数据交换管理系统的密钥管理体系①

唐雪晶[1,2]，廉东本[2]，帅小应[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](池州学院 计算机系，池州 247000)

摘 要：为解决辽河流域水环境数据的传输和共享问题，更好地实现水环境的监督和管理，设计实施建设数据交换管理系统很有必要。密钥管理体系是为具有域模型的数据交换管理系统提供安全服务，主要研究了数据交换管理系统的密钥管理体系中不同类别的密钥生成、密钥存储、密钥分散和密钥传输等问题。

关键词：密钥管理；密钥生成；密钥存储；密钥分散

Key Management of Data Exchange Management System

TANG Xue-Jing[1,2], LIAN Dong-Ben[2], SHUAI Xiao-Ying[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](Computer Science Department, Chizhou College, Chizhou 247000, China)

Abstract：To solve the problem of data transmission and sharing of Liaohe River water environment, to better supervise and manage the water environment, it is necessary to design implementation data exchange management system. Key management system is for a domain model of data exchange management system security communication services. This paper studied the data exchange management system key management systems of different types of key generation, key storage, key dispersion, key transmission and key problems such as the key generation and use of process key.

Key words：key management; key generation; key storage; key scattered

目前，我国正在实施跨越式经济发展战略，水环境保护面临巨大的压力，流域水污染控制作为我国的经济社会发展的重要战略目标，受到我国各级政府的高度重视。近年来，辽河流域水环境保护形式日趋严峻，为保护流域水资源、监控流域污染、防止流域水环境退化，辽河流域在水环境监测、监控与管理方面做了大量的工作，研制了各种水环境管理信息化系统。但是对于各个独立的信息系统，数据以不同的格式分散存放在不同的数据库、不同的系统中，很难将其集中起来进行分析和展现，查找和分析数据需要耗费大量的人力，资源不能有效地利用，难以满足水环境的综合管理需要。通过凝聚分散的信息系统的数据传输交换的需求，将分散的信息系统构建成数据交换管理系统，从而实现数据的传输和共享，更有效地实现流域水环境的监督和管理。

为满足辽河流域各个支流断面监测、干流断面监测，省控断面监测，大中型水库监测等不同级别的监测信息系统的数据传输和共享的需求，需要构建具有多级交换节点的数据交换管理系统。在数据交换管理系统中引入域模型的概念，从而将数据交换的计算量分散，那些只需要在某个域内交换的数据信息只消耗相应域的交换中心的处理能力，结合跨域通信的数据交换具有更好的扩展能力，能够更好地实现流域水环境的监督管理。密钥管理体系就是为具有域模型的数据交换管理系统的安全服务的。

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:2011-10-27;收到修改稿时间:2011-12-01

1 概述

密钥管理是处理从密钥产生到最终销毁的整个过程中的有关问题，不同的系统密钥管理方法不同[1]。本文中的密钥管理体系主要讨论密钥生成、密钥分散、密钥存储等与域模型设计相关的密钥管理问题。涉及到的密码学方法主要有 RSA 和 DES。

RSA 算法是一个基于初等数论定理的公钥密码体制的加密算法[2]。

算法描述：

①两个素数 p 和 q(保密的，选定的)

②n=pq(公开的，计算得出的)

③e，满足 gcd(φ(n),e)=1;1<e<φ(n)(公开的，选定的)

④d≡e-1(mod φ(n))(保密的，计算得出的)

私钥为{d，n}，公钥为{e，n}。假定用户 A 公布了他的公钥，B 发送消息 M 给 A，那么用户 B 计算 $C=M^e \bmod n$，并发送 C 给 A，用户 A 计算 $M=C^d \bmod n$，解密消息 M[3]。

DES 属于对称加密算法，即加密和解密使用相同的密钥，是目前最常用的加密算法之一。DES 加密明文的处理过程经过三个阶段，首先，64 位的明文经过初始置换（IP）而被重新排列。然后进行 16 轮相同函数的作用，每轮作用都有置换和代换。最后一轮迭代的输出共有 64 位，其左半部分和右半部分互换产生预输出，预输出被与初始置换互逆的置换（IP^{-1}）作用产生 64 位密文。DES 的密钥经过初始置换后，经过循环左移和置换分别得到子密钥 K_i 用作每一轮的迭代。每轮的置换函数都一样，但是由于密钥的循环移位使得子密钥互不相同。DES 解密密文的过程与加密过程一致，只是子密钥的使用次序相反[3]。

2 密钥管理体系的设计

2.1 密钥管理体系的分类

密钥管理体系是为流域水环境数据交换管理系统的域管理和系统管理服务的，与系统域模型对应，密钥管理分为中心域密钥管理，普通域密钥管理，非域节点密钥管理(系统管理)，客户端密钥管理。

域模型中，中心域节点之间是网状关系，中心域节点之上不再设计其它的域节点。中心域、普通域、非域节点都有各自的数据交换管理系统，域模型中的各个节点共同构成数据交换网络。一个单独的数据交换节点作为一个数据交换管理系统时，该交换节点必须是中心域。

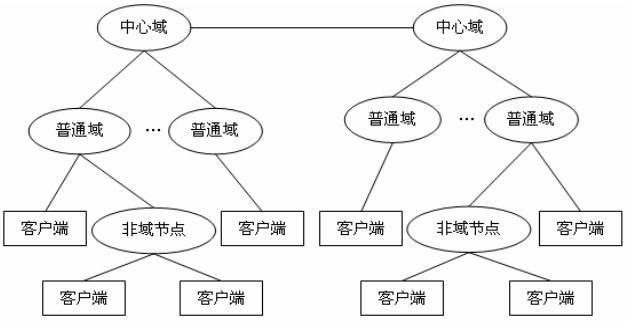

图 1 域模型拓扑图

在密钥管理体系中，过程密钥是节点之间发送数据时用于加密数据的密钥。域中各个节点都有各自的密钥，中心域密钥称为中心域母钥。

中心域的密钥管理主要包括中心域母钥的生成与存储，普通域密钥的分散与传输，中心域所辖相互信任的普通域间过程密钥的生成与传输等。

普通域密钥的管理主要包括普通域密钥的获得和存储，普通域节所辖非域节点和客户端的密钥的分散与传输以及普通域与其它信任域通信时过程密钥的获得。

客户端密钥的管理主要包括客户端密钥的获得与存储，客户端发送数据时过程密钥的生成等。

非域节点的密钥管理主要包括非域节点密钥的获得与存储，非域节点所辖客户端密钥的分散与传输以及与其它节点传递数据时过程密钥的生成与传输等。

2.2 密钥管理体系的基本框架

密钥管理体系的基本框架主要包括密钥的发放和过程密钥的使用。

密钥发放的过程如下图所示：

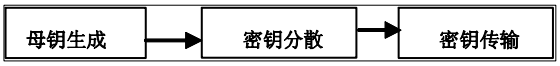

图 2 密钥发放示意图

过程密钥是数据交换管理系统中用于保证数据安全传输用到的密钥。在该密钥管理体系中的过程密钥主要有：

中心域与普通域之间通信的过程密钥，普通域之间通信的过程密钥，客户端与普通域和非域节点之间通信的过程密钥，非域节点与普通域之间通信的过程

密钥等。

2.3 密钥的分散与存储

密钥分散是上级的密钥与本级的特征相结合形成的本级密钥。密钥管理体系中的密钥主要包括中心域母钥，普通域、非域节点和客户端子钥。数据交换管理系统中数据传输时采用 DES 算法加密，该体系中的密钥为比特形式。

中心域母钥的生成方式如下：

①$Key_{中心域母钥}$= F(A) A 为某种生成随机数的方式

中心域母钥主要是用来生成中心域下普通域的子密钥。为了保证安全性，中心域母钥的存储采用秘密分享技术的思想[4]，将生成的母钥 key 分段存放在中心域所连接的数据库的不同的表中。

普通域子密钥的分散方法如下：

②$Key_{普通域子钥}$=F($Key_{中心域母钥}$ + f(B)) B 为加密因子

加密因子(密码学中称为分散因子)是存储在中心域的普通域的机器特征(如 MAC 地址)，F 可采用 DES 算法，则 f 为处理加密因子得到 DES 密钥的方法。

中心域在接收到普通域的注册申请之后，根据方法 f 得到生成 $Key_{普通域子钥}$需要的 DES 密钥，取出分段存放的母钥，按照指定的规则还原得到 $Key_{中心域母钥}$。由 DES 密钥和 $Key_{中心域母钥}$通过 DES 得到 $Key_{普通域子钥}$。中心域只存储普通域相关的加密因子，并不存储普通域的子钥。普通域在指定的地方保存自身的子钥。

非域节点和客户端子密钥的分散方法与普通域子密钥的分散方法类似，都是由所属上级节点密钥和自身的加密因子分散得到申请的子密钥。

密钥分散方法如下：

③$Key_{子钥}$ = F(A+f(B))

A 为上级节点的密钥(普通域在为非域节点和客户端生成子钥时，从中心域处获得的子钥作为自身的母钥)。

B 为非域节点或客户端的机器特征。

2.4 密钥传输

密钥传输是采用 RSA 非对称加密算法解决由母钥和加密因子生成的子密钥的传输问题[5]。

普通域申请子密钥时，首先生成 RSA 公/私钥对，私钥秘密保存，公钥和普通域自身的机器特征等信息封装成特定的消息发送给中心域。中心域接收到此消息后，取出中心域母钥和普通域的加密因子，生成子密钥，用普通域的公钥加密后，发送给普通域。普通域接收后，用秘密保存的私钥解密得到自身的子密钥。在数据交换管理系统中，普通域申请子密钥是在普通域申请注册时发生。

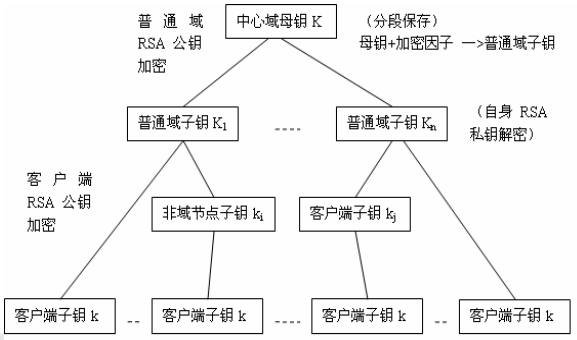

图 3　密钥体系示意图

非域节点向所属普通域申请非域节点子密钥。非域节点子密钥的传输方式与普通域子密钥类似，用自身 RSA 私钥解密从普通域获得的由自身 RSA 公钥加密的子密钥。

客户端子密钥的传输是客户端向所属节点申请客户端子密钥，同样是以特定的消息封装客户端自身的 RSA 公钥和机器特征等信息发送给所属上级节点，上级节点生成客户端子密钥，用客户端 RSA 公钥加密后发送给客户端，客户端用 RSA 私钥解密后在指定的地方保存子密钥。

2.5 过程密钥

过程密钥作为数据交换管理系统中传输数据时的 DES 密钥，并不是固定不变的，而是动态变化的[6]。每次传输数据之前生成或者获得过程密钥，数据传输完成后，该过程密钥不再有效。

一般过程密钥的生成方式如下：

④$Key_{过程密钥}$ = F($key_{子钥}$ + Random(n))

$key_{子钥}$是普通域、非域节点或客户端子钥;

Random(n)为发送数据的请求方生成的随机数。

中心域与普通域之间的过程密钥生成方式为，普通域的子钥作为 $key_{子钥}$，新生成的 64bit 的随机数作为 DES 密钥，F 采用 DES 算法生成 $Key_{过程密钥}$。如果是普通域向中心域发送数据，普通域生成随机数，普通域子钥和随机数生成过程密钥。用过程密钥加密发送的数据，把随机数放在报头中和数据一起发送到中心域，中心域通过接收到的随机数与计算得出的普通域子钥按照相同的规则生成过程密钥，解密接收到的数据。

如果是中心域向普通域发送数据，则随机数由中心域生成，中心域把随机数和计算得出的普通域子钥按照相同的规则生成 64bit 过程密钥，普通域接收到报文信息后，提取出随机数，按照相同的规则把随机数和自身的子钥生成过程密钥解密数据。

在数据交换管理系统的域模型中，只有相互信任的普通域之间才能够进行通信。假定普通域 A 和普通域 B 是中心域 C 下的相互信任的域，则 A 和 B 拥有各自的机器特征信息。A 向 B 发送数据之前，A 首先向中心域申请与 B 通信的过程密钥，中心域接收到申请，验证普通域 A 和 B 是相互信任的域后，用 A 的机器特征，B 的子钥和中心域 C 生成的随机数按照指定的规则生成 64bit 的过程密钥。

⑤$Key_{过程密钥}$ = F(F(B 子钥+A 特征) + C 随机数)

中心域 C 用 A 的子钥把过程密钥 DES 加密后发送给 A，将随机数发送给 B。普通域 A 用解密后的过程密钥加密要发送的数据，普通域 B 接收到数据后，等待从中心域 C 发送过来的随机数，普通域按照相同的规则生成过程密钥解密数据。如果 B 接收到 A 的数据后，在给定的时间限制内没有接收到中心域 C 的随机数，则此次通信作废。B 向 A 发送通信失败的反馈信息，域 A 重新发起与域 B 的通信。

客户端与普通域和非域节点之间通信时，如果客户端作为发起端，则过程密钥为客户端子密钥和客户端生成的随机数通过 DES 算法生成的 64bit 的 DES 密钥，客户端将随机数放在报头中与数据一同发送给作为接收端的普通域或非域节点，接收端提取出随机数和客户端子钥通过 DES 方法生成 DES 密钥解密数据。如果是客户端作为接收端，则构成过程密钥的随机数是由普通域或非域节点生成的，随机数和客户端子钥通过 DES 方法生成 64bit 的 DES 密钥，客户端提取接收到的随机数，取出自身子钥生成 64bit 的 DES 密钥解密数据。

非域节点域与普通域之间通信的过程密钥与客户端与普通域节点之间通信的过程密钥的形成方式类似，由数据传输的发起端生成随机数和非域节点的子钥生成 64bit 的 DES 密钥，随机数同数据一起发送给接收端，接收端将随机数和非域节点的子钥生成 DES 密钥解密数据。

3 结语

密钥管理体系作为系统数据传输安全的保障，是为域管理和系统管理服务的，是流域水环境管理系统重要组成部分。本文从系统域模型管理的需求出发，主要研究密钥管理体系中密钥的生成、存储、分散以及过程密钥的生成与使用等问题。目前密钥管理体系主要是满足密钥管理的基本需求，将进一步研究密钥的动态更新、销毁和跨中心域的密钥管理问题以及使用不同加密算法的密钥管理体系。

参考文献

1 闫鸿宾.密钥管理关键技术研究.南通纺织职业技术学院院报,2010,10(4):5–7.
2 向进.加密算法的安全性分析.吉首大学学报,2011,32(1):42–44.
3 Stallings W.孟庆树,王丽娜,傅建明,等译.密码编码学与网络安全:原理与实践.第 4 版.北京:电子工业出版社,2006.43–63,183–205.
4 庞辽军.秘密共享技术及其应用研究[博士学位论文].西安:西安电子科技大学,2006.
5 杨晓明.一种基于 DES 和 RSA 混合加密算法的研究. 电脑学习,2011,1:1–3.
6 马秀芳,时和平,时晨.基于密钥管理的密钥分发解决方案探析.电信快报,2004,28(14):53–56.

(上接第 68 页)

与发展,2001,38(3):328–333.
8 张宁.群体兴趣网的统计特性研究.上海理工大学学报,2008,30(3):243–246.
9 刘靖,陈福生.结合粗糙集和模糊聚类方法的属性约简算法.计算机应用软件,2004,21(11):72–74.
10 卜东波.分类聚类技术研究.北京:中科院研究生院,2000.
11 行小帅,潘进,李焦成等.基于免疫规划的 k-means 聚类算法.计算机科学,2003,(5):605–610.
12 张惟皎,刘春煌,李玉芳.聚类质量的评价方法.计算机工程.2005,31(20):10–12.
13 郭岩,白硕,杨志峰,张凯.网络日志规模分析和用户兴趣挖掘.计算机学报,2005,28(9):1483–1496.