

基于 IPv6 的 Internet 存储服务模型

吴英, 徐敬东, 吴功宜, 刘璟

(南开大学信息技术科学学院, 天津 300071)

摘要: 针对用户对远程数据存储与异地数据备份的需求增加, 提出一种基于 IPv6 协议的 Internet 存储服务模型。设计应用层的 Internet 存储访问协议, 结合 IPv6 协议的安全性特点设计安全存储模型, 为下一代互联网提供一种标准、安全的远程存储服务。

关键词: Internet 存储服务; Internet 存储访问协议; IPv6 安全存储模型

Internet Storage Service Model Based on IPv6

WU Ying, XU Jing-dong, WU Gong-yi, LIU Jing

(College of Information Technical Science, Nankai University, Tianjin 300071)

【Abstract】 With rapid increase of the requirement for remote data storage and backup, this paper proposes an Internet storage service model based on IPv6. It designs an Internet storage access protocol in application layer, and proposes a secure storage model based on the features of IPv6. The goal is to provide a standard and secure remote storage service for the next generation Internet.

【Key words】 Internet storage service; Internet storage access protocol; IPv6 secure storage model

1 概述

进入 21 世纪, 网络已广泛应用于社会生活各个方面, 政府部门、金融机构、企业的信息安全成为影响社会稳定的重要因素。保证关键业务的可持续性对这些机构至关重要。即使在信息技术应用水平较高的美国, 网络与信息系统的安全性也存在很大问题。造成业务非计划性中断的原因主要有: 自然灾害, 恐怖活动, 网络攻击, 病毒与内部人员破坏等。这些突发事件可能造成系统硬件、软件损坏与数据丢失等。成功的业务持续性评价标准是如何在系统故障时以最短时间恢复数据访问能力。支持业务持续性的核心技术是数据的异地存储与备份技术。

图灵奖获得者 Jim Gray 曾提出类似的经验定理: 网络环境中每 18 个月新产生的数据量等于之前产生的数据量之和^[1]。数据量的急剧增加带动存储技术不断革新, 直接附加存储(DAS)系统在存储性能与扩展性方面已不能满足要求, 近年出现了网络附加存储(NAS)、存储区域网络(SAN)与分布式存储等新技术。为了适应网络存储数据量的剧增、用户使用存储系统的数量与普及程度增加, 以及对存储系统性能与安全性的更高要求, 本文充分利用 IPv6 协议功能与安全性方面的优势, 参照标准 Internet 网络服务的设计方法, 把对存储系统的远程访问设计成一种在下一代 Internet 中运行的、标准的、安全的服务类型。

2 相关研究

本文涉及的研究领域是存储技术与网络技术的交叉。存储技术研究主要集中在 2 个方面: 分布式存储技术与网络存储协议。其中, 分布式存储系统是指构成存储系统的磁盘资源的分布性。目前, 分布式存储方面的研究主要集中在系统结构、数据布局与性能分析。这类课题的研究思路是利用软件代替专用硬件将 I/O 操作分散到网络中的多个节点, 并且大多采用分布式文件系统设计。

分布式文件系统在 20 世纪 90 年代初成为研究热点, 这

个阶段比较有名的研究课题包括: 无服务器结构的 xFS^[2], 基于 Petal 系统的 Frangipani^[3], 基于 Linux 集群的 PVFS^[4], 侧重于数据布局的 RAID-x^[5]。目前, 比较新的研究课题包括: SAN 文件系统 Storage Tank^[6], 基于对象技术的 Lustre^[7]。这类分布式存储系统多数仍处在实验阶段, 并未成为成熟的存储系统投入商业运行。2000 年后, 从事存储研究的课题组多数已转向 P2P 与网格方面。

网络存储协议的研究主要集中在 iSCSI, iFCP 与 FCIP。这类课题的研究思路是利用 IP 协议封装 SCSI 或 FC 协议, 在 Internet 环境中提供对 SAN 的远程存储访问, 针对的存储系统主要是基于光纤通道的 SAN, 例如用 iSCSI 或 iFCP 构建 IP-SAN、存储性能与安全性研究。当前缺乏存储系统访问手段方面的研究, 无法满足用户使用、维护存储系统的便捷性要求。

IPv6 是本文的另一个相关研究领域。IPv6 协议的主要特征为: 新的协议格式, 巨大的地址空间, 有效的分级寻址与路由结构, 有状态与无状态的地址自动配置, 内置的安全机制, 更好地支持 QoS 服务。IPv6 有 2 个特点有利于远程存储服务, 即地址结构与 IPsec 安全功能。国内外的 IPv6 相关研究主要集中在工作机制、安全问题、移动 IPv6 与 QoS 等方面。目前, 还没有将 IPv6 与存储服务相结合的研究。

3 存储服务的提出

网络存储技术的研究曾经有 2 种思路。存储技术研究人员的思路为: 在早期的磁盘冗余阵列(RAID)研究的基础上, 由 DAS 技术发展到 NAS, SAN 和基于 IP 的分布式存储。网络技术人员在早期 OSI 参考模型的应用层设计中, 试图将网络环境中的数据存储作为一种标准服务, 就像 FTP,

作者简介: 吴英(1973-), 男, 讲师、博士, 主研方向: 网络安全, 网络存储, 分布式计算; 徐敬东、吴功宜、刘璟, 教授、博士生导师

收稿日期: 2007-12-10 **E-mail:** wuying@nankai.edu.cn

Telnet, WWW 等服务一样, 在应用层制订相应的 FTAM(File Transfer Access and Management)协议, 并在此基础上开展网络数据存储服务研究。但是, OSI 参考模型在与 TCP/IP 协议的竞争中失利, 可用于网络存储的 FTAM 协议没有继续发展。

面对 Internet 应用范围的进一步扩大, 网络存储研究面临的形势也将发生变化, 主要表现在: 网络数据存储量急剧增加; 网络数据存储安全性要求越来越高; 用户将从大型信息系统中重要的政务、商务数据、大型网站的异地存储与备份发展到中小型企业的信息系统, 甚至个人信息的存储与备份, 使用网络存储服务的用户面快速拓宽; 用户对存储系统使用、维护的便捷性要求提高。这时, 可以借鉴 OSI 参考模型研究在应用层将数据存储作为标准服务的思想, 将专用的存储服务与系统研究转变为可以在下一代 Internet 中运行的标准服务研究。

本文将数据存储作为一种标准 Internet 服务来研究, 在协议设计中需要注意屏蔽具体使用的存储系统与设备差异性, 减小存储服务对存储系统硬件与软件的依赖, 增加存储系统使用、维护的便捷性与安全性, 以适应更大规模的网络存储应用发展的需要。同时, IPv6 协议的优势已开始被认识到, 并作为信息技术发展的重要方向得到国家支持。社会需求、前期研究基础、技术储备与发展水平为把网络存储设计成一种标准 Internet 服务提供了必要性与可行性。

4 模型与系统设计

Internet 存储服务的应用对象是远程数据存储与异地数据备份。通过分析得到以下 4 点服务需求: 在下一代互联网环境中实现安全的远程数据存储; 适用于 IPv6 网络平台上的固定与移动用户; 客户使用标准的客户端软件便捷地访问存储系统; 保证标准的存储服务与存储系统类型的无关性。

4.1 Internet 存储服务模型

在分析存储服务需求与运行环境的基础上, 为了实现向用户提供标准 Internet 存储服务, 首先要确定这种存储服务模型的基本设计原则: 用户对存储系统的访问方法与存储系统的实现技术、系统结构与实际位置无关。

图 1 给出了 Internet 存储服务模型, 包括 3 个部分: Internet 存储服务器, 前台的客户端系统与后台的存储系统, 采用 3 层结构的工作模式。其中, 客户端系统是用户访问存储系统的接口, 负责接收与处理用户发送的存储服务请求, 等待存储系统执行访问命令并返回处理结果; Internet 存储服务器的作用相当于代理服务器, 负责完成客户端对存储系统的访问功能, 实现客户端系统与存储系统在逻辑上的隔离; Internet 存储服务器采用 Client/Server 结构, 客户端与服务器的进程通信采用状态保持方式。

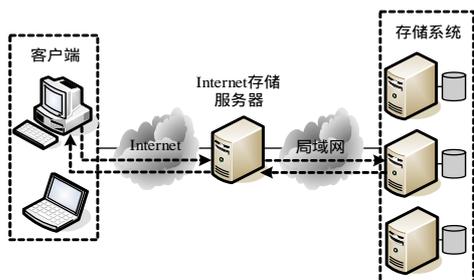


图 1 Internet 存储服务模型

4.2 Internet 存储访问协议

Internet 存储访问协议(Internet Storage Access Protocol,

ISAP)是针对 Internet 存储服务提出的, 它符合 OSI 参考模型对应的层次结构。ISAP 协议模型采用 Client/Server 结构。前台客户端可以称为 ISAP 客户机, Internet 存储服务器称为 ISAP 服务器。图 2 给出了 ISAP 协议模型。ISAP 协议模型在各层都选择或制定了协议, 应用层采用针对存储服务设计的 ISAP 协议, 传输层选择支持有连接服务的 TCP 协议, 网络层选择支持下一代 Internet 的 IPv6 协议。

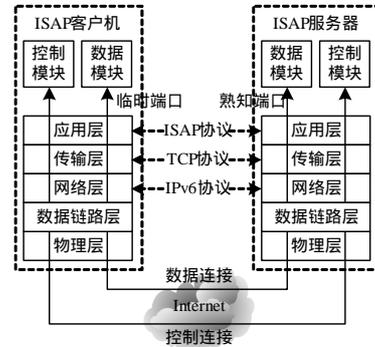


图 2 ISAP 协议模型

由于这种存储服务的数据量大而控制信息相对较少, 因此 ISAP 协议将通信分为控制连接与数据连接分别处理。控制连接负责完成用户连接、身份认证与异常处理等控制操作; 数据连接负责完成文件数据的传输。采用 2 种类型连接的优点是: 协议设计与实现简单, 文件数据与协议命令互不干扰。ISAP 协议对通信连接的建立与释放有严格规定。控制连接与数据连接必须事先建立, 控制连接必须在数据连接之前建立, 控制连接必须在数据连接之后释放。只有建立数据连接后才能传输数据, 并在传输过程中保证控制连接不中断。

ISAP 客户机与 ISAP 服务器之间通过不同端口建立 2 种连接。由于 Internet 存储服务在传输层采用 TCP 协议, 因此需要为该服务申请熟知的 TCP 端口号。ISAP 客户机与 ISAP 服务器的端口使用规则不同。ISAP 服务器通过熟知的控制端口与数据端口提供服务。ISAP 客户机只能用临时分配的端口与 ISAP 服务器建立连接。按照 RFC1700 文档对熟知端口号的分配原则, 向 IANA 提出标准 Internet 存储服务应用层协议的熟知端口分配建议。

ISAP 协议的工作流程分为 3 个阶段: 连接建立, 数据传输与连接释放。协议严格规定了各个协议阶段的实现顺序以及各个阶段中协议动作的实现顺序。它还规定了用于 ISAP 客户机与 ISAP 服务器通信的协议命令, 它包括命令名、书写格式与相关参数等。另外, 协议命令分为命令与响应 2 种类型。

4.3 IPv6 安全存储模型

Internet 存储服务在开放的 Internet 环境中提供, 开放性的特点造成 Internet 安全状况很差, 各种类型的网络攻击层出不穷, 因此安全性方面的研究相当重要。网络攻击对数据的影响主要分为窃听、截获、篡改与伪造。窃听与截获数据并不是安全模型所能解决的, 但可以通过加密防止数据内容泄漏。篡改与伪造数据是安全模型重点要解决的, 可以通过数据完整性认证验证数据是否被篡改, 通过身份认证方式验证数据的真实来源。

Internet 存储服务是一种安全可靠的存储服务, 不能像匿名 FTP 服务那样允许任何用户访问, 只能为通过身份认证的合法用户提供服务, 对合法用户也要进行访问权限控制。针

对 Internet 存储服务提出的 IPv6 安全存储模型符合 OSI 参考模型对应的层次结构。图 3 给出了 IPv6 安全存储模型。应用层协议提供用户身份认证与访问权限控制功能；网络层充分利用 IPv6 地址结构的优势，与 IPSec 协议结合提供安全功能。

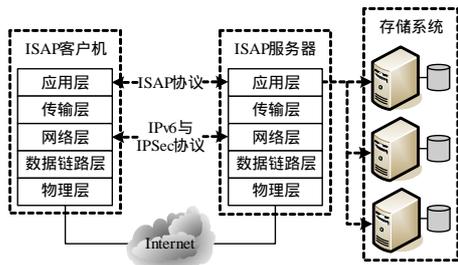


图 3 IPv6 安全存储模型

网络层的安全设计首先表现在 IPv6 地址类型的选择。地址选择的根据是将后台存储系统与外界隔离，所有用户只能通过 ISAP 服务器访问存储系统。ISAP 服务器的设计思路与代理服务器相似。根据 RFC3513 的相关规定，充分利用 IPv6 地址结构的特点，在客户端与 ISAP 服务器之间、ISAP 服务器与存储系统之间，使用不同 IPv6 地址类型限制外部节点访问存储系统，实行 IPv6 地址与 MAC 地址绑定，将无状态与有状态地址自动分配相结合，从网络层保证系统的安全性。

IPSec 是网络层的一组安全协议集，主要包括 AH 协议、ESP 协议与密钥管理协议。其中，AH 与 ESP 协议分别实现认证与加密服务；密钥管理协议为通信双方协商加密与认证所需参数。AH 与 ESP 协议被设计成与算法无关，可以使用 IPSec 认可的认证与加密算法。根据 RFC2401 与 RFC2402 的相关规定，结合 IPv6 头部结构与认证头部 AH，实现客户端 IP 地址、数据包完整性认证和抗数据包重放功能。利用 IPSec 安全关联与安全策略设计方法，设计客户端与 ISAP 服务器之间会话连接的动态安全策略、保障机制与工作模型。

(上接第 97 页)

定位精度^[3]是评价一个定位算法的首要指标。定位误差是指节点的估计位置与实际位置之间的欧氏距离，而定位精度一般指定位误差与节点无线射程的比值(式(4))。如图 4 所示，ATDV-Hop 算法的定位精度比 DV-Hop 算法的定位精度有较大降低，仿真结果显示，当区域内有 200 个节点时定位精度下降比例为 6.27%，300 个节点时为 7.32%，400 个节点时为 9.78%，500 个节点时为 11.80%，平均定位精度降低 8.79%。

$$\text{定位精度} = \frac{\text{定位误差}}{\text{节点无线射程}} = \frac{\sqrt{(X_{\text{实际}} - X_{\text{估计}})^2 + (Y_{\text{实际}} - Y_{\text{估计}})^2}}{R} \quad (4)$$

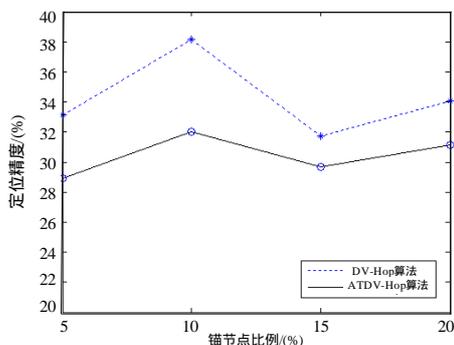


图 4 定位精度

4 结束语

仿真结果表明 ATDV-Hop 算法比 DV-Hop 算法在可定位

5 结束语

工作效率与安全性的矛盾是必须考虑的问题。在下一代 Internet 中，网络带宽对工作效率的影响会降到次要位置，系统效率瓶颈会转移到 Internet 存储服务器。这种存储服务的特点是短时间、大数据量传输，Internet 存储服务器对客户端与存储系统读写操作的处理能力很重要，提高安全性的代价将转移到 Internet 存储服务器。类似于代理服务器的节点负载均衡问题，目前已有很多研究与成熟技术，在这方面可以加以参考和利用。另外，需要深入研究协议自身安全性与系统防攻击能力。

参考文献

- [1] Gray J. What Next? A Few Remaining Problems in Information Technology[Z]. (1998-01-11). http://research.microsoft.com/~gray/talks/Gray_Turning_FCRC.pdf.
- [2] Anderson T E. xFS: A Wide Area Mass Storage File System[C]// Proceedings of the 4th Workshop on Workstation Operation Systems. Napa, CA, USA: [s. n.], 1993-10: 71-78.
- [3] Thekkath C A, Mann T, Lee E K. Frangipani: A Scalable Distributed File System[C]// Proceedings of the 16th ACM Symposium on Operating System Principles. [S. l.]: ACM Press, 1997-10: 224-237.
- [4] Carns P H, Ligon W B, Ross R B. PVFS: A Parallel File System for Linux Clusters[C]// Proceedings of the 4th Annual Linux Showcase and Conference. [S. l.]: IEEE Press, 2000-10: 317-327.
- [5] Hwang Kai, Jin Hai, Ho R. A New Distributed RAID-x Architecture for I/O-Centric Cluster Computing[C]// Proceedings of the 9th IEEE Symposium on High Performance Distributed Computing[C]. [S. l.]: IEEE Press, 2000-08: 279-286.
- [6] Menon J, Pease D A, Rees R. IBM Storage Tank: A Heterogeneous Scalable SAN File System[J]. IBM Systems Journal, 2003, 42(2): 250-267.
- [7] Cluster File Systems Inc.. Lustre: A Scalable High-performance File System[Z]. (2002-11-12). <http://www.lustre.org/docs/whitepaper.pdf>.

节点比例上提高了 24.05%，而平均定位精度降低了 8.79% (即定位误差降低 8.79%)，说明 ATDV-Hop 算法是一种优于 DV-Hop 算法的较好算法。当然 ATDV-Hop 算法在节点数量较小锚节点比例较低的情况下优势并不明显，这是由于在这种情况下可供选择锚节点数量较少有关。当节点数量增多时 ATDV-Hop 明显优于 DV-Hop。同时基于角度阈值的锚节点选择策略也同样适用于 Amorphous, APIT, DV-distance, Euclidean 和质心定位算法。

参考文献

- [1] Ren Fengyuan, Huang Haining, Lin Chuang. Wireless Sensor Networks[J]. Journal of Software, 2003, 14(2): 1148-1157.
- [2] Weiser M. The Computer for the 21st Century[J]. Scientific American, 1991, 65(3): 94-104.
- [3] 王福豹, 史龙, 任丰原, 等. 无线传感器网络中的自身定位系统和算法[J]. 软件学报, 2005, 16(5): 857-868.
- [4] 孙利民, 李建中, 陈渝, 等. 无线传感器网络[M]. 北京: 清华大学出版社, 2005: 135-155.
- [5] Niculescu D, Nath B. DV Based Positioning in Ad Hoc Networks[J]. Journal of Telecommunication Systems, 2003, 22(1-4): 267-280.
- [6] Niculescu D, Nath B. Ad-Hoc Positioning Systems[C]// Proc. of the 2001 IEEE Global Telecommunications Conf.. [S. l.]: IEEE Communications Society, 2001: 2926-2931.