高速边缘路由器安全数据库的研究与实现

荣 霓 韩智文 龚正虎
(国防科技大学计算机学院 长沙410073)

摘 要 随着计算机网络技术的发展,对网络核心设备的安全研究成为发展的热点。高速边缘路由器是骨干网和互联网/内部网之间的高速接入设备,在网络安全的研究中具有重要的意义。高速边缘路由器中的安全数据库管理包含了对安全策略的管理和对安全关联的管理,它的合理性和高效性是制约高速边缘路由器系统性能的重要因素。目前,安全数据库系统普遍采用集中式体系结构完成对安全策略和安全关联数据的管理,在系统的并行性、灵活性和访问效率方面都存在着较大的缺陷;分布式管理则由于各分布子系统间的一致性维护问题在高速边缘路由器中被充分放大而无法满足高速边缘路由器的设计要求。本文基于ForCES协议框架提出了一种高速边缘路由器的体系结构CeDita,并详细分析了基于该体系结构的安全数据库混合式管理模型SDM的特点。该模型综合了集中式管理的视图统一、操作简单等特点以及分布式管理的本地访问特点,具有较强的并行性、可扩展性和高效性,是一种适于路由器实现的高效的数据库管理模型。

关键词 高速边缘路由器,体系结构,安全数据库

Study and Implementation on the Security Database of High Speed Boundary Router

RONG Ni HAN Zhi-Wen GONG Zhen-Hu
(School of Computer,National University of Defence Technology,Changsha 410073)

Abstract With the ever increasing of the network security systems applied in wide range of critical domains,the requirement of high reliability and high availability of these systems tends to be more and more urgent,which leads to the emergence of the routers executing security protocols (i.e,IPSec) and the tendency of these routers used as the boundary equipments between the backbone and the Intranet/Internet. The security database management of these routers includes the management of the security policies and the security associations of the routers. The complexity of this management requires a flexible,scalable and efficient architecture. Centralized architecture can't meet this challenge due to the long access time and the poor parallelism. Neither can distributed architecture do because that the management of the security database is complex enough to maintain the consistencies between the multiple executors. This paper prompts an architecture called CeDita in the framework of the ForCES,and analyzes the hybrid architecture of the security database management which maintains a short access time and keeps the system flexible and scalable. Furthermore,detailed studies on the key implementation technologies of this architecture are presented in the paper as well.

Keywrods High speed boundary routers,Security database management,Hybrid architecture

1 引言

随着计算机网络技术的发展,网络安全问题成为研究的热点。路由器作为网络传输的重要设备,在网络安全的研究中具有重要的意义。目前,一种网络设计的思想是在高速骨干网和接入网中间设置服务区,由服务区中的设备(称为边缘设备)完成安全、服务质量等功能,以保证骨干网的传输速度和骨干网与接入网之间的速度匹配。高速边缘路由器(High Speed Boundary Router,HSBR)是一种具有较高的IPSec[1~4]报文转发速度和大容量的安全数据库存储的用于边缘服务的高速路由器,它通过执行IPSec协议来提供基于IP级的网络安全,并提供基于安全策略协议支持的域内IPSec安全数据的管理。按照边缘服务的特点,HSBR转发IPSec报文的线速应该达到G比特级,路由器总速度达到数十G,安全连接达到十万个。

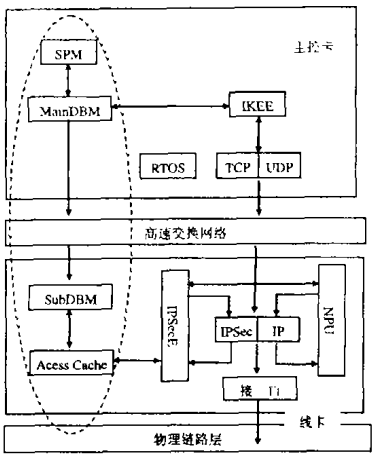
HSBR的安全数据库管理应该包含安全关联管理和安全策略管理两个部分。系统对安全关联的管理包括统一维护安全关联从素材阶段的产生、按照IKE协商的状态变化而修改、直至随着生存期到达而被删除并触发新的安全关联的生成。系统对安全策略的管理需要解决策略的定义、存取、管理、交换、验证、发现机制等问题以及系统自身的安全性问题。其中策略的表示和策略在动态交换中的安全性问题是策略系统的核心问题。

HSBR的高速性、安全性和大容量的特点决定了安全数据库的管理是一个速度和容量敏感的问题。特别是当HSBR被作为区域IPSec中心网关使用时,不仅需要对自身的大量安全数据进行管理,还需要对区域内的其他设备(主机、路由器)的安全数据进行管理。庞大的安全数据的数量和较高的访问速度对安全数据库的管理构成了严峻的挑战。

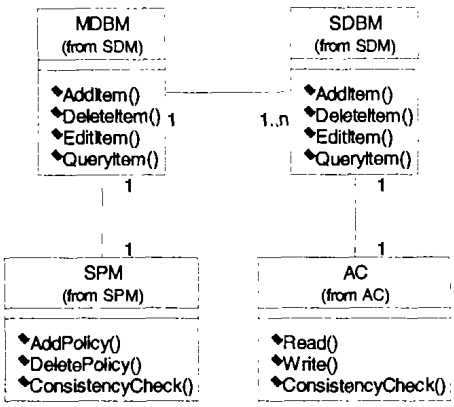
综上所述,研究和开发具有良好的开放性、可管理性和高效率的安全数据库管理系统,是HSBR体系结构研究和实现的重要部分。本文第2节将在HSBR体系结构模型CeDita的基础上介绍安全数据库管理系统SDM的结构;第3节将详细分析SDM的各种操作功能;第4节将讨论安全策略管理的问题;最后给出了整个讨论的结论。

2 基于CeDita的安全数据库管理模型

为了满足HSBR的设计要求,提出一种HSBR模型CeDita,如图1 A所示。图中,安全策略模块(Security Policy Module,SPM)、安全关联模块(MainDBM、SubDBM)和访问cache构成了系统的安全数据库管理系统,是本文的主要讨论对象。其中的安全策略模块和安全关联模块称为安全数据库管理体(Security Database Manager,SDM)。图1 B给出了基于UML的设计类图。



A 基于 RTOS 的 HSBR 结构



B 基于 UML 的设计类图

图1 CeDita 体系结构

根据以上的讨论，结合 CeDita 本身的特点，提出基于 CeDita 的安全数据库管理体系 SDM，如图2所示。

SDM 采用了和 CeDita 对应的混合式管理结构。主安全数据库存储了整个 CeDita 系统的所有安全策略数据和安全关联数据的中间模式。主安全数据库的 SA 池为虚池，负责存储协商阶段的 SA 素材和域内相关实体提交的安全关联；SP 池包含了本机入站 SP、出站 SP 和域内相关实体提交的 SP 等多个单体。接收组件的设置使得 IKE 执行器和安全策略管理器可以对主安全数据库进行访问，包括 HSBR 本身的访问和域内 IPSEC 实体采用 SPS 协议通过安全策略管理器的访问。接收组件中包含了向 IKE 执行器请求产生安全关联和接收 IKE 执行器产生的安全关联，以及接收安全策略管理器制订的安全策略的处理。访问组件负责主安全数据库的查询。管理组件对主安全数据库进行管理，管理组件包含了数据库维护的一些操作，例如查找、生成、更新、删除等处理，以及和管理组件代理相互通讯的功能。子安全数据库存储了本 IPSec 执行器使用的安全数据。同主安全数据库一样，子安全数据库也分为相应的 SA 池和 SP 池，包含多个单体。设置子访问组件，完成 IPSec 执行器对子安全数据库的访问。设置管理组件代理对子安全数据库进行管理。管理组件代理也包含了数据库维护的一些操作，以及和管理组件相互通讯的功能。

SDM 使用混合结构的优势在于：(1)集中式的安全策略存储将使得它的管理相对简单，特别是当 HSBR 充当安全域策略服务器的时候更是如此。(2)各线卡对安全策略的操作仅限于“读”操作，因此集中式的安全策略存储不会带来严重的一致性问题。可以通过设计轻权的策略而不是使用诸如监听协议或者目录协议等系统开销较大的协议来保证策略更新的一致性问题(将在本文第3节讨论)。(3)分布式的子安全数据

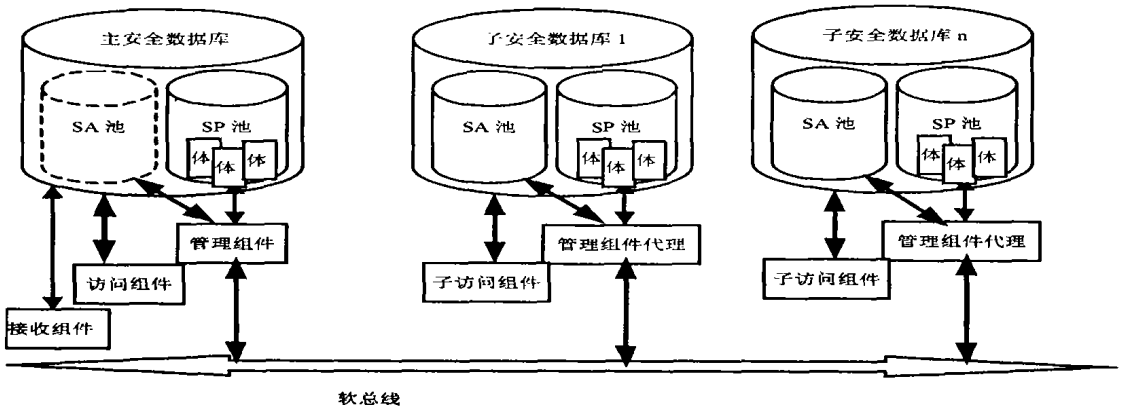


图2 SDM 体系结构示意图

库可以高效地向本地 IPSecE 提供所需的安全数据访问，以保证报文的线速转发。总体来说，混合式的 SDM 使得 HSBR 对于安全数据管理具有统一的视图和灵活的管理方式。

由于紧耦合的关系，SDM 没有考虑对 COPS[5]、LDAP[6] 等协议的支持，而是把它们和 SPP 一起放到了安全策略管理体中加以实现。基于 ForCES[7~9]协议框架的安全策略管理体将在第4节进行讨论。ForCES 协议使得安全策略管理体可以很方便地将 COPS 和 LDAP 等作为相关 FE，通过两阶段 PA 机制向 CE 进行能力申报和状态申报，从而完成对相关协议组件的加载和管理。

3 SDM 的功能说明

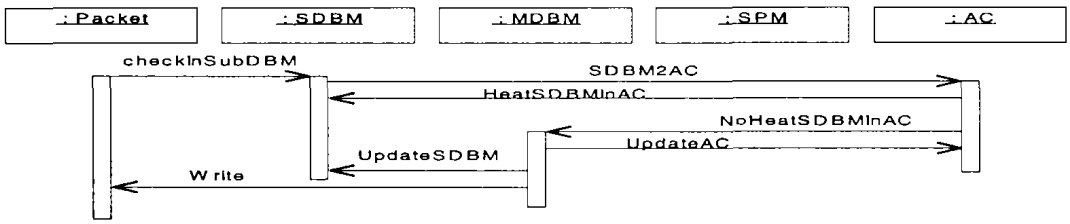
SDM 是一个结构灵活、层次清晰的安全数据库管理结构。如果将整个 SDM 作为一个黑盒系统，则系统的输入、输出对应了 HSBR 中 IPSec 报文的入站和出站操作。SDM 的功能是围绕报文的入站和出站操作设计的。根据 SDM 对入站、出站报文的处理得到的 UML 顺序图如下：

在介绍 SDM 的基本功能之前，先作如下的定义。

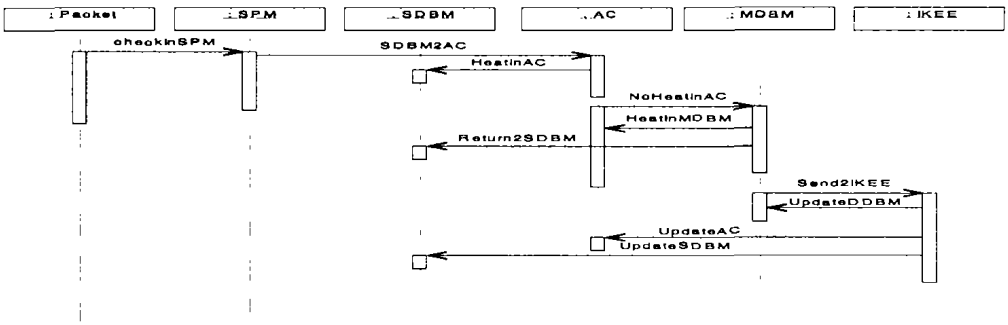
定义1(安全数据统一寻址标识 sd_ref) 安全数据统一寻址标识是一个二元组〈IPSEC 执行器号，体号〉。其中的 IPSEC 执行器号是 HSBR 系统中对线卡的统一编号，体号是安全数据库单体的编号。通过使用 sd_ref，可以方便地进行安全数据在接收体、访问体、管理体和管理体代理以及访问子体之间的全局访问。

定义2(安全数据表项 item) 安全数据表项是一个二元组〈sd_ref，表项内容〉。安全数据表项是安全数据库管理系统

SDM 中的安全数据在数据库间流动的存在。在 SDM 中，item 的存储采用了基于 HASH 的快速访问链表形式。安全关联 item 被连接到对应的 LINKED_LIST_NODE。对于主安全数据库，安全关联 item 是经过封装的 PS，或者外部对等实体的安全关联。子安全数据库中则是本地的安全关联。安全策略的 item 具有与安全关联不同的格式，包括源地址、目的地址、源端口号、目的端口号、安全策略(AH/ESP)、加密算法(TDES/SHA/CBC)等。为了在访问 SPD 表项时快速获得对应的 SA 表项，设置回溯指针指向对应的 SAD 数据项，以便通过 SPD 的访问快速地决定使用哪个 SA 来处理报文。



A 入站报文的处理



B 出站报文的处理

图3　基于 UML 顺序图的出、入站报文处理

SDM 的一些功能说明如下：

添加表项　添加表项发生在安全数据库管理组件收到接收组件提交的新建安全数据，或者是某 IPSec 执行体需要的安全数据在本地未找到而在主体中找到，则此时的安全数据库管理组件代理也需要执行添加表项的工作。

当安全数据库接收组件接受了 SA 素材或者 SA，接收组件将通知管理组件将它们写入主安全数据库对应单体。如果 SA 素材已经成为 SA(即 IKE 协商完成)，则接收组件把含有 SA 和安全数据统一寻址标识的安全数据表项交给管理组件，由管理组件交给对应的管理组件代理完成子安全数据库的表项添加工作以及回溯指针的调整，并在子安全数据库中更新对应的 SP 表项；同时，接收组件将删除主安全数据库中的安全数据表项(这就是主安全数据库中 SA 池为“虚池”的由来，因为它并没有真正存储本机的安全关联)和相关回溯指针。

当安全数据库接收组件接受了 SP，接收组件将通知管理组件将它们写入主安全数据库对应单体。这时，可能存在着策略冲突的问题，即新添加的策略和策略库中已有的策略冲突。鉴于策略冲突的复杂性，目前设计的 SDM 没有实现策略冲突的完全消解，而是通过在策略管理体和接收组件中为 SPP 预留的策略冲突消解模块来实现对后续系统的开放式结构。同时，SDM 实现了简单的基于 HASH 表的策略冲突预警，主要是通过 HASH 表的快速比对找到对应的源、目地址＋源、目端口号表项，然后对后面的协议位(两位)和加密算法位(5位)进行一次性异或比对，结果非0则表示可能有冲突，报警。

当安全数据库子访问组件在本地安全数据库中未找到对应数据而在主安全数据库中找到时(对于本机主要是指安全策略)，子安全数据库必须新增表项，方法是通过管理组件和管理组件代理将表项复制到子安全数据库中。由于存在着多个子安全数据库保持一个主安全数据库表项的副本，因此在主安全数据库表项修改、更新的时候将导致表项的不一致性。因此，引入登记表的管理机制。

定义3(登记表)　登记表是一个单向链表。每个主安全数据库中的安全数据表项通过指针指向一个登记表。登记表中的每个表项为使用该表项的一个全局标识 sd_ref(〈子体号、单元号〉)。

通过登记表，所有使用了主数据库某项安全数据表项的子体都被记录下来。在管理组件执行维护安全数据表项的操作时，根据表项的登记表依次对各子库的对应表项进行操作。由于采用了全局统一寻址编码 sd_ef，该操作可以简单快速地实现。

删除表项　删除表项主要发生在 SA 生存期到期或者安全策略管理器删除 SP 的时候。当管理组件代理发现某 SA 的生存周期到期后，作废子安全数据库中对应的 SA 表项。同时通过与管理组件的管道向接收组件发送产生新 SA 的请求。接收组件接受请求后，生成 IKE 报文原件，向 IKE 执行器转发。生存期按照协议规范的要求分为字节数/报文数，使用时间等。对于字节数/报文数的统计由子访问组件在接受本地访问时向管理组件代理提供。当安全策略管理器删除 SP 的时候，接收器接到删除请求，通过管理组件作废在主安全数据库的表项，并按照登记表向其他各使用者的管理组件代理发送作废指示。删除表项最重要的是保证主安全数据库中的表项和在多个子安全数据库中的对应表项副本的一起删除。通过登记表机制可以快速高效地实现。

修改表项　修改表项发生在 SP 表项被安全策略管理器修改的时候，以及 SA 表项的生命周期计时(SA 只有生成、使用和删除三种状态，修改生命周期发生在使用状态)。对 SP 表项的修改通过登记表机制可以保证数据的一致性要求。

查询表项　对表项的查询通过子访问组件或者访问组件来完成。对于子访问组件访问 SA 可以在 IPSEC 执行器本地完成。具体实现中可以通过基于目的地址和基于 SPI 的两次 HASH 来快速实现。对于子访问组件访问 SP，对子安全数据库和主安全数据库的访问同时进行，直到子安全数据库报找到或者主安全数据库报未找到。如果采用高效的 cache 调度算法，可以基本保证子安全数据库找到的概率，从而大大减少安全策略查找的时间。

4　基于 SPP 的安全策略管理体

策略是一系列规则集组成的，用以控制网络系统在不同环境下的不同行为的实体。文[10]给出的安全策略系统模型如图4所示。图中的 SPS 数据库存储了本地策略与安全域信息，策略服务器通过 LDAP 等协议完成安全数据的访问；外部策略服务器与客户端存储了非本地的策略，它们通过 SPP 与策略服务器进行通讯。

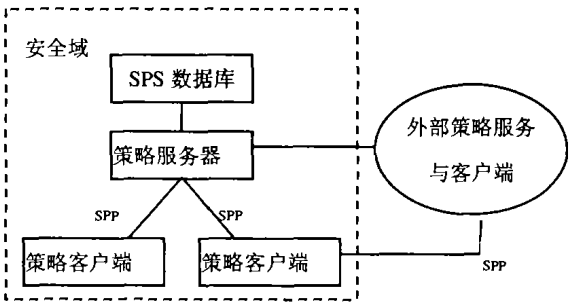


图4　安全策略系统模型

在 CeDita 模型中，设置了安全策略管理体作为 SPS 的策略服务器。主安全数据库对应 SPS 数据库，策略服务器的功能被分解到安全策略管理体中。同时，根据 IPSec 的策略管理框架设计了相应 SPP 信任、授权机制。按照安全策略系统协议框架的要求，实现安全策略系统要解决以下问题：安全策略系统内部安全性、安全策略存储、安全策略系统的授权、SPP 系统的认证。

安全策略系统内部安全性　基于 CeDita 的 HSBR 本身构成一个安全策略系统。由于 HSBR 系统本身的紧耦合性质，该问题本文不予讨论。对于 HSBR 系统和安全域内其他 SPS 的安全，可以采用必要的认证机制，例如 SPP 数字签名负载或者使用 IPSec 进行保护。

安全策略的存储　策略框架指出，在基于网络环境的策略存储问题上，策略的管理和实施采用集中存储与分布式控制相结合的方式。并给出了三种安全域中的策略存储模型：集中式存储、分布式存储和混和式存储。

CeDita 可以简单地实现前两种方式。对于混和式的支持，关键在于安全策略管理器中维护一个特定主机列表，然后对访问列表中主机的 SPP 报文进行相应的转发。自治主机列表是一个 HASH 链表，其中的每个表项为一个包含自治主机地址和相关 SA 指针的结构。当 SPS 模块收到请求报文后，查询自治主机列表，为列表上记录的自治主机的对应报文启动 IKE 协商并登记对应的 SA 指针，然后使用 IPSec 协议进行报文的转发。

安全策略系统的授权　授权是安全策略系统的重要部分，安全策略系统通过执行适当的经过授权的命令或者设置足够的存取控制规则来进行策略的运用。文[11]提出的基于属性证书的“推”模式可以应用在 SPM 的策略授权中。在这种模式下，策略客户端向 SPM 发送请求，SPM 根据请求中的数字签名获得客户端的身份，然后向 AC 中心发送请求以便得到客户端的 AC 并返回给策略客户端。超过安全域范围的域内策略客户端（例如，移动主机）使用 IKE 协议建立安全通讯信道，然后可以使用推模式获得授权。

在 SPP 里交换的策略采取 KeyNote[12]凭证的形式。该凭证是一组签名的策略语句，描述了可接受的 IPsec 选择符（源和目的地址及屏蔽码、传输协议和端口等）和 SA 参数（加密或认证算法、密钥长度等）的组合。通信端点的本地策略中还包含了能够制定凭证的公钥。SPP 里的策略服务器存储本地管理员创建的凭证和通过查询其他 SPP 服务器获得的凭证。这些凭证被交给对 SPP 查询加以转发的安全网关和初始化 SPP 协议的主机。在必要时密钥管理协议可以使用这些凭证来授权通信端点建立 SA。

在实现中，对 IPsec 的 SA 的管理很容易转化为信任管理问题[13]。为了解决该问题，设置两个一致性检查引擎：第一个是报文策略引擎 PPE（快速的报文过滤器，是 IPSec 体系结构所需要的）；第二个是 SA 策略引擎（即 Keynote 解释器，用于测试在创建 SA 时给出的 IKE 提议）。HSBR 通过自己的 keynote 策略来控制 SA 的创建，当发现需要和对等实体需要一个共同 SA 时，就向对方提议保证它们达到通信目标的“强度最弱的”报文过滤规则以及支持该提议的凭证。这些凭证之间的信任模式与具体实现相关，包括任意的 Web 信任、全局可信的第三方（如 CA），或者信任度处于这两者之间的任何方式。在创建 SA 时候，HSBR 查询自己的 SA 策略引擎以判断对方端点提议的过滤器和 SA 是否满足本地策略。如果一致的话，则创建一个包含指定过滤器的 SA。其他的 SA 属性也可由 SA 策略引擎控制（例如，一条 SA 策略可以规定可接受的加密算法和密钥长度、SA 的生命期、日志和记帐需求等）。

根据上面的模型，本文将策略管理的处理划分为两部分：(1)报文过滤。它根据作用到每个报文的简单规则来实施。(2)更复杂的信任管理。它根据协商来决定哪些规则是可以实施的。这种方法易于为大型网络制定安全策略，并且自然地集成了策略自动发布机制。

SPP 系统的认证　IPSec 协议被推荐为 SPP 的认证机制。对于 SPM 来说，一种简单的作法就是对 SPP 使用 IPSec 进行封装。SPP 系统认证的复杂性包括可能的多安全域之间的 SPP 认证和保护机制。对 SPP 系统的研究不是本文的重点，因此在这里不做进一步的研究，只是通过 SPM 中 SPP 本身所具有的基于 IPSec 协议的认证接口以及为其他方法预留的逻辑功能体接口来保证对于 SPS 系统的认证功能的实现。

总结　本文对安全数据库的管理特点进行了分析，给出了一种基于混合式体系结构的安全数据库管理系统 SDM。该系统综合了集中式和分布式模型的优点，可以通过管理、接收、访问等不同组件和相应的代理完成安全数据库的维护和访问。其中在 ForCES 规范下提出的基于 SPP 的安全策略管理解决了域内和域间安全数据（主要是安全策略）的管理问题，使得整个系统形成了完整的安全数据管理框架。从本文的讨论可以看到，SDM 具有良好的开放性、可扩展性和较快的访问速度，是一种适于工程实现的高效的安全数据库管理体系结构，完全可以满足 HSBR 系统的设计要求。

参 考 文 献

1　Kent S, Atkinson R. Security Architecture for the Internet Proto-

col. RFC2401. Nov. 1998
2 Kent S, Atkinson R. IP Authentication Header. RFC2402. Nov 1998
3 Atkinson R. IP Encapsulating Security Payload (ESP). RFC2406. Nov. 1998
4 Harkins D, Carrel D. The Internet Key Exchange (IKE). RFC2409. Nov. 1998
5 Chan K, Seligson J, Durham D, McCloghrie K. COPS Usage for Policy Provisioning(COPS-PR). RFC 3084. Mar. 2001
6 Hodges J, Morgan R. Lightweight Directory Access Protocol (v3): Technical Specification. RFC3377. Sep. 2002
7 Yang L, Dantu R, Anderson T, Gopal R. Forwarding and Control Element Separation (ForCES) Framework. draft-ietf-forces-framework-13. txt. Jan. 2004
8 Yang L, Halpern J, Gopal R, DeKok A, Haraszti Z, Blake S, Deleganes E. ForCES Forwarding Element Model. draft-ietf-forces-model-02. txt . Feb. 2004
9 Putzolu D. ForCES Protocol Evaluation Draft. draft-ietf-forces-evaluation-00. txt . Dec. 2003
10 汤隽,赵荣彩,宋成杰. 安全策略系统的研究及其在 IPSec 中的应用. www. Linuxipsecvpn. cosoft. org. cn
11 Farrell S, Housley R. An Internet Attribute Certificate Profile for Authorization. RFC3281. Apr. 2002
12 Blaze M, Feigenbaum J, Ioannidis J, Keromytis A. The KeyNote Trust Management System Version 2. RFC 2704. Sep. 1999
13 Blaze M, Ioannidis J, Keromytis A. Trust Management for IPSec. In: Proc. of the Internet Society Symposium on Network and Distributed Systems Security. SNDSS 2001. 139～151

(上接第117页)

ta Warehouse)指标的概念。它的集成性是由数据仓库的 QoD 来实现的,QoD 将各个模块连接起来的,并形成一种反馈机制,从而使得整个数据仓库系统朝着质量好的方向演变。

为了实现这个目的,必须定义数据仓库的质量指标,并对这些质量指标进行定量计算。在 WIEDW 中,整个数据仓库的综合质量指标是由若干个分质量指标组成的。分质量指标是指数据仓库的实际输出与理想状态下的数据输出在准确性方面的接近程度,它的一般定义可以用下面的公式来表示:

$$DW_i=(QI-QF)/QI \quad (1)$$

式中,QI 表示理想状态下数据仓库的某个质量指标,QF 表示实际环境下的相应的质量指标。因此,整个数据仓库的综合质量指标,定义如下:

$$QoD = a_1 * DW_1+a_2 * DW_2+\cdots+a_n * DW_n$$

其中,$a_1+a_2+\cdots+a_n= 1$

a_1, a_2, …,a_n 表示每个质量指标所具有的影响值,可以通过人为的方式指定。

可以把数据仓库的分质量指标 DW_i 分成三类:

(1)及时性 这是指数据仓库系统在接收到用户的请求之后将查询结果返回给用户时所花费的时间与理想状态下的值的接近程度,可以用式(1)来定量表示。

及时性由数据仓库本身的响应时间、数据仓库系统的响应时间组成。前者与数据仓库定义时所指定的数据的粒度、维度的定义方式有关;后者与数据仓库系统的并发用户、数据仓库实现模式有关。

(2)完整性 是指数据仓库返回给用户的查询结果是完整的。它的主要影响因素有:各个数据源数据抽取的频率、元数据的定义、数据仓库的更新算法、数据记录概括算法等。

(3)一致性 是指在不同用户的相同查询或同一个用户的多次查询请求中,所得到的数据应该是相同的。它包括数据结构的一致性、数据语义的一致性,如同一个字段的不同描述、产量在某一段时间内的增加与减少等。

它的主要影响因素有:数据抽取时设定的过滤规则、元数据的表达及维护是否合适、数据仓库的更新算法、数据记录概括算法等。

上述分析中,所涉及到的影响质量指标的因素可以用来作为数据抽取模块、OLAP 展示组件、元数据管理等模块做自我调整的参考。

结束语 基于 Web 的数据仓库集成环境的研究具有以下重要意义:1)改变了目前数据仓库构建过程中各个环节相互脱离的现象,为用户提供一个集成化的设计、运行、维护平台,提高了企业建立、维护数据仓库应用系统所需要的人力、物力投资,又大大缩短了企业建立数据仓库的开发设计周期;2)实现了最优算法、行业定制、企业定制算法的动态加载,使数据仓库的分析数据真正对企业的决策活动具有较好的指导意义。3)使用户能在任何地方借助互联网通过浏览器方便使用。

参 考 文 献

1 Ladley J. Data Warehousing Trends, Data Adviser, Jan. 1998. 35～37
2 Xin Tan, Yen D C, Xiang Fang. Web warehousing: Web technology meets data warehousing. Technology in Society, Jan. 2003, 25 (1): 131～148
3 Shim J P, et al. Past, present, and future of decision support technology. Decision Support Systems, June 2002, 33(2): 111～126
4 Li Xiu, Wang Xuerui, Liu Wenhuang, Liao Lin. The research of web-based data warehouse using XML. Info-tech and Info-net, 2001. In: Proc. ICII 2001 - Beijing. 2001 Intl. Conf. on, 2001, 5: 42～47
5 Liao Lin, Wang Ligang, Liu Wenhuang. Building the Web-Based Data Warehouse with XML. The Joint International Computer Computer Conference, Nov. 2000
6 Mikael R J, Thomas H M, Torben B P. Converting XML DTDs to UML diagrams for conceptual data integration. Data and Knowledge Engineering, March 2003, , 44(3): 323～346
7 McHugh J, Abiteboul S, Goldman R, Dallan Q, Windom J. Lore: A Database Management System for Semistructured Data.
8 NCSA. Introduction to NCSA Mosaic for X. Notional Center for Supercomputing Application, University of Illinois at Urbana-Champaign.
9 唐蕾,张剡,等. 数据仓库工具集 NGDW-1的设计与实现. 见:第19届中国数据库学术会议. 郑州,2002.
10 曹鲍光,王申康. 元数据管理策略的比较研究. 计算机应用, 2001, 21(2): 3～5
11 Hurwiz Group. Enterprise Metadata Management [R]. Hurwiz Group BalancedView Report, 1998
12 宋擒豹,杨向荣,沈钧毅. 数据仓库技术研究. 计算机工程, 2002, 28(1): 125～127
13 王珊,等. 数据仓库技术与联机分析处理. 北京: 科学出版社, 1998
14 ichael G , Woollen R, Emerson L. J2EE 应用与 BEA Weblogic Server. 邢国庆等译. 北京:电子工业出版社, 2002