于连接迁移技术的服务自组织方法。该方法根据服务处理流程将系统组件分解为通信组件、服务分发组件、数据存储组件；备份组件将其生存性信息实时发送给工作组件，并获取最新服务状态列表，当某一组件生存性最高时，根据组件的功能及其在体系结构中的位置，通过多种连接迁移技术进行服务自组织。利用仿真实验验证了生存性计算的有效性；并通过在网络环境中搭建一个Web服务器证明：在攻击情况下该方法可以有效提高稳态和瞬时的服务可生存性。

关 键 词 连接迁移； 信息系统； 组件结构; 冗余备份； 服务生存性

中图分类号 TP393 **文献标识码** A doi:10.3969/j.issn.1001-0548.2010.01.020

Self-Organization Method for Survivability Enhancement of Information System Service

ZHANG Le-jun[1], LI Zi-ping[2], GUO Lin[1], ZHANG Jian-pei[1], and YANG Yong-tian[1]

(1. College of Computer Science and Technology, Harbin Engineering University Harbin 150001;

2. Department of Computer Science and Technology, Beijing Youth Politics College Chaoyang Beijing 100102)

Abstract As a new direction in network security, the survivability of information systems is different from traditional network security. This paper presents a service self-organization method based on connection handoff. According to service processing flow, the system is divided into communication, service distribution, and service supply modules. Backup modules survivability information is send to online modules and gets the list of newest service states. When the survivability of a module is highest, the self-organization strategies are implemented using multi-handoff technology. The system possesses the merits such as transparency to users, flexibility and operability of the configuration. Experiments confirm that this method can enhance the quality of service and improve service survivability.

Key words connection handoff; information systems; modular construction; redundancy; service survivability

随着计算机和网络技术的广泛应用，安全问题已经成为信息系统研究的重要领域。一方面，人们越来越依赖于各种计算机系统；另一方面，现有的安全体系仍无法确保系统，尤其是系统对外所提供的一些关键服务的安全。传统的信息安全研究方法完全依赖于独立的安全机制和安全组件对系统进行保护，却忽略了组成系统的各个部件本身及部件之间交互时所应具有的安全特性。可生存性是文献[1]于1993年提出的，是指系统在面临攻击、失效和偶然事件的情况下仍然可以按照需求及时完成任务的能力。可生存性研究认为系统的任何一个部件(包括安全部件)的安全性都可能受到危害，系统的生存能力体现在整个系统而非单个部件在遭到入侵时仍然能够对外提供有效服务。

生存性增强技术已经成为网络安全技术的一个新的研究热点，许多组织和研究机构都在进行着这方面的工作。文献[2]将系统划分为安全核和可恢复两部分，并针对特定攻击模式，提出了相应的抵抗、识别和恢复策略。文献[3]提出了不均匀网络结构，可以有效帮助预防和低挡攻击，在分析了不同层次异构对生存能力影响的基础上，研究了不全等的网络元素之间互助时的功能弥补问题。文献[4]提出了以自适应主动漂移机制为手段的生存能力增强技术，该方法虽然能化解某些已知攻击对系统可生存性的威胁，但对于新型攻击和智能功击缺乏有效的生存性保障。文献[5-6]提出了一种针对时间同步网

收稿日期：2008－08－08； 修回日期：2008－12－15

基金项目：国家242信息安全计划(2007B31)

作者简介：张乐君(1979－)，男，博士，主要从事计算机网络与信息安全等方面的研究.

络的生存性增强方法，通过设计一个附加控制协议，使各节点能够自动搜索、选择并调整运行参数，部分节点失效时，系统整体仍然能正常提供服务。此外，文献[7]开展了“关键基础设施保护的信息可生存性”工程研究，包括关键基础设施的可生存性评测、军用和民用基础设施研究及可生存性体系结构工程等，但该理论还很不成熟，缺乏深入的理论研究和可实施性研究。

本文在连接迁移技术条件下，提出了一种通过组件间的协同自组织途径增强服务生存性的方法。

1 服务生存性

1.1 定义

定义 1 原子组件[8]保证网络系统持续提供服务必不可少的最小组件。

定义 2 信息系统可抽象地描述为各种组件的集合，通常包括服务通信组件、服务分发组件和数据存储组件等。通信组件负责与用户进行信息交互，分发组件负责根据客户请求内容的服务分发，存储组件负责数据的存储和处理。

定义 3 组件有且只有完好和失效两种状态。失效本质上是原子组件的状态发生变化，导致依赖于该组件的服务功能无法提供。

定义 4 服务情况用一个多维向量表示，向量的每个元素为一次服务从请求到结束的时间差，因此该向量描述了一段时间内服务的完成情况。

定义 5 服务生存性为网络环境中，服务节点能够正常提供服务的概率。其数值等于在服务处理时间t内系统处于完好状态的概率，因此，$\mathrm{sur}=\exp(-\lambda t)$[9]，$\lambda$与系统所处的内外界环境相关。

1.2 生存性计算

1) 参数计算。

由定义5可知，服务生存性与参数λ和服务处理时间t相关，因此只要获得了这两个参数，就可以对各原子组件所提供服务的生存能力进行计算。

(1) t为服务在原子组件上运行的时间，即原子组件处理服务所需时间，因此组件处理服务用平均时间$\overline{T}$估计。

(2) 服务生存性计算公式为$\lambda=-t^{-1}\ln(\mathrm{sur})$。由指数函数性质可知，只需要确定函数中的一个点即可获得参数λ。当取采样时间T_{test}，采样时间中失效点的个数L，间隔最近失效点的时间差$t_{\mathrm{val}}=\mathrm{Min}\{t_{\mathrm{interval}}\}$，因此采样周期内的任意失效点之前时间片$t_{\mathrm{val}}$所有的时间点都不满足在连续时间$t$内保持完好状态。组件服务生存性$\mathrm{sur}=(T_{\mathrm{test}}-Lt_{\mathrm{val}})/T_{\mathrm{test}}$，因此可得$\lambda=-t_{\mathrm{val}}^{-1}\ln((T_{\mathrm{test}}-Lt_{\mathrm{val}})/t_{\mathrm{val}})$。

2) 算法实现。

随着时间的推移，即使组件没有遭受外部攻击，由于环境和用户行为的变化，服务的正常响应时间也会发生变化。为了及时反映这种变化，本文使用最近一段历史时期的样本数据描述组件服务的行为，而不是所有的历史测量数据，因此，本文使用滑动窗口模型。

根据中心极限定理，无论被研究对象的总体服从什么样的分布，样本均值的分布接近正态分布，正态分布的均值等于总体分布的均值，方差等于总体分布的方差除以样本大小。当其超过置信区间上界$\overline{T}+zD/\sqrt{\mathrm{num}}$，判断其为失效状态。

失效分为瞬时失效和永久失效两种。瞬时失效表现为服务在一定时间内得到响应，但响应时间超过了置信区间的上界；永久失效是指服务在规定的时间内无法完成，对于该状态，在其滑动窗的相应位置填充一个“特殊字符”，不参与置信区间过程的计算。生存性计算算法描述如下。

输入：长度为n的服务响应时间数组；输出：服务生存性。

(1) 统计滑动窗内有效服务响应数 num；

(2) 计算有效响应时间数组均值$\overline{T}$；

(3) 计算方差 D；

(4) 计算参数$\beta=\overline{T}+zD/\sqrt{\mathrm{num}}$；

(5) 统计滑动窗口中失效点个数 L 及最小时间间隔t_{val}；

(6) 更新参数$\lambda=-t_{\mathrm{val}}^{-1}\ln((T_{\mathrm{test}}-Lt_{\mathrm{val}})/t_{\mathrm{val}})$；

(7) 计算服务生存性$\mathrm{sur}=\exp(-\lambda\overline{T})$；

(8) Return sur。

2 服务自组织途径

自组织是一种普遍存在的现象，如生物病毒自我复制进化等。自组织原理的核心思想遵循一组简单规则的多个个体之间能够自主地、异步地相互作用，整体显现出反应或自适应方式的特性[10]，它是通过个体微观行为实现系统宏观目标的一种方法。集中控制对网络系统进行优化的方法受到网络传输带宽的限制，影响了系统的实时性[11]。

本文研究原子组件如何根据自身的服务状态动态地采取自组织策略，保证系统整体提供的服务生存性最高。本文使用了三种连接迁移技术，包括DNS轮转的连接迁移；ARP协议连接迁移和基于重构现

场的TCP连接迁移[12]。

2.1 自组织前提

为了保证原子组件能够根据自己的生存性情况进行自组织，需要满足以下三个前提：

(1) 根据服务的处理流程，将系统组件分解为通信组件、服务分发组件、数据存储组件；

(2) 服务系统中具有多个功能相同的原子组件，可以选择不同的组件完成同样的服务；

(3) 接受连接请求的通信组件互相可见，具有独立的地址。

在服务自组织的过程中：当通信组件生存能力下降时，采用DNS轮转方法进行切换；当分发组件生存能力下降时，采用ARP协议迁移方法进行服务切换，当服务分发组件不在同一个交换网内时，采用代理技术进行服务分发，即通过代理IP接收服务请求，并转发给目标分发组件的方法；当存储组件生存能力下降时，对于正在处理的服务请求，采用重构现场的迁移技术，保证服务持续提供。服务的数据流如图1所示。

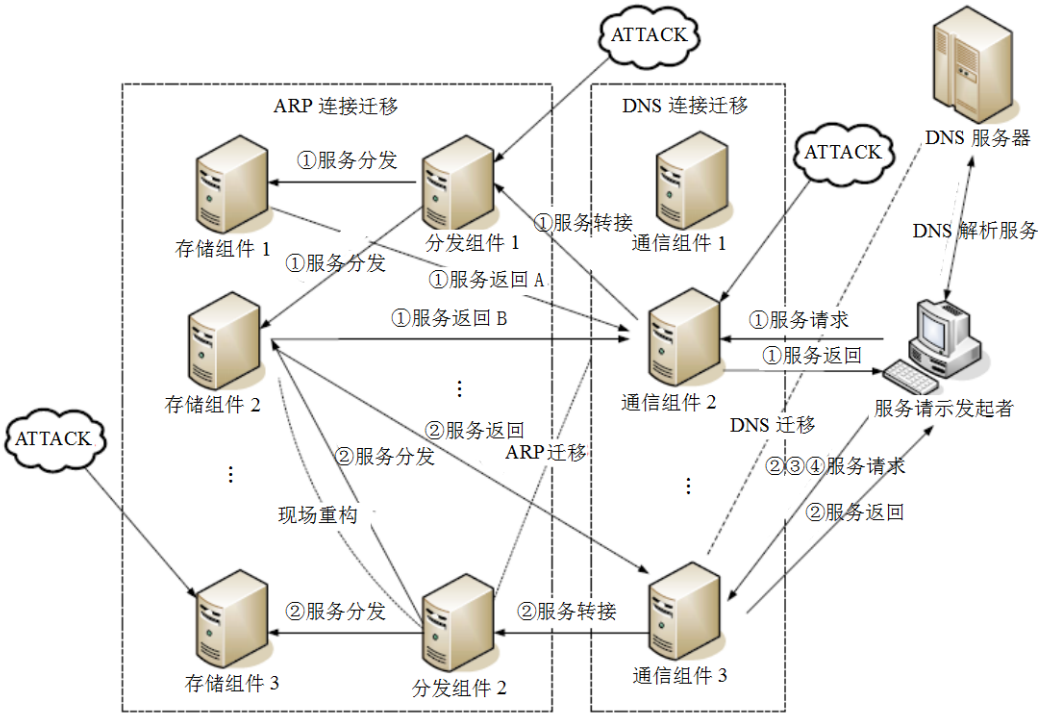

图1　服务数据流

由图1可见，当用户请求第一次服务时，由通信组件2为其提供服务，分发组件1根据其请求的内容，同时将请求数据发送给存储组件1和存储组件2，存储组件将数据返回给通信组件，并由其将结果返回给用户；由于通信组件2和分发组件1遭受攻击，导致其生存性下降，此时各组件分别采用了DNS轮转、ARP连接迁移策略；由通信组件3为用户提供服务，并将服务转接到分发组件2上，分发组件根据服务请求内容将请求转发给存储组件3，由于存储组件3遭受攻击，没有给出回应，分发组件在存储组件2上进行现场重构，并由其将数据返回给通信组件。

2.2 自组织算法

服务自组织算法描述如下。

输入：组件生存性矩阵；输出：自组织结果。

(1) 广播自己节点的服务生存性信息；

(2) if (收到服务生存性列表) then 更新服务组件生存性列表；

(3) else 得到令牌并接管服务；

(4) while (1) {

(5) if (具有令牌) {

(6) 接收其他节点提供的生存性信息，并排序；

(7) if (如果排序发生变化){

(8) 将最新的生存性列表信息广播给所有节点；

(9) }

(10) else 将最新的生存性列表信息广播给请求节点；

(11) if (No. A 组件节点生存性高于自己){

(12) 将令牌交给 No. A 组件；

(13) }//end if

(14) continue;
(15) }//end if
(16) else {
(17) 探测自身生存性信息并发送给服务主节点。
(18) if (没有得到回应){
(19) if (其本身不是次高节点) {
(20) 将具有次高服务生存性的组件设为主节点;
(21) continue;
(22) }//end if
(23) 得到令牌;
(24) 将得到令牌信息通知所有节点;
(25) continue;
(26) }//end if
(27) else{
(28) if (得到令牌) then 接管服务;
(29) continue;
(30) }//end else
(31) 等待一个时间周期;
(32) }//end else
(33) }//end while

算法中每个备份组件拥有一个全局统一的生存性列表，并且只有拥有令牌的组件才能接管服务；算法步骤(5)～(15)完成原子组件为服务组件的功能，服务组件负责收集其他相同功能组件的生存性信息并进行排序，然后将新生成的生存性列表广播给所有备份组件，当其他备份组件生存性超过其时，服务组件将令牌交给该备份组件，并进入备份组件状态；算法(17)～(32)完成备份原子组件功能，备份组件每隔一定时间周期探测其自身服务生存性状态，并将其发送给服务组件，如果没有收到服务组件的回应(服务组件失效)，则自动将生存性次高节点设置为服务节点，如果为次高节点则自动得到令牌，并广播给所有其他备份组件，接管服务；算法中选择每隔固定时间进行服务探测，是考虑到服务组件有可能收到攻击而无法接收和发送备份组件服务探测信息的情况，为了达到更好的效果，时间周期可根据服务处理的时间和频度动态更新。

服务自组织算法中，当组件处于服务状态时，由于其需要为所收集到的其他组件可生存性进行排序，因此计算时间复杂度为$O(n\lg n)$；当其处于备份状态时，需要获得本身的可生存性参数，计算时间复杂度为$O(n)$。

由于原子组件的生存性计算是基于真实环境下的服务质量探测，并且算法中始终选取具有最高可生存性的原子组件(各原子组件相互独立)，因此，从整体上来说系统服务具有最高的可生存性。

3 实 验

3.1 实验环境

本文采用C语言程序实现，对外提供HTTP服务，在2台机器上同时安装通信组件、分发组件和存储组件，组成服务网络。为了增强网络环境的真实性，另外再定时发DoS攻击请求至各组件，服务时间超过3 s认为此次服务未完成。

TCP连接迁移使用文献[13]介绍的方法实现，并对其进行了相应的改造和改进。主要包括：

(1) 在内核上修改数据包校验过程，将使用和目标主机相同IP地址的其他主机发送的数据包过滤机制屏蔽，以解决从存储组件到通信组件的通信屏蔽问题；

(2) 添加对服务探测数据包的处理模块，该探测模块不仅可对组件进行串行测试，还可以进行独立测试，提高了系统的部署灵活性；

(3) 改进了同机ACK数据包接受问题，由于同机之间的通信采用的是本地环回机制，不能解析IP协议，所以在数据包接受时，首先判断查找路由表，将目的地址为本机的ACK数据包直接交给协议栈。

3.2 实验分析

实验1 生存性计算验证实验。

为了证明生存性方法的准确性及有效性，本文采用随机模拟的方法进行仿真实验，实验步骤如下：

(1) 设定原子组件出错概率和服务平均响应时间；

(2) 根据出错概率随机产生固定数目个状态序列；

(3) 随机产生固定数目服务起始点，统计在不同平均响应时间内服务能够完成的概率；

(4) 根据公式计算生存性变化数值；

(5) 比较步骤(3)和步骤(4)中生成的数据差别，实验结果如表1所示。

分析表1，可以得到以下两点：

(1) 采用本文提出的生存性计算方法可以得到与实际值非常接近的结果；

(2) 服务生存性不仅与组件的失效率有关，还与组件处理服务的效率相关，与本文前面所提出的理论相吻合。

表1　生存性计算对比分析实验

序号	错误率/(%)	响应时间/s	步骤(3)	步骤(4)
1		2	0.961 0	0.952 6
2		6	0.893 2	0.887 1
3	0.2	10	0.798 3	0.822 2
4		14	0.764 1	0.767 8
5		18	0.683 0	0.707 3
6		2	0.902 1	0.902 7
7		6	0.746 2	0.755 1
8	0.5	10	0.597 8	0.596 5
9		14	0.499 6	0.488 7
10		18	0.392 6	0.403 4
11		2	0.825 5	0.823 0
12		6	0.563 0	0.544 8
13	1.0	10	0.358 9	0.356 9
14		14	0.277 0	0.235 0
15		18	0.166 2	0.153 7

实验2　服务性能分析实验。

由于基于服务自组织的生存性增强系统是在原服务系统的基础上把处理过程进行了切分，增加了服务处理的复杂度，因此本文在相同的测试环境下，对原有系统和增强系统的服务处理性能进行了对比分析。测试过程中，本文以不同的服务请求速率发送10 000个连接请求，并计算服务平均完成时间，如图2所示。在服务请求速度在150 个/s的情况下，自组织系统与原始系统的平均响应时间相差不大，当达到300 个/s时，自组织系统服务处理时间达到0.312 s，原始系统为0.105 s。总体来说，由于自组织系统增加了组建间的服务迁移以及重构过程，不可避免地较原始系统在性能上有一定下降，但整体差别不大，并不影响系统的实用性。

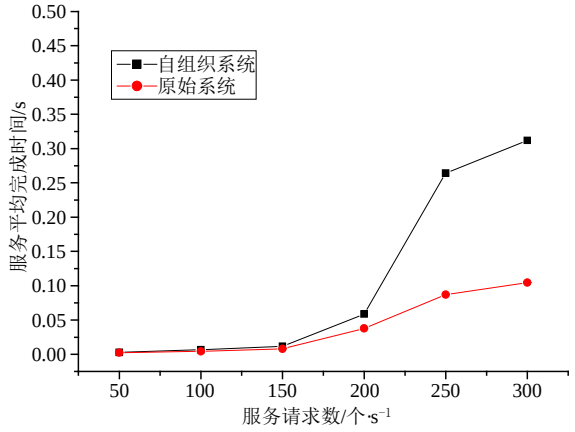

图2　性能对比分析图

实验3　自组织系统参数选择实验。

实验中，在自组织系统不同概率密度的条件下，分别对其服务生存性进行了对比分析。其中：正常服务以每秒 40 的速率每组发送 1 000 个连接请求，共 5 组，攻击强度从 280～520 个/s，实验结果如图 3 所示。

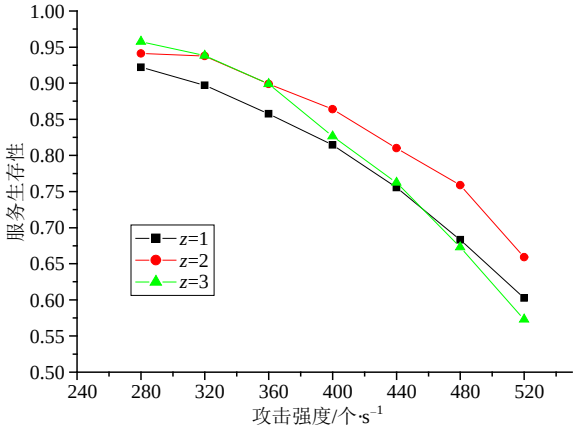

图3　不同概率密度下自组织系统对比图

分析图3可知，当攻击强度较小时概率密度为3的服务生存性最高，当攻击强度逐渐增大时，其服务生存性下降明显，主要原因是其置信区间过大，服务响应时间落在置信区间的概率高达99.73%，导致其攻击敏感性差；当概率密度为1时，服务响应时间落在置信区间上的概率为68.27%，这种情况导致其对攻击过于敏感，迁移过程频繁发生，影响了服务生存性指标；当概率密度为2时，服务响应时间落在置信区间上的概率为95.45%，其对攻击敏感程度介于前两者之间，平均生存性指标最理想。

实验4　系统性能分析实验。

对自组织系统进行性能测试分析时，选取的实验参数与参数选择实验相同。实验中，在不同强度的攻击下，分别对自组织系统和原始系统进行了稳态可生存性和瞬时可生存性测试。实验结果如图4所示。

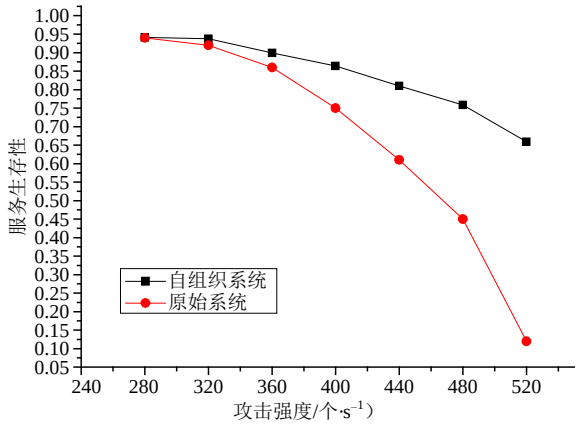

图4　攻击稳态系统性能分析图

图5显示，攻击强度为400 个/s时，攻击在5 s时开始，8 s时结束。

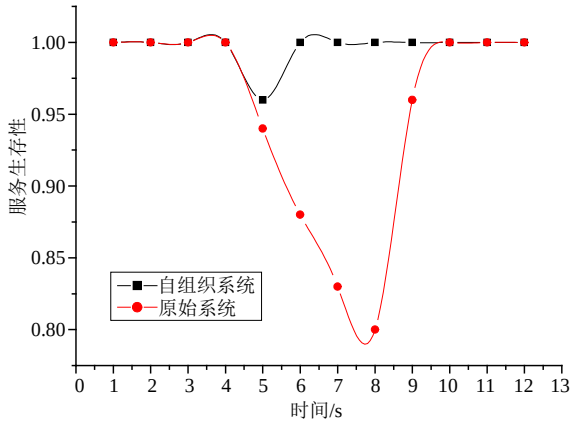

图5 攻击瞬时系统性能分析图

分析图4可知，自组织系统较原始系统在相同的攻击强度下，可生存性指标远大于原始系统；当攻击强度较低时，两个系统的可生存性指标相差不大，说明攻击对系统造成了较小的负面影响；随着攻击强度增大，两个系统的可生存性指标都下降，当攻击强度达到520 个/s时，服务生存性降到最低，但是自组织系统的可生存性指标比原始系统的指标高了近50%。

分析图5可知，自组织系统在遭受攻击时，服务生存性有一定下降，但其通过连接迁移技术以及自组织方法进行快速切换，保证了后续服务的生存性；攻击对原始系统服务生存性影响较大，在8 s时生存性达到最低，攻击结束后逐渐恢复。通过以上实验可以证明将连接迁移技术和自组织方法相结合，可以有效提升系统的服务生存性，降低攻击对系统的影响。

4 结 论

本文从服务的通信、分发和存储三个方面出发，将网络系统分解为服务通信组件、服务分发组件和数据存储组件，为组件的评估与服务切换提供前提；以DNS轮换、ARP协议欺骗以及连接现场重构为技术基础，提出了一种基于自组织的服务生存性增强方法，并通过试验验证了其有效性。传统的服务大多基于TCP协议，通过实现基于TCP层的连接迁移具有广泛的适用性，较少的改动就可应用到其他应用层协议服务生存性增强中。

本文在将服务迁移思想与自组织途径融合并深入研究的基础上，设计了一种增强服务生存性方法。当脆弱组件遭受攻击时，通过服务组件间的自组织途径实现服务漂移，达到增强服务生存性的目的。实验中发送服务请求以及攻击数据，并对整个攻击过程的服务生存性进行了充分分析，证明该方法可以有效提高服务质量，并达到增强服务生存性的目的。该方法的突出优点是无需借助于其他入侵检测系统，自组织机制的实施是根据组件处理服务的能力。

参 考 文 献

[1] HOLLWAY B A, NEUMANN P G. Survivable computer-communication systems: the problem and working group recommendations[R]. Washington: US Army Research Laboratory, 1993.

[2] FISHER J, LINGER R. Survivability: Protecting your critical systems[J]. Internet Computing, 1999, 3(6): 55-63.

[3]ZHANG Y G, VIN H, ALVISI L. Heterogeneous networking: a new survivability paradigm[C]//Proceedings of the 10th New Security Paradigms Workshop, Cloudcroft. New Mexico: [s.n.], 2001: 33-39.

[4] 黄遵国, 卢锡城, 胡华平. 生存能力技术及其实现案例研究[J]. 通信学报, 2004, 25(7): 137-145.
HUANG Zun-guo, LU Xi-cheng, HU Hua-ping. The survivability technique and its implementation caste study[J]. Journal of Communication, 2004, 25(7): 137-145.

[5] 包秀国, 蒋宗礼, 张 永, 等. NTP自主配置的自组织途径[J]. 计算机学报, 2005, 28(5): 759-766.
BAO Xiu-guo, JIANG Zong-li, ZHANG Yong, et al. Self-organizing paradigm for NTP autonomous configuration[J]. Chinese Journal of Computers, 2005, 28(5): 759-766.

[6] 张 永, 方滨兴, 叶建伟, 等. 时间同步网的可生存性增强[J]. 计算机研究与发展, 2006, 43(9): 1550-1556.
ZHANG Yong, FANG Bin-xing, YE Jian-wei, et al. Enhanced survivability of time synchronization network[J]. Journal of Computer Research and Development, 2006, 43(9): 1550-1556.

[7] KNIGHT J C, SULLIVAN K J. Survivability architectures: issues and approaches[C]//DARPA Information Survivability Conference and Exposition. [S.l.]: [s.n.], 2000: 157-171.

[8] 张乐君, 周 渊, 国 林, 等. 基于自主配置的系统生存性增强算法研究[J]. 通信学报, 2007, 28(12): 102-107.
ZHANG Le-jun, ZHOU Yuan, GUO Lin, et al. Research of survivability enhancement algorithm based on autonomous configuration[J]. Journal of Communication, 2007, 28(12): 102-107.

[9] LEWIS E E. Introduction to reliability engineering[M]. [S.l.]: John Wiley, 1987.

[10] GROVER W D. Self-organizing broadband transport networks[J]. Special Issue on Communications in the 21st Century, 1997, 85(10): 1582-1611.

[11] HE Jian-qiang, ZHANG Huan-chun, JING Ya-zhi. An integrated control and scheduling optimization method of networked control systems[J]. Journal of Electronics Science Technology of China, 2004, 2(2): 56-59.

[12] 汪 黎, 王正华, 章文嵩. TCPHA: 一个新型的高性能基于内容调度系统[J]. 计算机工程, 2006, 32(1): 151-153.
WANG Li, WANG Zheng-hua, ZHANG Wen-song. TCPHA: a new high efficient content-aware system[J]. Application Research of Computer, 2006, 32(1): 151-153.

编 辑 漆 蓉