分类号 _____ 密级_____

UDC _____

学 位 论 文

P2P 技术研究及其在计量管理系统中的应用

作 者 姓 名： 李海珍

指 导 教 师： 高福祥 教授

东北大学计算机系统研究所

申请学位级别： 硕士 学 科 类 别： 专业学位

学科专业名称： 计算机技术

论文提交日期： 2007 年 12 月 8 日 论 文 答 辩 日 期： 2008 年 1 月 21 日

学位授予日期： 答辩委员会主席： 夏利

评 阅 人： 史岚、刘浪涛

东 北 大 学

2007 年 12 月

A Thesis for Master Degree in Computer Technology

Study on P2P Technique and Its Application in Metering Management System

by LI Haizhen

Supervisor: Professor GAO Fuxiang

Northeastern University

December 2007

独创性声明

本人声明，所呈交的学位论文是在导师的指导下完成的。论文中取得的研究成果除加以标注和致谢的地方外，不包含其他人已经发表或撰写过的研究成果，也不包括本人为获得其他学位而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文作者签名：李海玲

日　　期：2008.1.23

学位论文版权使用授权书

本学位论文作者和指导教师完全了解东北大学有关保留、使用学位论文的规定：即学校有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。本人同意东北大学可以将学位论文的全部或部分内容编入有关数据库进行检索、交流。

（如作者和导师不同意网上交流，请在下方签名；否则视为同意。）

学位论文作者签名：　　导师签名：

签字日期：　　签字日期：

P2P 技术研究及其在计量管理系统中的应用

摘 要

随着信息技术的飞速发展，企业信息化建设已成为企业在全球化竞争时代的生存之道。计量检测和管理水平是衡量一个企业技术水平的重要尺度，将网络、数据库和 P2P 等先进的计算机信息技术用于计量管理，对企业提高产品质量、降低成本、增加经济效益至关重要。

本文在对首钢计量管理工作进行深入调查的同时，主要研究了现有的几个计量管理系统，包括：ERP（物资计量网）、电力网以及企业计量信息系统之间资源共享问题。为了充分利用现有几个系统的资源，更好地为企业管理者提供计量决策依据，提出了 P2P 在计量管理系统中的设计应用。

论文首先从现代计量管理系统引进的背景、需求和意义谈起，然后，重点介绍了 P2P 技术如何在诸多计量管理系统之间进行系统架构，实现资源共享。体系架构部分从计量管理工作各个模块功能分析着手，给出了系统模块协作完成计量管理目标的流程，并对实现方法做了详细的说明；安全性考虑部分介绍了 P2P 存储系统的引入，为企业计量管理系统间协作提供了技术支持。最后，论文对 P2P 技术在计量管理系统中的应用设计进行了总结。

关键词：P2P；计量；应用

Study on P2P Technique and Its Application in Metering Management System

Abstract

With the rapid development of information technologies, information construction becomes the determinate factor for enterprises in the future. The maturity of measurement and management is a key point to evaluate a company's technical level. Using the advanced technology like networks, database and P2P on metering management is very important for enterprises to improve production quality, decrease cost and increase benefit.

After studying the management of Shougang Corporation, some problems of resource sharing among existed metering management systems like ERP(Material Computation Network), Power Network and MISare discussed in this thesis. The thesis proposed the metering management on which P2P is applicated for using resource in the existed systems. It provides manager ways to make policy.

In this thesis,the background, requirements and significance of metering management systems are firstly introduced, then the benefits of importing P2P into architechture of collaborated multiple metering management systems to share resource are explains. Functions of each module are analysed in the architecture section. The flow of modules achieving the target interactedly is proposed and the implementation method is analysed detailedly. Importing of P2P storage systems which provides technical support for the collaboration of metering management systems is introduced in security consideration. Summary of the application design on P2P-based metering management system is also presented at last.

Key words: P2P; Metering Management; Application

目 录

6

第1章 引 言

1.1 背景

计量，过去在我国称之为“度量衡”，其原始含义是关于长度、容积和质量的测量，主要器具是尺、斗和秤[1]。原是物理学的一部分，随着科技、生产和社会的发展，计量的概念和内容也在不断地扩展和充实，并逐渐形成了一门学科——计量学。

计量学，是关于计量理论与实践的知识领域，是一门综合性的学科，是现代科学的重要组成部分，发展至今，已从自然科学扩展到了社会科学[2]。计量作为现代社会不可缺少的技术基础，是体现工业企业素质及其管理现代化的基本条件之一，计量技术在一定意义上标志着国家的科技和经济发展水平。

计量工作是经济建设、科学进步和社会发展的重要技术基础。

计量管理工作是各项工作的基础，是企业管理、生产、经营决策的一个重要环节。要加强企业管理，就应首先从加强计量管理工作入手，使企业的生产经营、成本核算有一个较科学的依据和法律依据，做到“数出一家，量出一门”。因此说，“加强计量管理是转换企业经营机制、提高经济效益的有效途径”[3]。

计量工作在企业生产中的重要作用集中反映在保证产品质量上，而产品质量是企业生产技术、经营管理水平的综合反映。产品质量的特征是以一定计量数据特性来表征的。并且是在生产控制中依靠完善的计量检测实现控制的。如果现在还依靠传统方法管理企业的计量工作，将不可能使产品质量稳步提高，无法提高企业的经济效益。俗话说：“计量”就是“计钱”，充分体现了计量工作在企业中的重要性。计量管理就是运用科学手段正确反映客观事物“量”的信息工作，计量的产品是事物“量”的信息流。

随着中国加入 WTO 和市场经济的进一步深化和发展，钢铁企业面临着越来越严峻的竞争考验。企业要在竞争中立于不败之地，采用规范化的管理手段，建立高效的管理信息系统（MIS）是企业的必然选择。

但是，近几年来，首钢面对前所未有的压力和挑战和前所未有的发展机遇。2005 年 2 月国务院批准了首钢搬迁调整方案，总公司党委审时度势，重新确定了以钢铁业为核心产业，实施“一主四优”的战略决策，向北京以外地区开辟新的发展空间，先期启动迁钢公司、首秦公司建设，顺义冷轧 2005 年 7 月开工建设，目前已进入设备安装阶段，即将于今年底投产。2007 年 3 月首钢京唐钢铁厂正式开工建设，标志着首钢搬迁调整进入全面推进的新阶段。

近年来逐渐形成了以首钢北京总部经济为核心，以信息化为支撑，构建产权结构多

元化、对外开放合作更加广泛的现代企业制度和管理架构，确立了“一业多地”的管理体制。建设21世纪的新首钢，必须做到“管理一流”。新世纪、新阶段的首钢计量管理工作同样面临着前所未有的压力、挑战和发展机遇。

首钢近年来面临“一业多地”的管理模式要求，对MIS提出了更高的要求，计量管理工作包括计量标准量值传递管理、物资计量、能源计量以及计量结算数据等的技术基础工作。近年来首钢在信息系统方面做了些工作，成立了信息部，并有首自信公司提供技术支持，建立了ERP（现仅限于物资计量管理）、电力网（仅限于能源电量的数据统计管理），并引入了企业计量信息系统（用于计量标准量值传递），但其功能还远远不能满足首钢“一业多地”的信息管理要求。特别是，现有的这几个信息系统都是“独立作战”，未能做到数据共享，无法进行数据动态控制，更谈不上“管理一流”。

1.2 需求

党的“十六大”报告提出了“以信息化带动工业化”的战略方针，首钢作为国家特大型企业积极响应国家号召，大力进行信息化改革。

要建设现代化大型企业，在科学、严格、规范、精细管理上需要不断夯实基础，提高水平。

从宏观形势看，我国经济已进入“立足科学发展、着力自主创新、完善体制机制、促进社会和谐”的历史新阶段。首钢要按照国家要求，落实科学发展观，加快建设21世纪新首钢的步伐。

按照首钢“三步走”发展战略，今后五年是承前启后、实现首钢历史性转变的关键时期。在这五年里首钢要全面落实科学发展观，以提高自主创新能力为核心，以搬迁调整为主线，以创新创优创业为动力，以人才建设为根本，实施品牌战略，深化改革开放，转换体制机制，加强企业管理，提高发展质量，完成首钢“十一五”发展规划，制定和实施“十二五”发展规划，为实施第三步发展战略奠定基础，把首钢建设成为自主创新型、运行高效型、循环经济型、和谐发展型企业，在钢铁业竞争力和综合实力方面居国内一流水平。

在首钢的五年总体工作规划中，要求加强企业管理，尤其是对“一业多地”下的管理方式提出了新的要求。

现代化首钢得以持续稳定地健康发展，计量管理工作尤为重要，成为企业有序运行的基石，起到了重要的技术支撑作用。

近些年，首钢对信息化、自动化产业的重视程度史无前例，提升到加快实现首钢“两个转变”的创新载体高度，尤其是4月2日首钢总公司领导视察工作时，做出了“三大

希望、五个有利条件”的重要阐述，提出了“信息化、自动化是首钢实现发展战略的基础”，进一步继承和发展了“两个载体”的观点，与两个创新载体作用一脉相承，可以说这是我们自动化人又一里程碑。如何更好地发挥战略基础和创新载体作用，在首钢发展新形势下，充分利用首自信公司现有的五个有利条件，把五个有利条件转化为无比的动力、激发更大的活力、提升更高的能力、积累更强的实力，从而实现信息化自动化产业跨越式发展。

政府 2006 年提出了计量技术服务平台，即：按照建设创新型国家的要求，以技术创新为重点，形成量传溯源体系为核心的计量技术服务平台。要建设一个适应国家科学技术、经济建设和社会发展需要，具有一定先进性和与国际一致性的计量基准体系。这个平台的建设将对企业计量的发展起到带动作用，用平台建设本身离不开企业计量，需要企业参与，尤其是像首钢这样的大型企业。但是，只有经济发展的需要，才是计量发展的动力。因此，作为特大型企业的首钢，更应该尽快、尽好的融入计量平台建设并最大限度地从中受益。

企业信息化是现代企业实现科学管理的基础。企业计量提供的质量数据、能源和维护消耗数据以及生产过程中各种与产量、作业效率、原材料等有关数据，是企业科学决策、责权明确管理的基础和保证。尤其是首钢“一业多地”的管理模式，在各地获得大量有效的实际计量数据和信息后，如何集中分析、处理，做出正确的决策，实现量化的企业管理，是首钢面临的重大难题。

首钢计量管理系统经过几年的投入与改进，形成了庞大的网络系统，其具有如下特点：

(1) 计量网络系统覆盖范围广；

(2) 被控端计算机与主控端计算机的距离都比较远；

(3) 当被控端计算机程序不能正常运行时，处理故障必须及时，否则会给生产或计量数据结算带来影响；

(4) 有时故障原因比较简单，故障处理的时间远比花在路上的时间短。

(5)“一业多地”的各种数据都往总部计算机传输，致使总部计算机存储数据冗余，传输速度慢，出错率高。总部分配任务时，再将文件或数据下传给各地的计算机，降低了工作效率。同时造成数据动态性很差。

(6) 由于首钢计量机构层次比较多，各个层面对企业计量内容侧重点不同，如果将全部内容均加入到每台机器中，一是不适应首钢局域网的条件，二是数据的私密性差。

因此，新首钢的管理模式提出了计量管理系统要做到：功能全程化；管理体系科学化、规范化；运用综合化；手段现代化；高容错率；数据动态化；数据安全化等。

P2P 存储系统具有高扩展性,高容错性和高性价比等优势。其访问控制算法(SecureDataStore), 便于数据所有者能够在数据分发后仍然对其实施控制。大大提高了数据的安全性管理。

P2P 在文件共享方面应用前景看好，其充分利用了网络带宽，解决了服务器的瓶颈问题，增加了可用资源数和在线时间，充分利用了边缘网络资源。

为更加方便地服务于首钢“一业多地”的计量管理工作，把 P2P 技术应用到首钢计量管理信息系统势在必行。

1.3 意义

在 P2P 模式的应用中，每个参与节点(Peer)都既是服务的提供者又是服务的消费者，从而可以充分利用网络中的边缘资源(Edge Resources) ，来解决传统模式下的性能瓶颈和单节点失效等难题。实现文件共享(File Sharing)、协同办公(Collaboration)、分布式计算(Distributed Computing) 。成为构建新型首钢“一业多地”互联网应用的主要结构和技术之一。

P2P 存储系统的访问控制算法(SecureDataStore)， 该算法没有中心服务器,在不降低系统可用性的前提下,能够以期望的概率实现访问控制的目的,从而满足首钢“一业多地”对不同数据（或文件）访问、使用的需求。

P2P 存储系统可解决数据传输出错率高、扩展性差、传输速度慢、动态性差、数据存储不安全等问题。

通过应用 P2P 技术，可以把首钢“一业多地”的数据充分利用起来，更好地进行分析、处理，建立起了一个统一科学的企业计量管理系统，为首钢生产和经营活动提供准确可靠的信息流，供领导层和管理部门做科学分析，以实现最佳决策目的，从而创造出可观效益。

P2P 技术在计量管理信息系统中的应用，达到了以企业战略竞优、提高效益和效率的目的，真正做到了企业高层决策、中层控制、基层动作的集成化的人机系统。它不仅仅是一个技术系统，而且是一个管理系统，更成为了一个社会系统。

第 2 章 P2P 技术研究

2.1 简介

从 Service 观点，每个 Peer 都是：Consumer、Provider、Register；从设计者观点，每个 Peer 都是：Server、Client、Router；在计量管理系统应用中，我们可以把节点理解为一台计算机。在部分研究者的论文中，P2P 是：没有服务器、完全对称、可扩展性好。

早在 Internet 发展之初，网络的目的就是在两台电脑之间直接共享数据，可以说：曾经，Internet 就是 P2P 的。最初的 P2P 应用大约产生于 20 年前，并且其中的许多至今仍然被使用，如 ARPANet、DNS、USENT（1979 年，是一种分布式系统，能够为各个地方提供新闻组）、FidoNet（1984 年，让不同 BBS 系统中的用户们互相交换信息）等应用非常成功的验证了 P2P 的魅力。尽管这些早期应用的核心就是 P2P，但由于大多数的使用者并未感觉或接触到，因此通常并不认为它们是 P2P 技术。

后来，客户机/服务器体系结构出现了，垃圾信息处理、拥塞控制使得网络节点之间不再协作，防火墙、动态 IP、NAT 的出现中止了开放网络时代，客户机/服务器体系结构由于利于开发、使用、管理，成为很多网络应用的首选，HTTP、FTP 等协议成为了 Internet 上最普遍的网络应用模式。到 2000 年后，以 Napster 和 ICQ 等为代表的 P2P 应用再次赢得世界的认同，新的 P2P 模型不断被提出。无论 IT 业界还是学术界都开始热情洋溢的展开了对 P2P 的研究[4]。可以说到目前为止，对 P2P 的研究工作已经达到了百花齐放的状况。图 2.1 展示了 2000 年以来的 P2P 研究成果。

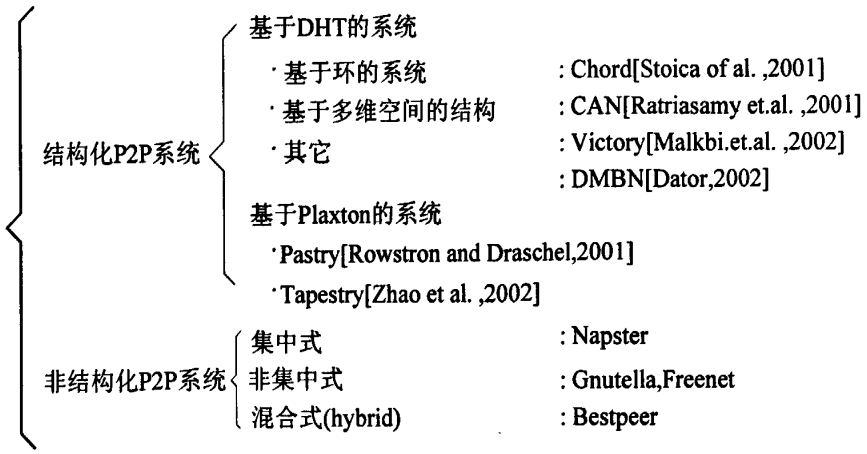


图 2.1　2000 年以来 P2P 的研究成果

Fig.2.1 History of P2P progress from year 2000

从最初的 ARPANET 和 DNS，到后来的 Napster[5]、FreeNet[6]、Jabber 等，以及现

在流行的几个软件 CoolStreaming[7]（流媒体多播）、BitTorrent（文件共享）、KaZaA[8]（搜索和共享）、SETI@home（共享计算）等，点对点网络已经变得非常热门和流行。它的主要思想是：每个节点是自治的，系统以非集中式的方式进行计算机资源的共享，包括存储、计算、带宽等。可扩展性、稳定性、公平性、匿名性、安全性和激励机制等成为了点对点系统中的重要参数。

图 2.2 是著名的 CacheLogic 在 2005 年做的统计[9]，说明了 P2P 的迅猛发展和互联网的变迁。

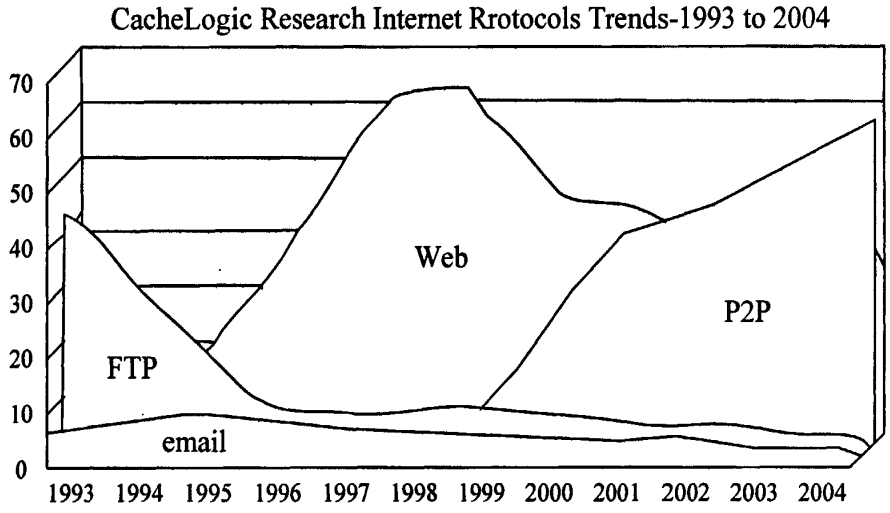


图 2.2 P2P：未来内容分发方式

Fig.2.2 P2P：Content Distribution Medium for the future

“Peer-to-Peer” 这个名字意味着各个 peer 之间的关系是平等的，并且它们之间的联系是直接的（如图 2.3 所示）。这有别于传统的 C/S（客户端/服务器）架构的最大特征（如图 2.4 所示）。正规的描述是：P2P 接近分布式系统范畴，为了实现边缘资源共享和协作，所提出的一种计算模式。

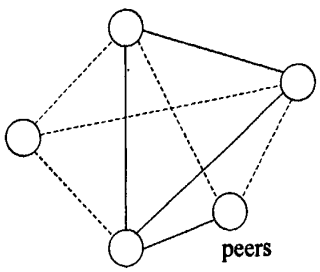


图 2.3　P2P 架构

Fig.2.3 Peer-Peer Computing

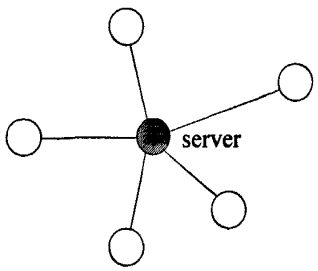


图 2.4　C/S 架构

Fig.2.4 Tradition C/S Computing

在 P2P 模式的应用中，每个参与节点(Peer)都既是服务的提供者又是服务的消费者，从而可以充分利用网络中的边缘资源(Edge Resources)，来解决传统的 C/S 模式下的性

能瓶颈和单节点失效等难题。所以自2000年以来，P2P技术得到了蓬勃的发展，在文件共享(File Sharing)、流媒体多播(Media Steaming Multicast)、协同办公(Collaboration)、分布式计算(Distributed Computing)，以及其他很多领域（如：电子商务、在线游戏、病毒围堵等等）都已经形成了一些为学术界和业内认可的成果[10][11]，成为构建新型大规模互联网应用的主要结构和技术之一。

P2P具有如下三个最大的特征：

动态性：节点可以随时退出和进入，所提供的服务可以随时加入和中止。

分布性：服务分布在边缘节点上，维护路由表和执行查询操作的开销相对较大。

异构性：每个节点的服务能力和服务质量，用户行为和选择策略等，也不尽相同。

这些特性同时也是“边缘资源”的特性。当然了，由于动态性，标识等操作变得相当困难，再加上分布性， 审计等操作也变得难以实施。异构性导致服务质量难以控制，甚至某些服务不可达。在一个大规模使用的P2P系统上，实施MLS (Multiple layer security多级安全）之类的接近不能。也正是因为约束条件较少，才让P2P比Grid（网格计算）获得了更大的扩展性，其节点规模是Grid的千万倍。

这些特性决定了P2P相对与其他模式具有许多优势，比如：

(1) Resource aggregation (improved performance)and interoperability（资源聚集功能和互操作性）

(2) Enabling ad-hoc communication and collaboration.（允许进行ad-hoc沟通协作）

(3) Improved scalability/reliability.（增强了扩展性和可靠性）

(4) Cost sharing/reduction（性价比降低）

(5) Increased autonomy.（更多的自主性）

(6) Anonymity/privacy（匿名性/隐蔽性）

(7) Dynamism（动态性）

2.2 P2P拓扑结构

有学者把P2P的拓扑结构可以被分类为四类[12]：

Centralized Topology（中心式拓扑结构）

Decentralized Unstructured Topology（分布式无结构拓扑）

Decentralized Structured Topology（分布式有结构拓扑）

Partially Decentralized Topology（混合结构拓扑）

2.2.1 Centralized Topology

中心式拓扑结构的特点：资源的发现依赖中心化的目录系统，具有最好的发现和查

询效率（O(1)），支持复杂查询。其缺点：B/S 模式的通病，中心服务器容易单节点失效（single point failure）和系统扩展性差，面对法律和数字版权比较脆弱。最具代表性的实例：Napster。

Napster 设计框架如图 2.5 所示：每个节点向索引服务器注册和搜索文件，数据的传输是通过节点之间直接互联来实现的，不再依赖于中心服务器。

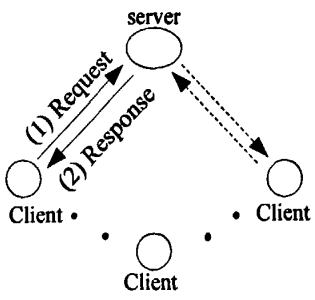


图 2.5(a) C/S 模式

Fig2.5 Traditional Client Server Mode

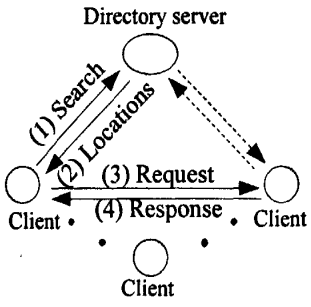


图 2.5(b) N/S 模式

Fig.2.6 Napster-style Computing

2.2.2 Decentralized Unstructured Topology

分布式无结构拓扑的特点：纯粹的 P2P 系统，没有索引服务器，它量用了基于完全随机图的洪泛（Flooding）或随机转发（Random Walk）机制。为了控制搜索消息的传输，通过 TTL (Time To Live)的减值来实现。 定位迅速，动态容错能力好，同时支持复杂查询。最坏情况是 O(n)数量级，查询结果不完备。典型代表：Gnutella。

Gnutella：采用 Flooding 洪泛模式（一个节点向周围节点发送请求，该请求被邻居节点转发给邻居的邻居节点……）进行数据的搜索，通过设置 TTL 方式来减轻系统压力。

2.2.3 Partially Decentralized Topology

又称混合结构(Hybrid Structure)，特点：结合了中心式和全分布式的优点，可以进行高效的查询，同时具有更好的可用性和扩展性。典型用例：KaZaA。

KaZaA：它结合了 Napster 和 Gnutella 共同的优点，带有 Super Nodes 和 Ordinary Nodes 的分层结构，又称 Hybrid Structure。在 KaZaA 系统中，大约有 3 万个 SN，每个 SN 连接 40-60 个其他 SN, 每个 SN 连接 100-200 个 ON。KaZaA 的拓扑结构如图 2.6 所示。

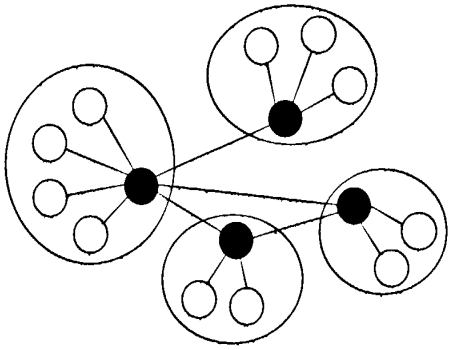


图 2.6 KaZaA 拓扑结构

Fig.2.6 KaZaA Structure

SuperNode(SN)是通过机器的 CPU 和网络带宽来确定的；ON 会选择物理位置较近的 SN 进行连接，该 SN 会保存其文件的索引信息；SN 间不断的通过 Gossip 协议来交换邻接表数据和查询请求，SN 间存在长连接和短连接。这样让 SN 形成一个符合 Power-law 分布的随机网络（实际的测量验证了这一点）。ON 的搜索首先会转发给自己的 SN，然后再由 SN 负责此次查询；SN 间不断的通过 Gossip 协议来交换邻接表数据和查询请求。

2.2.4 Decentralized Structured Topology

分布式有结构的拓扑的特性包括：

(1) 采用分布式散列表（DHT）：它是一个由广域范围大量结点共同维护的巨大散列表。散列表被分割成不连续的块，每个结点被分配给一个属于自己的散列块，并成为这个散列块的管理者。

(2) 有着良好的可扩展性、鲁棒性、结点 ID 分配的均匀性和自组织能力。只要目的结点存在于网络中 DHT 总能发现它，发现的准确性得到了保证。

(3) 基本上都是，O(LogN)的邻接表，O(LogN)的跳数，以及上下线节点需要 O(LogN)的修复。

这种拓扑的系统结构如图 2.7 所示，数据和节点都被 DHT 映射到同一个空间里面。数据的搜索变成了映射值之间的匹配。典型用例：Chord。

DHT 经常会出现以下问题：

(1) 出现混乱现象，每个节点上下线都要 O(LogN)的修复操作，开销很大，系统不稳定。可以采取增大邻接表，增加发布及搜索冗余的方式解决。

(2) 无法支持模糊查询，缺省支持单一关键字查询。可以采取：不按照节点 ID 组织 DHT，而按照关键字组织的方式解决。

(3) 出现异质性（弱节点被分配到热门关键字），可对热门关键字作高速缓存或采

用分层 DHT 结构的方式解决此问题。

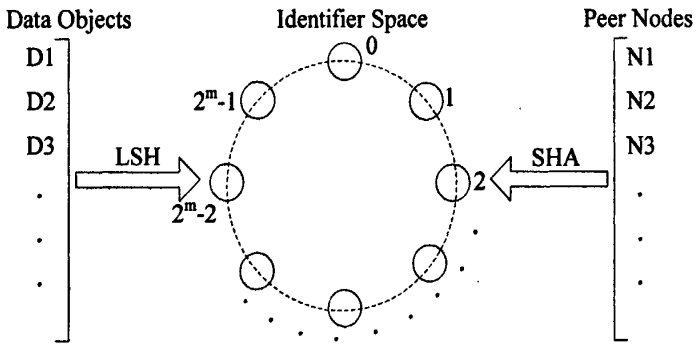


图 2.7 DHT 拓扑结构

Fig.2.7 DHT Topology Structure

2.2.5 各种拓扑结构性能对比

为了便于对比和理解，现将四种拓扑结构在可扩展性、可靠性、可维护性以及发现算法效率和复杂查询方面的性能进行了比较，列于表 2.1 中。

表 2.1 四种拓扑结构性能对比表

Table 2.1 Performance comparation of four typical topologies

比较标准 / 拓扑结构	中心化 Napster	分布式无结构 Gnutella	分布式有结构 Chord	混合结构 KaZaA
可扩展性	差	差	好	中
可靠性	差	好	好	中
可维护性	最好	最好	好	中
发现算法效率	最高	中	高	中
复杂查询	支持	支持	不支持	支持

2.3 P2P 关键技术

图 2.8 被国人做综述时候反复引用；它表示的是对于全分布有结构的拓扑环境下，路由表的大小和搜索深度成类反比的关系[13]。不同的算法，多是时间和空间之间的不同的折衷方案。

P2P 的关键技术可以被分类为：定位/搜索、系统模型和行为分析（台激励、声誉）等。下面讨论这些技术。

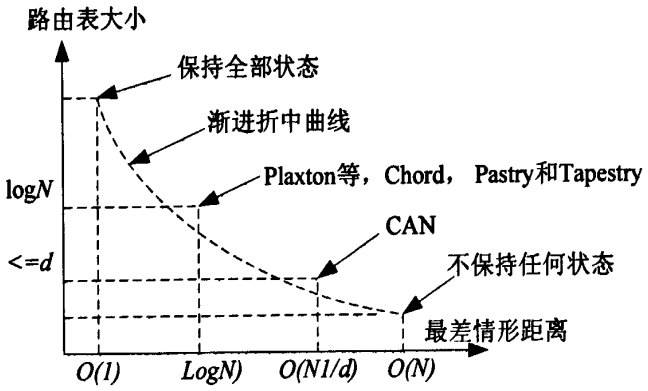


图 2.8 路由器和搜索深度的关系图

Fig.2.8 Relation between routine and search depth

2.3.1 资源定位和搜索

资源定位：基于 DHT 的覆盖网络不需要搜索，资源的定位和底层的覆盖网络的设计紧密相关，一般为 O(LogN)的量级。

资源搜索：适用于非结构化的 P2P 覆盖网络，如：Gnutella 网络：最差可能是 O(N)，研究的热点：Gossip、Random-walk、 Locality，Social Network etc；Kazaa 等 Super-Node 网络：可扩展性好，流行文件能在 1-Hop 内找到；eDonkey、DC++、Maze 等有强大中心索引服务器的网络：1-Hop 的强大搜索，但是实时性较差，新资源需要中心服务器索引更新后才能被别的检索到（Maze 中可能需要数分钟甚至更多）。

两大类方法的比较：非结构化的 Gnutella 网络更适合查找热门资源，而且统计表明：这符合人们的行为，所以其运作很好。结构化的 P2P 网络定位快速，所以可以快速的定位资源。但是问题在于：首先冷门资源的文件数目也同样巨大，在 Churn 高的网络上维护这么多 key 开销也很大。eDonkey2000（eMule）运行的不错，用 DHT 去定位全面的非热门资源的，避免中心服务器失效；采用一系列的中心服务器来提供热门资源的搜索。

搜索方法研究动向：以前的搜索方法多被归类为：盲目搜索（Blind Search），诸如 Flooding（后来加入了启发性 BFS、Random-walk 等）。很多时候，精心设计的搜索/路由方法，未必就好过 Random/Gossip 很多，后者成为热门研究方向。其他搜索概念，如信息搜索：采用 Cache Method：不管是中央节点还是简单节点都存有路径信息，类似 DNS；或者 Mobile Agent based Method：引入搜索 Agent。

2.3.2 流数据及块数据的区别

在我们的计量管理系统设计中，需要考虑数据交换的格式。主要的数据格式包括：流数据和块数据。他们的区别是在于块数据的下载类似于普通文件续传的方式，而流数

据格式更类似于实时数据采集。这里重点介绍一下流数据在实现上的不同之处：

流数据有三个约束条件。

(1) 实时性，强调缓冲区滑动窗口内的数据。

(2) 有序性，原子数据块的流向不会构成环。

(3) 可用性，必须达到数据流平均速度下限。

这三个约束条件使得目前主流的在线视频、VOD和IPTV等应用技术难以像文件共享那样丰富（都长得很像）。目前我们的计量管理信息系统主要使用块数据。

既然原子数据流向构成一个树，这就意味着：存在大量的叶子节点，他们毫无贡献。所以各种复杂的树（如多树、带横向连接的树）被构造出来。

构建流数据分发的难处：

主要的问题是构造数据分发的结构，即数据流动的路径。假设：只涉及一个源结点和许多目的结点，目的是尽快地把数据从源结点散发到所有的目的结点。

常见的有两种描述形式：构造最小生成树和构造MPR集合。

其数学描述一：

给定覆盖网的带权连接图G=(V, E)－其中V代表所有的参与结点，E表示覆盖网的连接。理论上，这个问题转变成构造一棵以源结点为根的最小生成树的问题。但是：在互联网上取得完整的覆盖网的连接图实在不容易。

数学描述二：

节点I的邻居节点集合中的某个子集，这个子集合中的节点转发消息I发出的广播消息，这些消息在一步内能够达到的节点与I的所有邻居节点都转发这个消息所能达到的节点相同。满足这个条件的所有子集合中的最小集合称为该节点的MPR(Multi-Point Relays)集合。但是：在数学上已经证明，计算最小MPR集合是NP-hard问题。

数据流分发结构构建实际考虑的问题是：

(1) 减少延迟和提高带宽；

(2) 容错，提高健壮性；

(3) 降低构造的难度，特别是用分布的方式。

(4) 有利于数据流分发的编码技术，如：MDC（Multiple Description Coding）和LDC（Layered Description Coding）。

2.3.3 应对P2P的动态性和分布性

节点总是动态的，解决方法有：备份数据，缓存更多的路由信息，节点之间进行实时的检测。

节点总是分布的，可能的操作有：把数据也均匀地分布到各个节点上，让数据之间的交换高度并行，经常更改一下关系网可以搜索的更多一些。

2.3.4 P2P 近期研究中的理论进展

(1) Small World 理论

P2P 系统中的 Small world 特征和 Power law 规律证明：实际网络的拓扑结构既不是非结构化系统所认识的一个完全随机图，也不是 DHT 发现算法采用的确定性拓扑结构。所以目前 P2P 结构虽然采用了诸如星星结构、全连通图、树形结构（含多数）、网状结构、环状结构等等，但都无法非常准确的模拟 P2P 的实际拓扑。

幂规律分布的含义可以简单解释为在网络中有少数结点有较高的“度”，多数结点的“度”较低。Small world 模型的特性：网络拓扑具有高聚集度和短链的特性。P2P 发现算法中如何缩短路径长度的问题变成了如何找到这些“短链”的问题。

(2) Internet 拓扑模型

Internet 建模是一个开放性问题，目前常用的有：

随机型：即认为 Internet 拓扑图处于一个完全无序的状态,在大尺度上是均一的。

层次型：来自对 Internet 结构所具有的层次特征的认识,在同一层上的节点出度接近,不同层间节点出度差别很大。

幂率型：发现 Internet 拓扑中存在着 4 条幂律。

对 Internet 拓扑建模的进展，也影响了 P2P 拓扑模型的研究，最常用 GT-ITM(层次型)。

(3) 激励与声誉

为什么要去研究激励(Incentive)、声誉(Reputation)？这是因为：

Free-rider：最近的测量表明 80%的 eDonkey 用户不共享任何资源，大概 60%的 Maze 用户不上传资源。或者用户为了降低自己的负载，倾向于把热门资源移出共享而保留那些非热门的资源。

Pollution/Fake-file（超过 50%的音乐不再是原版文件）、共谋等不合作行为。

不合理的拓扑结构（如：叶结点太多）。

减少 Free-rider 的方法有：

1) 带有奖惩的激励策略(如：BT 采用 Tit-for-Tat-ism 机制）；

2) DC++，限制加入网络的人必须共享一定数目的文件；

3) eDonkey、Maze 都根据历史上载记录来提高下载排名；

4) 默认的把下载资源添加到共享里。

防止污染文件的方法有：

1) 下载前预防（如：BT网站管理员筛选，对BT很有效）；

2) 下载后警告（如：预览、用户投票、评注等，效果不佳）；

3) 监控恶意行为；

4) 通过（中心式）审计识别用户行为。

2.3.5 P2P的业界支持

业界对开始重视P2P的研究，目前比较知名的举措包括：Sun公司发布JXTA平台（如图2.9）；Microsoft发布.Net平台；Intel发布Accelerator Kit平台；GGF创建P2PWG；中国互联网协会成立宽带P2P联盟[14]，计划发布相关标准。

P2P的经济模式也在探索之中，目前比较知名的方案有：Apple公司的基于Real Network的Music sales计划，Skype发布的CDN-like的Service Sales。

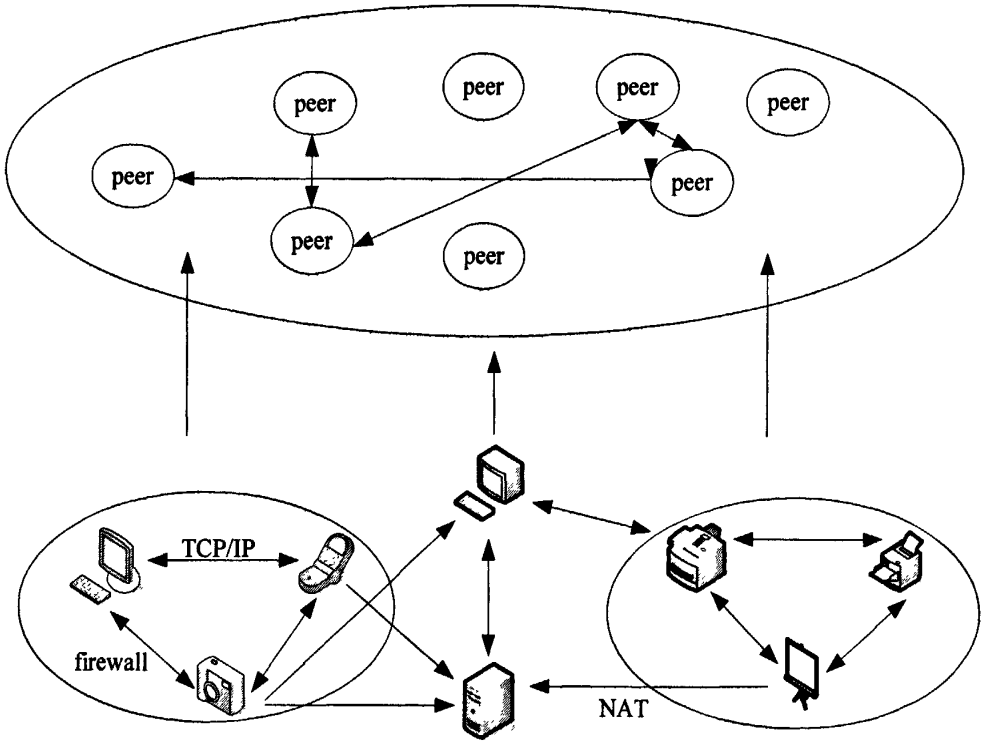


图2.9 P2P在JXTA的应用

Fig.2.9 Implement of P2P with JXTA

但是P2P在应用和推广过程中也受到了不小的压力，处境有些尴尬，其中至少包括：

(1) 内容服务商：封杀发布服务器、起诉P2P用户（如RIAA的律师函）和污染P2P数据。

(2) 网络服务商：限制P2P流量，更改计费模式；禁用P2P端口，隔离IP地址段。

(3) 本地网络：设定防火墙和网络地址转换，进行P2P协议过滤。

造成这些问题的原因有很多，比如数字版权问题、内容分发网络服务商的利益问题等。但是，最主要的是对P2P的不信任使P2P技术处于如此尴尬处境。随着业界对P2P的不断支持，相信P2P技术会有很好的发展前景。

2.3.6 P2P对计量管理的支持

通过对P2P技术的初步了解，可知P2P技术在企业计量管理中应用具有如下优势：

(1) 对计算机的分布无严格要求，也就是说每个节点是自治的，系统可以以非集中式的方式进行计算机资源共享，充分利用了边缘资源，非常适应首钢“一业多地”的管理模式。

(2) 动态性：每个节点可以随时退出和进入，所提供的服务可以随时加入或中止。避免了“领导不在，无法办公”的问题。

(3) 解决了数据传输出错率高、扩展性差、传输速度慢、动态性差、数据存储不安全等问题。

(4) 应用P2P技术，可以更好地实现首钢多个信息系统之间资源共享，避免了“独立作战”、互不来往的弊端，真正做到企业计量管理现代化。

(5) P2P的搜索、定位技术，可以帮助我们在应用计量管理信息系统过程中，及时、准确地找到所需要的文件或数据。

(6) 无论处于计量管理信息系统中的每个节点属于什么拓扑结构，P2P的动态性和分布性都能将节点上的数据进行实时监控，并将其及时分发到所需节点。

第3章 系统需求分析与总体设计

近些年，首钢对信息化、自动化产业的重视程度史无前例。不仅从组织机构上进行了变革，而且在总公司成立了信息部， 将原电子公司和计控室进行了优化组合，成立了首自信公司，具体负责首钢“一业多地”的信息化及计量管理工作。并在资金上给予了很大的支持，上了ERP系统。

3.1 需求分析

目前，首钢计量工作采取的是从首钢总公司信息部到各生产厂矿、班组分级管理的工作模式。总公司信息部下设一计量管理处，宏观管理首钢计量工作。具体的计量数据采集、统计以及日常计量管理工作，由首自信公司完成。计量工作主要分物资计量管理、能源计量管理和量值传递管理三大块内容。分别由ERP、电力网、企业计量管理信息系统三个专业子系统进行管理。每个子系统之间互不链接，为首钢整体计量管理工作带来不便。现根据各子系统的运行情况简单介绍首钢计量管理系统的改造需求。

3.1.1 物资计量管理现状

首钢在没有应用管理信息系统之前，物资计量管理基本属于传统的管理模式。计量数据的传递依靠人工作业，由计重员编制传统的手工制单，逐级汇总、分析，将计量数据传递到企业管理者面前。环节多，效率低，易产生差错，不利于生产调度、指挥和决策，不适应市场经济快速高效运行的需要。

首钢ERP（Enterprise Resource Planning）系统一期成功上线运行后，使总公司初步实现了生产经营的信息化管理。也促使计量工作原有的传统管理方式发生了变革，物资计量管理从原来单一的提供计量单据和统计报表，扩展到对全公司的物流结算过程进行全方位管理。ERP系统的投用，减少了中间管理环节，增加了各专业管理工作的透明度，实现了信息资源共享。提升了计量在数据管理中的地位。

3.1.1.1 ERP离线物资计量数据管理原状

ERP上线前物资计量数据流程为：车辆到各计量站进行计量，运输部门将计量相关信息（如供需工厂、物料、车号等）报给计量站，计量员维护相关信息的同时完成计量操作。出具计量单，计量单上包括这些信息。由计量部门完成计量数据及计量信息的传递工作，包括：湿基计量数据、日统计(日报)、旬统计(旬报)、月统计(月报)完成后，最后生成最终物资计量结算数据，作为各单位之间的结算干基数据。其中计量部门提供计量单、日统计报表、旬统计报表、月统计报表等。

ERP上线前计量部门建立的物资计量网，其计量数据和与计量相关的各种信息，公司各部门间不能共享，不利于公司统一管理。特别是与计量业务密切相关的单位如供应公司、销售公司、生产厂、质检、计财等多个部门，由于没有实现计算机网络管理，透明度低，导致计量数据信息数出多家，造成双方结算失真扯皮等问题。例如，公司原料供应厂际计量结算点设在翻车机，使计量数据不能作为计量结算唯一依据。由于各部门数据不能共享，公司不能统一管理，厂际之间物资结算并不以实际计量数据为准，更多的是相互协商进行平衡来解决，造成上下工序、单位之间的结算自由度很大，随意性强，不能真实反映生产成本。

ERP上线前的物资计量结算基本是由计量部门出据计量数据、计量结算报表，各单位（上下工序）自行进行结算，结算结果报公司有关部厅。

3.1.1.2 ERP在线物资计量数据管理现状

ERP上线后物资计量数据流程为：计量前各单位在ERP系统上维护计量相关信息主数据，系统创建计量申请，生成计量申请单。需计量的车辆到各计量站进行计量，系统提供该车辆申请计量的编号，计量员在ERP系统中调出该车辆的计量相关信息并采集计量湿基重量，此计量数据在ERP系统中可以共享，将此计量数据扣杂、扣水算出干基，上传到ERP进行计量数据传递，SAP系统收货后据此数据进行结算，并出具物料凭证和财务凭证。计量部门在ERP系统中需提供时时的计量结算数据。

ERP上线以后，计量部门负责提供全公司所有物资的计量数据；并负责厂际间转移物资的计量结算。使原有的物资计量业务工作流程、管理方式，发生了根本性的变化，物资计量管理从原来单一的计量专业管理，扩展到对全公司的物流结算过程进行全方位管理。计量部门提供的计量结算数据，作为公司财务结算的唯一依据，实行网络化管理，计量资源共享，真正体现计量数据的真实性、准确性、权威性。

ERP上线后的物资计量结算由于实现了信息资源共享，从计量开始到结算过程完成是时时进行的。相关信息和结算数据直接影响到各单位成本、效益，因此各单位在计量前，必须准确录入相关信息，生成《计量申请单》，从网络上把计量信息传递给计量部门。计量部门通过锁定计量申请单号和计量车号等信息与计量重量湿基数据相互匹配，经过扣杂、扣包装、扣水等流程操作，自动运算出计量干基重量，按照SAP规定的统计原则（同订单、同工厂、同物料、同检验批），计量数据进入系统，经过质检部门出具的质检结果和订单价格，系统生成物料凭证和财务凭证，完成物流与资金流的合一，最终完成结算。

通过ERP一期的上线运行，推动了首钢计量工作的变革，使信息围着数据转，数据围着管理转，管理围着效益转，实现了计量工作的良性循环发展。在首钢“一业多地”

的基本框架下，在集团广域网建设的过程中实现集团的计量数据共享，为集团的生产、经营、决策提供准确、及时、可靠的计量保证。通过加强计量基础工作，充分利用现有条件和技术手段，强化信息资源的开发和利用，全速推动首钢信息化和计量工作更快的前进。

首钢通过实施ERP，取得了如下效果：

(1) 系统运行集成化，软件的运作跨越多个部门，达到了“一业多地”的需求；

(2) 业务流程合理化，各级业务部门根据完全优化后的流程重新构建管理思路；

(3) 绩效监控动态化，绩效系统能即时反馈以便纠正管理中存在的问题；

(4) 管理改善持续化，为首钢物资计量管理工作建立一个可以不断自我评价和不断改善管理的机制。

但是ERP在首钢的运行现在仅限于物资计量管理工作，实现了物资计量数据共享，基本实现了企业高层决策、中层控制、基层动作的目标。

3.1.2 能源计量管理现状

首钢能源计量主要包括水、电、煤气、压缩空气、氮气、氧气、氩气、重油等的计量。能源是企业生产成本的重要组成部分，降低能耗，既节能又降低成本[15]。加强能源计量管理，是首钢实现节能降耗、减少环境污染、提高经济效益、加强能源综合利用、发展循环经济，从而实现能源科学管理必不可少的技术手段。可以说首钢近几年的搬迁调整与能源计量管理工作有密切关系[16]。

首钢能源计量工作在实现信息化方面也做了些工作，但进展很慢。ERP一期在能源计量方面未做过多的设计，现在仅实现了电计量管理的局部网络化，首钢内部称之为电力网。

能源计量数据流程为：各能源计量点进行计量，每日由维护班组人员到现场进行抄量，并将计量数据电话报给上级部门的数据统计人员，数据统计人员进行日统计(生成日报)、旬统计(生成旬报)、月统计(生成月报)。每日、旬、月数据统计人员将能源计量结算数据报至总公司，总公司将这些数据进行平衡后分发给动力厂、电力厂、氧气厂等相关部门，由其财务科进行能源结算。目前能源计量结算的报表包括各种能源介质的日报、旬报、月报。

能源计量目前的基本现状是由计量部门每日进行抄量（报量）、出据计量统计数据，进行能源计量结算。根据目前的基本现状和各单位生产经营情况，出具《首钢总公司能源统计报表》，每月数据输入ERP系统，供方财务部门按计量结算数据与用方各单位财务部门进行结算。计量数据结算有争议，由计量部门牵头，组织核查。计量部门最终

决定仲裁计量结算数据。

能源计量实现了部分能源计量点的计算机联网。2000年到2002年先后在第二线材厂、第三线材厂、氧气厂组织完成了能源计量点的计算机联网工作，目前运行情况良好。其中：第二线材厂能源计量计算机联网进机计量点8个、第三线材厂能源计量计算机联网进机计量点18个、氧气厂能源计量计算机联网进机计量点45个。在炼铁厂、烧结厂、第三炼钢厂、型材轧钢厂等单位实施的能源计量点的计算机联网工作也在进行中。

在电量计量方面，首钢总公司的电量计量计算机网络系统（即电力网）从1998年开始规划，1998年4月从八总降开始实施，1999年四季度开始逐步投入使用。截止到目前在规划的16个子站中，已有一总降、五总降、六总降、新八总降、老八总降、十一总降、十四总降、热电站等全部完成。但是现在的电力网不能做到各计量点自动采集、自动传输数据，基本处于手工抄数、电话报量、人工统计、汇总结算数据。电力网形同虚设，仅起到了数据计算，最终数据传输的功能。

能源计量目前存在的最大问题是能源点分散，计量点建设不全、损坏、管道跑冒及损耗是制约能源计量的关键，各种能源介质基本属于手工抄数，电话报量，人工统计、汇总结算数据，手工报表等人工处理状态，存在费时费力，容易形成人为数据错误等缺点。所以目前的能源管理已完全不适应信息化的需要，当务之急是尽快完善能源计量体系网，满足各单位成本结算的需要。

3.1.3 量值传递管理现状

首钢公司的量值传递工作主要内容是：计量机构管理；计量标准管理；计量检定管理；计量器具管理；计量人员管理；计量检定原始数据管理；计量文档管理；以及计量数据统计、分析、报表管理等内容。

主要涉及的单位有：首钢总公司信息部计量管理处、首自信公司运行事业部、运行事业部标准计量站以及各生产厂矿计量管理部门。

首钢公司的量值传递工作由首自信公司负责，首自信公司已经通过了北京市质量技术监督局的38项标准考核，并取得了授权证书[17]。具体由首自公司标准计量站负责首钢公司“一业多地”的量值传递工作。

根据量值传递管理的特点，现已有公司开发研制出了企业计量信息管理系统。其功能模块设置如图3.1所示，基本满足了首钢量值传递管理需求。

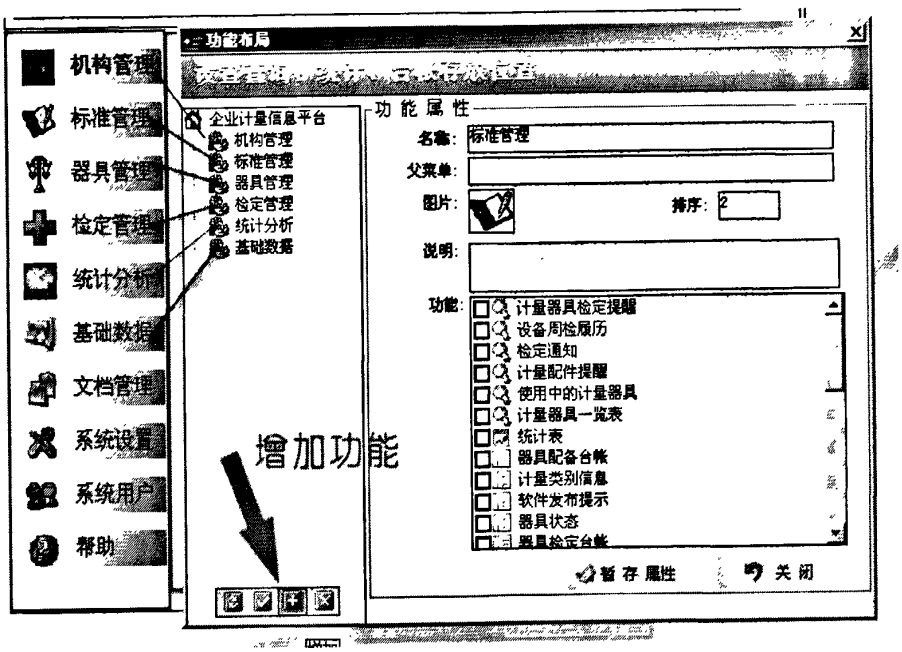


图 3.1 企业计量信息管理系统的管理功能模块设置图

Fig.3.1 Configure of management function module in ERP

系统中主要设计功能有台帐设计、查询设计、统计设计、报表设计四大功能,能灵活的设计各种台帐、提醒、统计及报告等。如图 3.2 所示。

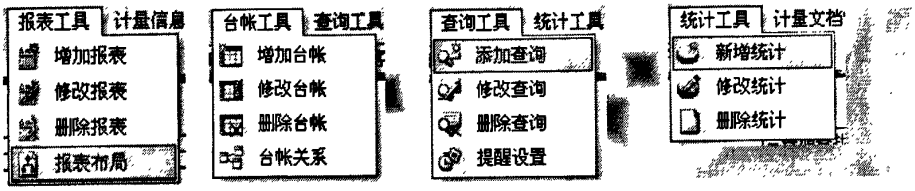


图 3.2 企业计量信息管理系统的统计功能模块设置图

Fig.3.2 Configure of audit function module in ERP

应用企业计量信息管理系统后对首钢量值传递工作产生了很大影响。首先实现了规范化（标准化），帮助首钢建立了一个完善的量值传递管理流程。

从外部的计量机构管理评估到内部计量室的人员管理都可以进行监控与监督。形成了一个计量机构管理体系。计量信息一览表之间可以联系，如把外校清单的仪器与维修清单的仪器建立联系之后，当点击外校清单或维修清单里的任一仪器时会展出另一个清单里相关与它的信息。（可以按自己的需求和意愿来任意设定多个清单之间的联系）可以任意的创建新的一览表,去满足当前管理的需求。以达到持续改进和更新的能力。

从计量标准管理到内部校准，它的提醒功能可以避免仪器未能及时的校准，可以分多次提醒，如十天内要校准的，一个月内要校准的，二个月内要校准的，来预警要到期的检测设备，可以根据实际的情况提前对工作进行安排和调整。包括检定人员证件到期提醒，以便管理者合理安排资金的使用。

统计功能,从可以统计每个月每个部门校准仪器数量到每个月每个部门的校准费用,都可以进行详细的分析与预测，为每年的仪器年度校准费用预算和计划提供支持。

报表功能，为新建和编辑校准报表提供了广阔平台，可以编辑出任何的表格，并与清单里相关的信息建立联系，如当你点击清单里某一仪器时，按鼠标右键，弹出一个窗口里有其校准报告和履历表。报表功能提供了非常友好的用户接口，降低了用户培训和使用的开销，提高了工作的效率和正确性，具有 Excel 不可比拟的技术优势。

应用企业计量信息管理系统实现了专业化。其系统模块设置完全根据计量管理的特点开发出来的，专业的划分出计量管理模式，按此专业的模式来对自己公司计量管理流程进行优化和改进，适合当前计量发展趋势。

应用企业计量信息管理系统提高了工作效率。本系统录入数据高效快捷，设计了对 Excel 表格进行导入和导出功能,这样实现了对原有的数据高效方便切换到系统内管理,避免了大量的手工输入,提升了效率。系统有唯一性设定,可以预防和提示管理信息(如管理编号)的重复。系统有引用数据功能，可以避免大量重复性的数据手工输入。系统有必须填写功能，避免了人为漏写。有强大的 E-mail 功能，可以根据你的需要给任何人发出校准信息。强大的数据保障功能，由每一个月、每个星期或每次推出，都会把系统数据进行备份,避免数据的丢失,也对历年计量仪器管理进行有效评估提供数据支持。

此系统在首钢量值传递工作中，基本实现了以下管理功能：

(1) 设定数据操作权限，保证数据变动的唯一性；

(2) 实现人员持证动态化管理；

(3) 自动计算制定测量设备周期确认计划；

(4) 自动统计总公司测量设备总台帐、单位测量设备总台帐和分类帐；

(5) 自动统计在用测量设备检测台帐和 A、B、C 台帐；

(6) 自动计算制定工艺测量设备改造计划；

(7) 自动打印计量检定规程、校准规范等文档；

(8) 自动编制测量设备追加确认计划。

3.1.4 需求总结

ERP、电力网、企业计量管理信息系统三个专业子系统近年来虽然在首钢公司范围内分别在物资计量管理、能源计量管理以及标准量值传递管理等方面起到了重要作用，但三个系统间的互不衔接，为首钢整体计量管理工作也带来了很大不便。尤其是不能满足首钢改制后的“一业多地”的管理模式。主要体现在“一业多地”及各个部门间对计

量数据或信息的共享、原始数据管理和数据传输等方面不能做到现代化、科学化和规范化。

所以在后面章节中，主要阐述了如何利用 P2P 技术实现三个子系统间的数据共享、数据管理以及数据传输等，真正实现首钢公司计量管理系统的现代化、一体化。

3.2 系统总体设计

3.2.1 基于 P2P 的系统集成框架

MIS 系统的关键在于集成，集成所完成的效益是每个独立系统单独工作所无法完成的，而且是 1+1≥2. 因此计量管理在三个子系统建立运行后，还要将它们集成系统，利用先进的 P2P 技术，让各子系统以及各子系统之间具有良好的可重组性和可重构性，使各级部门的办公实现自动化，便于部门之间协作，使不同部门、“一业多地”之间需要协作的工作变得更快、更流畅。使各种信息能快速传递、迅速处理、充分共享，为领导决策科学化提供科学的依据，推进计量事务的电子化进程；并使得每个部门、“一业多地”之间，上下、左右沟通更为通畅，让计量管理工作进入良性循环，通过这一举措同时也可以提高计量业务的严密度与可信度。只有这样才能真正发挥出计量管理系统的作用。集成后的计量管理系统功能模块结构图如图 3.3 所示。

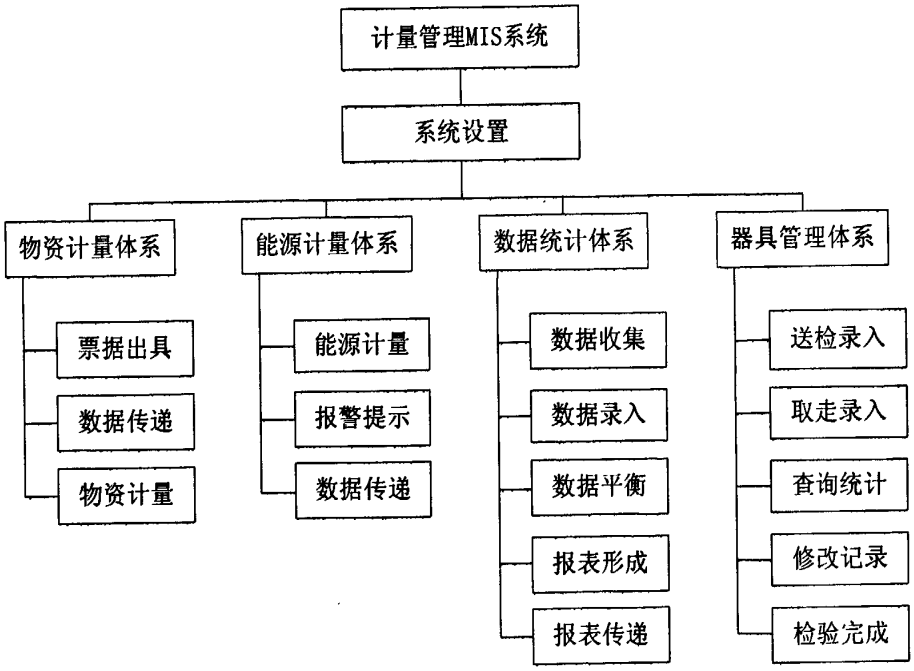


图 3.3 集成后的首钢计量管理系统图

Fig.3.3 Architecture of improved Shougang metering management system

系统功能模块描述：系统功能模块的描述主要是描述出系统功能模块的功能和处理内容。主要是用文字去描述，而不是用图形图表描述。

(1) 计量管理MIS系统：是三个子系统集成后的总界面。

(2) 物资计量体系：首钢的物资量计量体系涉及到原料、销售、财务、供应、运输、公安、计量管理等部门。计量管理部门负责首钢一、二级物资计量的全过程管理；负责首钢一、二级物资计量交割点计量监测数据的采集传递、统计分析、平衡修正及计量结算数据出具。

首钢北京地区的物资计量点已全部实现了单秤的自动计量、自动采集数据。每个计量数据及其相关信息都已保存到了此模块。各级计量管理人员根据自己唯一的授权权限查询相应的数据、票据等相关内容。

此系统设置物资计量、数据传递和票据出具三个模块。

物资计量模块：需计量的车辆到达计量点后，计量点操作人员点击此模块，输入需计量的车辆的相关信息，与ERP系统中保存的信息核对无误后，开始进行计量。

数据传递模块：计量完毕后，此模块会将采集到的计量湿基重量，及扣杂、扣水算出的干基数据，自动上传到ERP进行计量数据传递。此数据可以在系统中共享。

票据出具模块：点击此模块，相关人员可以根据需求打印出物料凭证和财务凭证。

(3) 能源计量体系：计量管理部门负责首钢一、二级能源计量交割点的设置及测量设备的设计、选型、安装、调试、投运、维护、确认工作；负责一、二级能源计量结算数据的采集、抄报、平衡、出具、存档等工作；参与技改、工程项目能源计量交割点测量设备设计方案论证和配备审查等。

此体系完成：数据采集及通信；数据计算统计；报表形成及显示，包括分、时、班、日、旬、月报表；报表打印；计量回路最大最小流量设置；各计量回路仪表系数、管道比重等常数设置；数据修改后记录备查；异常状态报警；数据备份、数据恢复等基本功能。

此系统设置能源计量、报警提示和数据传递三个模块。

能源计量模块：点击此模块可了解首钢现有能源计量交割点分布、运行及其相应参数等情况。

报警提示模块：点击此模块可查询存在异常状况的计量点情况，据此计量管理人员可安排专业人员到现场进行维护，消除隐患，保障能源计量点运行正常后，解除报警。

数据传递模块：此模块中的数据有的是自动采集，有的是人工现场抄量、平衡后输入进来的数据。

(4) 数据统计体系：此体系是依托在物资计量体系和能源计量体系之上的，负责对两系统提供的计量数据进行统计分析、平衡修正工作，并负责及时、准确地出具计量结算数据。

此系统设置数据收集、数据录入、数据平衡、报表形成和报表传递五个模块。

数据收集模块：此模块完成物资量及能源量中可以自动采集点的数据收集工作。

数据录入模块：此模块完成能源量中需要人工抄数的计量点的数据采集工作。每天由能源计量点抄表人员电话报量，数据统计人员人工将数据录入到此模块。

数据平衡模块：此模块完成报表出具前的数据平衡工作，由相关计量管理人员输入权限口令完成数据平衡工作。

报表形成模块：此模块可自动完成相关报表及其打印工作。

报表传递模块：根据权限，点击此模块，可将生成的报表传递到相关部门，并打印出来。

(5) 器具管理体系：此体系主要是针对首钢的量值传递管理设置的。依托于前面所讲的企业计量信息管理系统。此体系的作用主要是进行测量设备管理。进行测量设备管理的目的是保证首钢生产经营的数据真实、准确，确保测量设备的特性满足规定的计量要求。

为保证测量设备的计量特性满足预期使用的计量要求，企业要对测量设备的配备、采购、贮存、管理、检定/校准等工作进行管理，为达到这些要求，此系统设置了送检录入、取走录入、查询统计、修改记录和检验完成共五个模块。

送检录入模块：各单位所用的测量设备根据其使用情况，均设置了检定日期、检定周期和检定有效期。各单位在测量设备检定有效期前按检定计划要求，将测量设备送到标准计量站进行检定/校准。标准计量站收发人员将送检的测量设备相关信息录入到此模块。并打印出收（发）记录交与送检人员作为将来领取测量设备的凭证。

取走录入模块：检定/校准工作完成后，将测量设备及其检定证书等相关资料传至收发室，并通知送检单位人员持送检凭证来取此测量设备。送检单位人员取走测量设备后，收发人员在此模块中进行记录。

查询统计模块：此模块可以查询测量设备受检状态，可以分日、月、年等自动完成检定/校准工作量的统计工作。

修改记录模块：在测量设备的检定/校准工作中，可能会出现原始记录、检定证书的填写、录入等的失误，在此模块可以进行修改记录，但此功能在使用前必须得有相关管理人员的确认、批准。

检验完成模块：此模块由检定人员进行录入，输入测量设备检定/校准结果，包括检定原始记录、检定证/校准证书等内容。

根据以上给出的计量管理系统功能模块结构图，拟制定基于 P2P 的计量管理系统的拓扑图如图 3.4 所示。

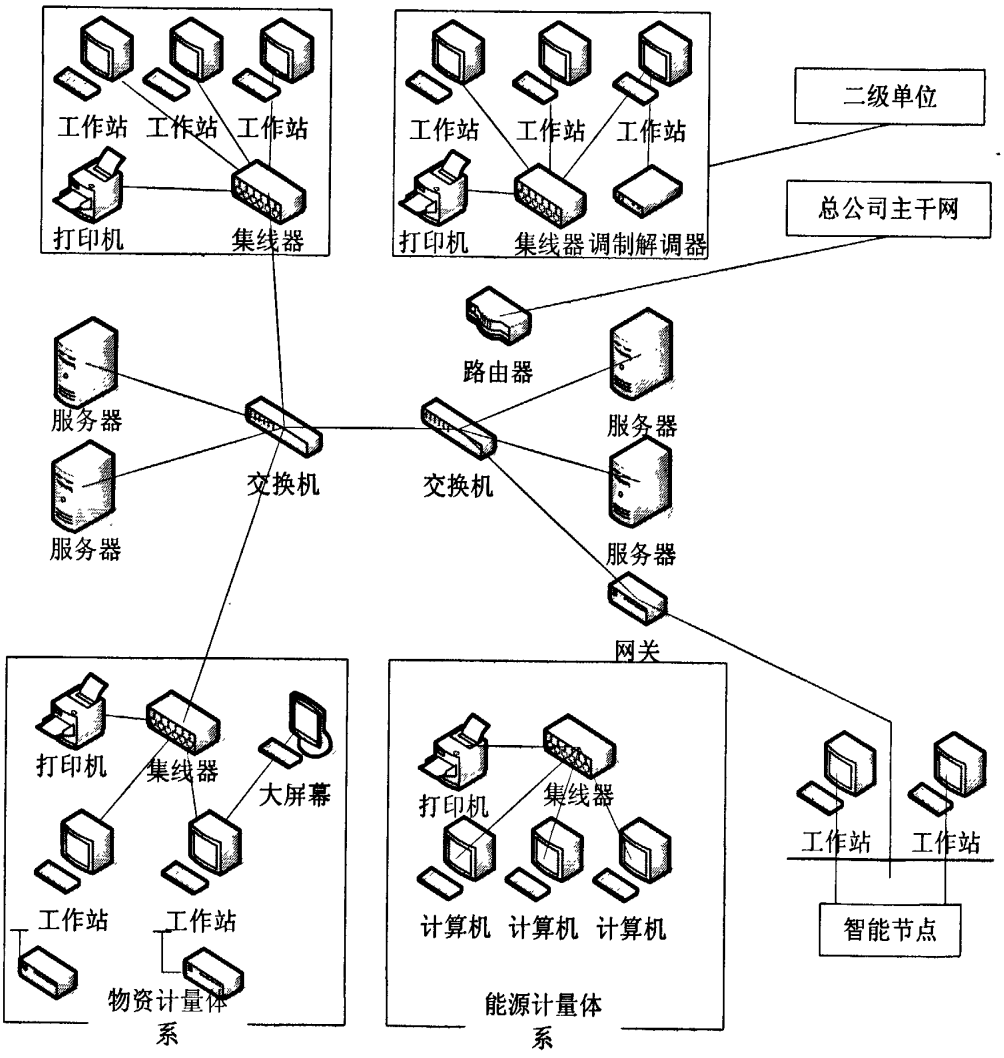


图 3.4 集成后的首钢计量管理系统拓扑图

Fig.3.4 Topology of improved Shougang metering management system

3.2.2 计量管理系统中的数据库设计

首钢的计量管理信息系统主要由物资计量管理系统、电力网和主要用于量值传递的企业计量信息管理系统三个子系统组成。其网络中节点构成方式多种多样，有的完全是由服务器节点以对等方式组成，有的是完全由用户桌面机组成，有的是服务器与桌面机共同以对等的方式组成的系统。其复杂多样的拓扑结构，对总的集成系统中的数据或信息存储提出了很高的要求，以保证数据或信息的安全性。可以说，集成后的首钢计量管

理信息系统，既要满足专业的大型存储任务，又要将分散在首钢“一业多地”的桌面机资源组织起来形成互助存储网络。这样首钢计量管理信息系统的存储系统相比传统的存储系统要求更高些。

在P2P技术方面，由于采用对等互连的技术，P2P 存储系统相比传统的存储系统有如下优点：

高扩展性：不依赖中央控制，系统具有高扩展性，且不存在单点性能瓶颈问题；

高容错性：各个节点功能对等，使得整个系统在缺失部分节点后仍能正常工作；

高性价比：由于高扩展性和高容错性进而使得利用廉价机群搭建大规模高性能存储服务成为可能；

拥有开销：由于没有也没法进行中央控制，P2P 存储系统能够极大减小存储系统总的拥有开销（Total Cost of Ownership）

传输速度：由桌面机组成的 P2P 存储系统，每个节点将可以利用互联网的边界带宽资源存储数据，极大的提高传输速度。由于首钢计量管理信息系统中每个节点都可能随时暂时或永久的离开系统，而且节点之间是对等的，拥有很大的自治性和不可信性，所以一旦一个节点的数据发布到多个节点上，数据的发布者常常失去了对数据的控制，同时由于单个节点实施访问的可信性取决于节点的可信性，往往对数据的访问过程也会带来不安全性。所以在后面章节中提出了一种在多个节点实施访问控制的算法，在不降低系统可用性的前提下，提高了访问控制的可信性。

计量管理系统的三个子系统之内共有6个数据库。其分布如图3.5所示。这里对每个数据库的设计功能分别进行了描述。

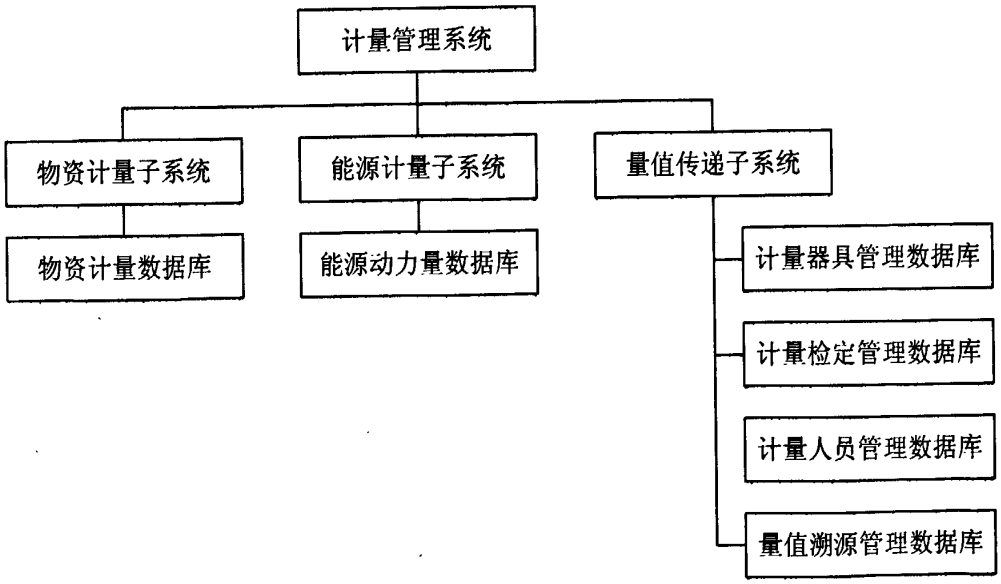


图 3.5 计量管理系统中用到的数据库

Fig.3.5 Database Set used in MMS

物资计量数据库：物资计量数据全部进入 ERP 系统，可根据需求，自动生成相关报表或台帐。包括衡器配备台帐、衡器检定计划等，可以随时查询、统计各个计量点物资计量数据或相关信息。

能源动力量数据库：能源量包括水、电、煤气、压缩空气、氮气、氧气、氩气、重油等动力量，现在只有电量实现了数据库保存，并实现了自动计算、自动生成报表的功能。其它动力量均由数据统计人员进行人工统计、计算、生成报表，不在电力网之内，只是以 Excel 的报表形式保存而已。

计量器具管理数据库：计量器具的管理工作是计量工作的一项基础工作。它是实现企业量值统一的物质基础，根据《计量法》，计量器具是监督部门主要的监督对象。在此数据库中包括企业最高标准器（装置）、工作标准计量器具和工作计量器具相关内容。计量器具的信息最终存储在此数据库中，数据库设置自定义浏览和打印功能。在管理、查询时，可以按需求自动生成 Excel 报表、台帐，比如生成最高标准器台帐、工作标准器台帐、工作计量器具台帐、计量检测点的计量器具配备台帐、工作计量器具修理信息台帐、ABC 分类台帐、工作计量器具低值易耗资产统计、送检费用统计台帐等，进入此系统可以随时查询、确认标准器具和工作计量器具的管理状态（如在用、在库、限用、禁用、报废、降级、丢失、不合格....等）。

计量检定管理数据库：周期检定是一项复杂的系统工程，周期检定的目的是尽可能的防止使用失准的计量器具，以免造成量值混乱。在企业中由于计量器具种类多，使用分散，检定周期不同，往往不便于管理，常常出现漏检的情况。设计计量检定管理数据库，可以辅助计量人员编制计量年度检定计划及月度计划，自动编制检定通知单，贮存检定信息及统计各种需要检定的计量器具的数量等等。

计量人员管理数据库：在首钢公司内计量人员不仅包括计量检定人员，还包括 ISO9000 内审员[18]、ISO/IEC17025 内审员等。为不断改进提高内部计量审核的效果，保证首钢计量体系的正常运行，加强计量人员的管理非常重要。 所以设计了计量人员数据库。此数据库内容包括：计量人员自然情况、培训情况、检定人员持证情况等。可以根据需要自动生成相应报表或台帐。

量值溯源管理数据库：量值溯源是指量值是如何传递的。根据国际标准的要求，“所有测量设备都应可溯源到国际或国家测量标准的测量标准进行校准”，以保证量值传递的准确性。因此在量值传递过程中不合格计量器具的控制非常重要，只有确保不合格计量器具不流入量值传递环节或者合理修正不合格计量器具带来的误差，才能保证量值传递的准确性，不会对企业生产造成损失。此数据库包含了追溯对象（不合格产品或不合

格计量器具）、工作计量器具信息、工作计量器具检定信息、工作计量器具检定记录到追溯到标准检定装置等相关数据内容。

数据最终保存在数据库中，这主要是为了充分利用数据库的高并发性、安全性和查询效率等优势。数据在 P2P 环境中进行交换和共享的时候，中间结果用 Excel 格式来保存。所以本系统中还增加了数据库与 Excel 格式的转换的支持。

3.2.3 计量管理系统节点架构

计量管理系统节点架构，分为三层：服务集中支撑层、安全增强层及加密传输层。集中支撑层下面集成了计量管理系统的主要三个功能模块，通过安全增强层的接口，可以在 P2P 网络上实现数据的安全分发和管理。配置管理面板可以完成对各层参数的设置。节点的架构如图 3.6 所示。

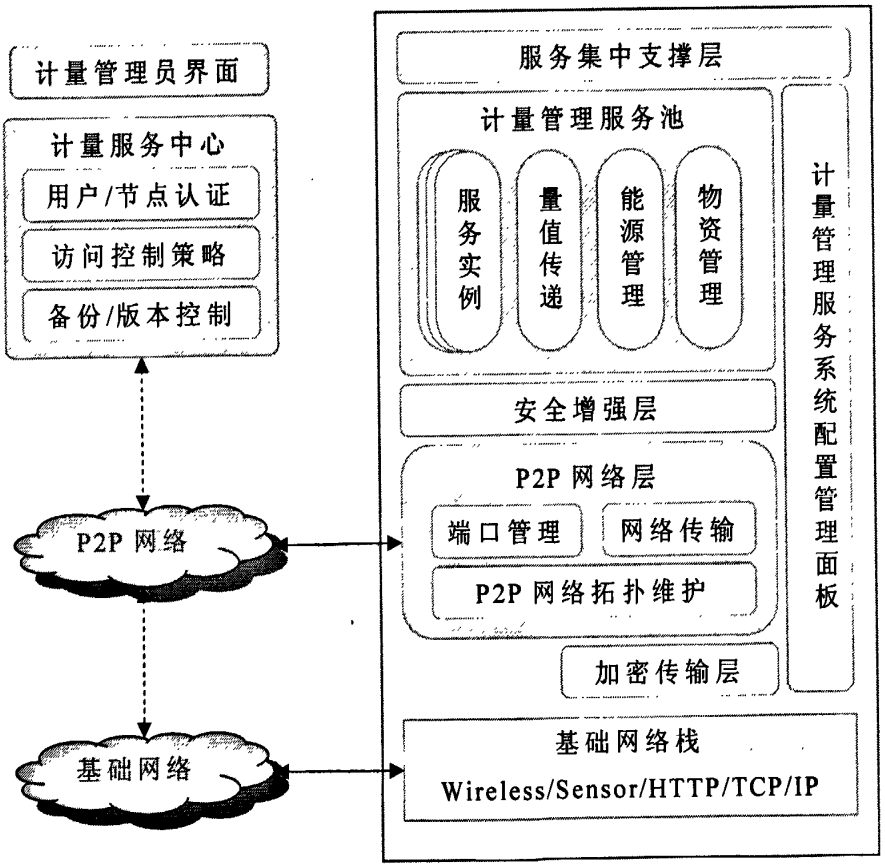


图 3.6 计量管理系统节点架构

Fig.3.6 Metering Management System (MMS) Peer Architecture

系统面板对本地服务和安全的 P2P 支撑层（含安全传输、P2P 网络和访问控制）的状态和参数进行监控，允许用户对其中的部分参数进行设置。应用扩展层是指依托于三个典型的计量服务进行扩展的应用，用户通过应用扩展层来使用本地计量管理服务池提供的各项服务；这些服务可以是本地的，也可以是通过 P2P 的方式进行分布式发现的。

计量服务中心负责对系统进行集中式的管理和监控；对于企业应用，中心式的管控还是非常必要的。具体选择哪种架构可以根据实际需求来定。下面介绍两种典型的运行方式：

有中心的运作方式：

统一的用户管理、统一的策略设置、统一的版本控制、统一的事件审计，这些是有中心的运行方式的显著特征。这些功能上，采用的是 C/S 结构的框架。在计量服务的发现、管理和传输上，都可以采用 P2P 的方式进行管理。

中心服务器的弊端就是：single-point-failure（单点失效）和 bottleneck（瓶颈）。遇到这种情况，下面给出一些可能的缓解方案：

(1) 如果中心服务器忙碌或者失效，普通节点的用户可能会无法加入系统，此时可以把用户作为 Guest 或者以匿名(Anonymous)的身份进入系统，授权使用那些密级较低的计量管理资源。这就意味着应用场景变成了：普通的节点加入网络，是可以使用公开资源的；只有涉及到访问高密级的内容，享用特定权限（如读写、管理、备份）等时候才需要用户身份认证。

(2) 缓冲中心式决策结果（如策略、用户权限等）。

无中心的运作方式：

缺少中心服务器的场景下，具有更好的扩展性；但是同时也因为缺少可信中心或者可信第三方的环境，在实施用户管理工作中将变得比较困难。其它问题还有，比如：

(1) 策略不兼容的，访问被拒绝；

(2) 版本控制：手动提交备份，往自愿接收备份数据的节点上复制数据和数据描述。

3.2.4 计量管理系统节点安全增强设计

图 3.7 主要介绍了带有安全增强的计量管理节点构件，该构件主要用于进行上层应用的数据通信及安全增强保障。安全增强的一个应用就是实施访问控制。访问控制的算法细节请参见第 4 章的设计部分。

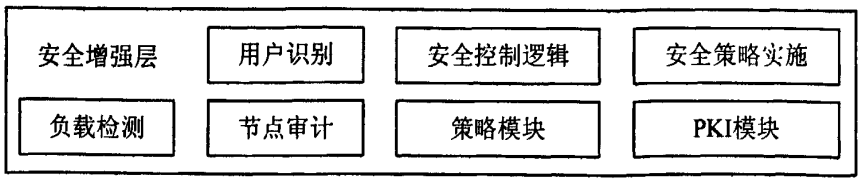


图 3.7 安全增强层模块

Fig. 3.7 MMS Security Enhanced Layer

如图 3.7 所示，安全增强层由用户识别、策略模块、PKI 模块、节点审计、负载检测、安全控制逻辑及安全策略实施等模块组成。其中，用户识别模块负责鉴别和标识用

户身份，作为主体代表用户访问客体（即边缘资源）。策略模块负责操作和解析策略定义；PKI模块负责鉴别用户身份和证明服务管理器中各服务的可信性；节点审计模块包括识别、记录、存储和分析节点上与可信相关活动有关的信息。通过检查审计记录结果可以用来判断发生了哪些可信相关活动以及哪些用户要对这些活动负责。为了便于观测和管理节点的运行状况，MMS 还添加了图形化的拓扑察看器、负载监视器以及日志审计功能。安全增强中的访问控制主要由安全策略实施和安全控制逻辑两部分组成。安全策略模块负责管理全局安全策略，安全策略逻辑负责计算访问控制权限，安全策略实施控制用户对计量管理数据的访问操作。

图3.7中的安全策略逻辑和管理模块与其它模块的交互关系可以参照图3.8所示。

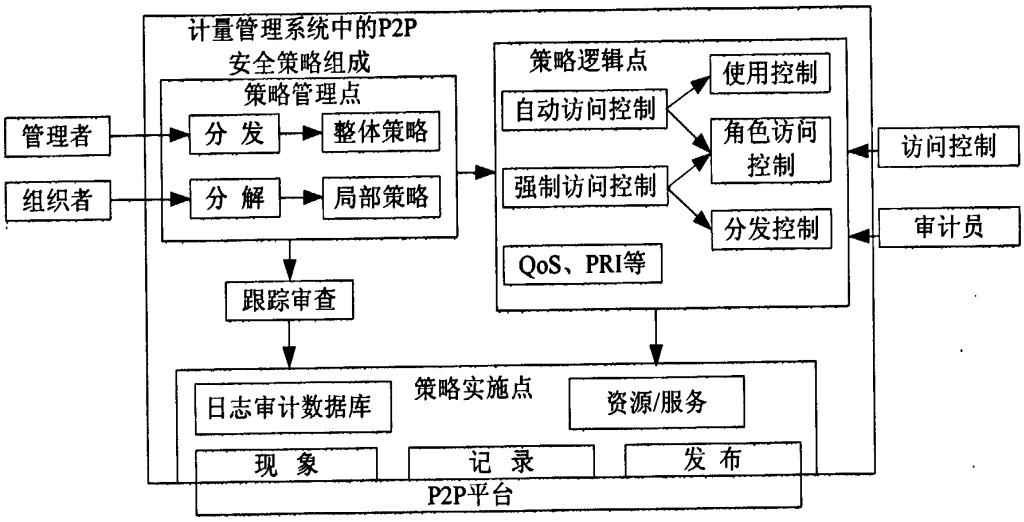


图 3.8 计量数据的访问和管理

Fig. 3.8 Metering Data Access Control and Management

图3.8中的管理者(Manager)和审计员(Auditor)对应于图3.6中的管理中心，也即计量管理部的领导角色。组织者(Organizer)对应计量子系统的管理者。访问客户(Requestor)对应于计量数据的最终用户。用户在访问计量数据的时候，在PEP、PMP和PLP的协作下可以完成授权操作。其中PEP、PMP和PLP都是传统的访问控制（如RBAC）所常见的功能，不再细说。访问控制的流程在实现部分有更多的解释，请参见下一章。

3.2.5 系统设计小结

P2P技术在计量管理系统中的应用过程中，必须得到首钢相应的保障措施，只有各项保障措施都得到了落实，才能确保P2P技术在整个系统中的研究顺利进行。

(1) 得到管理层的大力支持。这个应用研究项目如果在各个层次上都能得到管理人员的支持，那该研究就有可能被用户和专业开发人员从正面给予理解。而且管理层的重视还会保证研究得到足够的资金和其他必要的资源支持。

(2)相关人员进行培训。P2P 技术及 MIS 系统的使用对管理人员来说是新事物，绝大部分不懂或懂得甚少，这就要求管理人员对其技术和使用进行再培训。培训中应注意以下问题：

1) 信息化人才的需求是多方面和多层次的。

2) 应重视信息化应用开发的教育培训。

3) 走出单纯重技术的误区。

4) 非学历与非信息化人才的培训问题。

提高信息化人才的素质是根本。

(3) 节点预留问题。现在的应用研究仅限于首钢“一业多地”范围内的计量管理系统，必须要考虑的是今后与相关企业及其他单位的链接问题。只有这样才能把诸如原材料的购入量、消耗量、产品的产量、能源量的产出和消耗量等情况以定量的形式及时准确地反映给首钢决策部门。只有这样，首钢领导层才能通过定量分析，得出成本、利润、效益的定性结论，并及时发现问题，采取措施对生产的各个环节、经营活动的各方面进行有效的组织、调整和控制，以达到高质量、高效益的目标。而且通过 P2P 技术信息传输既安全可靠，又节省了一笔传输费用。

(4) 安全措施。计量管理系统上存有首钢的重要资源，其中包括一些专用的、保密的、具有战略意义的内容，并存有许多竞争对手之间非常敏感的数据，当计量管理系统运行后，为防止这些信息的外泄、被破坏、窃取、篡改，保证工作的高效性和合理性以及计量工作的正常运行，加强 P2P 技术的安全性应用甚为重要。

论文第四章就重点阐述系统的实现技术，比如：P2P 技术在计量数据存储方面的安全性保障技术。

第4章 系统详细设计与实现

4.1 基于P2P的数据存储设计

计量管理系统由三个子系统组成，每个子系统中存有大量的数据和信息，这些数据和信息基本是以数据库的形式进行保存的。每个子系统中保存的数据不同，但通过P2P技术可以实现数据与信息的共享。此节重点阐述每个子系统中的数据库设计内容。

4.1.1 物资计量子系统

该子系统只有一个数据库：物资计量数据库。该数据库的数据采集及查询操作如下。

4.1.1.1 数据采集流程

物资计量的方法有轨道衡计量；汽车衡计量；成品秤计量；工艺秤计量；其它秤计量等。无论是哪种计量方法，其计量数据或信息进入 ERP 系统流程基本相同，以进厂物资的轨道衡计量数据采集流程为例进行如下描述：

供应公司与用户签订供应物资合同的同时，将相关信息全部入机，内容包括：合同号、用户发站、发货单位、收货单位、物资品名、型号规格、合同数量等。同时将这些主数据信息全部入机传递到L4系统。然后录入车列号、车号、到站日期、原发重量等信息，核对无误后将这些数据信息时时传递到L3系统。并负责开具《质检委托单》和《计量申请单》（内容包含质检批次），选择处理方式（如直拨、卸地、打尖等），这些信息进入L3系统。

物资计量前，由运输部门提前通知计量站车辆计量情况，内容包括计量信息号、首尾车号、物资品名等信息，目的是让计量员作好计量准备，计量员提前将计量物资的信息从L3系统调出，等待进行下一步的计量操作。

动态衡自动采集（静态衡人工操作）确认保存计量数据。计量操作完成的同时，计算机界面自动合成相关匹配的计量信息，在操作无误正常情况下，计量数据与计量相关数据全部匹配，确认无误后，计量员把计量后的数据传递发送到L3系统。

根据L4系统下载订单信息和计量申请质检批次的统计原则，大宗原燃料使用原皮结算，车辆不用回皮的物资，L3系统统计出计量净重汇总数据，发送到L4系统；贵重物资必须回皮的车辆，等到车辆回皮后，回皮数据传送到L3系统，计量毛重、皮重匹配合成后，结算出具计量净重数据再发送到L4系统，物资计量操作才算全部完成。

L4系统接到进厂物资计量数据后，自动触发物资入库，质检部门根据批次，手工录入质检数据。

供应公司根据计量、质检数据，生成干基、成份品位、确定价格等条件数据。

财务部门根据物资流向确认数据，完成财务结算。

正常计量数据通过L3系统时时发送到L4系统；非正常情况由于计量部门的原因，计量物资没有计量结果或计量数据不准确，经过原因分析和领导同意，有权出具计量修正数据并上报计量管理部门。由于其它原因不具备计量条件的物资，计量管理部门通过物流过程管理，确定有发货单位的计量申请，有收货单位收料确认，有权出具最终的结算数据。月末公司结算，特殊情况需要异议仲裁，修正调整数据，采取在L4系统的物流过程中来办理对冲票手续，以实现完成全公司计量结算的管理。L4必须提供阶段性结算数据（盘库、压车在途、计量仲裁、计量异议等）的接口。

4.1.1.2 数据检索流程

这些数据和信息均在ERP上可以实现共享，各级人员首先输入自己的授权号及密码，然后进入ERP系统查询或打印所需信息。

数据检索功能的接口描述如图4.1所示。

工厂编码	1111	物料编码	0001
物料描述	焦炭	发货工厂编码	京发001
发货库存地编码	京001	收货工厂编码	京收005
收货库存地编码	京005	成本中心编码	0047

图 4.1 物资计量系统数据检索接口定义

Fig. 4.1 Interface definition of query in goods metering subsystem

根据输入的条件进行数据库查询，并将查询结果反馈给用户；输出的界面，支持用户将查询结果打印到屏幕上。

4.1.2 能源计量子系统

该子系统只有一个数据库：能源动力量数据库。其数据采集及查询操作如下。

4.1.2.1 数据采集流程

凡属厂际间能源量风、水、气(汽)等计量仪表的数据，由计量部门专人定期抄录、复零或监督；在公司各总降内的电能仪表，由电力运行人员定期抄录；非公司各总降内的电能仪表，由业主单位设专人定期抄录；其他人员不得任意复零或调量。各单位按时将各种能源量上报首自信公司能源计量管理部门。由数据统计人员将能源量耗用(或生产)量，人工方式以旬测算、月结算报表的形式进行数据保存，并将月分配表每月按规定时限交换给信息部，信息部经平衡后发给有关单位作为结算依据。

4.1.2.2 数据处理流程

各维护班组上报动力量数据后，由数据统计人员进行核对、计算，生成报表。其中电量数据一部分由电力网进行自动采集、处理，一部分是人工抄数进行录入。数据统计

人员接到电量后，由专人正确输入服务用户名、密码进入电力网系统，与电力网中传输的数据进行核对，并进行修改，数据以维护班组人工报数为准。核对修改完毕，执行运算功能，电力网系统自动进行数据处理，并可以生成相应电量报表。

4.1.2.3 数据检索流程

唯有动力量中的电量通过电力网进行数据采集（或人工录入）、数据处理、保存并打印报表。该报表的格式如表4.1所示。

表 4.1 能源（电量）计量系统数据格式定义

Table 4.1 Data format definition in power metering subsystem

单位	用电总量(kWh)	分配总量(kWh)	分配峰量(kWh)	分配谷量(kWh)	分配平量(kWh)
焦化厂	7931588	7931588	2591704	2763124	2576760
炼铁厂	9626820	9915623	3486941	3569135	2859547
氧气厂	843750	869062	322192	228927	317943
……					

4.1.3 量值传递子系统

根据量值传递工作的内容（如3.2.3所述）设有计量器具管理数据库；计量检定管理数据库；计量人员管理数据库和量值溯源管理数据库。这四个数据库的数据采集及查询操作如下。

4.1.3.1 计量器具管理数据库：

计量器具的管理工作是计量工作的一项基础工作。它是实现企业量值统一的物质基础，根据《计量法》要求，计量器具是监督部门主要的监督对象。

(1) 数据采集流程：每年底由首钢总公司信息部、首自信公司以及各生产厂矿进行计量器具台帐核对，内容包括：器具出厂编号、内部编号、器具名称、规格、型号、测量范围、准确度（不确定度或最大允许误差）、ABC 分类、管理状态、使用部门、安装地点、使用人员、检定日期、有效日期、确认间隔（检定周期）、检定部门、检定证书编号、检定费用、资产价值、计量类别、生产厂家等相关信息。其中企业最高计量标准装置（器具）数据信息由总公司信息部与首自信公司进行核对，工作标准计量器具和工作计量器具数据信息由首自信公司与各生产厂矿进行核对，核对无误、双方确认后即可纳入计量器具管理数据库。

(2) 数据处理流程：计量器具台帐核对准确后，由首自信公司标准计量站授权人员按数据库字段要求逐一输入计量器具相关数据及信息。用户可以一次录入一个计量器具的台帐和管理信息，不必在多个菜单下录入。如果一次购入相同的计量器具多个时，不

用一条一条的录入，可以点击利用新建并复制当前项功能进行复制（只需修改内部编号），大大加快了录入速度。

(3) 数据检索流程：计量器具数据和管理信息存入计量器具数据库后，各级计量人员录入相应授权用户名和密码后，可以对数据库中的计量器具相关数据和管理信息进行检索、查询和打印。

此数据库可以自动生成首钢最高标准器、工作标准计量器具和工作计量器具总台帐；工作计量器具配备台帐；计量器具修理信息台帐；工作计量器具管理目录等相关台帐。

此数据库可供确认标准器具和工作计量器具的管理状态（如在用、在库、限用、禁用、报废、降级、丢失、不合格……等）；帮助计量管理人员掌握每个计量点有多少计量器具？应配备多少？使用者是谁？检测那些项目？MCP 值是多少？确定配备的计量器具是否满足计量检测的设计要求。各计量器具是否在检定周期之内等内容，便于计量器具的监控管理。系统中设计了 MCP 值的计算公式，输入相应内容（T、u1 及 u 值）即可自动算出 MCP 值。计算公式如图 4.2 所示。

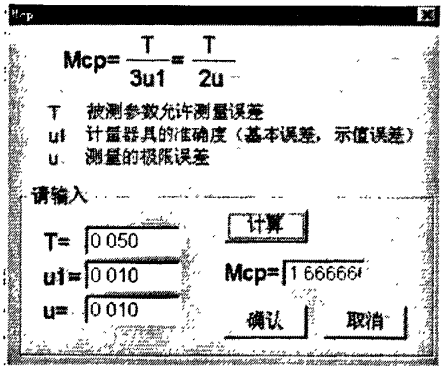
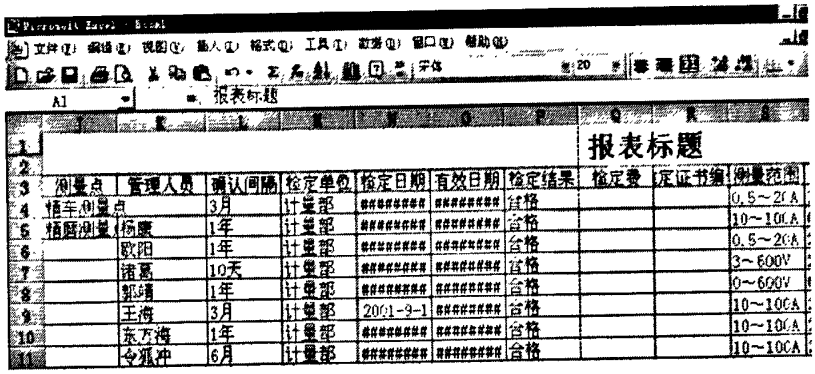


图 4.2　Mcp 计算方式

Fig.4.2 Calculating Formula of Mcp

表格自定义功能的设计，便于计量管理人员更加灵活的浏览、查询和打印，打印各种分类的器具清册。用户如果要打印屏幕显示的信息内容，可以点击设计的“Excel”按钮，系统将自动将窗口所显示的内容调入“Excel”软件中，以 Excel 报表的形式进行保存。

计量器具管理数据库实现后的总界面如图 4.3 所示。



报表标题

测量点	管理人员	确认间隔	检定单位	检定日期	有效日期	检定结果	检定费	证书编	测量范围
轧车间量点		3月	计量部	########	########	合格			0.5~2CA
精整测量	杨康	1年	计量部	########	########	合格			10~100A
	欧阳	1年	计量部	########	########	合格			0.5~2CA
	诸葛	10天	计量部	########	########	合格			3~600V
	郭靖	1年	计量部	########	########	合格			0~600V
	王海	3月	计量部	2001-9-1	########	合格			10~100A
	东方海	1年	计量部	########	########	合格			10~100A
	令狐冲	6月	计量部	########	########	合格			10~100A

图 4.3 计量器具管理数据库总界面

Fig.4.3 Overview of Metering Ware Management Database

4.1.3.2 计量检定管理数据库：

周期检定是一项复杂的系统工程，周期检定的目的是尽可能的防止使用失准的计量器具，以免造成量值混乱。在企业中由于计量器具种类多，使用分散，检定周期不同，往往不便于管理，常常出现漏检的情况。设计计量检定管理数据库，可以辅助计量人员编制计量年度检定计划及月度计划，自动编制检定通知单，贮存检定信息及统计各种需要检定的计量器具的数量等等。

(1) 数据采集流程：最高标准计量器具属于强制检定计量器具，由北京市计量检测科学研究院或中国计量科学研究院进行检定或校准。每月由首钢总公司信息部下发最高标准器周检计划，首自信按计划要求将最高标准器送至检定机构。检定完毕，由首自信人员取回最高标准器和相应检定证书。并将检定证书上的数据、信息人工录入计量检定管理数据库。数据信息内容包括：证书编号、检定日期、检定有效期、检定周期、检定单位全称、三级人员（批准人、核验员、检定员）、不确定度、检定依据、检定结论、检定结果等。

首自信公司标准计量站对工作计量标准和工作计量器具检定完毕后，由首自信标准计量站人员进入计量检定管理数据库，输入相应的检定原始记录数据信息[19]，内容包括：送检单位、器具名称、检定环境温度、湿度、标准示值、器具示值、允许偏差、平均偏差、结论及标准装置号等。同时输入相应计量检定证书内容，包括：证书编号、检定日期、检定有效期、检定周期、三级人员（批准人、核验员、检定员）、不确定度（或误差）、检定依据、检定结论、检定结果。

(2) 数据处理流程：相关数据、信息录入计量检定管理数据库后，可以动态刷新测量设备的检定状态，可以将选择的相关数据信息进行统计、查询、编制相关计划、报表等。

(3) 数据检索流程：此数据库可实现自动编制年度检定计划（如表4.2所示）、月度检定计划、检定通知单、抽检通知单、器具档案资料等，形成Excel 或 Word 文档进行保存或打印；

表4.2 年度检定计划

Table.4.2 Annual Checking Plan

送检单位	器具名称	规格型号	测量范围	检定日期	检定周期	检定单位	备注
标准计量站	传感器	92288011	6N	2008.01	1年	中国计量科学研究院	
电力厂	压力表	YB-150B	0-25MPa	2008.10	1年	标准计量站	随机
---	---	---	---	---	---	---	

计量器具检定证书[20]样式如图4.4所示。

首 钢 总 公 司

检 定 证 书

___字 第_____号

计量器具名称_____

规 格 型 号_____

制 造 厂_____

出厂编号

设备编号

送检单位

根据检定结果，准予该计量器具作_____使用。

主　管_____

校 验 员_____

检 定 员_____

检 定 日 期　　年　月　日

有 效 期 至　　年　月　日

图4.4 检定证书格式

Fig.4.4 Format of Authentication Cerfitification

可动态查询、掌握计量器具的管理状态、历史信息以及所执行的国家计量检定规程编号和规程名称；

可动态统计到期需检的计量器具数量；所需计量检定费用；计量检定费收入情况；统计应检率、受检率、合格率、一次检定合格数；各班组工作量；

可帮助计量管理人员确定检定周期的合理性，是否有必要调整确认间隔。如遇计量纠纷，可以随时查看当时的计量检定记录，提供仲裁依据。

4.1.3.3 计量人员管理数据库：

在首钢公司内计量人员不仅包括计量检定人员，还包括 ISO9000 内审员、ISO/IEC17025 内审员等。为不断改进提高内部计量审核的效果，保证首钢计量体系的正常运行，加强计量人员的管理非常重要。所以设计了计量人员数据库。

(1) 数据采集流程：计量人员经过培训、取证后，由计量管理人员将其相关情况如姓名、性别、出生日期、文化程度、民族、参加工作时间、职务、职称、专业、身份证号码、培训内容、取得的证书编号、证书有效期、检定人员所取得的检定项目、每个检定项目所依据的计量检定规程等数据或信息均录入计量人员管理数据库。

(2) 数据处理流程：相关数据、信息录入计量人员管理数据库后，计量管理人员可以选择相关数据信息进行统计、查询、编制相关培训计划、报表等。

(3) 数据检索流程：此数据库可实现自动统计、打印计量人员自然情况、培训情况、检定人员持证情况台帐。

管理人员可动态查询、掌握计量检定人员持证情况是否满足计量检定工作要求。随时可以编制计量人员培训计划。

人力资源部门可根据需要检索出相关人员培训信息，并将其纳入参加培训人员人事档案。如图 4.5 所示。

姓　名	王平	性别	女	身份证号码	1101071970********
文化程度	大学	民族	汉	职称	工程师
培训日期	2007.10	培训内容		ISO9000 内审员	
证书编号	1205	证书有效期	2010.10	培训费用	1200

图 4.5　检定人员培训信息

Fig.4.5 Trainning Information of Meterman

计量管理部门可根据检索出计量检定人员持证情况，如图 4.6 所示。可以随时掌握计量检定员证到期情况及统计每月操作证复核培训费用。

姓名	赵非	性别	男	身份证号码	110107**********
文化程度	大专	职称	无	专业	长度
工作单位	首钢	证书编号	京 2005	培训费用	1000
持证项目	压力表	有效期	2010.10.05	检定规程	压力表检定规程

图 4.6 检定人员持证信息

Fig.4.6 Licence for Meterman

4.1.3.4 量值溯源管理数据库：

量值溯源是指量值是如何传递的。根据国际标准的要求，“所有测量设备都应可溯源到国际或国家测量标准的测量标准进行校准”，以保证量值传递的准确性。因此在量值

传递过程中不合格计量器具的控制非常重要，只有确保不合格计量器具不流入量值传递环节或者合理修正不合格计量器具带来的误差，才能保证量值传递的准确性，不会对企业生产造成损失。此数据库包含了追溯对象（不合格产品或不合格计量器具）、工作计量器具、工作计量器具检定信息、工作计量器具检定记录到追溯到标准检定装置等相关数据内容。

(1) 数据采集流程：在计量器具检定过程中，若发现该计量器具检定不合格，检定部门通知计量器具送检单位对其测量过的计量点及相应产品或传递过的计量器具进行追踪。以防止不合格产品的产生，对企业生产工序产生无可挽回的影响。

(2) 数据处理流程：量值溯源管理数据库设计了“不合格计量追溯”，检定单位发现不合格计量器具后，将其基本信息从计量器具管理数据库中调出，增加不合格事实描述、不合格追溯对象字段、追溯日期等内容。随同计量器具的检定不合格报告一起返回送检单位，由计量器具使用单位组织相关人员对不合格计量器具带来的可能后果进行追溯，将其结果录入量值溯源管理数据库。

(3) 数据检索流程：溯源查询主要用于查询不合格计量器具的量值传递关系。从发现的不合格产品（或不合格计量器具），一直追溯到标准检定装置。用户可以从这个量值传递链中查询其中引起不合格的因素，从而制定相应的纠正和预防措施，自动生成“不合格计量器具报告”，格式如图 4.7 所示。此表由计量器具使用部门进行备案。

使用部门	计量器具名称	编　　号
内部编号	规格、型号	测量范围
追溯日期	被追溯对象	
追溯结果		
不合格事实描述		
纠正措施	纠正措施验证	
预防措施		负责人签字

图 4.7 不合格报告格式
Fig 4.7 unacceptable report format

4.2 基于 P2P 的网络通信设计

4.2.1 网络通信流程

这里选取查询过程为例，查询请求发出后，本地服务会首先返回结果；查询请求会继续往 P2P 网络分发；其他节点的响应会异步的返回。本地计量服务需要对这些结果进行整理和聚类，反馈给用户。网络查询时序图如图 4.8 所示。

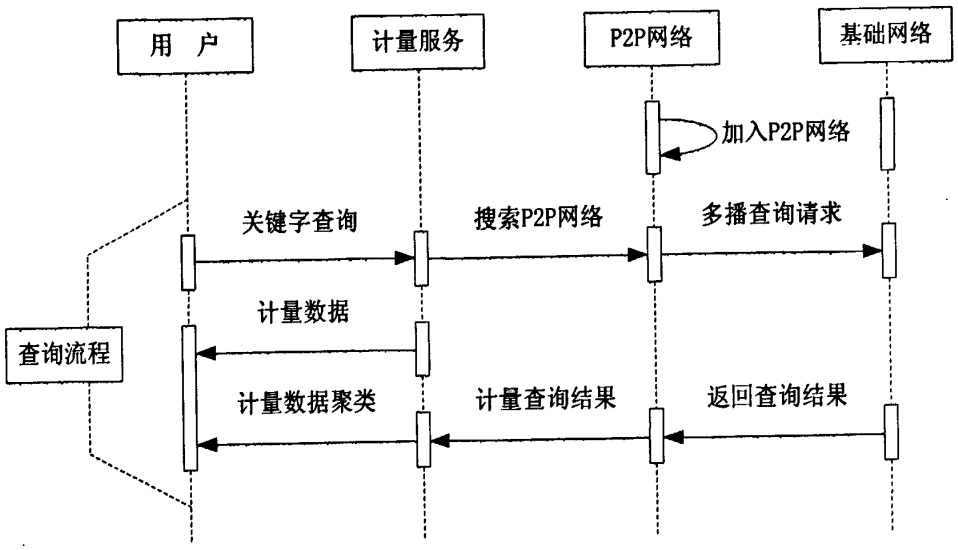


图 4.8 网络查询时序图

Fig. 4.8 Workflow of network query

整个过程中需要两种关键的通信模式：

(1) 单播（Unicast）：两个节点之间直接通信，数据从一个计量节点发出，然后被另外一个计量节点接收，中间也不会发送到其它节点上。这种情况我们称之为单播。单播适用于特定的有限的节点之间进行通信。两个节点的单播过程如图 4.9 所示。

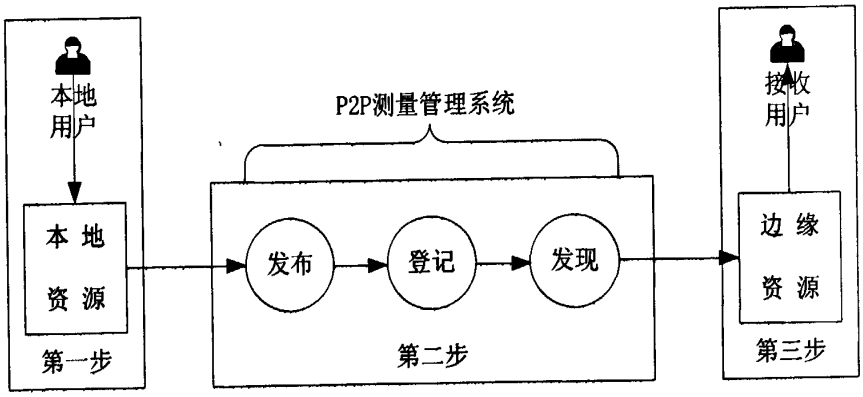


图 4.9 单播流程

Fig. 4.9 Workflow of unicast

(2) 多播（Multicast）：当一个计量节点需要从多个计量源获得数据，或者发出信息给这些计量节点，就需要一种类似广播（Broadcast）的方式进行通信。虽然多播可以用一组单播来实现，但是无论网络开销还是时间开销都是难以接受的。

4.2.2 单播和多播的实现

本文实现了两种通信方式：单播通信（Unicast）和多播通信（Multicast），用来支持策略变化和框架调整。前者用于两个模块之间有明确交互对象的一对一通信场景，比如：访问权限查询、安全策略下载等；后者用于向一组交互对象通信的一对多的通信场

景，比如：策略更新信息、节点退出信息等。以单播通信协议为例，为了应对网络拥塞和节点失效等带来的通信失败问题，本文设计了一个轻量级自适应单播通信协议。单播通信信息发送操作的算法如下：

```
MMS.Unicast.SendMessageThread.Run(){
    while(running){
switch(SendMessageWithTimeOut(Sender,Receiver,Message).getInterruptException()){
            HASNEWMESSAGETOBESEND:
                addNewMessageToMessageBuffer();
                continueSendMessageWithTimeOut();
            TIMEOUT:
                composeMessagesBufferToOneMessage();
                continueSendMessageWithTimeOut();
            SUCCESSACKNOWLEDGE:
                removeSuccessMessageFromBuffer();
                break;
            TIMEOUTTOOMANYTIMES:
                processReceiverIsDown();
                break;
        }
    }
}
```

接收信息操作的算法类似，不再赘述。

多播通信的通信协议相对比较简单。多播的发送者发送多播信息给一组接收者，无需等待信息的回应；多播的接收者采用多线程阻塞监听的方式来接收多播信息。发送者也可以监听自己的多播信息，从而确定信息发送的成败与否，以及监测其他节点冒充自己发送多播信息的非法行为的发生。但是多播通信需要约定一套多播端口协商生成算法，保证多个接收者都可以获得多播信息的目标端口，并监听在该端口上。比如：计量管理中心需要通过多播通信群发策略变更的信息给多个计量管理节点，在原型开发中，可以采用将多播目标端口写入计量节点的描述信息的方法，让计量节点可以监听到该计量管理中心的多播信息。针对不同的 P2P 平台可能会有不同的实现方式，但是要注意避免广播风暴的发生。

为了保证通信过程中信息的机密性和完整性，有必要采用加密技术。本文建议：敏感操作（如申请安全标签、用户身份鉴别等）必须使用加密方式进行通信；带有敏感数据的多播通信，可能需要改成易于加密的单播通信，或者使用组加密通信技术。加密可

以采用SSL等现有方法，不是本节讨论的重点，不再多说。

4.3 安全性考虑及访问控制算法

4.3.1 安全需求

前面几章主要阐述了P2P技术在计量管理系统中的应用优势，但在计量管理系统实际应用中，每台计算机（即节点）都有可能随时暂时或永久的离开计量管理系统，而且这些节点是对等的，拥有很大的自治性和不可信性，这些节点均负责存储数据，一旦某节点暂时离开，存在其上的数据就将暂时不可访问，假如此台计算机彻底瘫痪，形成此节点永久离开，更会造成数据的丢失。因此，如何保证数据的持久存储，屏蔽这些系统错误，成了计量管理系统有序运行的重要需求。

节点的安全性低的部分原因来自于节点具有一定的自治性和可信性，特别是那些由闲散桌面机组建的存储系统，这些节点机除了执行计量管理系统中P2P存储功能外，还为所属用户提供其他服务，此节点将受到理性用户[21]和恶意用户的干扰和破坏，破坏正常节点的路由，有可能造成整个计量管理系统的瘫痪。

由于节点的对等和自治，会造成一旦一个节点将其存储的数据发布到多个节点上，此节点常常会失去对数据的控制的局面。这意味着单个节点可以直接向其他节点请求和交换边缘资源。其他节点是否响应数据请求，发布节点无法直接干涉和控制，从而可以绕过传统模式下访问控制中心，引入了信息泄露等安全问题。由于访问控制等安全技术的难以实施，信息被篡改及破坏[22],[23]和恶意行为及信息泄露[24]等大大降低了资源和节点的安全性和可用性。

如何保证信息的安全性和私密性，一直是学术界研究的热点[25]。在新型网络环境下，如何保障数据发送后的可控制性，有关专家提出了P2P存储系统中的访问控制算法[26]，就很好地解决了这一问题。

4.3.2 访问控制算法

为了提高数据的可用性，P2P存储系统常常选用一种基于纠删码的门阀方案，通过冗余和分块的方式来提高数据的可用性。

纠删码（Erasure code）是由一个四元组(k, n, b, k')来确定的编码。设其编码函数为E，解码函数为D，对于消息 $M = (M_1, M_2, \cdots, M_k)$，其中 $M_i(1 \leqslant i \leqslant k)$为大小为b bits 的消息包，编码后的消息 $E(M) = (M'_1, M'_2, \cdots, M'_n)$，其中 $M'_i(1 \leqslant i \leqslant n)$大小仍为b bits。设E(M)'为E(M)中任意k'(k'≥k)个包组成的子消息，则D(E(M)') = M，即对E(M)中任意k'个消息包进行解码就可以得到原始消息[27]。

纠删码（Erasure code）作为一种 FEC (Forward Error Correction)技术，主要应用在高可用和低成本的通信中来避免包的丢失。 P2P 存储系统可以利用它来提高存储的可靠性，如图 4.10[28]所示。首先将要存储在系统中的文件分割成 k 块，然后对其编码得到 n 个文件碎片并进行分布存储，这样只需要存在 k'个可用的文件碎片，就可以重构得到原始文件。

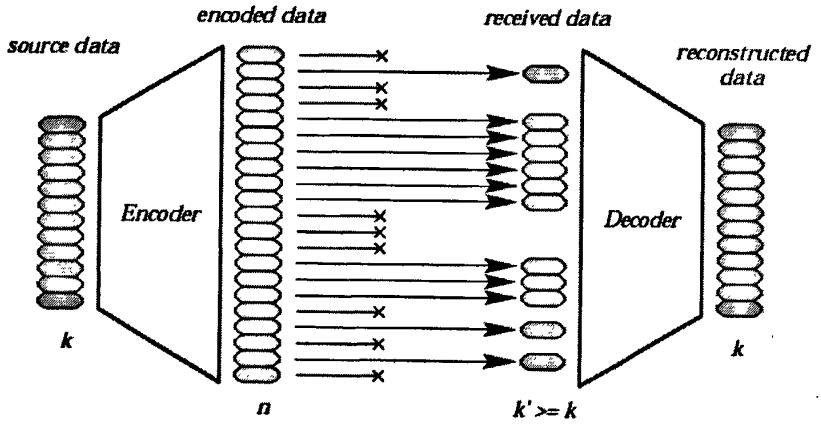


图 4.10 编/解码过程的图示

Fig4.10 A graphical representation of the encoding/decoding process

下面简化描述访问控制算法在 P2P 存储系统中的应用方式：

put(index, data): 将数据发送到 P2P 存储系统里面，这样别的节点就可以找到该数据。index 指示了数据(data)的存储节点位置。文中，我们称之为 broker 节点。

Value = get(index)：请求 index 所指向的数据。

remove(index): 从系统中删除 index 所指向的数据。

这里的 data 是指所要存储的数据对象，也即控制中的客体(Object)。本节还令 Erasure Code 的编码过程记成 EC Encode，编码过程记成 EC Decode。一个客体的提供者(或者发布者，记成 (Object Provider)，他会为需要控制的客体定制一份安全策略(记成 Policy)，再发布 Object 的同时发布 Policy。保存数据的中间节点称为 Broker Peer，希望访问客体的用户称为 Object Requestor。整个访问控制的过程如图 4.11 所示。

Object Provider 在发布数据之前，首先使用 EC Encode 将 Object 编码成 n 个块 (记着 ObjBlock)，每块都附上一个完整的策略，然后将 n 个带有安全策略的 ObjBlock 发布到 n 个独立的节点上。

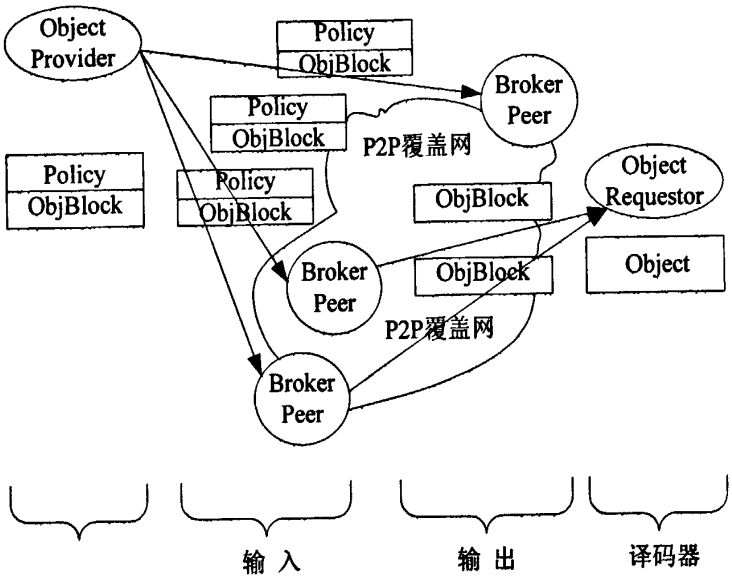


图 4.11. 基于 P2P 的安全解决方案中的数据和策略分发算法

Fig.4.11 Data and policy distribution for peer-side security enforcement

Object Requestor 想访问数据时，将分别向多个 Broker Peer 请求他们各自所持有的数据块 (ObjBlock)，然后将获得的数据块使用 EC Decode 还原成原来的数据 (Object)。

Broker Peer 是数据块的持有者，它同时负责实施 Object Provider 所设定的策略，来决定是否授权 Object Requestor 的访问请求。当一个 Object Requestor 获得了它所请求的数据块，那就意味着：至少 k 个 Broker Peer 授权了它的访问，并且提供了真实可用的数据。

我们将上面的访问过程总结成两个协议：Write 和 Read。Write 用于发布数据，Read 用于访问数据。

Write 发布数据的算法如下：

```
// Encode the Object into blocks using erasure code.
BlockSet = ECEncode(Object, eKey, policy, k, n)
//Publish blocks to n different broker peers.
Counter = 0
for each block Bi in BlockSet
  if put(Bi.Ii.key, Bi) successfully
      counter++
//Check if no less than k blocks were published
if counter++ >= k
return success
return false
```

Read 访问数据的算法如下：

// Calculate the keys of blocks

KeySet = M'(keywords)

//Request all the blocks asynchronously

for each key K_i in KeySet

NewThread { $Block_i$ = get(K_i) }

//Wait until at least k verified correctly blocks are received or timeout.

Wait();

if number of verified correctly blocks ≥k

return ECDecode($Block_{i,}$)

return null

Write 和 Read 中还添加了私密性保护的内容，即使用了一种称为 keyless encryption [29]的方法，来保证数据块的私密性。它的原理是：选择随机数(ekey)作为密码来加密数据(Object)；然后加密后的 Object 和 key 一块儿被 EC Encode 编成 n 块。Read 协议将收集到足够多的块 (>k) 来还原 ekey，然后用它来解密 Object，获得原始的 Object。Write 协议中块的索引生成的算法 M' 如下：

$$index_i = M'(keywords) = \left(M(keywords) + \frac{2^d \times i}{n} \right) \%2^d, i = 1,...,n. \qquad (4\text{-}1)$$

它的作用是将各个块最大程度的分散[30]。讨论了不同的放置策略的优缺(比如：顺序保存和随机保存等)，这样 M'的算法可以保证一定程度的负载均衡；在处理随机错误的情况下，虽然它和随机放置的性能是差不多的，但是这种方法可以提高检索的效率。

也就是说，在计量管理系统中，每个节点在系统中发送数据或信息时，均会为其相关节点同时发送数据或信息的安全保障信息，在需求者访问这些数据或信息时，P2P 技术会通过其控制算法自动将其还原成原始信息供需求者使用。所以 P2P 存储系统的访问控制算法，保证了数据所有者在数据分发后仍然对其实施控制，在不降低系统可用性情况下，保证了计量管理系统内信息访问的可信度。

4.3.3 算法有效性分析

当一个 Object Requestor 向一个 Broker Peer 请求数据块时，有两种情况会造成访问失败，即使 Object Provider 的策略是允许的：

Broker Peer 是不可用的 (unavailable)：有很多原因可能造成节点的不可用，比如：网络故障；节点失效；数据篡改；软件错误；配置错误等等。

这个 Broker Peer 是不诚信的 (dishonest)：Broker Peer 不严格执行数据块所附策略

的行为，被称之为不诚信的。

Broker Peer 的 unavailable 降低了系统的可用性，但是 dishonest 却可能造成信息泄漏：在 Object Provider 的策略是拒绝的情况下，让 Object Requestor 获得访问该数据的权力。

为了达到较好的效果分析， 我们设定下面的假设条件：

节点标识和块索引是均匀独立的分布，而且是可以抵抗 Sybil Attack[31]的；

Broker Peer 的 unavailable 和 dishonest 行为是均匀独立的分布；

节点之间的通信是安全可靠的，所有的失效主要发生在节点上。

同时，我们约定下面一些变量来表示系统状态，如表 4.3 所示。

表 4.3. 分析中用到的常见变量

Table 4.3 Common variables used in analysis

Var.	Definition
n	total number of blocks
k	number of blocks needed for reconstruction
r	code rate, i.e. r=k/n
p	dishonest rate of peers
q	unavailable rate of peers
P_0	probability that an object is available when the access request should be satisfied according to object provider's policies
P_1	probability that an object is available when the access request should be rejected according to object provider's policies

P_0 表示了访问控制的可信性，是指当策略应该授权访问的时候，Object Requestor 可以访问数据的最小概率。P_1 表示了访问控制的不可信性，是指当策略应该拒绝访问的时候，Object Requestor 可以访问数据的最大概率。那么根据二项式分布,我们可以计算二者的值为：

$$P_0 = \sum_{i=k}^{n} \binom{n}{i} ((1-p)(1-q))^i (p+q-pq)^{(n-i)} \quad (4\text{-}2)$$

$$P_1 = \sum_{i=k}^{n} \binom{n}{i} (p-pq)^i (1-p+pq)^{(n-i)} \quad (4\text{-}3)$$

如果系统中有 10%的节点是不可用的，10%的节点是不诚信的，使用 r = ½ 的纠删码编码的访问控制系统，将一个客体分成 32 块，那么 P0 = 0. 99998，而 P1 = 0.000000003。如果调整 r = 14/32，那么 P0 = 0.9999994 而 P1 = 0.0000002。

显然，r 在 P_0 和 P_1 之间扮演了一个平衡器的作用。对于一个实践中的系统， 我们

会期望 P_0 和 P_1 有一个大致的范围(称之为安全需求)，如不等式(4-4)所示。下面的算法将给出 r 满足的条件的解。

$$\begin{cases} P_0 \geq \alpha, \alpha \to 1 \\ P_1 \leq \beta, \beta \to 0 \end{cases} \tag{4-4}$$

使用代数简化和正态分布来逼近二项式分布的方法，我们可以得到:

$$\begin{cases} r_1 \leq (1-p)(1-q) - \sigma_1 \sqrt{\dfrac{(1-p)(1-q)(p+q-pq)}{n}} \\ r_2 \geq p(1-q) + \sigma_2 \sqrt{\dfrac{(1-p+pq)(p-pq)}{n}} \end{cases} \tag{4-5}$$

其中 σi,i=1,2 是标准偏差，对于期望的安全需求，当 n 足够大(大于 16 即可)时候，满足下面的表 4.4。 表 4.4 还给出了 n 为 32 时候的标准偏差的取值，这是一组更为标准的值。

表 4.4 α, β 期望水平下的临界值

Table 4.4 Critical Values for desired level of α, β

α and 1- β	σi,$n \to \infty$	σ, n=32
0.800	1.282	1.309
0.900	1.645	1.694
0.950	1.960	2.037
0.975	2.326	2.449
0.990	2.576	2.738
0.995	2.807	3.365
0.999	3.291	3.622

比如：如果希望 P0 ≥ 0.99 且 P1 ≤ 0.0001，而且 n = 32，σ1 应该 2.738 而且 σ2 应该 3.622。如果 p = 0.2 且 q = 0.1，那么 r 则有解[0.426, 0.503]，即 k 的取值范围是[14, 16]。如果 r 无解，则说明预定的安全需求无法满足。

从前面的分析中，我们可以得出下面的结论：

(1) 当不诚信节点的规模不是很大的时候(比如：低于 50%)，该算法可以有效的保证访问控制实施的可信性；

(2) 调整参数 r=k/n，可以有效的平衡访问控制的最小可用性和最大不可信性。

前面的算法中，假设节点（包括：不可用节点和不诚信节点）是均匀分布的，当不诚信节点占总结点的比例不是太大的时候，该算法可以有效的保证访问控制实施的可信性。这个得法仍存在一些有待改进的地方，他们是：

(1) 难以检测被污染和破坏的数据块。因为只有在数据块下载完了，才知道数据块是否可用的，这种无差别的下载顺序，对于一个数据块损坏率为 f 的系统，所需要传输块数的期望值是 min{n, k/(1-f)}，需要访问的节点数的期望值是 min{n, k/(1-f)}。这降低了系统的存取效率。

(2) 无法限制不诚信结点数目。不可用节点降低了 Write 和 Read 协议的成功率，不诚信节点增加了访问控制实施的失效的概率。如果不能检测和限制不诚信节点的数目，则难以提高访问控制成功实施的概率。

为了解决这两个问题，应用了一个基于推荐的改进算法，通过节点投票的方式来检测不诚信节点和不可用数据块，并尽量孤立这些节点，减少访问控制失效的概率。算法改进思想：

Object Provider 发布数据(Object)之前，先尝试获得各个目标结点的推荐值，然后将数据块发送到诚信度和可用度高的节点上；

Object Requestor 请求数据(Object)之前，先尝试获得各个目标结点的推荐值，然后优先请求诚信度和可用度高的节点；下载完成或者失败超时时，发布自己对某个 Broker Peer 的推荐值，供其他节点参考；

Broker Peer 除了要保存数据块、执行安全策略外，还要保存推荐值，并根据不断收到的同一个数据块的推荐值进行加权计算；Broker Peer 所持有的数据块和这些数据块的推荐值不应该在同一个结点上，因为一个非诚信节点有恶意篡改自己持有块的推荐值的动机。

由于在全分布式系统中假设一个可信第三方来保存推荐值的方式是不和谐的，所以推荐两种可能的推荐值保存方式如下：

(1) 仍然保存在同一个 Object 的多个 ObjBlock 所在的 Broker Peer 上，不过并不是一一对应的保存，而是对 $ObjBlock_a$ 的推荐值保存在 $ObjBlock_i$ 上，其中 i=1,...,a-1,a+1,...,n。采用这种冗余的保存方式，可以采用 Byzantine 的方式来避免一些恶意节点修改自己所持有的推荐值。

(2) 保存在跟保存 ObjBlock 不相关的节点上。这样做的好处是，推荐值的数据是可以控制的，对于一些不诚信节点少的系统，不需要使用太多的推荐值就可以有效的检测恶意节点了。

这样改进的 Write'用于发布数据，Read'用于访问数据。其算法分别如下。

Write'发布数据的算法如下：

```
KeySet = M'(keywords)
//Request all the recommendation values
for each key Ki in KeySet
RecSet.insert(get(Ki) );
//Sort the KeySet according based on recommendation
SortKey(KeySet, RecSet);
```

```
// Encode the Object into blocks using erasure code.
BlockSet = ECEncode(Object, eKey, policy, k, n)
//Publish blocks to n different broker peers.
Counter = 0
for each block Bi in BlockSet
    if put(Bi.Ii.key, Bi) successfully
        counter++
//Check if no less than k blocks were published
if counter++ >= k
    return success
return false
```

Read' 访问数据的算法如下：

```
KeySet = M'(keywords)
//Request all the recommendation values
for each key Ki in KeySet
RecSet.insert(get(Ki) );
//Sort the KeySet according based on recommendation
SortKey(KeySet, RecSet);
//Request all the blocks asynchronously
for each key Ki in KeySet
NewThread { Blocki = get(Ki) }
//Wait until at least k verified correctly blocks are received or timeout.
Wait();
//send out the recommendation requestor self.
for each key Ki in KeySet
put(Recommendation(Ki));
if number of verified correctly blocks ≥ k
    return ECDecode(Block_i,)
return null
```

换句话说，访问控制失效的一个因素在于一定量的数据块分布在不可用节点和不诚信节点上，访问控制的成功率和系统的可用性受到了这部分数据块的影响。改进后的Write'和Read'协议可以检测和避开这些节点，从而有效的减少首钢计量管理信息系统中不可用节点和不诚信节点上的数据块的数目。从而达到了在不降低系统可用性的前提下，能够以期望的概率安全实现数据或信息的访问控制。

第5章 系统测试及应用

为了验证本文设计中的算法的有效性，以及整个系统的可行性，本节分别采用仿真和实际布置的方式对系统特性进行了验证。

5.1 基于P2P的计量管理仿真验证

鉴于目前基于P2P的首钢计量管理系统尚未获得大规模的部署和实践，为了验证数据分发和访问控制的效果，本文采用了仿真的方式对算法进行了测试和验证。仿真是一种高效和可再现的测试方式，是大规模网络的仿真的必要手段之一。

5.1.1 仿真验证工具选择

现在已经有了好几个用来做P2P仿真相关的平台，如PlantLab，GT-Item，PeerSim，GPS等，前面两个出现的频率比较高一些。需要补充的一点：著名的仿真器NS2，并不太适合于P2P的仿真。做P2P仿真需要实现的几个功能：

(1) 网络拓扑的生成（如：满足小世界模型）

(2) 节点的加入和退出（如：满足正态分布）

(3) 策略的制订和实施（如：前提假设和算法）

(4) 数据的收集和分析（如：开销、延时）。

在众多的仿真器中，各个仿真器的功能、规模都不尽相同[32]。虽然可以自己实现自己的仿真环境，但是这样的环境常常缺乏可信性和可比性。本文中，选择P2PSim[33]作为算法的仿真原型，理由如下：

(1) P2Psim是C++语言开发的，具有更好的执行效率；

(2) P2Psim是由离散事件驱动的仿真环境,更符合我们场景的需要；

(3) P2Psim上面已经实现了多种DHT协议，便于进行协议对比；而且支持新的DHT协议的设计，具有很好的可二次开发性。

(4) P2PSim中使用的协议已经在其所属实验室的其他产品上得到应用（比如CFS），熟悉P2PSim的代码便于日后使用该其对应的开发包（SFSLite)来开发真实的产品。

5.1.2 P2PSim介绍

P2PSim[33]是由麻省理工大学（MIT）的计算机与人工智能实验室（CSAIL）的并行和分布式系统研究组（PDOS）开发出来的，它是一个免费的、多线程的、基于离散事件的仿真软件，由C++语言开发出来的。P2PSim可以运行在类似于unix的系统中，主

要是对 P2P 协议的仿真。目前已经支持 Chord, Accordion, Koorde, Kelips, Tapestry 和 Kademlia 等协议。P2PSim 是 IRIS 项目的一部分。使用者可以自己添加协议来实现 P2P 协议的仿真。官方网站声称：P2PSim 可以支持 3000 个 Chord 节点的仿真。最新版本(P2PSim-0.3)已于 2005 年 4 月份发布。

P2PSim 主要包含了以下几大类：协议类(ProtocolFactory)，事件产生类(EventGeneratorFactory)，评述类(ObserverFactory)，拓扑类(TopologyFactory)，事件类(EventFactory)，失效模型类(FailureModelFactory)，事件队列(EventQueue)，线索(Threaded)。p2psim 的主要类如图 5.1 所示。

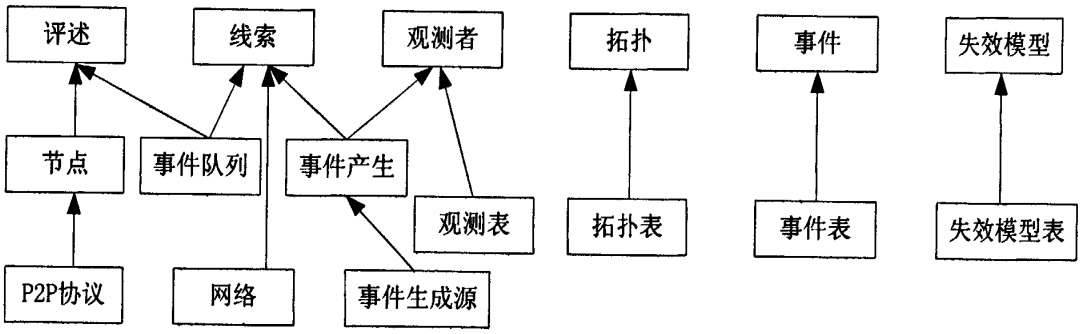


图 5.1 p2psim 的主要类

Fig. 5.1 Main class of p2psim

下面将简单介绍上述所提到的类。

(1) 协议类(ProtocolFactory)是系统中协议的一个集合，里面实现了 Chord, Accordion, Koorde, Kelips, Tapestry 和 Kademlia 等协议，这些协议都是完整的实现了，可以直接用这些协议进行仿真。其中有个 Sillyprotocol 的空类，这个空类没有实现任何的功能，只是提供了一种接口，自己可以在这个空类里面实现自己的协议进行仿真，提供了很大的方便。

(2) 事件产生类(EventGeneratorFactory)是系统中产生事件的一组类，其中包含了 ileEventGenerator ，ChurnEventGenerator，ChurnFileEventGenerator 和 SliiyEventGenerator 四个产生事件的类，这其中前三个是已经完整实现的事件产生类，可以直接调用，通过调用这些类可以产生在仿真过程中所需要的事件。在每次仿真中，只能调用其中的一个产生事件的类。SillyEventGenerator 是一个空的产生事件的类，只是实现了一个接口，可以在这个空类中定义自己在仿真中需要的一系列事件，结合 ProtocolFactory 中的 Sillyprotocol 空类，实现自己需要仿真的协议，然后在利用 SillyEventGenerator 实现仿真协议所需要的一系列事件就可以完成对协议的仿真。

(3) 拓扑类(TopologyFactory)是系统中协议仿真所需拓扑的一组类，主要有 gtitm, G2Graph, Euclidean, E2ETimeGraph, E2ElinkFailGraph, ConstDistTopology, DVGraph,

E2EGraph, E2EAsymGraph 等类，这些类是一个接口，可以利用专门的拓扑产生器生成相应的拓扑，然后利用 topology 中这些类读取这些拓扑的数据。

(4) 事件类(EventFactory)是一组事件的类，这其中的事件是仿真中协议所需要的一系列事件。其中主要有三类事件，NetEvent、p2pEvent 和 simEvent。P2PEvent 包含了 P2P 系统中一些常见的事件，包括了 Join，crash，lookup，nodeevent 事件。Simevent 中主要包含的是仿真结束时的 exit 事件。程序的最后通过调用这个事件结束程序的仿真。

(5) 失效模型类(FailureModelFactory)主要包含了一些失效的模型，这些模型是对数据包失效后所采取措施的一组模型，主要有 ConstantFailureModel，NullFailModel 和 RoundtripsFailure 模型，在每种模型中都对数据包失效后采取了不同的处理方法。

(6) 固定失效模型类(ConstantFailureMode)是在数据包失效后，将其延迟固定的时间后再发送，RoundtripsFailur 是在数据包失效后，将其延迟 rtt(roundtrip time)时间的一半后再发送，由于每次仿真中的 rtt 时间不一定相同，延迟的值也将随着 rtt 的时间的变化而变化。

(7) 评述类(ObserverFactory)包含了一组 Observer 信息，主要含有 ChordObserver，DataStoreObserver，KelipsObserver，OneHopObserver，ProtocolObserver，TapestryObsever 六个类。

其中，对于搭建一个全新的协议，最主要的类是实现自己的 EventGenerator 和 Protocol。主要是因为：Topology 已经支持多种拓扑生成器的生成结果，而 Observer 不是必需的。

P2PSim 是一个离散事件驱动的网络仿真软件，系统中的状态只是在离散的时间点上会发生变化，而且这些离散的时间点是随机的。每当有一个事件出现后时间往前推进，也就是时间是跳跃前进的。一个仿真时间点上可以同时出现多个事件，事件的发生可以有疏密的区别。

用事件的观点来分析真实系统，通过定义事件及每个事件发生引起系统状态的变化，按时间顺序确定并执行每个事件发生时有关的逻辑关系，这就是事件调度法的基本思想。按这种策略建立模型时，所有事件均放在事件表中。模型中设有一个事件控制模块，该模块从事件表中选择具有最早发生时间的事件，并将时钟修改到该事件发生的时间，然后调用与该事件相应的事件处理模块，该事件处理完后返回时间控制模块。这样，事件的选择与处理不断地进行，直到仿真终止的条件或程序事件产生为止。如图 5.2 所示。通过离散事件驱动的仿真机制实现了在进程级描述通信的并发性和顺序性，再加上事件发生时刻的任意性，决定了可以仿真计算机和通信网络中的任何情况下的网络状态和行为。

每个仿真都要维持一个单独的全局时间表，其中的每个项目和执行都受到全局仿真时钟的控制，仿真中以事件顺序调度事件列表中的事件，需要先执行的事件位于表的头部。当一个事件执行后将从事件列表中删除该事件。

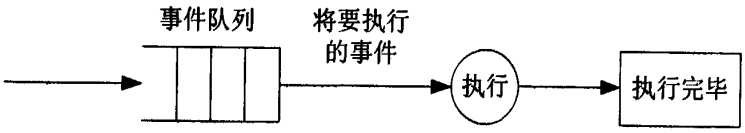


图 5.2 仿真调度模型

Fig. 5.2 Simulation scheduling model

在 P2PSim 中，事件分为三类：

(1) P2PEvent，包含了在P2P协议中常见的一些事件，如 join，crash，lookup，nodeevent 事件。这些事件对应着节点的一些动作行为。

(2) netEvent，这类事件处理的是 packet 的接收事件，包含了数据报文和控制信息。当节点收到数据发送的节点发送的数据时，应该将数据包接收事件加入到仿真队列中，当调度器调度到该接收时间时再根据事件句柄进行处理。

(3) simEvent 事件，这类事件主要包含了 exit 事件，系统就是通过该事件来退出仿真过程。每次仿真前，都要先将 exit 事件添加到事件队列，然后再添加其它的事件。

5.1.3 P2PSim 安装配置

P2PSim 的安装环境需要： openssl, libcrypto 和 libgmp，这其中的 libcrypto 是包含在了 openssl 中，因此只需要安装 opensell 和 gmp 就可以。安装完这两个之后，再安装 P2PSim。注意 GCC 的版本问题，如果编译时遇到语法错误，需要修改对应部分代码，或者设置编译条件。目前在缺省安装的 FreeBSD-6.2 中，在编译之前需要进行如下的修改：

1) cd /usr/ports/devel/sgb;make;make install

否则，在 p2psim-0.3 里面运行./configure，会提示 WARNING: Stanford graph base not available。

2) vi {$P2PSIM-0.3}/topologies/gtitm.c 修改如下

((int)ip1)--;==>((int*&)ip1)--;

((int)ip2)--;==>((int*&)ip2)--;

否则，gmake 的时候，会提示：gtitm.c:ISO C++ forbids cast to non-reference type used as lvalue；这是 GCC 版本兼容性造成的。

3) vi {$P2PSIM-0.3}/libtask/taskimpl.h 修改如下

注释掉 setcontext 这部分代码

否则，gmake 的时候，会提示：taskimpl.h:56: error: conflicting types for 'setcontext',

以及 context.c 的冲突；这是 P2PSIM 为了兼容 5.0 以下的 freebsd 遗留的。

其他的，可参照官方页面的提示。

5.1.4 测试方法及测试结果

所实现的主要的功能包括三部分：事件生成器(SecureDataStoreEventGenerator)、监视器(SecureDataStoreObserver)以及协议(SecureDataStoreProtocol)。仿真验证架构如图 5.3 所示。

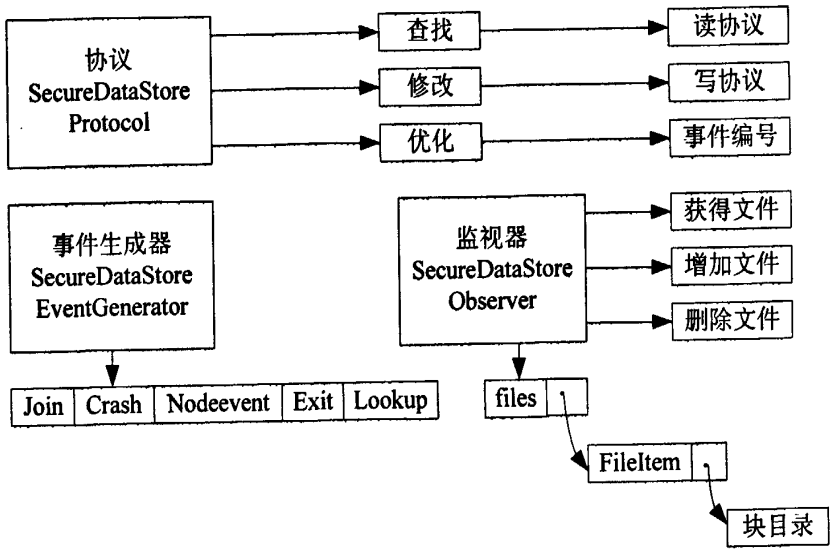


图 5.3 仿真验证架构

Fig. 5.3 Architecture of simulation

下面对其功能分别进行介绍：

(1) SecureDataStoreEventgenerator 可以生成五种事件：join、crash、nodeevent、exit、lookup；SecureDataStoreProtocol 主要处理其中的 lookup 和 nodeevent。这是因为 lookup 对应查找工作，nodeevent 对应于优化工作。其他的三种事件：join 让节点加入，crash 让节点暂时退出，exit 让节点永久退出。这些主要是修改节点状态和路由信息的操作，跟文件操作无关。所以可以通过继承其他协议(如 Chord)来实现。这样做的主要目的就是：尽量做到底层协议无关，以求可以在不同的协议上进行对比。

(2) SecureDataStoreObserver 负责监视所有的文件状态，主要包括添加文件/删除文件/获取文件信息操作。 SecureDataStoreEventgenerator 生成 lookup 事件的时候，由它提供随机的文件 ID；SecureDataStoreProtocol 则从它获取文件的信息(如文件大小、分块方式等)。

(3) SecureDataStoreProtocol 是协议的主体，包括读协议、写协议、以及优化协议等；每一个 SecureDataStoreEventgenerator 的事件需要处理的时候，将调用对应的协议功能。如：lookup 事件处理的时候，将调用 SecureDataStoreProtocol 的 lookup 函数。该函数会

调用 read 协议。

这些协议的算法已经在前面章节介绍过了，所以本节不再细述。下面是采用仿真方法获得的测量效果。

测试结果，见如图 5.4 和图 5.5 所示，非常好的验证了本文提出的访问控制算法。

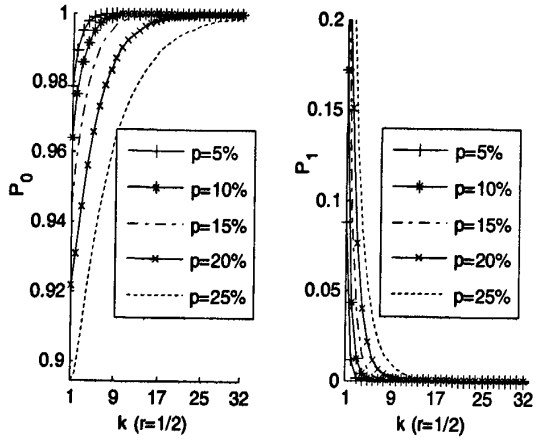


图 5.4 当不诚信比例增加而不可用比例不变时 P_0 和 P_1 的变化趋势

Fig. 5.4 Tends of P_0 and P_1 when the dishonest rate p increasing with a fixed unavailable rate (i.e. q=10%)

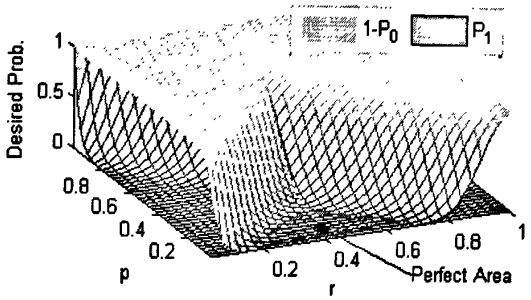


图 5.5 性能和安全的折衷区域

Fig. 5.5 An example of Perfect Area

5.2 系统部署及应用

根据预期，完善后的系统将在首钢的全部计量相关部门进行了安装和部署。在此之前，我们为试运行阶段制定了一个可以迭代的五阶段的部署和应用方案。

(1) 软件安装和网络配置。 首先为首钢公司 4 个层次的计量部门所用机器安装了本系统的原型版本。并且设置防火墙、文件目录权限等保证系统可以运行。由开发和测试人员进行上门安装。

(2) 员工培训。召开培训会议，为试用该系统的员工进行了试用和操作培训，提供使用和操作手册，并记录和反馈员工提问。

(3) 系统试运行。在指定时间，启动系统，采集计量数据，进行多部门的系统协同操作。提供试运行操作手册，并提供实时在线的技术支持。

(4) 收集意见和建议，以及各节点的运行日志。

(5) 关闭系统，根据新提出的需求和发现的问题，指定下一阶段的重构计划。

这五个阶段的工作为一个部署和测试周期，每一个版本的MMS软件都将根据这五个阶段进行操作，然后根据汇总的需求和问题，改进和升级软件功能和版本。

第6章 结 论

6.1 本文工作总结

(1) 较深入地研究了 P2P 技术。

(2) 在深入调研了首钢现有的几个计量管理系统的应用情况下，提出了改进首钢计量管理系统的需求和实现意义，提出了将 P2P 技术应用到首钢计量管理系统中来的设想。

(3) 基于 P2P 技术，实现了将首钢的物资计量系统（ERP）、能源计量系统（电力网）、量值传递系统（企业计量管理信息系统）数据的集成，从而在首钢计量管理工作中形成一个强大的管理系统，真正做到资源共享，充分发挥计量工作在企业中的重要技术基础作用，较好地实现了计量工作的良性循环。

(4) 经过深入研究，基于 P2P 技术的动态性、分布性、异构性，及其多种多样的拓扑结构，实现了适宜首钢“一业多地”的管理模式，充分利用了边缘资源，解决了数据传输速度慢、出错率高等问题。

(5) 在 P2P 的文件存储系统中应用了先进科学的访问控制算法，有效地解决了计量数据或计量信息传输过程中的安全性问题，使 P2P 技术在计量管理系统中的应用更完美。

P2P 技术在首钢现有三个信息网间的集成，使首钢各个部门、“一业多地”之间，上下、左右各方面计量工作的沟通更为通畅，真正发挥了计量管理系统在首钢这样的大型企业中的重要作用，促使首钢计量工作整体更上一层楼。P2P 技术在首钢计量管理系统中的成功应用，真正实现了计量工作在企业中的技术基础作用。

6.2 进一步工作展望

P2P 技术在首钢计量管理系统中的应用，除了要满足计量工作的不同需求外，还要进行功能增强和完善。

首先，需要一套增强的更加安全、更加可信的通信方式来保障计量管理系统运行在可知可信的状态。比如采用属性证书（如 X509.v4 格式的数字证书）的方式以及硬件的电子钥匙来保证用户身份的可信性，允许远程验证用户身份的合法性；使用带有安全芯片（TPM 芯片）的机器，授权通过评估的可信的机器和用户进行数据访问操作。

其次，增强系统的可控性。一个可能的方案是：引入审计子系统，加强管理中心的存储和管理功能。

最后，需要设计一套更加友好的用户操作界面。除了进行人员 P2P 知识培训外，还需要对用户界面的友好性上进行改进，让用户更加容易习惯和接受这一系统，并简化计量工作操作流程，增加在线帮助系统和更加详细的图文手册。

参考文献

1. 王立吉. 计量学基础[M]. 北京: 中国计量出版社, 1988, 1-10.
2. 国家技术监督局武汉培训中心. 计量技术管理[M]. 北京: 中国计量出版社, 1993, 1- 20.
3. 北京市质量技术监督局计量监督处, 北京计量协会计量管理委员会, 企业计量工作资料汇编[M]. 北京: 中国计量出版社, 2001, 1-30.
4. 马丁. 网络革命/P2P/Lean/The digital estate:P2P[M]. 上海: 上海远东出版社, 2000, 1-246.
5. Tomoya, K, Shigeki, Y. Application of P2P (peer-to-peer) technology to marketing[A]. Cyberworlds, 2003. Proceedings. 2003 International Conference on[C]. 2003, 372-379.
6. Wei Yu Boyer, C Chellappan, S; Dong Xuan. Peer-to-peer system-based active worm attacks: modeling and analysis[A]. Communications, 2005. ICC 2005. 2005 IEEE International Conference on[C]. 2005, 295-300.
7. 杨天路. P2P网络技术原理与系统开发案例[M]. 北京: 人民邮电出版社, 2007, 1-313.
8. 朱卫平. P2P 技术应用研究[J]. 福建电脑, 2006, (06): 21-26.
9. 吕志锋. P2P 技术的应用与思考[J]. 甘肃科技纵横, 2003, 5(32): 5-12.
10. Hughes, D Walkerdine, J Coulson, G Gibson, S. Peer-to-peer: is deviant behavior the norm on P2P file-sharing networks?[J]. Distributed Systems Online, IEEE, 2006, 2(7): 10-15.
11. 汪小帆, 陈关荣. 复杂网络理论及其应用[M]. 北京: 清华大学出版社, 2006, 1-270.
12. 程学旗. P2P 技术与信息安全[J]. 信息技术快报, 2004, (05): 59-71.
13. 孟嘉. 对可控制 P2P 网络应用的研究[A]. 第六届全国因特网与音视频广播发展研讨会[C]. 2006, 35-41.
14. Venkataramani, R Kramer, G Goyal, V K. Multiple description coding with many channels[J]. IEEE Trans. on Information Theory. 2003, (03): 40-62.
15. 张钟年. 我国古代度量衡的辉煌成就及现代计量的自主创新[J]. 中国计量杂志, 2007, (05): 63-68.
16. GB17167-2006, 用能单位能源计量器具配备和管理通则[S]. 2006.
17. JJF1033-2001, 计量标准考核规范[S]. 2006.

18. 陈渭. 测量设备的计量确认体系宣贯指南[M]. 北京: 中国计量出版社, 1995, 20-50.
19. 唐丽. 如何做好计量检定原始记录[J]. 中国计量杂志, 2007, (12): 13-17.
20. 申燕玲. 检定证书结论用语应规范[J]. 中国计量杂志, 2007, (12): 52-56.
21. R Spencer, S Smalley. Tue Flask Security Architecture: System Support for Diverse Security Policies[A]. In proceedings of the Eighth USENIX Security Symposium[C].1999, 123-139.
22. J. Liang, R Kumar, Y Xi, K.W. Ross, Pollution in P2P File Sharing Sys- tems[A]. in Proc. INFOCOM[C]. 2005, 12-25.
23. 张明杰. 新型计量管理系统的分析与设计[J]. 福建电脑, 2006,(09):30-36.
24. S Nielson, S Crosby, D Wallach. A Taxonomy of Rational Attacks[A]. In Proc. IPTPS[C]. 2005, 10-17.
25. 田敬, 代亚非. P2P 持久存储研究综述[J], 软件学报, 2007, 18(06): 1379-1399.
26. 林闯, 封富君, 李俊山. 新型网络环境下的访问控制技术[M]. 软件学报, 2007, 18(04): 955-966.
27. 张春田, 苏育挺. 数字图像压缩编码/信号与信息处理丛书[M]. 北京: 清华大学出版社, 2006, 1-487.
28. 田敬, 张大为, 代亚非, 韩华. ESStore: P2P 网络的可靠存储协议[A]. 全国网络与信息安全技术研讨会[C]. 2005, 273-285.
29. D Ellard, J Megquier. DISP: Practical, Efficient, Secure and Fault Tolerant Data Storage for Distributed Systems[J]. ACM Transactions on Storage (TOS), 2005, 1(01): 71- 94.
30. Lian Q, W Chen, Z Zhang. On the Impact of Replica Placement to the Reliability of Distributed Brick Storage System,[A]. ICDCS 2005[C]. 23-36.
31. J R Douceur. The Sybil Attack[A]. In Proc. of the 1st International Workshop on Peer-to-Peer Systems[C]. 2002, 251-260.
32. Naicken S, Basu A, Livingston B, Rodhetbhai S. A Survey of Peer-to-Peer Net- work Simulators[A]. The 7th Annual Postgraduate Symposium[C]. 2006, 131-137.
33. 沈春雨. 基于 P2P 的网络存储系统的研究[D] . 武汉: 武汉理工大学, 2006.

致 谢

在论文完成之际，首先感谢我的导师高福祥教授，感谢他在学习和工作上对我严格的要求，生活上对我无微不至的关心，感谢他给了我社会实践、体验生活和体验工作的机会，感谢他在我论文的撰写过程中给予的指导，感谢他对我的严厉和关心。

感谢我的好朋友刘奎恩博士，感谢他给予我的P2P方面的知识，感谢他帮我把P2P技术引入到首钢计量管理工作中，祝愿他生活愉快、工作顺心、学术有成。

感谢实验室的夏利、史岚、刘浪涛、刘辉林、王剑、姚兰等老师，感谢他们在我学习期间对我的指导和帮助。感谢他们一丝不苟的工作态度，感谢他们诲人不倦的教学态度，感谢他们平易近人的生活态度，感谢他们，感谢他们给我树立了榜样，感谢他们并祝愿他们生活愉快，工作顺心。

感谢实验室所有的兄弟姐妹在我攻读硕士研究生期间对我学习、工作和生活中的诸多帮助，感谢他们创造了实验室良好的学术氛围和融洽的生活环境，感谢他们让我体验到了这个大家庭的温暖，感谢他们并祝愿他们学业事业有成。

感谢首自信公司信息事业部有关人员，给了我深入了解物资计量网、电力网的过去和现状，并亲身体验其在计量管理工作中带来的管理效率。感谢他们坦诚不公地暴露物资计量网和电力网的运行缺陷，从而给我提供了这次很好的研究机会。感谢他们并祝愿他们生活愉快，工作顺心。

感谢首自信标准计量站的全体人员，感谢他们在我日常计量管理工作中对我的帮助和支持，感谢他们在使用计量管理软件中提出的宝贵意见和建议，使我有机会提高自己的业务水平。感谢他们并祝愿他们生活愉快，工作顺心。

感谢首自信运行事业部的全体领导和同仁，感谢他们在我攻读硕士研究生期间对我学习、工作和生活中的诸多帮助，感谢他们创造了良好的工作氛围和融洽的生活环境，感谢他们让我体验到了这个大家庭的温暖，感谢他们并祝愿他们事业有成。

感谢我的父母我的家人，感谢他们在我人生成长道路上给予我无微不致的关怀，感谢他们对我无尽的支持，感谢他们对我无尽的爱护，没有他们就没有我的今天，感谢他们，感谢他们给我的浓浓亲情，感谢他们，感谢他们让我拥有乐观面对生活、乐观面对人生的积极态度，感谢他们并衷心祝愿他们身体健康，心情愉快。

感谢曾经给予我帮助的所有朋友，感谢他们在学习、工作和生活上给我的帮助和支持，感谢他们并祝愿他们幸福快乐。