

组件式 GIS 系统的设计^{*}

汪林林 覃小琪

(重庆邮电学院软件学院 重庆400065)

摘 要 组件式 GIS 系统是适应软件组件化潮流的新一代地理信息系统。本文基于组件技术和 GIS 技术,提出了一种组件式 GIS 系统的设计方案,并重点介绍了组件式 GIS 系统的核心—组件仓库的详细设计方法。

关键词 GIS, 组件仓库, 组件式 GIS 系统

The Design of GIS System of Component Style

WANG Lin-Lin QIN Xiao-Qi

(Chongqing University of Post and Telecommunications, Chongqing 400065)

Abstract Component GIS is the new generation which adapts general component tendency of software. On the basis of component technology and GIS technology, this article presents a design method of Component GIS, and chiefly introduces the detail design of the kernel part of Component GIS—GIS Component Repository.

Keywords GIS, Component repository, Component GIS

长期以来, GIS 应用系统的开发都是在 GIS 基础平台上进行二次开发。这种模式下, 程序开发人员必须要熟悉 GIS 平台所提供的繁多的函数、命令及参数, 这不但会增加系统的开发难度, 延长系统的开发周期, 还会增加系统的成本。这种开发模式下, GIS 应用系统的功能取决于 GIS 基础平台功能的强弱, 以及系统开发人员理解和掌握 GIS 平台函数和命令的程度。这在某种程度上影响了系统的质量。而且, 一旦 GIS 平台软件升级换代了, GIS 应用系统无法随之自动升级换代, 要升级换代就必须投入相当的精力在新的 GIS 平台上进行新的开发。这一方面加大了 GIS 应用系统的成本, 另一方面, 也大大地阻碍了 GIS 的推广和发展。

随着软件技术的演进, 组件及其相关技术的出现与兴起, 给 GIS 产业带来了一个新的发展机遇。由于组件具有标准化的接口、语言无关性、重复可用性等特点, 可以快速开发新系统, 并且降低了系统建设及维护成本, 从根本上解决了困扰传统 GIS 行业的上述问题, 因此国际上大多数 GIS 软件公司把开发组件式软件作为重要的发展战略。目前国内在 GIS 应用系统的设计和开发方面主要选用国外的开发工具, 对具有自主知识产权的 GIS 组件仓库和组件式 GIS 系统的研究则相对较少。本文在介绍了组件技术在 GIS 领域中的应用后, 提供了一种组件式 GIS 系统的详细设计方案。

1 组件技术在 GIS 领域中的应用

从发展历程看, GIS 软件技术体系经历了 GIS 模块、集成式 GIS、模块化 GIS、核心式 GIS, 从而发展到组件式 GIS 的过程。组件式 GIS 是一种全新 GIS 软件技术体系, 它基于组件对象平台, 具有标准的接口, 允许跨语言应用, 它的出现为传统 GIS 面临的多种问题提供了全新的解决思路。组件技术是新一代 GIS 应用系统的重要基础, 组件式 GIS 就是面向对象技术和组件技术在 GIS 软件开发中的应用。在组件技术的概

念模式下, 软件系统可以被视为相互协同工作的对象集合, 其中每个对象都会提供特定的服务, 发出特定的消息, 并且以标准形式公布出来, 以便其他对象了解和调用。组件间的接口通过一种与平台无关的语言 IDL (Interface Define Language) 来定义, 而且是二进制兼容的, 使用者可以直接调用执行模块来获得对象提供的服务。由于组件技术的出现, 软件产业的形式也将会有所改变。大量组件生产商会涌现出来, 并推出各具特色的组件产品; 软件集成商则利用适当的组件快速生产出用户需要的某些应用系统; 大而全的通用产品将逐步减少; 很多相对较为专业, 但用途广泛的软件, 如 GIS 系统, 都将以组件的形式组装和扩散到一般的软件产品中。因此, 把 GIS 的功能适当抽象, 以组件形式供开发者使用, 将会带来许多传统 GIS 工具无法比拟的优点。

(1) 小巧灵活, 高性价比 在组件模型下, 各组件都集中地实现与自己最紧密相关的系统功能。组件化的 GIS 平台集中提供空间数据管理能力, 并且能以灵活的方式与数据库系统连接。在保证功能的前提下, 系统表现得小巧灵活, 而其价格仅是传统 GIS 开发工具的十分之一, 甚至更少。这样, 用户便能以较好的性能价格比获得或开发 GIS 应用系统。

(2) 直接嵌入 MIS 开发工具, 开发简捷 传统的 GIS 一般都提供一套独立的二次开发语言, 这对开发者和使用者来说都是一种负担, 而且, 使用系统所提供的二次开发语言, 开发能力往往受到限制, 难以处理复杂问题。组件式 GIS 则不需要专门的 GIS 二次开发语言。组件的生产建立在严格的标准之上, 因此, 凡符合标准的组件, 都可在目前流行的各种开发工具上使用。这样, VB、VC、Delphi、Power Builder、FoxPro、Access 等都可直接成为 GIS 系统的优秀开发工具, 它们各自的优点都能够得到充分发挥。对于广大开发人员来讲, 只要对组件技术有所了解, 就可以自由选择他们熟悉的开发工具, 建立普通的 GIS 应用系统。这与传统 GIS 专门性开

^{*} 该论文受重庆市科技发展基金的资助。汪林林 教授, 硕士生导师, 主要研究方向为分布式数据库系统, GIS 系统, 数据仓库及数据挖掘。覃小琪 硕士研究生, 主要研究方向为地理信息系统 (GIS)。

发环境相比,是一种质的飞跃。

(3)强大的 GIS 功能与无限扩展性 在组件式软件技术背后,有一个十分庞大的组件仓库,用户可以从其中挑选需要的组件与组件式 GIS 一起集成应用系统,这极大地扩展了 GIS 的功能。因此,在管理大数据的能力或处理速度方面,GIS 组件绝不逊色于传统 GIS 软件。GIS 组件完全能提供拼接、裁剪、叠合、缓冲区等空间处理能力和丰富的空间查询与分析能力。

(4)Internet 应用 组件技术加上 DCOM 分布式平台可以实现 Internet 应用。组件式 GIS 是实现下一代对象 WebGIS 的重要途径之一。WebGIS 是一种基于因特网/内联网的技术标准和通信协议的网络化 GIS,它是 GIS 技术和因特网/内联网技术相结合的产物。GIS 通过 WWW 功能得以扩展,真正成为一种大众使用的工具。从 WWW 的任意一个节点,Internet 用户可以浏览 WebGIS 站点中的空间数据、制作专题图,以及进行各种空间检索和空间分析,从而使 GIS 进入千家万户。

2 组件式 GIS 系统的设计

2.1 GIS 组件仓库

设计组件式 GIS 系统的前提是构建好 GIS 组件仓库,这是组件式 GIS 系统开发的“血液”和“原料”。从组件提供的服务类型来看,从服务模型的角度按逻辑方式进行分组,整个 GIS 组件仓库从逻辑上可以划分为:用户服务、商业服务和数据服务三种模型,每一模型的逻辑领域又都包含着若干物理性的组件。如图1所示,给出了组件与各模型的关系。

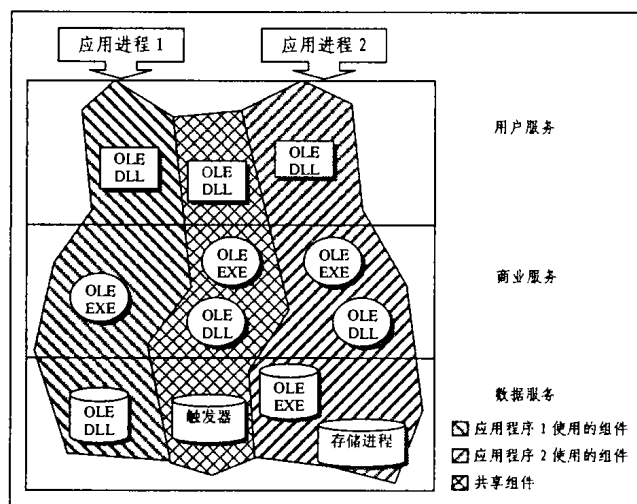


图1 组件仓库的逻辑分类示意图

用户服务层的组件主要为客户提供可视的界面,用以观察信息和数据。它们可以向用户服务层或商业服务层中的组件发出服务请求,也可执行部分商业服务功能。只有通过用户服务层组件用户才能访问封装的商业逻辑。用户服务层的组件一般都包含在用户的应用程序中。

由于用户服务层组件不能直接与数据服务层联系,商业服务层组件是二者联系的桥梁。它实现了正式的进程和定义好的商业规则,它们控制商业任务的执行流程。商业规则与组件的任务相比,是一个应用系统中变化最频繁的部分,所以将商业逻辑从应用程序逻辑中分离出来,有助于生成健壮的、可重用和易于维护的应用程序。

数据服务涉及到所有数据处理活动,包括数据的获取与修改,以及其它与数据库相关的任务。数据服务的关键是没有

实施商业规则,但它可以满足商业组件提出的服务请求。数据服务组件的存在,使得访问异构数据库成为可能。并且当与数据服务组件相连的数据源改变时,不影响它继续提供数据服务。

2.2 组件式 GIS 系统的基本框架结构

组件式 GIS 系统由三个层次(组件组)组成:可视化组件组、功能组件组和数据访问组件组,如图2所示。

可视化组件组接受用户输入并显示相关信息。这个组件是用户管理和操纵地理信息的接口。可视化组件是所有 GIS 应用所必需的。

功能组件组提供处理地理信息所必需的功能。可视化组件组可以调用这些包含在功能组件组中的功能。对用户来说,功能组件组是可以定制的。用户可以选择性地安装能满足需要的功能组件,而不必全部安装所有组件。对开发人员来说,功能组件组是可以很方便地被扩展的。开发人员能够在功能组件组中添加或更新一些功能,甚至能够添加或更新组件以提高系统的质量和性能。

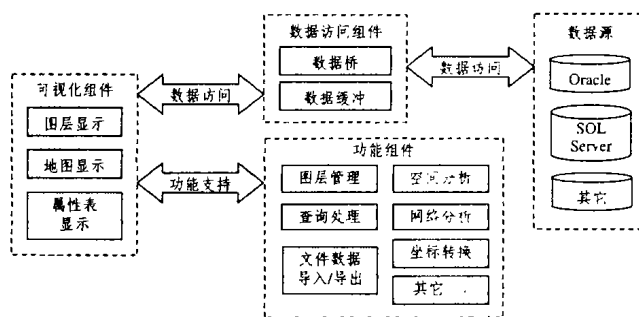


图2 组件式 GIS 系统基本框架结构

数据访问组件组提供了一组方法以供其他组件访问在缓冲区、本地磁盘或者远程服务器中的地理信息。同时,数据桥组件提供用户授权和连接服务器的方法,以及一些诸如此类的方法。设计数据访问组件组的动机是为了在客户端和服务端间保持数据结构的相对独立性。因此,运行在客户端上的组件就可以拥有自己的数据结构。然而,在客户端和服务端间的数据结构的折中还是必需的,因为很复杂的数据结构和经常转换这些结构将降低系统的性能。事实上,在数据访问组件组中有两个基本组件,一个是数据桥组件,另一个是数据缓存组件。数据桥用于访问远程服务器中的数据,针对不同的数据源,应有不同的数据桥接口的实现。这就使得组件能以相同的方式处理不同数据源的数据。数据缓冲组件用来访问存储在本地缓冲区中的数据。

2.3 组件式 GIS 系统的生产过程

传统的 GIS 应用系统开发过程,通常包括以下几个步骤:用户调研、可行性研究、用户需求分析、系统总体设计、系统详细设计、GIS 基础平台选择、熟悉 GIS 基础平台、进行二次开发、系统测试、系统维护和系统使用。

组件技术的兴起改变了上述传统的软件生产方式和生成过程。在标准的组件式 GIS 应用系统的开发模式中,组件的生成者和 GIS 应用系统的开发者有着明显的分工。组件生产者负责生产和提供组件。而 GIS 应用系统的开发者则向生产者请求所需要的组件,并将其集成组装为所需的应用系统。从组件式 GIS 应用系统开发的角度来看,软件生产过程应包括以下几个阶段:用户调研、用户需求分析、系统总体设计、组件检索与获取、系统集成、系统测试、系统维护和系统使用。这种

方式下,软件开发人员不必进行程序编写,只需要将获取的组件进行集成组装,最终得到一个 GIS 应用系统。这种方式下的 GIS 应用系统开发过程如图3所示。

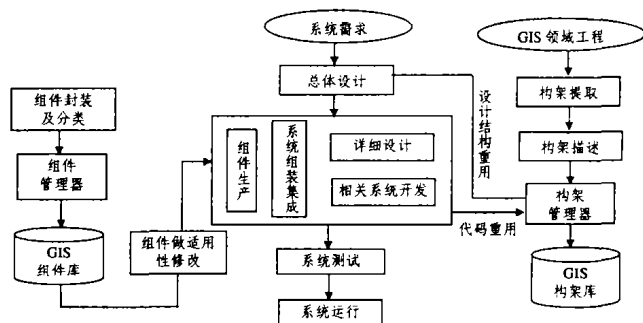


图3 组件式 GIS 应用系统开发过程

(上接第191页)

算法中使用的函数与 MISTY^[6]中使用的函数具有相同的设计指标,不同之处在于前者加了一个左循环移位,这个改变并没有影响软硬件的规模和速度,但使得攻击者更难分析。 FL 函数的设计指标是当函数的输入 H_{i-1} 固定时,函数必须是线性的,这样就不会增加算法的平均线性和差分概率。而且由于函数的结构都是一些逻辑运算 AND, OR, XOR 和循环移位,使得软硬件实现的速度非常快。

4 安全性分析

4.1 生日攻击

这种攻击方法不涉及算法的结构,可以攻击任何 Hash 算法。由于算法具有可变的散列长度,生日攻击方法所需的操作数分别为 $2^{64}, 2^{80}, 2^{96}, 2^{112}, 2^{128}$ 。Preneel^[7]指出用生日攻击的方法获得具有160比特消息散列值的一对消息碰撞至少要20年的时间。Pieprzyk 和 Sadeghiyan^[8]建议用128比特的消息散列值来抵抗这种攻击方法。

4.2 随机攻击

随机攻击就是攻击者随机选取一个消息或消息的一部分,并且期望该消息的散列值与给定消息的散列值相同。这种攻击成功的概率为 $1/2^r$, r 表示散列长度。消息散列值为64比特就可以抵抗这种攻击。

4.3 中间相遇攻击

这是一种选择明文/密文的攻击,是生日攻击方法的一种变形。用于攻击使用轮函数的 Hash 算法,其成功的概率与生日攻击相同。我们的算法可以抵抗这种攻击。

4.4 差分密码分析

Tom Berson 用差分密码分析成功攻击了 MD5 的单轮^[9],但此种攻击对全部四轮无效。相比之下,Bert den Boer 和 Antoon Bosselaers 的攻击成功得多,他们使用 MD5 中的压缩函数产生碰撞^[10]。但是,他们的攻击方法对我们的算法无效。其原因与 SHA 算法抗这种攻击的原因相同,在算法中增加了变量,没有使用 F_i 已经使用过的 b, c, d, e, f, g , 而且,由于引入了 FL 函数使得攻击算法的全部四轮更加困难。

5 算法比较

与 MD 系列, SHA 和 HAVAL 算法相比,我们的算法既继承了他们的优点,又做了相当的改变。主要的改变是添加了 FL 函数和线性变换。

· 结束语 根据国内外 GIS 技术的发展现状,本文较为详细地提出了一种组件式 GIS 系统的设计方案,目前笔者主持开发的组件式 GIS 系统已初具规模,希望笔者的研究能对建立具有自主知识产权的地理信息系统产生积极的促进作用。

参考文献

- 1 黄杏元, 汤勤. 地理信息系统概论[M]. 北京: 高教出版社, 1998
- 2 周心铁, 刘毓华. 组件技术与 GIS 的发展[J]. 计算机世界, 1998, 3
- 3 宋关福, 钟耳顺. 组件式地理信息系统研究与开发[J]. 中国图像图形学报, 1998, 5

(1)同 SHA 算法一样,增加了第四轮。但是已经证明 MD 系列和 SHA 使用的布尔函数具有等价结构。我们重新设计了每轮使用的非线性函数,这些布尔函数具有良好的性质。

(2)与 HAVAL 算法一样,算法的输出也是可变的。但是我们对消息进行了扩展变换,变换的方法与 SHA 不同。而 HAVAL 算法和 MD 系列都是采用相同的消息,只是每一轮使用的次序不同。

(3)算法保留了 MD4 和 SHA 的方案,每隔20轮重复使用相同的轮常数。

(4)添加了线性变换,这将达到最佳的雪崩效应。

(5)增加了 FL 函数,可以抵抗将来的未知攻击。

(6)速度。我们对算法进行仿真(Inter Celeron Processor 500MHZ, C 语言编程),用160比特的散列输出与 SHA 算法比较,前者平均速度为3.70Mbyte/s,后者为6.64Mbyte/s。虽然算法的运行速度比 SHA 算法慢了45%,但是对于实际的需求来说,算法的速度已经足够了。

参考文献

- 1 Damgard I. A design principle for hash functions. In: G. Brassard, ed. Advances in Cryptology-Proceedings of Crypto'89. Lecture Notes in Computer Science, Springer-Verlag, 1990, 435: 416~427
- 2 Schneier B. Applied Cryptography: protocols, algorithms, and source code in C, 2nd Rev edition. John Wiley, 1996
- 3 Zheng Y, Pieprzyk J, Seberry J. HAVAL-A one-way hashing algorithm with variable length of output. Advances in Cryptology-AUSCRYPT'92 Proceedings, Springer-Verlag, 1993. 83~104
- 4 温巧燕, 等. 现代密码学中的布尔函数. 科学出版社, 2000
- 5 Anderaon R, Biham E, Knudsen I. Serpent: A proposal for the advanced encryption standard. NIST AES Proposal, 1998
- 6 Matsui M. New block encryption algorithm MISTY. Fast Software Encryption, FSE'97, LNCS 1267, Springer-Verlag, 1997. 54~68
- 7 Preneel B. Analysis and design of cryptographic hash functions. PhD thesis, Katholieke University Leuven, Jan. 1993
- 8 Pieprzyk J, Sadeghiyan B. Design of hashing algorithms. Springer-Verlag, 1993
- 9 Berson T. Differential cryptanalysis Modwith applications to MD5. Advances in Cryptology-EUROCRYPT'92 Proceedings, 1992. 71~80
- 10 den Boer B, Bosselaers A. Collisions for the compression function of MD5. Advances in Cryptology-EUROCRYPT'93 Proceedings, Springer-Verlag, 1994. 293~304