可信计算及其关键技术研究*)

王志刚[1,2] 李师贤[2,3]

(楚雄师范学院计算机科学系 楚雄675000)[1] (中山大学计算机科学系 广州510275)[2]

(中国科学院计算技术研究所智能信息处理开放实验室 北京100080)[3]

The Study on Dependable Computing and its Key Technology

WANG Zhi-Gang[1,2] LI Shi-Xian[2,3]

(Department of Computer Science, Chuxiong Normal Institute, Chuxiong 675000)[1]

(Department of Computer Science, Zhongshan University, Guangzhou 510275)[2]

(Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080)[3]

Abstract The dependability is the latest and highest techno-target used to evaluate the performance quality of a distributed computing system in open network environment, it includes traditional reliability, availability, robustness, survivability, security, data integrity and software protecting ability, etc. A dependable system should not only be provided with fault tolerance ability, but also withstand from risk and recover from disaster, its realization foundation is the high availability of the information transmission network and survivability, fault tolerance and security safeguard of the system. This paper presents a survey of the survivability mechanisms such as long-distance backup, cluster and system recovery, while discussing the techniques of fault tolerance design and information network system security safeguard, and analyzing the information redundant dispersal strategy and model for survivability and security safeguard.

Keywords Dependability, Dependable computing, Survivability, Disaster tolerance, Fault tolerance, Security, SAN, Information redundant dispersal

1. 计算机系统的可信性

随着世界经济全球化的加剧,计算机系统应用呈现出日益广泛而深入的发展态势,政治、经济、商业运作和各类事务处理越来越严重地依赖于计算机数据服务,在国防军事、核反应堆控制、飞机航行控制、火控及化学反应控制等关键应用和医疗、金融、交通、通讯、气象、电力、石油化工、Web 服务、联机事务处理 OLTP、科学计算等重要应用中尤其如此。与此同时,目前基于 Internet/Intranet 的分布式计算机系统及开放式网络环境增加了系统的复杂度、故障率和不安全因素,这种形势促使人们不得不对计算机系统的性能和服务质量提出严格以致苛刻的高要求,那就是高质量和低风险以致无风险的可信赖服务,而传统上使用的"可靠性"(reliability)已不足以描述这种性质,因此国外计算机界在20世纪90年代提出了"可信性"(dependability)的性能指标。

可信性(dependability)[1~4]用来定义计算机系统的这样一种性质,即能使用户有理由认为系统所提供的各种服务确实是可以充分信赖的。

从词语本身来看,可信性(dependability)与可靠性(reliability)是同义词,但作为描述计算机系统性能的术语,两者的内涵和外延已经有了不相同的特指和约定。可靠性通常是指计算机系统在规定正常时间内和规定正常条件下能稳定工作的能力,一般用平均故障间隔时间 MTBF(mean time between failures)来量度,它习惯上主要用于评估早期以集中控制与管理为特征的封闭式本地计算系统,并侧重于硬件系统、设备和元件性能稳定性的评价。到20世纪80年代,人们对传统上基于本地计算的可靠性系统的最高指标要求是 RAS(可靠性+可用性 Availability+可维修性 Serviceability),其典型特征是容错(fault tolerance,故障容忍),即要求系统在遇到有关故障时,能够有效地自动检测、屏蔽或排除故障以确保计算任务的正确执行(图1)。

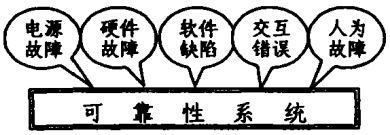

图1 传统可靠性系统的容错功能

而可信系统不仅要求容错,而且要求能够抵御风险和容忍灾难(图2)。因此可信性不仅包含了可靠性、可用性、健壮性(robustness)、可测试性(testability)、可维护性(maintainability)等内容,而且尤其强调抗毁性(survivability,或译为生存性、可存活性)、保险性(safety)、安全性(security),它体现对开放式网络环境下分布计算系统整体性能质量的评价,并侧重于数据完整性(integrity)和软件保护能力的度量,是一个真正反映"无忧计算"理念的用语,人们有时也用"高可靠性"或"高可用性"表示与可信性相近的含义。可信性的主要构成如图3所示。

*)本文得到国家自然科学基金委员会(NSFC)与香港研究资助局(RGC)联合科研资助基金资助(编号:79910161989)。王志刚 副教授,主要研究兴趣为可信计算与容错技术、软件工程与软件技术。李师贤 教授,博士生导师,主要研究兴趣为软件理论、软件工程与软件技术。

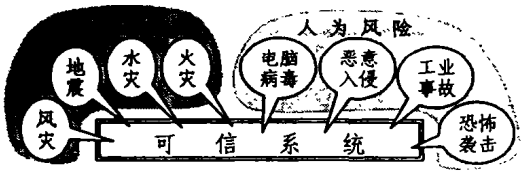

图2 可信系统所应对的各种风险

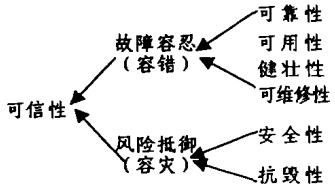

图3

也正因为如此，由 IFIP（国际信息处理联合会）从1979年开始举办的“可靠计算与容错 RCFT（Reliable Computing and Fault Tolerance）”会议特此改名为“关键应用可信计算 DCCA（Dependable Computing for Critical Applications）”会议；由 IEEE（国际电气与电子工程师学会）主办、IFIP 支持和协办的 IEEE 太平洋沿岸容错系统会议于1999年改名为 IEEE 可信计算会议，而从1971年起连续举行了29届的 IEEE 国际容错计算年会（FTCS）到2000年也与 IFIP 主办的关键应用可信计算 DCCA 会议合并，从此改名为 IEEE“可信系统与网络 DSN（Dependable Systems and Networks）”国际学术会议。

可信与容错计算已经发展成为计算机科学技术的一个核心分支领域，IFIP 专门设立了“可信计算与容错工作组”——WG10.4，负责主办 IFIP 有关可信计算的国际会议，并关注以下的研究内容：可信性的理解、定义、规范化、设计和实现方法；可测试性和可校验性（verifiability）的确认与设计；通过建模和度量来评估可信性等等。

本文结合最新应用和发展着重对可信性指标中的抗毁性、容错性和安全性及其实现方法与技术作介绍和分析。

2. 可信系统的抗毁机制

抗毁性是指系统在遇到严重故障或意外灾难而导致毁损的情况下恢复任务运行的能力。网络应用增加了系统结构的复杂性和风险，但无疑也为计算机系统抵御风险和容忍灾难提供了更大的空间和更多的选择，可信系统的抗毁机制也主要依赖于传输网络的可用性和远程备份及恢复的容灾能力。

2.1 Internet 网络的高可用性保护[5~7]

在 Internet 通信网络的光层（如 WDM）和 IP 层都提供了独立的保护和恢复技术方案，其故障恢复能力的前提条件是必须具备冗余带宽和空闲资源。在 IP 层可以通过 IP 动态路由、MPLS（multi-protocol label switching，多协议标志交换）保护交换等故障恢复技术来提高网络可用性。

在 WDM 层保障网络可用性可以采用 APS（Automatic Protection Switching，自动保护交换）和 SHR（Self-Healing Ring，自愈环）等预设计保护技术；根据 WXC（Wavelength Cross-Connect，波长交叉连接）功能、通信量请求、性能要求和网络控制的情况，可在 WDM 层采用反应型（Reactive）或前摄型（Proactive）两类故障恢复方法。

2.2 基于 FC-SAN 的抗毁性技术[8,9]

SAN（Storage Area Network，存储区域网络）就其存储功能角度而言，是一种基于网络传输的存储 I/O 方法，其体系结构可以划分为三大部分：（1）磁盘、磁带等目标设备，实现网络存储；（2）服务器、工作站等发起设备，提交计算应用的存储任务；（3）互联设备，包括交换机、HUB（集线器）、HBA（Host Bus Adapter，主机总线适配器）等网络传输部件。目前 SAN 通常运行于 FC（Fibre Channel，光纤通道）之上，WDM 及其他技术可以把 FC 的距离扩展到100公里，从而在保证时效性的同时达到容灾的目标，提供抗毁性保障。

同一个 FC-SAN 上可以配置多台服务器以及多个磁盘阵列等存储设备，并允许把设备之间的从属关系改而设置为平等的地位，从而使任何一台服务器均可存取网络中的任何一个存储设备。因此，SAN 具有极高的数据独立性，可较充分地体现资源共享。

2.2.1 *基于 SAN 的远程备份技术* 基于 SAN 的 LAN-free 虚拟专网备份技术通过把服务器、存储阵列以及磁带子系统与 FC-SAN 相连，可以把备份数据流从 LAN 移向 SAN，从而使 LAN 得以摆脱用户网络流量的重负，解决了企业局域网络的数据拥塞问题。

为了进一步减轻服务器的负载，SAN 解决方案还提供了更为优化的 Server-less（无服务器）“第三方”备份技术，可以把备份相关的硬件控制和软件资源从服务器转移到 SAN 中的其他智能组件单元（如 HUB、路由器、交换机或主机 I/O 控制器等），以其充当“数据移动器”和“备份代理”直接独立完成备份处理任务。

2.2.2 *基于 SAN 的集群计算可信系统* 在 FC-SAN 的结构下，形成集群的多台服务器可以实现对公共存储设备的平等存取，当某服务器出现故障时，其他服务器可通过 SAN 存取出故障服务器中的处理数据，确保数据的随时可用。为了确保系统的高可用性，还可以在服务器和存储设备之间提供冗余的数据路径，如图4所示的结构中，每台服务器配备两个 FC-HBA，其中一个 HBA 作为主数据路径附接于 FC-HUB 或交换机上，而另外一个 HBA 作为辅助数据路径附接于第二个 FC-HUB 或交换机上，通过冗余交换机提供了多个路径选择；RAID 子系统同样拥有主、辅两个 FC 接口，如果主 FC 出现故障，另一个通道能够接管。网络传输通过光纤通道路径 FCP 可实现较长距离的异地容灾。

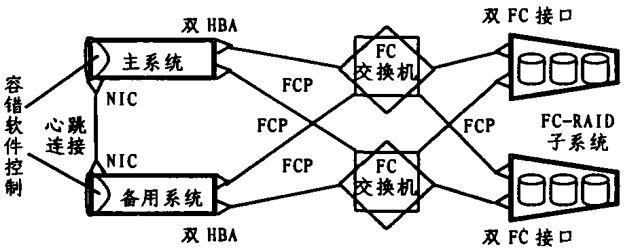

图4 基于 SAN 的可信系统 Cluster 结构

FC-SAN 首先被应用于视频影像制作和印前图形编辑等方面的可信计算应用，此类应用需要使用 SAN 所提供的多数先进功能--高速数据传输、对等连接、大规模存储阵列存取、高可信性以及对大量单一配置工作站的支持；除此而外，SAN 技术也正在应用于电力、通讯等重要领域。

3. 可信系统的容错功能设计

可信计算是在容错计算的基础上发展起来的，因此一个可信系统首先应该是容错的。

容错技术的本质是冗余方法，有硬件冗余、软件冗余、信息冗余和时间冗余四种具体方式。硬件冗余即 MMR(Multi-Modular Redundancy，多个硬件模块冗余)结构，典型技术方案如 RAID(Redundant Array of Independent Disk，独立磁盘冗余阵列)、多 CPU 配置、多机热备份系统、Cluster(集群)系统等，最新的 CPU 热拔插、内存热拔插、冗余内存阵列、负载均衡等动态冗余技术进一步提高了硬件冗余的可用性。

软件冗余即通过多重计算(Design Diversity，也称为设计多样性)实现对软件故障的容错，其基本方法是恢复块 RB(Recovery Block)技术和多版本编程 NVP(N-Version Programming)技术[10]，较新的方法有 Scott 提出的一致性恢复块和 Avizienis 提出的免疫系统概念模型[11]。

在资源静态或动态冗余的基础上，借助于故障检测、诊断定位、重试、故障包容(Fault Containment)、故障恢复(Fault Recovery)等机制，容错最终通过故障屏蔽(Fault Masking)或系统重构(Reconfiguration)这两种基本途径来实现，并可选择容错硬件或容错软件的实现方式。

4. 信息网络系统安全保障技术

网络系统安全包括以下三个方面的内容：①保密性(Confidentiality)，确保信息不被非授权用户访问；②完整性(Integrity)，确保信息不被未授权用户更改，但对授权用户开放；③确定性(Authentication)，确保访问它的用户就是它所声明的使用者。

信息网络系统安全保障问题主要涉及以下方面：

(1)信息安全立法、信息安全等级标准、信息安全工程实施、评估及管理规范等；

(2)信息安全基础设施、安全操作系统、安全 DBMS、安全协议等；

(3)网络系统安全保障技术，如防火墙技术、入侵检测技术、计算机病毒防范技术；智能卡技术、访问控制和用户权限管理技术、信息验证与数字签名技术以及基于指纹、声纹、面像和 DNA 遗传信息等生物特征的新型身份验证技术等；

(4)数据安全保障技术：包括数据加密技术、数字水印技术等。

信息安全是目前信息科学与计算机科学研究的热点领域，著述极多，此处予以从略。

5. 可信系统的抗毁性与安全性分析[12~14]

在分布式计算环境 DCE 下，与中国古代哲学“狡兔三窟”同理，可信系统正是通过信息冗余分散来保障抗毁性和提高安全性，达到抵御风险和容忍灾难的目的。

5.1 信息冗余分散模型

可信系统的信息冗余分散(Information redundant dispersal)模型定义为三元组(D,S,I)，其中：

① D(Data)表示系统数据信息，D 分解为 n 个子信息，即 $D=\{d_1,d_2,\cdots,d_n\}$，$\forall\ i,j\in[1,n]$，若 $i\neq j$，则 $d_i\neq d_j$。

② S(System)表示存放信息的系统，S 分解为 m 个子系统，即 $S=\{s_1,s_2,\cdots,s_m\}$，$\forall\ i,j\in[1,m]$，若 $i\neq j$，则 $s_i\neq s_j$。

③ I(Include)表示子系统与子信息之间的关系，故有 $I\subseteq S\times D$，$(s_i,d_j)\in I$ 当且仅当 s_i 子系统中存放有信息子集 d_j，或记为 $d_j\in C(s_i)$，$C(s_i)$ 表示子系统 s_i 中存放信息的集合。

④ 在一次灾难事件后，若幸存的 r 个子系统满足 $C(s_{i_1})\cup C(s_{i_2})\cup\cdots\cup C(s_{i_r})=D$，$i_1,i_2,\cdots,i_r\in[1,m]$，$r\in[1,m]$，则表明系统信息可以重构恢复。

⑤ 在遭遇一次安全攻击事件后，若被攻击失陷的 r 个子系统所包含的信息足以重构恢复系统，即满足 $C(s_{i_1})\cup C(s_{i_2})\cup\cdots\cup C(s_{i_r})=D$，$i_1,i_2,\cdots,i_r\in[1,m]$，$r\in[1,m]$，则表明系统已经失密。

5.2 几种基本模型及分析

若系统中每一子信息冗余存放在 k 个子系统中，则每个子系统中需存放的子信息数目为 kn/m。在一次灾难后，只要遭到毁损的子系统数目不超过 $k-1$，即至少有 $m-k+1$ 个子系统完好，则系统全部信息均可恢复重构；另一方面，只要被攻陷 $m-k+1$ 个子系统，则整个系统失密。

因此，随着 k 值的增大，$m-k+1$ 值减小，系统抗毁性增强，同时系统安全性下降，系统存储与网络传输的开销则相应加大。在构建可信系统时，必须综合权衡考虑抗毁性、安全性、投入成本和实现难度等各方面因素，恰当地选择设置 n,m,k 的值并制定系统的冗余分散策略。以下列举四种基本的冗余分散模型(均设定 $m=n$，$i=1,2,\cdots,n$)。

模型①：S 的每一个子系统 s_i 内都冗余存放着系统信息全集 D，即有 $C(s_i)=D$。

模型②：S 的每一个子系统 s_i 内冗余存放着除 d_i 之外的 $n-1$ 个子信息，即有 $C(s_i)=D-\{d_i\}$。

模型③：S 的每一个子系统 s_i 内冗余存放着 d_i 及其前驱共两个子信息，即有 $C(s_1)=\{d_n,d_1\}$，$C(s_i)=\{d_{i-1},d_i\}$。

模型④：S 的每一个子系统 s_i 内只存放子信息 d_i，即有 $C(s_i)=\{d_i\}$。

其中模型①和模型②是两种有代表性的高抗毁性模型，模型①只需有一个子系统幸存即可重构恢复系统，而模型②只需有两个子系统幸存亦可重构恢复系统；但系统的安全风险也最大，模型①只要被攻陷一个子系统则整个系统失密，而模型②只要被攻陷两个子系统，则整个系统失密。这一类高抗毁性模型适用于保密性要求较低的重要公用信息服务系统。

而模型③和模型④则是两种有代表性的高安全性模型，模型③系统中只有当其中 $n-1$ 个子系统被攻陷，才会导致整个系统失密，而模型④系统中只有当全部 n 个子系统均被攻陷，才会导致整个系统失密。但系统的抗毁性也极低，模型④系统的抗毁能力为0，模型③中只要有两个子系统遭到毁损，则系统不可恢复。因此这一类高安全性模型应用的前提必然是传输网络和各子系统局部具有极高可靠性和安全性，包括技术、管理和设施等方面的保障措施和条件，确保各子系统不会在灾难中遭到损毁。

5.3 信息冗余分散中的抗毁性和安全性策略

(1) 在信息冗余分散模型中，为了提高系统的安全性，可以适当增加信息冗余分散的节点，并适当减少同一子信息的冗余存放份数；可用阈控(Threshold schemes)方式分解核心关键信息，使得当且仅当 k 个子信息同时被破解，各子信息方可被利用，从而增加系统安全性[12]。

(2) 尽量降低各子信息及各子系统之间相关性。例如，在某次病毒为害的事件中，可能多个冗余的 Windows 子系统都同时被损，从而使冗余分散失去意义。因此，为了降低相关性，各子系统宜分别置于 NT、Linux、UNIX 等多种非同构环境之

下，并对各子信息分别采用不同的加密方法、访问控制及用户身份鉴别机制。

结语 本文介绍了可信计算的主要内容、基于FC-SAN的远程备份、集群与系统恢复等抗毁机制，讨论了系统容错功能设计和信息网络系统安全保障技术，并分析了用于保障抗毁性和提高安全性的信息冗余分散策略和模型。网络技术的发展和应用使得可信计算有望成为商业应用的可能目标。

为适应发展需要，计算机系统正在日益复杂化，其系统结构已从20世纪80年代中期以前的本地集中计算模型发展为本地分布计算模型，再进一步发展到目前基于Intranet/Internet的广域分布计算模型，人们对于计算机及系统的性能评价也从最早的单一可靠性指标，发展到RAS(Reliability＋Availability＋Serviceability)指标，并进一步发展到RASIS(RAS＋完整性Integrity＋安全性Security)指标，再发展到如今的可信性指标。

目前正在发展的网格(Grid)计算技术将力求把Internet上包括硬件、软件、数据库和各种信息获取设备等所有资源，连接成一个整体，使整个网络如同一台资源极其丰富的超强计算机，向每个用户提供高性能的服务；网格技术时代的信息存储是基于虚拟存储架构VSA(Virtual Storage Architecture)和存储公用设施模型SUM(Storage Utility Model)的广域分布和高度共享方式，必将为可信计算提供更有力的支持和更灵活的选择。

可信性及其研究标志着计算机技术向更高层次发展和跃升。2000年12月11日，由美国CMU与NASA的AMES研究中心牵头，包括MIT(麻省理工学院)、华盛顿大学、乔治亚理工学院和IBM、COMPAQ、SUN、HP、Microsoft、Sybase、Adobe等12家公司成立了高可信计算协会(High Dependability Computing Consortium)，致力于对高可信性计算进行基础研究、实验研究和工程研究[15]，可见其受到学术界和产业界的重视程度。

参考文献

1 Avizienis A, Laprie J C, Randell B. Fundamental Concepts of Dependability[A]. In: Proc of the ISW-2000[C]. Boston, MA, Oct. 2000

2 Laprie J C. Dependable computing: concepts, limits, challenges [A]. In: Special Issue FTCS-25[C]. Pasadena CA. 1995. 42～54

3 Kyriakopoulos N, Wilikens M. Dependability of complex open systems[A]. In: Proc of the ISW-2000[C]. Boston, MA, Oct. 2000

4 IFIP WG10.4 on Dependable Computing and Fault Tolerance [EB/OL]. http://www.dependability.com, 2002

5 Mohan G, Murthy C S R. Lightpath Restoration in WDM Optical Network[J]. IEEE Network, 2000, 14(6): 24～32

6 Fumagalli A, Valcarenghi L. IP Restoration vs WDM Protection [J]. IEEE Network, 2000, 14(6): 34～41

7 Zhou Dongyun, Subramaniam S. Survivability in Optical Networks[J]. IEEE Network, 2000, 14(6): 16～23

8 Clark T. Designing Storage Area Networks[M]. Longman Inc., 1999

9 Farly M. Building Storage Networks[M]. McGraw-Hill Inc., 2000

10 Avizienis A. The N-Version Approach to Fault-tolerant Software [J]. IEEE Trans Sof Eng, 1985, 11(12)

11 Avizienis A. Toward Systematic Design of Fault-tolerant Systems [J]. IEEE Computer, April 1997

12 Wylie J J, Bigrigg M W, et al. Survivable Information Storage Systems[J]. IEEE Computer, Aug. 2000. 61～68

13 Hiltunen M A, Schlichting R D. Enhancing Survivability of Security Services Using Redundancy[A]. In: Proc of The Int'l Conf on Dependable Systems and Networks (DSN'01)[C]. Goteborg, Sweden, 2001. 173～182

14 Snow A P, Straub D, et al. The Survivability Principle: IT-Enabled Dispersal of Organizational Capital [EB/OL]. http://www.cis.gsu.edu, 2002

15 High Dependability Computing Consortium (HDCC) [EB/OL]. http://www.hdcc.cs.cmu.edu, 2002

16 王志刚. 存储系统可信性及其保障技术探析[J]. 计算机研究与发展, 2003, 40 (5. 增刊)

17 王志刚. 计算机容错技术及其发展与应用综述[J]. 计算机应用, 2002, 22 (8. 增刊)

(上接第60页)

统计语言模型提高词类标注的正确率和排歧能力，需进一步描述词的上下文依赖关系。

参考文献

1 Rosenfeld R. Two decades of statistical language modeling: where do we go from here?. In: Proc. of the IEEE, Vol. 8, 2000

2 Huang F-L, Yu M-S. Analyzing the properties of Smoothing Methods for Language models. IEEE 2001

3 Chen S F, Goodman J. An empirical study of smoothing techniques for language modeling. Computer Speech and Language, 1999, 13

4 Church K W, Gale W A. A comparison of the enhanced Good-Turing and deleted estimation methods for estimating probabilities of English bi-grams. Computer Speech and Language, 1991, 5

5 Nadas A. On Turing's formula for word probabilities. IEEE Trans. On Acoustic, Speech and Signal Processing, 1985, ASSP-33

6 Witten L H, Bell T C. Zero-frequency problem: estimating the probabilities of Novel events in Adaptive text compression. IEEE Transaction on information theory, 1991, 37

7 Su K Y, Chiang T H, Chang J S. A overview of corpus-Based statistical-oriented techniques for natural language processing. Computational Linguistics and Chinese language processing, 1996, 1

8 Ney H, Essen U. On smoothing techniques for bi-gram-based natural language modeling. In: IEEE intl. conf. on Acoustic, Speech and Signal processing, 1991

9 Essen U, Steinbiss. Cooccurrence smoothing for Stochastic language modeling. IEEE international conference on Acoustic. Speech and Signal processing, 1992, 1

10 Kenser R, Ney H. improved backing-off for m-gram language modeling. IEEE international conference on Acoustic, Speech and Signal processing, 1995

11 Jiang Ming, Zhu Xiaoyan 等. Braille to print translations for Chinese. Information and Software Technology, 2002, 44

12 周强. 规则和统计相结合的汉语词类标注方法. 中文信息学报, 1995, 9(3)

13 朱靖波, 等. 基于对数模型的词义自动消歧. 软件学报, 2001, 12(9)

14 赵石顽, 等. 基于统计的中文词分类. processing of the 3 World congress on intelligent controln and automation, 2000

15 http://www.icl.pku.edu.cn/Introduction/corpustagging.htm