第 32 卷 第 18 期 计 算 机 工 程 2006 年 9 月
Vol.32 № 18 Computer Engineering September 2006
·安全技术· 文章编号：1000—3428(2006)18—0127—03 文献标识码：A 中图分类号：TP393.08

基于Agent的证书路径构建方法

李卓凡，杨树堂，陆松年
(上海交通大学电子信息与电气工程学院，上海 200030)

摘 要：提出了一种采用 Agent 辅助 PKI 用户获得证书路径的方法，设计了基于 Agent 的 PKI 信任模型及 Agent 内部结构，并提出了 Agent 的证书路径更新算法。理论分析表明，在 5 个节点的混合信任模型及通信网络中各节点只存在一跳的情况下，该方法能提高效率约 2.6 倍。
关键词：公钥基础设施；交叉认证；证书路径

Agent-based Certification Path Building Method

LI Zhuofan, YANG Shutang, LU Songnian
(Department of Information and Electronic Engineering, Shanghai Jiaotong University, Shanghai 200030)

【Abstract】 This paper provides a means to assist the PKI user to build the certification path by using an agent. It also proposes PKI trust model based on agent and agent structure, as well as the updating algorithm of certification path. It has been proved by analysis that under the circumstances of only one hop between each node in communication network and with 5 nodes in hybrid trust model, this method could improve the efficiency to 2.6 times than that of the traditional method.
【Key words】 Public key infrastructure; Cross-certification; Certification path

随着互联网应用的日益增加，特别是电子商务、电子政务的兴起，互联网的安全要求越来越为人们所重视。为了防范安全隐患，许多新的安全技术规范不断涌现，公钥基础设施(Public Key Infrastructure, PKI)便是其一，PKI 是基于公钥加密算法建立的安全基础设施，为用户提供私密性、身份确认、完整性及不可否认性等安全服务。

由于交叉认证操作比较繁琐，影响了 PKI 信任域间的互操作性，阻碍了 PKI 发展及应用。证书路径构建是验证交叉认证的前提，建立过程比较繁琐，影响了用户的效率，所以国内外都对建立证书路径的问题做了很多研究。

在国内现有的证书路径构建方法有基于分区证书路径构造方法[1]，该方法的思想是把各信任域都定义一个分区号，各域内的CA也给予编号，原理等同电话系统分区，构建路径时就采用这些编号来辅助创建。

在国外，一些方法是采用改变证书格式或交叉认证方式来简化建立路径的时间，所提出的方法有采用嵌套证书来代替传统的证书[2]或合并CA的方法来取代交叉认证[3]，从而简化了证书路径。

本文将针对采用 Agent 来加快用户证书路径构建的方法进行研究。

1 基于 Agent 建立证书路径的设计

1.1 基于 Agent 的 PKI 信任模型

本 Agent 设置在各 PKI 中，与信任锚连接，它需要本信任域信任锚 CA 协作来完成证书路径建设。本 Agent 适合层次结构模型、网状模型及混合型模型之间的证书路径建立，具体框图如图 1 所示。图 1 是一个混合信任模型，各个信任锚都拥有一个 Agent。

由于在层次结构模型中只存在单一信任锚，用户证书到信任锚的证书路径只有一条，因此路径建立很容易；另一方面，网状模型不存在惟一信任锚，各 CA 都可充当信任锚，而且用户证书由 CA 直接签发，所以能直接得到用户证书到信任锚的证书路径。

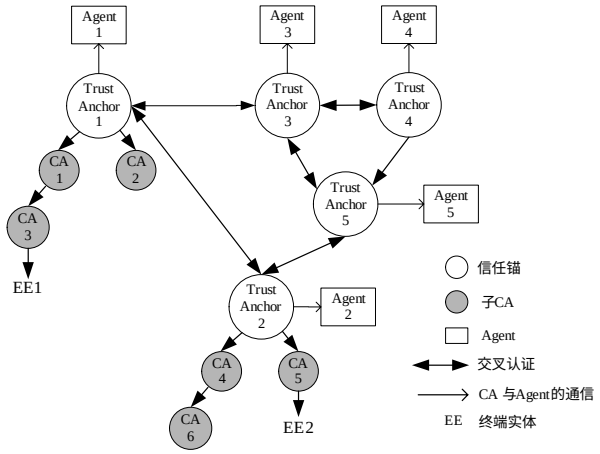

图 1 基于 Agent 的信任模型

综上，不同信任域的两用户间的证书路径实际上是两用户各自的证书到其信任锚的路径加上信任锚间的证书路径[4]。可见建立证书路径的难点在于在两信任锚之间寻找证书路径，所以只需要在各个信任锚中加设Agent就能辅助构建证书路径。Agent的主要工作是寻找证书路径(只针对本信任域已建立交叉认证的信任域的各证书路径)、实时更新路径、路径的优先级排序、管理保存已建立的证书路径，以及为用户提供证书路径。

基金项目：国家“863”计划基金资助重大项目(2002AA145090，2005AA145110)
作者简介：李卓凡(1981—)，男，硕士生，主研方向：PKI 及访问控制；杨树堂，副教授；陆松年，教授
收稿日期：2005-09-04 **E-mail：**cheokfan@sjtu.edu.cn

1.2 Agent 结构设计

Agent 采用图 2 的结构。Agent 共有 3 大模块及 3 个通信接口，其中用户通信接口是用户与 Agent 通信的接口，从证书路径存储模块中读取用户所需的证书路径并返回给用户。

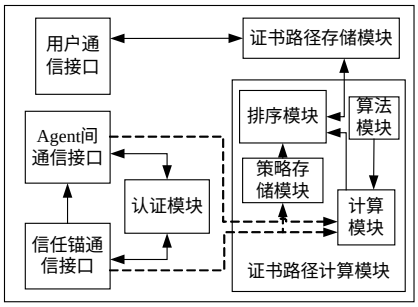

图 2 Agent 结构框图

Agent 间通信接口负责 Agent 之间的通信，当两信任域的信任关系变化时，Agent 通过此接口通知其它 Agent；当接口收到信任关系改变信息时，它会把此信息提交给认证模块，验证其真实性，确认后，该接口再通知证书路径计算模块重新计算各路径。

信任锚通信接口负责处理信任锚与 Agent 的通信，当信任锚与其它信任域取消或建立交叉认证时，信任锚就会通过此接口通知本域 Agent。Agent 收到通知后，先通过认证模块认证此请求，确认后，一方面要求 Agent 间通信接口告知其它 Agent 信任关系变更，另一方面通知证书路径计算模块重新计算路径。若本信任域的策略改变，信任锚也要求 Agent 重排现存的各证书路径优先级，所以本接口的第 2 个任务是接收新策略。

认证模块负责认证 Agent 收到的信息。为了防止其它人冒充本域信任锚或其它 Agent 来攻击本 Agent，令 Agent 胡乱计算路径而影响其效率，所以有必要对各 Agent 或信任锚的信息作认证。因此以上两种信息都要附有他们的签名信息，如此本模块就可以通过认证数字签名来确定信息的真伪。

证书路径计算模块是 Agent 的核心模块，它负责构建证书路径，并通过本域策略来进行路径排序，计算结果保存在证书路径存储模块。本模块包括策略存储模块、算法模块、计算模块及排序模块。其中：

(1)策略存储模块保存本域的策略、接收来自信任锚通信接口发送过来的策略更新以及为排序模块提供策略。

(2)算法模块为计算模块提供路径构建的算法(如 Cygnacom路径构造试探法[5])。

(3)计算模块负责计算所有路径并把计算结果传到排序模块。

(4)排序模块根据策略存储模块提供的策略对来自计算模块的证书路径进行优先级排序，把结果发送到证书路径存储模块保存。

证书路径存储模块保存最新的证书路径，响应来自用户通信接口的路径查询请求并返回结果。

1.3 证书路径更新算法

针对以下两种情况来讨论 Agent 的证书路径更新算法。

(1)两域信任关系变更

当某两信任锚间的交叉认证中止或建立后需要更新 Agent 中已存储的证书路径，这类更新是不常发生的。以图 1 为例，这里定义 Trust Anchor 为 TA、Agent 为 A、更新信息为 Update(TA3, TA4)，它的格式为：TA3 向 TA4 撤销交叉认证，更新算法如下：

1)TA3 向 TA4 撤销交叉认证，则他们的信任关系结束；

2)TA3 要求 A3 发送 Update(TA3, TA4)；TA4 要求 A4 发送 Update(TA3, TA4)；

3)A3 向 A1、A5 发送 Update(TA3, TA4)，A4 向 A5 发送 Update(TA3, TA4)；

4)A5 及 A1 同时判断是否第 1 次收到更新信息，若是，则继续第 5)步，否则跳到第 7)步；

5)A5 向 A2 转发 Update(TA3, TA4)，但不用转发给通知它此次更新的 A3 或 A4，以免出现循环通知，从而影响通信带宽及 Agent 效率，A1 也向 A2 转发 Update(TA3, TA4)，但不用转发给 A3；

6)A5、A1、A2 各自重新计算证书路径并保存；

7)更新结束。

这种更新方法与路由器更新路由表的方法相似，通过只通知相邻的 Agent 就能告知整个 PKI 交叉认证的变更。

(2)本域策略变更

因为每个信任域都各有一套管理策略，该策略影响证书路径优先级的排序，所以当策略变动后，各个已存路径的优先级也需要重新排列。具体步骤如下：

1)信任锚把新的策略及其数字签名发送到信任锚的通信接口；

2)信任锚通信接口把信息交给认证模块作认证；

3)若认证通过，则把新的策略传给策略存储模块保存，同时通知排序模块对已存的证书路径重新排序，否则不作任何改变。

1.4 用户与 Agent 通信设计

若采用本方法获得证书路径，首先要知道 Agent 的位置，所以必需在用户的证书中加入 AgentLocation 扩展项。它是告知用户本域 Agent 的位置，其值可以是 URL 或 URI。

用户得知 Agent 所在后，就可以向它查询证书路径，过程如下：

(1)用户向用户通信接口发送查询证书路径请求，此请求内容包括目标证书的序列号，以及其信任锚的一些资料；

(2)用户通信接口分析此请求并向证书路径存储模块查询证书路径；

(3)证书路径存储模块把结果返回给用户通信接口；

(4)用户通信接口把结果打包成返回信息发给用户。返回信息包括用户证书到信任锚的证书路径、目标证书到其信任锚的证书路径和两信任锚之间的多条证书路径(已排序的)。

用户接收到返回信息后，即可按需要来选择采用哪条路径并进行有效性验证。

2 效率分析

2.1 理论分析

以下就用户采用 Cygnacom 路径构造试探法与采用本文提出的基于 Agent 的路径构造法做效率上的对比分析。

Cygnacom 路径构造试探法是美国联邦政府 PKI 体系中构造路径时采用试探法的一个例子。构造过程中用户需要从目标证书开始沿正向不断查找连接本信任锚到目标证书信任锚的所有中间 CA 交叉认证证书，试图找出连接两信任锚的路径；当遇到死端或路由回绕时，则原路返回到一个已知点开始继续构造路径。

假设通信网络中各节点间只存在一跳，一条信息从发送端到达目的端需 10ms，出现路由回绕时，从已收到的路径信

息中找出另一条路径需 20ms。针对图 1 的 PKI 信任模型，现在需要寻找 EE1 到 EE2 的证书路径，若采用 Cygnacom 的方法，具体步骤如图 3 所示。

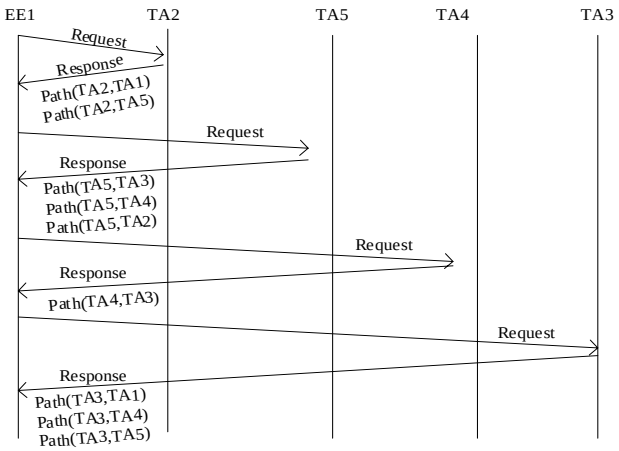

图 3 路径构造时序

说明：

(1)查询路径请求信息从原端 EE1 到达目的端 TA2 需 10ms；

(2)从 TA2 返回路径 Path(TA2,TA1)及 Path(TA2,TA5)到 EE1 需 10ms；

(3)选择 Path(TA2,TA5)，EE1 向 TA5 查询路径需 10ms；

(4)从 TA5 返回路径 Path(TA5,TA2)、Path(TA5,TA3)及 Path(TA5,TA4)到 EE1 需 10ms；

(5)选择 Path(TA5,TA4)，EE1 向 TA4 查询路径，需 10ms；

(6)从 TA4 返回路径 Path(TA4,TA3)到 EE1 需 10ms；

(7)选择 Path(TA4,TA3)，EE1 向 TA3 查询路径需 10ms；

(8)从 TA3 返回路径 Path(TA3,TA1)、Path(TA3,TA4)及 Path(TA3,TA5)到 EE1 需 10ms；

(9)若选择 Path(TA3,TA5)，则出现路由回绕，需要原路返回到 TA3 查找另一条路径，需 20ms；

(10)最后选择 Path(TA3,TA1)，因此最终路径为 Path(TA2,TA5) ＋ Path(TA5,TA4) ＋ Path(TA4,TA3) ＋ Path(TA3,TA1)，建立路径共需 10ms×8＋20ms＝100ms。

与上面讨论的步骤相似，还有以下 4 种可能情况：

(1)完成上述(1)～(4)步后采用路径 Path(TA5,TA3)＋Path(TA3,TA4)，此时出现死端，需要原路返回到 TA3 选择另一条路径 Path(TA3,TA1)，得到最终路径为 Path(TA2,TA5)＋Path(TA5,TA3)＋Path(TA3,TA1)，需 100ms；

(2)正常情况取得最终路径 Path(TA2,TA5) ＋Path(TA5,TA4)＋Path(TA4,TA3)＋Path(TA3,TA1)，需 80ms；

(3)正常情况取得最终路径 Path(TA2,TA5) ＋Path(TA5,TA3)＋Path(TA3,TA1)，需 60ms；

(4)正常情况取得最终路径 Path(TA2,TA1)，需 20ms。

从以上分析可知查找时间在 20ms～100ms 之间，找到一条证书路径所需平均时间为 72ms。

采用本方法只需简单地处理一个请求信息及一个响应信息即可得到多条证书路径，耗时 20ms，效率提高了 2.6 倍。信任模型中中间节点数增加，出现死端和路由回绕机会随之提高，本方法的效率也会更加提高。

综上所述，从用户的角度看，采用 Agent 方法可以省略很多复杂操作，并可以大大提高工作效率，从而提高交叉认证效率。

2.2 与现有方法进行比对分析

国内也有采用移动Agent来实现证书链搜索的方法[6]，用户建立路径时，把一些相关参数提交给代理层，它会创建移动Agent实例，根据一定的分布点地址，把执行这次搜索任务的Agent实例在相关联实体间散布，搜索有效路径。可见，路径没有预先建立好，而是用户需要构建路径时才要求Agent层完成建立，同时需要在网络上向其他节点Agent层传输当前已搜索到的路径，通过多次传输完成路径搜索。所以随着当前路径长度的增长，向下一个Agent层传输的路径信息量也不断增加；另外，Agent层间没有身份认证，可能会出现假冒的情况。

本方法中，证书路径已事先通过 Agent 建好，而且因为 Agent 实时更新，所有路径都是有效的，用户只需通过一个请求信息就能即时得到证书路径，所以查找速度比文献[6]的方法快；Agent 间通信信息量少，可以减少网络流量；同时 Agent 间通信是通过数字签名作身份认证，保证 Agent 可靠，因此本方法在安全性上较完善。

3 结论

由于构建证书路径的复杂、繁琐，大大影响信任域间的互操作能力，阻碍了 PKI 发展。本文提出的 Agent 框架简单明确，在不影响各 PKI 信任模型下，只需在各信任锚中设立 Agent 就可以辅助用户建立证书路径。当两信任域间的信任关系出现变化时，各 Agent 能实时更新证书路径，所以 Agent 保存的路径都是有效的。

从用户角度来看，只要访问 Agent 就能获得证书路径。当中请求及处理响应信息等操作简单，不用耗费太多资源，即可以提高用户效率及交叉认证效率。

参考文献

1 刘保言, 陈泳章. 公钥基础设施的分区证书路径构造方法的研究[J]. 计算机工程与应用, 2004, 40(22).

2 Levi A, Caglayan M U. Verification of Classical Certificates via Nested Certificates and Nested Certificate Paths[C]. Proceedings of the 8th International Conference on Computer Communications and Networks, 1999-10-11: 242-247.

3 Koga S, Sakurai K. A Merging Method of Certification Authorities Without Using Cross-certifications[C]. Proc. of the 18th International Conference on Advanced Information Networking and Applications, 2004: 174-177.

4 黄 璐, 魏海平. 一种基于垂直 PKI 结构的证书链构建[J]. 计算机工程, 2004, 30(6).

5 Nash A. 张玉清译. 公钥基础设施(PKI)实现和管理电子安全[M]. 北京: 清华大学出版社, 2002.

6 齐竞艳, 黄 皓, 崔 伟. 用移动 Agent 实现的分布式证书链的搜索[J]. 计算机工程, 2004, 30(22): 119-121.