

PKI 中桥信任模型的优化

常晋义, 李明杰

(常熟理工学院 计算机科学与工程系, 江苏 常熟 215500)

摘要: PKI 中存在多个可信任点和无终止的可信任环的可能性, 使证书认证路径的有效发现复杂和耗时, 路径构造的任务非常繁重。提出的基于路径代理的桥信任模型利用路径代理服务器, 采用生成树算法提前进行路径构造存储, 从而将复杂的路径构造问题转化为路径查询问题, 实现了对 PKI 桥信任模型的优化。

关键词: 生成树算法; 桥信任模型; 路径代理服务器; PKI

中图分类号: TP393.08

文献标识码: A

文章编号: 1673-629X(2007)08-0155-03

Optimization of Bridge Trust Model in PKI

CHANG Jin-yi, LI Ming-jie

(Department of Computer Science & Engineering, Changshu Institute of Technology, Changshu 215500, China)

Abstract: In PKI technique, by making use of CA certification can available avoid active attack. In each CA certification area can build hierarchical models or network models, then by traditional bridge trust model can also reach intercommunication among different areas, so that CA and entities can trust each other. But in PKI, perhaps exist more than one trusted dits or an endless circle, thus discovery an certification's path is becoming very complex and time-consuming, so the task that build the path will be an overwork. In the paper by using a path agent server in path agent bridge trust model, by adopting spanning tree algorithm built and store the path ahead of schedule, thus the complex task that build the path is converted into a task that search paths, therefore realize the optimization of the bridge trust model in PKI.

Key words: spanning tree algorithm; bridge trust model; path agent server; PKI

0 引言

桥信任模型被设计成用来连接不同的 PKI 体系, 以克服层次模型、网状模型等的缺点。桥信任模型需要与多种不同的 PKI 架构进行连接, 具备现实性强、良好的灵活性和扩展性。但由于桥信任模型可能会涵盖网状 PKI 结构, 使得 PKI 中存在多个可信任点和无终止的可信任环的可能性, 这样证书认证路径的有效发现可能是非常复杂和耗时的操作, 路径构造的任务非常繁重。在桥模型的 PKI 系统中, 用户端需要支持多种检索协议来搜寻所需要的证书路径信息, 因此需要采用一些新机制来有效发现和验证复杂的证书路径, 以解决桥信任模型的证书路径处理困难的问题。

桥 CA 模型中, 证书路径的有效发现和确认比较困难, 这样证书路径处理效率低下。针对这一问题, 文中提出一种优化的解决方案——基于路径代理的桥信任模型。

任模型。

1 基于路径代理的桥信任模型

1.1 系统模型

如图 1 所示, 与桥 CA 进行互连的多个信任域中, 不论是层次信任模型, 还是网状信任模型, 每个域都要确定一个可以代表域的 PCA(Principle CA)与桥 CA 进行互连。如果是层次模型, 根 CA 就作为 PCA 与桥 CA 建立交叉认证; 如果是网状信任模型, 域内就要找出一个可以代表域的 CA 作为本域的 PCA 与桥 CA 建立交叉

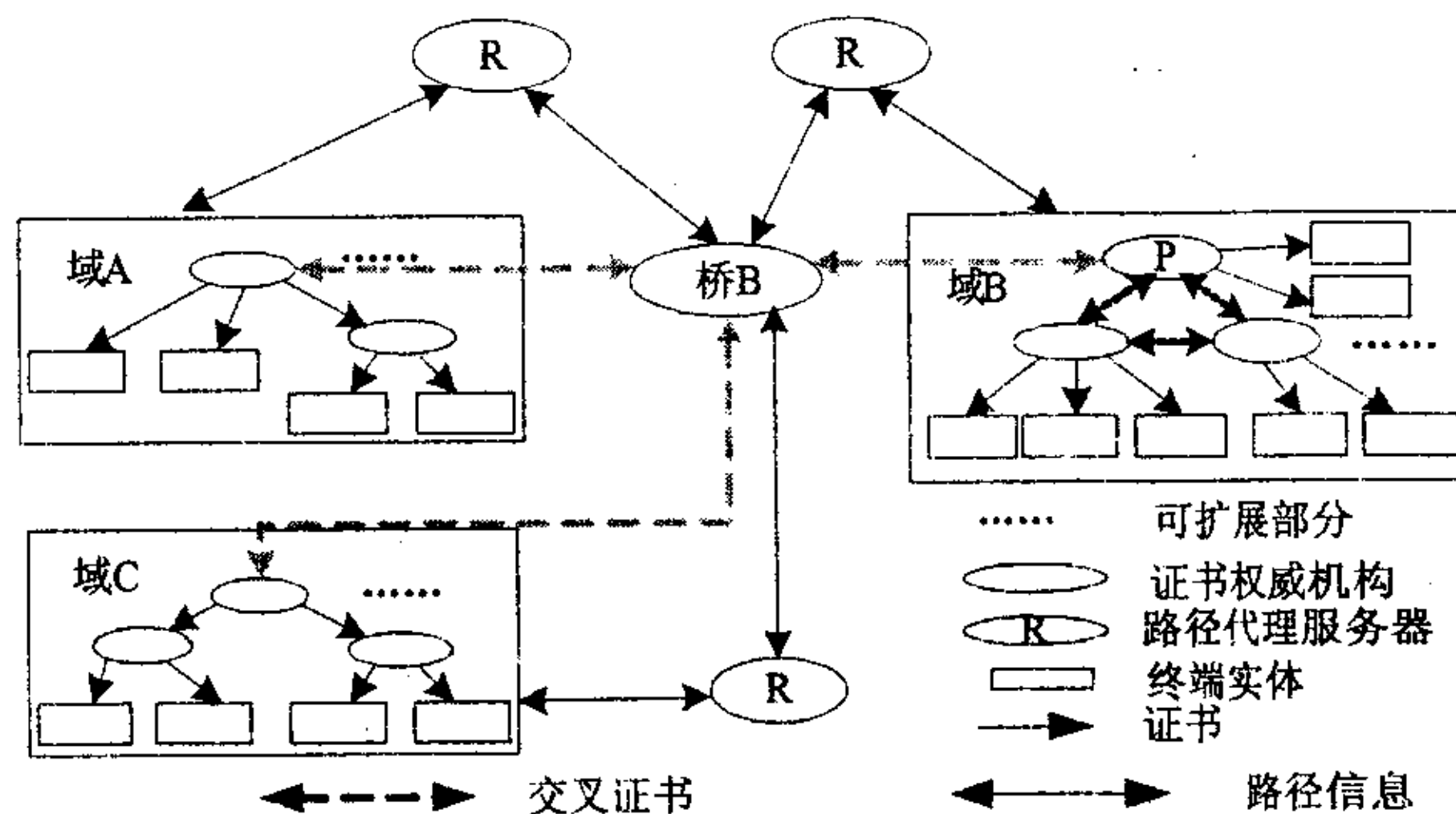


图 1 基于路径代理的桥信任模型

收稿日期: 2006-10-19

基金项目: 江苏省高校自然科学基金计划资助项目(03KJD51002)

作者简介: 常晋义(1955-), 男, 山西忻州人, 教授, 研究方向为空间决策支持系统、信息系统安全。

叉认证^[1]。同时,每一个信任域都构建一个路径代理服务器(Path Agent Server,PAS),任意信任域间的 PAS 都与桥 CA 进行可信连接,PAS 负责进行域内 CA 间的信任路径信息和路径相关证书的收集和发布、废除、评估、更新、存储,并提供信任路径的查询服务^[2]。

1.2 设计思想

假设域 A 中实体 A 和域 B 中实体 B 间相互认证时,实体 A 和 B 之间的路径是完全未知,验证方需要通过本域、桥 B 及通信方域构造一条完整证书路径(证书链)。在这个过程中,可能会遇到多个可信任点和无终止的循环路径存在的可能性。这样证书信任路径的有效发现可能是非常复杂和耗时的操作,路径构造的任务非常繁重。因此有可能存在构造到最后才发现 A、B 之间无可信任路径,或者是存在信任路径而无法有效的发现。

在每个域中加入路径代理后的证书路径处理方式如图 2 所示,通过路径代理服务器 PAS 收集、构造、存储本域内信任路径信息和路径相关证书。这样,当两实体间需要验证时,不需要每次去发现与构造实体间的证书路径,而是直接查询 PAS 内存储的路径信息,从而将复杂的路径构造问题转化为路径查询问题,以提高证书路径处理的效率。

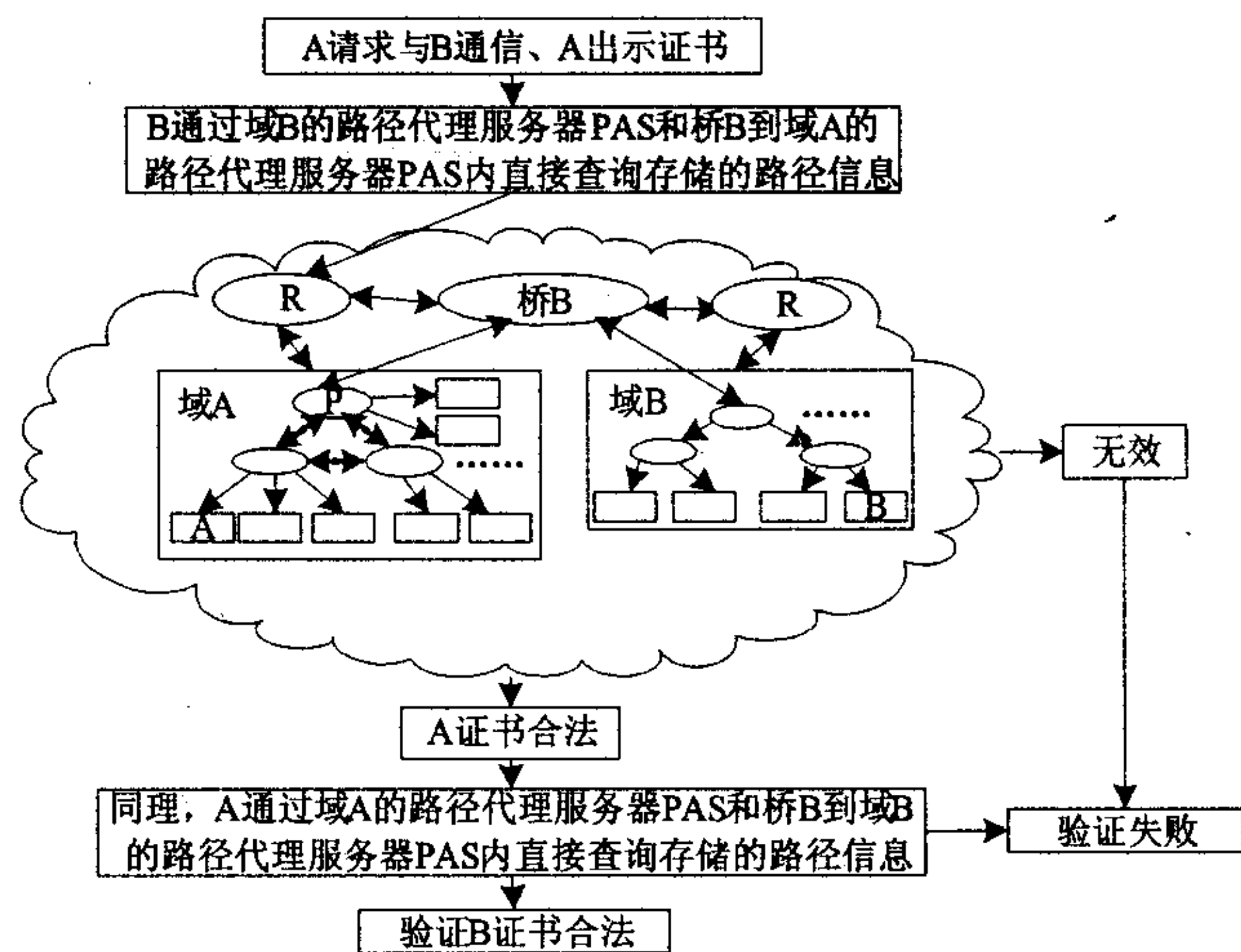


图 2 基于路径代理的桥信任模型路径处理过程

1.3 路径代理服务器设计

构建路径代理服务器 PAS 是基于路径代理的桥信任模型的核心,每个域内 PAS 负责进行各个域内 CA 间的信任路径信息和路径相关证书的收集、发布、废除、评估、更新、存储,并提供信任路径的查询服务^[3]。为了保证 PAS 提供的路径信息的权威性、公正性和可靠性,最好是由域内 PCA 的构建机构进行建设。

在选择域内信任模型和对域内所有的 CA 进行管理的时候,域内各个 CA 的常规信息应该保存在 PAS

服务器中,例如证书权威机构 CA 的名称、策略以及它的 LDAP 的目录服务器 IP 地址等等。

证书通常是存放在目录中的。X.509 证书中的主题及颁发者名称是层次式的名称,它们直接映射到目录中的相应目录项。由于证书查询操作频繁,速度要求也很高,而且证书本身数据量并不大,因此通常采用 LDAP 进行存储。一个特定证书可以存放在颁发者的目录项中,也可以存放在主题的主题的目录项中,或者同时存放在两处。PAS 路径的构造是依赖于证书目录服务器以及证书在目录中的存放位置的。

2 域内信任模型及路径构造

2.1 域内信任模型

基于路径代理的桥信任模型在传统的桥 CA 模型的基础上扩展后,一个域可以是企业内部单独的 PKI 体系,也可以是一个行业或者一个地区的 PKI 体系。这样,在基于路径代理的桥信任模型的域内,各个 CA 也必须选择一种合适的信任模型来组织构建。域内建议采用层次模型和网状模型,如果域内 CA 较多且信任关系较为复杂,可以考虑建立域内桥信任模型,通过构建子桥 CA(Subordinate Bridge CA,SBCA)来连接域内其他各个 CA,其路径的处理情况与域间处理的情况相同,相当于在整个模型内部嵌套了一个 SBCA,域内选取 SBCA 作为域内 PCA^[4]。

不同的信任域之间仍然通过桥 CA 建立对等的信任关系,使得来自不同信任域的 CA 通过桥 CA 相互建立起信任关系。任何模型的 PKI 都可以通过桥 CA 连接在一起,实现彼此之间的信任,每一个单独的信任域都可以通过桥 CA 扩展到整个信任模型中^[5]。

2.2 构建域内层次信任模型

基于路径代理的桥信任模型的域内层次信任模型是指桥 CA 连接的信任域内部采用层次模型组织各个 CA。层次模型的最大好处是其自上而下的管理,在域内采用层次信任模型,其信任路径构造与查找都比较简单。在严格的层次信任模型中其信任锚点就是它的根 CA,同时又是模型中域内的 PCA,从信任锚点到任意点路径的存在是唯一的,即任意 CA 到根 CA(同时又是 PCA)的路径是唯一的。PAS 需要收集的路径信息简单且唯一。

在域内层次信任模型中,PAS 需要收集的路径信息简单且唯一,即需要将任意 CA 与 PCA(层次信任模型根 CA)的路径信息收集、存储到 PAS 路径信息数据库中:

正向路径信息: CAX《CAX》CAX《CAX》… CAX_n《CAX_n》CAX_n《PCA》

反向路径信息:PCA \langle CAX $_n\rangle$ CAX $_n\langle$ CAX $_n\rangle$
CAX $_n\cdots$ CAX \langle CAX \rangle CAX \langle CAX \rangle

桥 CA 与根 CA 建立交叉认证,互相颁发交叉证书,因此可以将域内各个 CA 到 PCA 的路径信息扩展到桥 CA,得到如下的路径信息:

正向路径信息:CAX \langle CAX \rangle CAX \langle CAX $\rangle\cdots$ CAX $_n$
 \langle CAX $_n\rangle$ CAX $_n\langle$ PCA \rangle PCA \langle 桥 CA \rangle

反向路径信息:桥 CA \langle PCA \rangle PCA \langle CAX $_n\rangle$ CAX $_n$
 \langle CAX $_n\rangle$ CAX $_n\cdots$ CAX \langle CAX \rangle CAX \langle CAX \rangle

2.3 构建域内网状信任模型

域内网状信任模型是指桥 CA 连接的信任域内部采用网状模型组织各个 CA。网状模型具有高度的灵活性,是构造桥信任模型不可或缺的域内信任模型,但网状模型中的路径构造相对于层次模型复杂得多,任意 CA 间的路径将会有多条,模型中需采用一定的算法解决域内网状信任模型的信任路径构造复杂的问题。PAS 在域内网状信任模型中进行路径构造时,需解决构造的路径无循环路径,以及在已建立信任的 CA 多信任路径之间构造一条最短且可信度最高的路径。

如图 3 所示,假设在一个网状信任模型域内,有 6 个证书权威机构(CA),分别用 $X_1, X_2, X_3, X_4, X_5, X_6$ 表示,其中 X_1 为本域 PCA,各个 CA 间建立了如下的信任关系:

$[X_1, X_2], [X_1, X_5], [X_2, X_3], [X_2, X_6], [X_2, X_5], [X_3, X_4], [X_3, X_6], [X_4, X_5], [X_4, X_6], [X_5, X_6]$,其对应的可信度 $PW(X_m, X_n)$ 分别为 0.7, 0.9, 0.8, 0.9, 0.7, 0.8, 0.7, 0.6, 0.9, 0.8。可得到风险度 $W = \log_x PW(X_m, X_n)$ 分别为 0.51, 0.15, 0.32, 0.15, 0.51, 0.32, 0.51, 0.74, 0.15, 0.32。

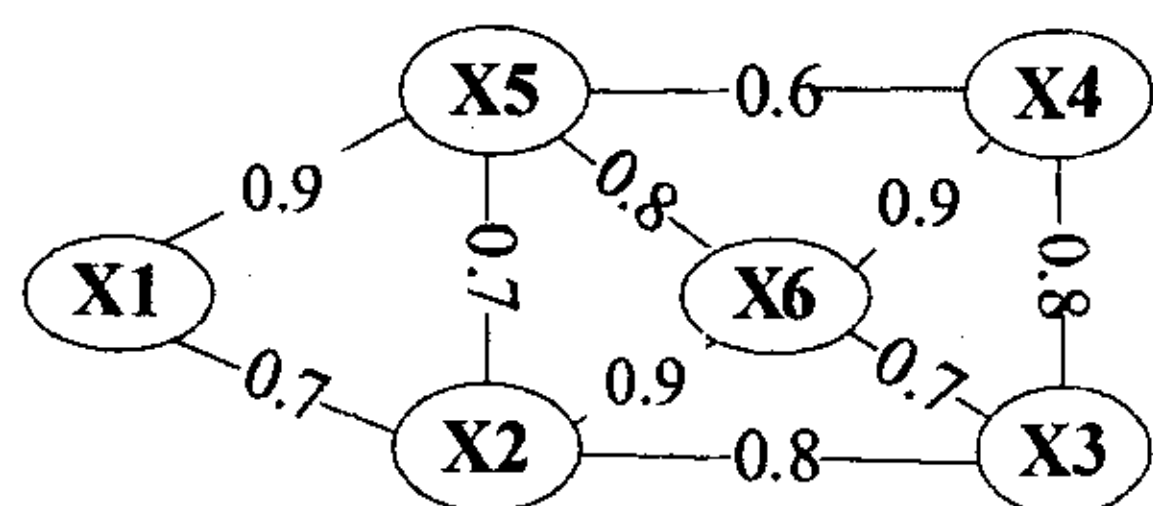


图 3 基本连通图

因此可得如图 4 所示的加权连通图。

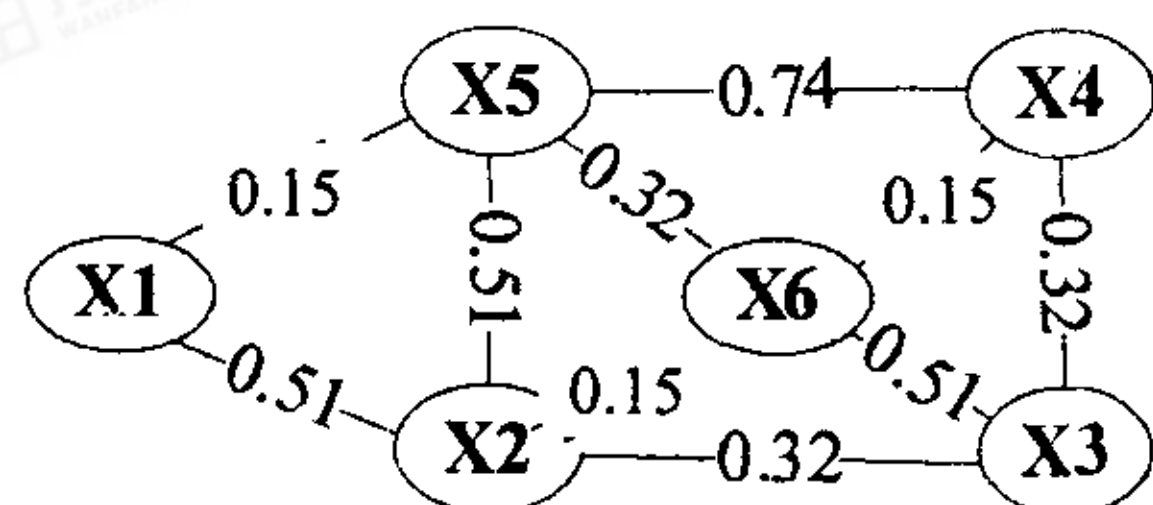


图 4 加权连通图

$G = \langle X, E, W \rangle$, 其中 $X = \{X_1, X_2, X_3, X_4, X_5, X_6\}$; $E = \{[X_1, X_2], [X_1, X_5], [X_2, X_3], [X_2,$

$X_6], [X_2, X_5], [X_3, X_4], [X_3, X_6], [X_4, X_5], [X_4, X_6], [X_5, X_6]\}$

根据上述算法,可得到下面的结点和边序列:

$X_1, X_5, X_6, X_4, X_2, X_3$

$[X_1, X_5], [X_5, X_6], [X_1, X_2], [X_6, X_4], [X_2, X_3]$, 如图 5 所示。

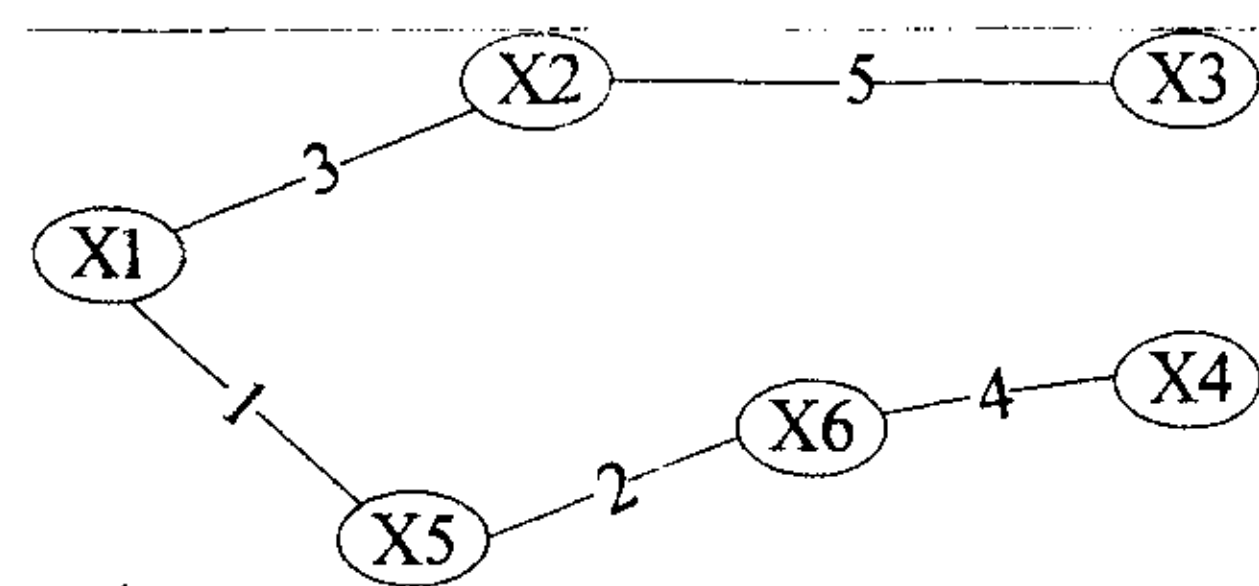


图 5 结点和边图

上述算法说明可以将网状信任模型内多条路径信息简化,收集整理后,构造出域内各个 CA 间的可信任路径,且其路径最短,可信度最高。当 PCA 与桥 CA 交叉认证的时候,可以构造各 CA 与桥 CA 的信任路径。

3 结束语

基于路径代理的桥信任模型继承和保持了传统桥信任模型信任域间高度自主性的特点,保证了信任域间的对等性。同时,该模型比传统桥信任模型构建 PKI 体系有更高的灵活性和可扩展性,添加一个 PKI 体系到桥信任模型中是十分容易的,只需要 PAS 收集和整理域内相关的路径信息就可以了,不会对已有的域产生任何影响。基于路径代理的桥信任模型扩展了域的概念,既可以是传统的域,也可以是那些没有和桥 CA 相连但是相互间已建立起信任关系的 PKI 之间建立的广义的域,解决传统桥信任模型中证书路径的有效发现和确认比较困难的问题。

参考文献:

- [1] PKIX Working Group. Memorandum for multi-domain Public Key Infrastructure (PKI) Interoperability [M]. [s. l.]: PKIX Working Group, 2005.
- [2] PKIX Working Group. Internet X. 509 Public Key Infrastructure: Certification Path Building [M] [s. l.]: PKIX Working Group, 2005.
- [3] 文 彬. PKI 中基于路径代理的桥信任模型的研究与优化 [D]. 乌鲁木齐:新疆大学, 2005.
- [4] 蒋辉柏, 蔡 震, 容晓峰, 等. PKI 中几种信任模型的分析研究[J]. 计算机测量与控制, 2003, 11(3): 201-204.
- [5] 余胜生, 龙 春, 周敬利, 等. 一种 PKI 混合多级信任模型的分析 and 实现[J]. 计算机应用, 2003, 23(10): 18-20.