文章编号:1001 - 9081(2006)06 - 1324 - 04

信息系统灾难恢复模型研究

王 琨[1],周利华[1],袁 峰[2]
(1. 西安电子科技大学 计算机网络与信息安全教育部重点实验室,陕西 西安 710071;
2. 国家信息安全工程技术研究中心,北京 100093)
(wangkun@mail.xidian.edu.cn)

摘 要:为保障业务系统在灾难状态下具备持续服务能力,提出健壮的灾难恢复系统模型。模型强化通信保障能力以提供安全可靠的灾难恢复控制;提出自我监测能力监测灾难恢复系统自身的完整性和安全性;使用可视技术使灾难恢复系统易于使用、管理和维护。模型适用于电子政务、银行等安全级别较高的环境。在模型的指导下某电子政务灾难恢复系统已经建设完毕。实践和仿真实验证明系统能够满足网络收敛和应用响应时间要求。

关键词:信息安全;电子政务;持续服务;灾难恢复
中图分类号: TP309 **文献标识码**:A

Study on disaster recovery model for information system

WANG Kun[1], ZHOU Li-hua[1], YUAN Feng[2]
(1. *Key Laboratory of Computer Network and Information Security of the Ministry of Education, Xidian University, Xi'an Shannxi* 710071, *China;*
2. *National Information Security Engineering and Technology Research Center, Beijing* 100093, *China*)

Abstract: A robust disaster recovery system model was presented to make information systems own continuous service talent even under disaster condition. The safe communication ability was strengthened to guarantee the secure command on disaster recovery. The self-supervision talent was introduced to watch the integrality and the security of disaster recovery system itself. Real-time visible platform was suggested to makes disaster recovery systems easier to use, manage and maintain. This model suits critical security environments such as e-government and bank. A key e-government disaster recovery system of China has been constructed guided by the model. It is verified that the network convergence and application response time can satisfy the system requests through the practice and matching simulation.

Key words: information security; e-government; continuous service; disaster recovery

0 引言

随着各种应用日益严重依赖信息技术,信息系统失效也会直接影响应用。对于某些关键应用,即使短时间失效也是无法忍受的,必须建设灾难恢复系统(Disaster Recovery System,DRS)保障关键应用具备持续服务能力。这里"灾难"已经超出了自然灾害的范畴,它指任何有可能导致信息系统持续一段时间失效的危害,包括病毒、黑客攻击、误操作、火灾、地震等。如何更好地保护系统,提供灾难恢复和持续服务能力已经成为国际上的研究热点,灾难恢复系统模型研究就是其中的关键研究之一。

目前已经有一些灾难恢复系统模型,例如 Business Continuity Planning (BCP)[1]、RoboCup-Rescue[2]、CoStore[3,4]、Disaster Management System (DMS)[5]、Continuity of Operations Planning (COOP)[6]、Disaster Recovery Cluster Software System (DRCSS)[7]。BCP 是一种过程驱动的通用模型,它通过分析和更新商业持续计划实现灾难恢复。由于它侧重于商业领域,对一些安全问题涉及不够,不能保障系统自身的安全性和完整性,不适用于对安全性要求非常高的环境。并且它没有涉及系统管理,不便于系统的使用与维护。RoboCup-Rescue 论述了使用机器人和人工智能技术应对灾难的重要性,在系统的可视化方面有很好的表现。CoStore 研究建设可靠、高可用的存储系统。在校园网规模的环境中,它可以在不影响系统性能的情况下提高存储系统的待命性。DMS 被设计用于减少重大灾难中人员生命损失,降低灾难恢复的代价。它集成传感器技术、建模和仿真工具、遥感和计算平台,为决策者提供预警、灾难发生中和灾难恢复中的信息,提高应对灾难的能力。COOP 能够保障政府处理和应对各种突发事件的能力。它包含开始持续应对计划、标识应急时间、明确部门职能、确定保护重要系统和部门、开发高效通信方案、测试评估和修改持续应对计划。DMS 和 COOP 都不是专门为保护信息系统而设计的。DRCSS 试图解决软件系统的灾难恢复问题。用户系统使用 DRCSS 编程接口初始化多个同时分散在网络中不同节点的应用程序实例,DRCSS 同步这些应用实例的状态,检测网络节点的失效,使应用系统能够容忍网络和计算结点灾难。这些灾难恢复模型有的不适于保护信息系统;有的模型虽然可以保护信息系统,但由于它基于应用服务供应商[8,9],安全性不高;有的模型无法承受重大灾难;还有的

收稿日期:2005 - 12 - 19;**修订日期**:2006 - 04 - 19 **基金项目**:国家"十五"重点科技攻关计划(2002AA1Z67101)
作者简介:王琨(1973 -),男,陕西西安人,博士研究生,主要研究方向:网络与信息安全; 周利华(1942 -),男,江苏苏州人,教授,博士生导师,主要研究方向:网络与信息安全、网络多媒体; 袁峰(1970 -),男,河北石家庄人,高级工程师,主要研究方向:网络与信息安全.

模型不便于系统的使用、管理和维护。

由于对安全性、可靠性和系统性能要求高,加之国内缺乏可借鉴的成功经验,在深入研究中国电子政务体系[10,11]、多种灾难和灾难恢复系统的基础上,本文提出健壮的灾难恢复系统模型(Robust Disaster Recovery System Model,RDRSM)以指导 EEDP 中 DRS 的建设。与其它模型相比,RDRSM 强化了安全性和可靠性,创新地提出系统模拟与监测,实现对系统自身完整性和安全性监测和对灾难的模拟;RDRSM 格外强调通信系统的可靠性;它重视结合地理信息系统(Geographic Information System,GIS)提供实时的 2D、3D 操作平台,更易于 DRS 的使用、管理和维护。在论文研究工作的帮助下,我们制订了国家电子政务安全支撑平台规范,该规范已经正式发布,用于指导我国电子政务项目的建设。

1　健壮的灾难恢复系统模型

RDRSM 模型如图 1 所示,它包括咨询与培训(Consultation and Training,CT)、风险评估(Risk Assessment,RA)、灾难恢复计划(Disaster Recovery Planning,DRP)、模拟与检测(Simulation and Supervision,SS)、灾难恢复控制(Disaster Recovery Control,DRC)和系统管理(System Management,SM)这几个环节。

由于性能、安全性、带宽等众多因素的互相制约,为实现业务可持续性,设计 DRS 上的应用系统时不得不权衡高性能与高可靠性之间的关系。对于高安全性的应用可以使用 2 - safe,它的原子特性能保证数据中心与备份中心数据的一致性,避免损失已经处理完毕的事务。但它会增加资源竞争的冲突,减少吞吐量,而且备份中心出现故障时,数据中心必须改变它正常的工作方式。1 - safe 可以减少由于资源竞争带来的事务处理延迟,即使备份中心不可用时数据中心仍然可以正常工作,更容易实现一个数据中心支持多个备份中心,但是灾难发生时会丢失一部分未来得及传输的事务。为实现安全性与系统性能的折中,可以在关键部分使用 2 - safe,次要的地方使用 1 - safe。此外,在保障 DRS 及时有效地切换系统、指挥调度、故障排除的同时,为实现 DRS 的安全、可靠和易用,RDRSM 还有如下总体要求:

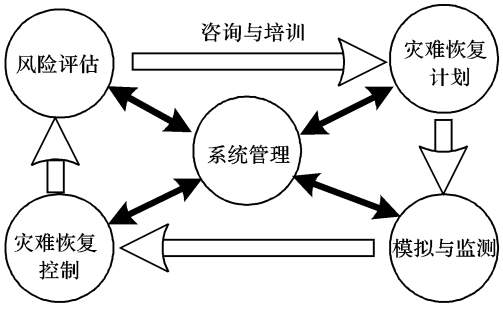

图 1　健壮的灾难恢复系统模型

1) 安全可靠的通信保障是灾难恢复的关键,必须尽可能利用多种通信手段,确保通信的畅通无阻。尽可能采用不同安全级别的密码技术保护数据的存储、传输和访问控制。

2) 采用决策支持系统(Decision Support System,DSS)分析海量数据,为决策者提供科学的决策依据。

3) DRS 通常覆盖范围较大,使用 GIS 提供直观的操作平台,便于 DRS 的使用、管理和维护。

1.1　咨询与培训

CT 是实现 DRS 的最初步骤,它也贯穿 DRS 所有环节中,是非常重要,并且也是最容易被忽略和出问题的环节。EEDP 之所以进展顺利,首先得益于在项目建设及系统运行过程中,始终有良好的咨询与培训。DRS 涉及面非常广、牵扯行业非常庞杂,这迫切要求聘请众多领域的资深专家。CT 的内容涉及 DRS 及所有相关的问题,例如政策、法规等。

灾难恢复方面,在咨询、培养信息安全专家的同时,还要普及安全教育,课程设置要理论与实践相结合。灾难恢复往往需要不同部门的工作小组共同协作才能完成,必须使 DRS 中所有协调人员都具备必要的安全理念,使 DRS 中所有设计、开发、使用、管理和维护人员掌握熟练的专业技能,能够互相协调应对意外灾难。与传统的安全培训不同,灾难恢复的培训主要集中在新安全技术的设计、开发和使用方面。需要强调的是,由于人们很难直接解决所有的问题,因此,还要着重培养学生判断和识别信息保护程度,以及在适当情况下与相关部门协调工作的能力。

1.2　风险评估

风险指某个安全威胁发生的可能性,以及由此而引起的经济、信誉和商业伙伴损失等,需要建立长期的风险评估机制评估应用和灾难类型。RA 是 DRP 的基础。另一方面,RA 能够收集 DRC 的反馈信息,使 DRS 总结经验教训,不断提高系统性能。EEDP 中把灾难抽象成安全威胁和危害级别。

在发生现场 L,具有某种危害动机 M,采用危害行动 A,某个危害实施者 D 会对系统造成危害,安全威胁是四元组(D,M,A,L)。危害级别 G 是对安全威胁可能造成的破坏等级的评估。

$$G = (D,M,A,L) \tag{1}$$

必须明确标识所有安全威胁和需要保护的应用与资源,通过分析不同安全威胁对不同应用与资源的破坏程度,应用与资源对破坏的时间、经济敏感度,区分应用与资源的优先级。这对于 DRP 非常重要。

1.3　灾难恢复计划

DRP 通过有序的计划应对意外灾难,它包含许多子灾难恢复计划(SDRP,Sub DRP)。DRP 需要与 DRC、RA、SS 和 SM 交互,它协助 SM、DRC 管理、控制和维护 DRS;它协助 SS 模拟灾难,发现系统的不足,不断完善系统。RA 对安全威胁、资源及其优先级分析完成后,就可以开始 DRP 了。虽然 DRP 至关重要,目前人们却更侧重于开发灾难恢复的软硬件工具,而在 DRP 方面的研究还远远不够。EEDP 的经验证明:设计一个好的 DRP 是非常重要的,同时也是非常困难的。

DRP 包括商业影响分析和恢复计划设计。商业影响分析研究某个应用或资源的中断对其它应用的影响。主要有两个度量:一个度量是某个应用或资源崩溃后,其它应用还能持续正常运行的最大时间;另一个度量是恢复崩溃应用需要占用的资源。应该尽量要找到两者的最佳接合点,优化灾难恢复。恢复计划设计涉及灾难恢复中的许多策略和计划,例如数据备份策略,组建救援维护小组,资源维护计划,权衡维护或替换损毁设备的代价等。

必须确保 DRP 中没有遗漏任何重要资源,保证所有 SDRP 需要的人力、物力、甚至时间等资源是都可行的,不同 SDRP 之间不会产生冲突。信息系统在灾难发生时出现的故障具有大批量的特点,因此在 DRP 的设计中应制订排除大量并发网络和系统故障的计划。必须避免 SDRP 单独可行,不同 SDRP 在相同时刻却由于资源竞争冲突导致它们在一起时却不可行这种现象。由于 DRS 本身固有的复杂性,仅凭直觉

和经验要从众多可选的 SDRP 中选择最优的子集用于灾难恢复几乎是不可能的,因此,迫切需要对 DRP 进行深入研究,建立数学模型,对 DRP 进行精确量化的分析,帮助决策者控制灾难恢复[12]。此外,作为一种特殊的项目,DRS 也具有所有项目的共性,这意味着很可能由于不可预见的因素 DRP 中某些部分会失败,从而影响灾难恢复。

1.4 灾难恢复控制

借助于 DRP、SM 的帮助,DRC 最终实现灾难恢复。正常情况下业务运行在数据中心,当数据中心某些子系统发生故障时,系统会自动快速切换到数据中心的正常设备,实现本地故障恢复。当数据中心崩溃时,备份中心会接管数据中心继续提供服务,同时,DRC 广泛采集各方面的数据,控制系统从灾难中恢复过来。数据中心修复后,备份中心将数据和运行状态同步回数据中心,将业务处理切换回数据中心。系统由正常工作状态进入灾难恢复状态有自动控制和人为控制两种方式,让 DRS 自动区分瞬时故障与灾难是非常困难的,因此,通常需要人为控制使系统进入灾难恢复状态。

根据系统安全需求,备份中心应与数据中心保持足够远的距离,并且使用足够的带宽相互连接;备份中心必须具备足够的计算能力接管数据中心的业务;两个中心之间应用的切换必须快速可靠。EEDP 中备份中心建设在五百公里之外,通过 622Mb/s 带宽链路与数据中心相连,两个中心的配置基本相同,并且同时运行相同的软件,以减少灾难发生时备份中心装载软件所带来的延迟,实现迅速切换。

通信安全事关灾难恢复的成败。出于安全原因,目前中国政务涉密网禁止使用无线计算机网络。EEDP 中结合密码技术,使用多种有线、无线通信系统保障安全可靠的通信。必须在网络中保持适当的冗余,由于 PSTN 拥有大量的冗余节点和链路,结合密码技术,有时它反而比专线通信更安全。

1.5 模拟与监测

SS 包括灾难模拟和系统监测。SS 与 DRP、SM 和 DRC 交互,通过 2D、3D 操作平台模拟灾难,或者根据以往灾难中采集的数据重放灾难。模拟结果会反馈给 CT、DRP、SM、DRC,在灾难前及早发现、解决 DRS 中技术、管理、协作等方面存在的问题。

系统监测用于不断发现和排除系统在功能、性能和安全方面的隐患。作为一个健壮的系统,DRS 需要运行在安全的环境中,这就需要本地和远程攻击监测。EEDP 中就部署了很多防病毒、防火墙、入侵监测、日志审计等系统。此外,SS 中还包括网络性能监测、安全性能监测和业务性能监测等。

需要格外注意的是由于对 DRP 进行完整的测试非常困难,因此首先必须集中监测 DRP 中的所有 SDRP,保证所有 SDRP 单独可行。在此基础上根据实际情况尽量制订多种联合监测方案,确保多个 SDRP 在一起时也是可行的,从而在某种程度上确保 DRP 的有效性。

1.6 系统管理

与 CT 一样,SM 也是非常重要,而又容易被忽视的环节,DRS 往往由于管理上的缺陷而导致整个系统达不到预期目标。EEDP 特别加强了这一环节,除日常使用、维护人员外,还建立了专业的应急事件响应小组,制订了应急事件响应工作流程框架。采用良好的管理工具更有助于管理各环节中的资源和灾难恢复的实施。必须牢记:技术不能解决一切问题,管理同样非常重要。

2 案例分析

建设 DRS 之前,必须深入研究系统需求、需要应对的灾难、需要保护的资源及系统弱点。EEDP 必须能够应对众多人为、自然因素灾难[1,13],尤其是 National Research Council 重点强调的恐怖主义袭击,它们破坏性巨大,而且在灾难恢复过程中还继续存在人为干扰和破坏。EEDP 的网络连接如图 2,系统由 ATM 交换机构成主干网,连接下级政府部门、上级政府部门和它的异地分支部门、异地备份中心。通过专线电话、PSTN、无线电话网、有线计算机网络和卫星通信提供可靠的通信保障。EEDP 的 DRS 在灾难发生后能够实时完成系统切换、通信、指挥、调度操作;结合密码技术,实现系统数据、通信、指挥控制等的认证、保密性、完整性和抗抵赖性;提供详尽的灾难恢复计划,以迅速、适当地应对灾难;使用 GIS 和 DSS,使 DRS 更易于使用、管理和维护。

当数据中心崩溃后,即使立即实现它与备份中心之间的切换,仍需要一定的收敛时间网络才能够达到新的稳定状态。收敛时间指从网络拓扑结构发生变化到网络上所有相关路由器都得知这一变化,并相应做出改变所需要的时间。收敛时间越短,网络变化对全网的扰动就越小。OSPF 是一种内部网关协议,它允许路由器在自治域内部交换路由信息。它在邻居之间交换链路状态信息建立链路状态数据库,利用最短路径优先算法计算路由表。在稳定的网络中,更新信息以预定时间发送,但在网络中发生变化时,链路状态表会通过扩散立即更新,实现网络拓扑变化时迅速收敛。此外,OSPF 还支持大型网络、负载均衡、变长子网掩码,并且带宽占用率低[14]。由于 EEDP 网络覆盖范围广,包含多于 30 个节点,每个节点又包含 1 至 4 个主干路由器,因此选用 OSPF 作为路由协议。

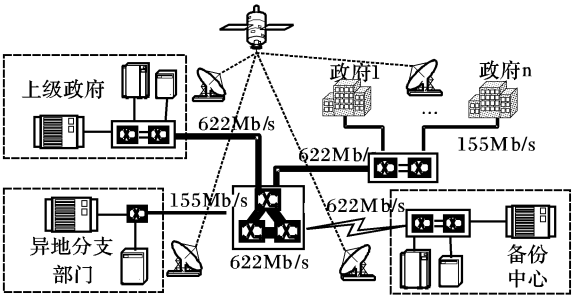

图 2 EEDP 网络连接

需要进一步分析网络收敛时间和应用系统的性能。然而对于如此复杂的系统,考虑到安全、应用等多方面的原因,在实际系统中进行灾难恢复实验是不现实的,只能进行仿真实验,分析系统的收敛时间和应用系统的性能。由于系统中几乎所有应用都需要数据库支持,并且绝大多数应用基于 Web 浏览器,因此需要使用 HTTP 协议。电子邮件同样是系统中非常重要的应用,此外还有不少应用系统使用 FTP 协议进行文件传输。因此 EEDP 的网络通信流量主要被数据库应用、HTTP、Email 和 FTP 所占用。我们使用 OPNET 对整个 EEDP 网络建模。模型中包含 35 个节点,仿真多个政府部门。每个节点根据其位置不同,包含 1 至 4 个主干路由器。根据具体情况,每个节点中包含 50 至 200 个用户。每个节点都包含数量不等的数据库、Web、E-mail 和 FTP 服务,为本节点和网络中其它节点的用户提供服务。

在研究网络收敛时间时,设置仿真系统中所有路由器使用 OSPF 协议,协议的 Hello 分组间隔时间为缺省的 10s,重传间隔为 5s,分别研究系统中每个节点在运行中崩溃,由此引发的网络收敛情况,共 35 个仿真场景。图 3 显示系统中 35 个节点分别崩溃时的收敛时间,其中收敛时间的最小值为 57.29s,最大值为 74.10s,平均收敛时间为 63.35s。由此可知网络收敛时间能够满足设计要求。

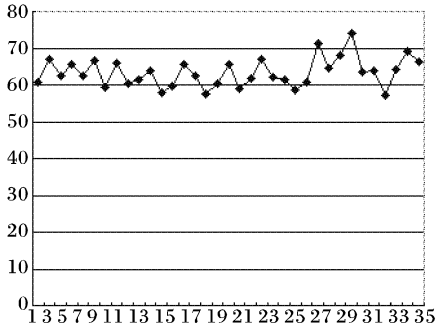

图 3　网络收敛时间

还需要进一步研究系统中应用的性能,这里我们主要分析不同应用的响应时间。设置仿真运行时间为两小时,在仿真运行一小时后,数据中心节点永久性崩溃,与此同时,启动备份中心节点,研究整个过程中应用的响应时间变化情况。

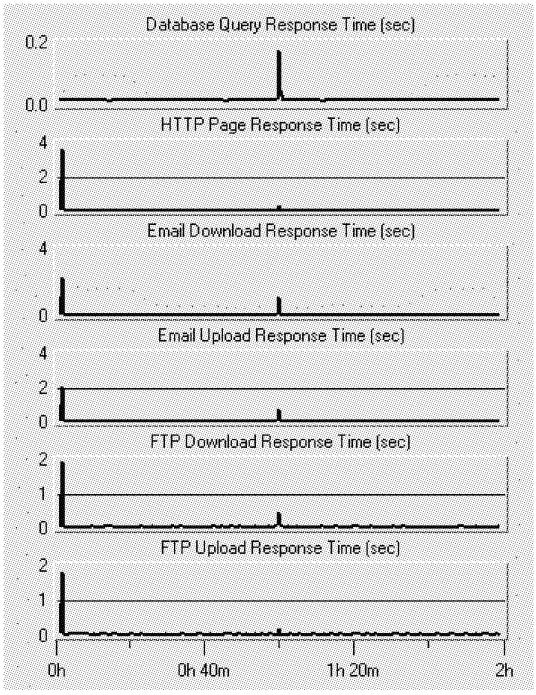

图 4　应用响应时间

仿真结果如图 4 所示。在仿真稳定后,系统的数据库查询响应时间约为 0.015s,HTTP 页面响应时间约为 0.08s,接收和发送电子邮件的响应时间约为 0.071s 和 0.06s,FTP 上传和下载响应时间约为 0.045s 和 0.06s。在数据中心节点崩溃后,网络没有达到收敛状态期间,应用系统对网络中位于不同节点中不同用户的响应时间差异巨大,对有的用户响应时间较快,对有的用户响应时间较长,平均响应时间均不同程度增加。其中数据库查询响应时间最大增至 0.173s,HTTP 页面响应时间最大增至 0.3s,接收和发送电子邮件的响应时间最大增至 1.092s 和 0.72s,FTP 上传和下载响应时间最大增至 0.442s 和 0.17s。在此次仿真中,经过约 66.42s 后网络收敛,各应用系统平均响应时间逐渐恢复正常。仿真结果证明在灾难发生后,系统应用性能也能够满足要求。

3　结语

根据某电子政务试点示范工程的要求,论文提出健壮的灾难恢复系统模型。模型的自我监测和实时可视平台使 DRS 更易于使用、管理和维护;模型加强了安全性与健壮性,适用于安全级别较高的环境。在 RDRSM 的指导下,该电子政务工程的灾难恢复系统已经建设完毕并且投入运行,仿真实验和实践验证了模型的可行性。

参考文献:

[1] LAM W. Ensuring business continuity[J]. IT Professional, 2002, 4(3): 19-25.

[2] KUWATA Y, SHINJOH A. Design of robocup-rescue viewers-towards a real world emergency system[J]. Lecture Notes in Computer Science, 2001, 2019: 159-168.

[3] YONG C, NI LM, XU CZ, *et al.* CoStore: A reliable and highly available storage system using clusters[A]. Proceedings of 16th Annual International Symposium on High Performance Computing Systems and Applications[C]. Los Alamitos, CA, USA: IEEE, 2002. 3-11.

[4] CHEN Y. CoStore: A Storage Cluster Architecture Using Network Attached Storage Devices[D]. PhD, Michigan State University, 2002.

[5] UDDIN N, ENGI D. Disaster management system for southwestern Indiana[J]. Natural Hazards Review, 2002, 3(1): 19-30.

[6] EHRLICH RL, DRONEBURG JW. Preparing for an Emergency: COOP Planning for State Agencies[EB/OL]. http://www.umaryland.edu/healthsecurity/docs/Manual%20Final.pdf>, 2004.

[7] MYERS BJ. A Software System for User Application Tolerance of Network and Computing Node Failures[D]. PhD, University of Houston Clear Lake, 2002.

[8] LIU BJ, CAO F, ZHOU MZ, *et al.* Trends in PACS image storage and archive[J]. Computerized Medical Imaging and Graphics, 2003, 27(2-3): 165-174.

[9] LIU BJ, CAO F, DOCUMET L, *et al.* A fault-tolerant back-up archive using an ASP model for disaster recovery[A]. Proceedings of SPIE-The International Society for Optical Engineering[C]. San Diego, CA, USA: The International Society for Optical Engineering, 2002. 89-95.

[10] WANG K, SU RD, LI ZX, *et al.* Study of secure complicated information system architecture model[A]. Proceedings of 1st International Conference on Semantics, Knowledge and Grid[C]. Beijing, China: IEEE, 2005. 893-889.

[11] 国家信息安全工程技术研究中心,国家信息安全基础设施研究中心. 电子政务总体设计与技术实现[M]. 北京: 电子工业出版社, 2003.

[12] WANG K, YIN ZH, YUAN F, *et al.* A mathematical approach to disaster recovery planning[A]. Proceedings of 1st International Conference on Semantics, Knowledge and Grid[C]. Beijing, China: IEEE, 2005. 485-491.

[13] FALLARA P. Disaster recovery planning[J]. IEEE Potentials, 2004, 22(5): 42-44.

[14] YAN BY, LU W, HUANG R. A study on OSPF routing protocol [J]. Journal of Sichuan University (Natural Science Edition), 2002, 39(3): 460-464.