数据交换管理系统域模型①

吴一博[1,2]，廉东本[2]，蒋 宁[3]

[1](中国科学院研究生院，北京 100049)
[2](中国科学院 沈阳计算技术研究所，沈阳 110171)
[3](沈阳师范大学 教育技术学院，沈阳 110034)

摘 要：辽河流域水环境管理系统应用分布地域广，层次级别多，省市区县节点之间需要进行数据的传输和交换，为了解决这样一个庞大体系中的复杂交换，设计并实现了域模型。对域模型的整体结构和各个元素进行了阐述，并对域模型中的关键模块—域标识、信任模型、路由及跨域通信进行了重点描述。

关键词：数据交换；域模型；路由；信任模型

Domain Model in Data Exchange Management System

WU Yi-Bo[1,2], LIAN Dong-Ben[2], JIANG Ning[3]

[1](Graduate School, Chinese Academy of Sciences, Beijing 100049, China)
[2](Shenyang Institute of Computering Technology, Chinese Academy of Sciences, Shenyang 110171, China)
[3](School of Education Technology, Shenyang Normal University, Shenyang 110034, China)

Abstract: Liao River Basin Water Environmental Management System is wide in geographic distribution. It has multi-level, provincial and municipal districts of data between nodes need to transmit and exchange. Liao River Basin Water Environmental Management Information System is involved in many departments. The multi-node need data transmission and exchange. In order to solve such a large system of complex exchange, design and implement the domain model. The overall structure of the model of domain and each element is discussed, and the key module-domain identification module, trust models and cross-domain communication is introduced emphatically.

Key words: data exchange; domain model; trust model

近年来，为了保护辽河流域水资源、监控流域污染、防止流域水环境退化，辽河流域研制了各种水环境管理信息系统。这些管理信息系统是由不同的软件支撑平台和硬件产品构成，是在不同时期、不同规划，采用不同标准和规范创建的，为了有效地和充分的利用数据资源，降低查找和分析数据耗费的大量人力成本，采用计算机技术、计算机网络技术构建的数据交换网络，使应用系统进行信息（数据）的交换和传输，最大限度地提高信息资源的利用率成为信息化建设的重要目标。

水环境系统应用分布地域广，层次级别多，为了实现各涉水部门（横向）和各级环保部门（纵向）之间的数据传输与交换，创建了具有多数据交换节点的数据交换网络。

在多数据交换节点的数据交换网络中，中心节点、普通节点和交换客户端节点间需要进行数据的传输和交换。为了解决这样一个庞大体系中的复杂交换，使其具有更好的开放性，引进了域管理理论及技术，从而使数据安全有序的交换和传输，更好的实现跨部门、跨平台的数据交换。

1 域模型的设计

1.1 域元素

域元素包括中心域、普通域、非域交换节点、域

① 基金项目:国家水体污染控制与治理科技重大专项(2009ZX07528-006-05)
收稿时间:2011-07-19;收到修改稿时间:2011-08-24

客户端、非域客户端。

基于分级的域模型结构[1]，如图 1 所示。

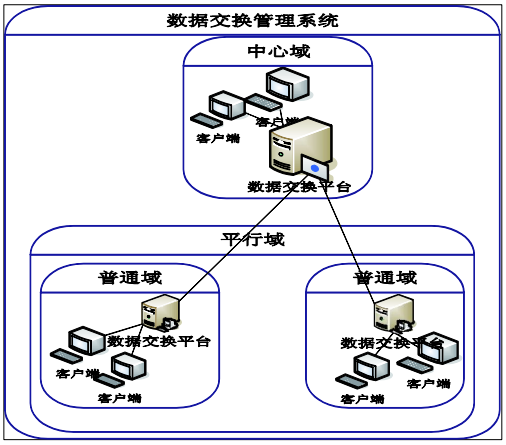

图 1　基于分级的域交换示意图

1 客户端

客户端为用户提供了基本的管理和操作界面。

2 普通域

一个普通域包括一个数据交换管理系统和多个客户端。这就是单个数据交换平台，适用于规模较小的情况。一个普通域下的各个客户端通过数据交换管理系统即可以进行数据交换。

3 中心域

一个中心域包括多个普通域。中心域的作用：

(1) 提供域注册/域注销功能：普通域的交换管理系统在中心域注册；

(2) 建立/注销信任域：两个普通域之间有信任关系时，才能通信；

(3) 权限控制，发放令牌：普通域通信时，需要中心域的令牌；

(4) 发放密钥：数据加密时需要的密钥；

(5) 查询域间关系：两个域间是否为信任域。

不同普通域通过中心域进行联通。所有普通域的数据交换管理系统需要在中心域注册。当不同普通域进行数据交换时，先到中心域查询两个域间是否为信任关系，若不是信任域，先建立信任关系，然后中心域发放令牌，两个普通域的不同客户端即可以进行数据交换。

4 非域客户端

不属于域，即没有在普通域注册的客户端

5 非域交换节点

不属于域，即没有在中心域注册的域

1.2 域关系

平行域：节点之间的关系是对等的。比如中心域管辖范围内有几个普通域，普通域和普通域之间的关系是对等的，他们是平行域关系。

垂直域：节点之间的关系不是对等的。比如普通域和普通域通信时，需要向中心域申请令牌，中心域有权限控制作用，中心域和普通域之间是垂直域关系。

普通域和普通域通信需要在中心域建立信任委托关系；中心域管理着各个普通域间的关系，形成信任链；当普通域向中心域申请与另一个普通域建立信任关系时，中心域先查询是否有这两个域间的信任路径，如果有，则不需要再建立信任关系，若没有，则建立信任关系。

2　域模型中实现的关键模块

2.1 域标识管理

为了方便的进行跨域数据交换，数据交换管理系统需要完整的域标识机制[2]，具体包括：

(1) 域的唯一标识符。系统按照一定的规则给予域唯一且永久的名字。

(2) 域注册。存储域名以及域的相关属性。

(3) 域注销。

2.1.1 域标识的设计

域标识用于唯一地标识一个域，域标识的设计包括两部分：固定标识和可变标识。

其中，固定标识类似于数据库的主键，唯一地标识一个域，一个域只能有一个固定标识，它和域有相同的生命期。类似固定标识，可变标识也唯一地标识一个域，但是，可变标识是一段人们可理解的字符串。固定标识是普通域注册成功后，中心域发放给普通域的域编码；而可变标识是由域的注册者创建的，即普通域传给中心域的域名称。

2.1.2 域注册

1) 中心域生成序列号，并向普通域颁发序列号；

2) 普通域向中心域申请建域，消息包括（消息编码，序列号，域名称，账号，密码，ip,端口号，公钥，随机数，区代码,MAC 地址），其中（消息编码，域名称，账号，密码，ip,端口号，公钥，随机数，区代码,MAC 地址）用 RSA 算法生成的私钥加密；

3) 中心域认证普通域发来的序列号失败，则不允

许建立普通域；认证成功，则允许建立普通域，生成普通域的子钥和域编码，并返回用公钥加密后的子钥和域编码；

4) 普通域将私钥解密后的域编码和子钥及相关本域的信息存进域注册表，并更新系统用户表，标明本用户属于本域。

2.1.3 域注销

1) 普通域向中心域申请注销，发送消息（消息编码域编码，MAC，用户名，密码）；

2) 中心域认证通过后，将此普通域的域名及相关属性删除，并删除域关系表中与此域相关的信任委托域；

3) 注销成功后，普通域也删除中心域的相关信息和本域子钥。

2.2 信任模型

信任模型包括建立信任关系，删除信任关系等。

2.2.1 安全域间信任关系

本节从信任的角度来讨论域间通信行为的可信性，即通过分析两个域间的输入、输出及动作序列是否符合主客体的预期，来判断域间通信行为是否可信。下面给出安全域间信任关系的定义[3]:

定义 1. 当两个域 P、Q 满足：

① Q 对 P 进行的操作已经得到授权，并且严格执行预期操作；

② Q 对 P 进行的操作未得到授权，但该操作并不影响 P 的输出，称域 P 信任域 Q。

用 Trust 表示系统中两个域间的信任关系，若 da 信任 db，则表示成：Trust(da,db)。

用二元组 Trust(P,Q)来表示域 P 信任域 Q 的信任关系，用 R 表示这类二元组的集合，定义信任关系的对称性为：

定义 2. 若 Trust(P,Q)|R,可以推出 Q 信任 P，即 Trust(P,Q)→Trust(Q,P),则称该信任关系具有对称性，表示为 S-Trust(P,Q)。任意的两个域 da 和 db，若有条件 da 信任 db，从该条件能够推出 db 信任 da，则称域间的信任关系满足对称性，表示为 S-Trust(db，da)。

定义 3：三个域 P、Q、S，若 P 和 Q 的信任关系满足对称性，且有 Q 信任 S，那么 P 也信任 S，

即 S-Trust(P,Q)，且 Trust(Q,S)，有 Trust(P,S),则称 P 和 Q 的信任关系具有到 S 的传递性，表示 H-Trust(P,S)。

任意的三个域 da、db、dc,若 da 及 db 满足信任关系的对称性，且 db 信任 dc，则有 da 信任 dc，即域 da 和 dc 满足域间信任关系的传递性，表示为 H-Trust(da,dc)。

2.2.2 普通域之间建立信任关系

1) 域 A 向中心域申请与域 B 建立域信任关系，消息包括：消息编码+本域编码(A)+域名称+账号+密码+MAC+目的域编码(B)；

2)中心域认证成功后，在域关系表中查询 A、B 的信任关系，如果 A、B 有信任关系(即只要有路径可达即可)，则不允许 A、B 建立信任关系；反之，则允许；

3) 如果中心域允许建立信任关系，则中心域在域关系表中增加此信任关系(A，B)。

2.3 路由

1 路由规则

在数据交换管理系统中，存在着横向和纵向的多个交换节点，这些交换节点并不是对等的，而是依据政府的组织结构，有上下级之分。任意单位的数据并不是随意传递的，需要按照一定的规则传递[4]。设定的规则如下：

1) 区县客户端同属于一个普通域，则通过此普通域进行数据交换；

2) 平级单位的普通域不能直接相连，应该通过上级的中心域互连。

2 路由解析

跨域访问时，从域关系表中寻找源域与目的域之间节点的路径，即源域和目的域是否是信任关系。如果有可达路径，则源域和目的域是信任关系，两域之间可以通信；否则，不能通信。

查找信任关系的算法：这里采用递归搜索算法

```
/*point1 和 point2 为两个普通域节点,points 初始为 point1,path 初始为""  */
String findPath(String point1,String point2,String points,String path)
{//获取某点除了父辈和兄弟节点以外的直接信任节点
 List<String> pointsList
 =getPointsNotParentsorBrothers(point1,points);
  path += point1;
  if(pointsList.size()<=0)
```

```
{/*递归结束，返回*/
return "";
}
else if(pointsList.indexOf(point2)!=-1)
{/*找到了 point2，存在信任路径*/
return path+point2;
}
for(int j=0;j<pointsList.size();j++)
{/*添加兄弟节点*/
points+=","+pointsList.get(j)+"";
}
String result="";
for(int i=0;i<pointsList.size();i++)
{/*递归*/
result=findPath(pointsList.get(i),point2,points,path);
if(!"".equalsIgnoreCase(result))
{
break; /*找到一条信任路径即可，停止查找*/
}
}
return result;/*返回信任路径*/
}
```

2.4 跨域通信

2.4.1 域间通信(A、B)

1) 域 A 向中心域申请与域 B 通信，消息包括(消息编码，本域编码，用户名，密码，目的域编码)；

2) 中心域认证通过后，路由解析判断本域和目的域是否有可达路径。有可达路径，则域 A 和域 B 可以通信；否则，不能通信；

3) 有可达路径后，中心域向域 A 发送令牌和过程密钥（令牌是由 B 的子钥+随机数计算得出，过程密钥是由令牌+A 的特征值计算得出）；向域 B 发送随机数；

4) 域 A 得到中心域发来的令牌和过程密钥后，向域 B 发送消息(消息编码，令牌，MAC,消息包体)，用过程密钥加密消息包体；

5) B 端通过中心域发来的随机数和自己的子钥得出令牌，和 A 端发来的令牌相比对，若比对成功，则返回成功消息；反之，则返回失败消息；

6) 令牌比对成功后，域 B 用算出的令牌和域 A 的特征值(MAC)得出过程密钥，解密域 A 发来的数据。

2.4.2 跨域安全

多域情况下的信息安全机制;具体包括域和域之间进行可信任连接的方式、域内访问控制策略、身份认证策略等的设计与实现等。此外，通信协议具备足够的能力以支持通信安全和系统审计[5]。

安全的跨域数据交换主要包括以下几部分:

1) 基础的安全手段:提供加密，数字签名，公证，时间戳，消息摘要等手段对数据的安全交换提供基础技术支持。

2) 安全机制:在上述安全手段基础上提供数据完整性、保密性、抗抵赖性。

3) 安全服务:提供安全的身份认证和安全的访问控制。安全的身份认证使用了第三方身份认证机制来确保跨域用户所声称的身份的真实可信性，采用了数字签名和验证的过程来确保用户和所声称的身份相吻合。

3 结语

为了有效的管理有多个数据交换节点构成的数据交换网络，本文设计并实现了域模型，并对其中的域标识、路由、信任及跨域通信等关键模块做了相应的设计。域模型的设计已经应用到实际项目中，取得了较好的效果。今后还要对路由算法及域内的管理进行进一步的研究和实现。

参考文献

1 王宁,王延章,叶鑫.一种基于数据中心的政府信息资源整合系统架构设计.计算机应用研究,2005,22(9):67−68,71.

2 邓磊,吴健,张昌利,马满福.电子政务中跨域可信数据交换模型设计与实现.计算机工程,2007,33(12):4−6,9.

3 Abrams MD, Joyce MV. Trusted system concepts. Computers and Security, 1995,14(1):45−56.

4 曾一,袁纲.基于 Web 服务的电子政务数据交换中心的设计和实现.计算机科学,2007,34(11):98−102.

5 陈帆.数据交换中的域管理模型研究与设计[硕士学位论文].西安:西北工业大学,2007.