

文章编号:1001-9081(2006)10-2315-03

## 一种对等信任模型的研究与实现

毕方明, 张 虹, 闫大顺

(中国矿业大学 计算机科学与技术学院, 江苏 徐州 221008)

(bfm@cumt.edu.cn)

**摘 要:** 要证明公开密钥的真实性, 分布广泛的 PKI 需要处理数量巨大的关于数字证书的询问。现有的信任模型, 不能高效地解决大量节点的可信度计算问题。据此, 以 Chord 协议和数字证书为基础, 研究了一种新的对等网络环境下的信任模型, 给出该模型的分布式实现方法, 并分析了该模型在可信度计算的效率。

**关键词:** 对等网络; 公开密钥基础设施; 信任

**中图分类号:** TP393.08 **文献标识码:** A

## Research and realization of one trust model based on Peer to Peer

BI Fang-ming, ZHANG Hong, Yan Da-shun

(Department of Computer Science and Technology, China University of Mining and Technology, Xuzhou Jiangsu 221008, China)

**Abstract:** In order to verify the authenticity of public keys, a widespread PKI has to deal with a large number of queries about digital certificates. Current trust model could not deal with the trust computation efficiently. a Peer-to-Peer trust model was presented in this paper, which was based on chord protocol and digital certificate. A distributed implementation method was given, and the efficiency on trust computation was also analyzed.

**Key words:** Peer to Peer; public key infrastructure; trust

## 0 引言

随着 Internet 的发展, Napster、Gnutella 等对等网络 (Peer to Peer, P2P) 共享软件迅速传播, 对等网络越来越受到人们的关注。它是一种分布式网络, 网络的参与者共享他们所拥有的一部分资源, 这些共享资源需要由网络提供服务和内容, 无需经过中间实体, 就能被其他对等节点直接访问, 数据在对等节点之间直接传递。在此网络中的参与者既是资源提供者, 又是资源获取者。而不象以往的客户/服务器模式那样把数据存放在集中的服务器上。并且与传统的分布式系统相比, P2P 技术也具有无可比拟的优势, 具有广阔的应用前景。对等网络具有可扩展性好、非中心化、健壮性、及负载均衡等特点。但仍然缺乏建立节点之间的对等信任机制, 因此, 有必要建立一种分布式信任机制, 有效地提高系统整体的可用性。

PKI (Public Key Infrastructure) 对建立节点之间的信任, 提供了强有力的保证。PKI 是公开密钥基础设施, 采用证书管理公钥, 把用户的公钥和用户的其他标识信息 (如名称、角色、E-mail 等) 捆绑在一起, 在 Internet 上验证用户的身份。通过把要传输的数字信息进行加密和签名, 保证信息传输的机密性、真实性、完整性和不可否认性, 从而保证信息的安全传输。信任公钥加密方法的先决条件是关于被用公钥真实性的确实证据。即 PKI 要确认声称拥有公共密钥的人的真正身份, 与数字证书中的公钥之间捆绑的真实性。它是分布式系统和电子商务的一种重要的安全技术。而一个广泛的 PKI 依

赖于一个能有效、可信的存储和检索证书的机制。本文的目的就是研究一种基于完全分布式结构化拓扑网络, 即以 Chord 协议为基础, 作为证书和推荐的分布式数据库的 PKI, 来处理对等网络中对等实体之间的信任关系, 帮助实体进行信任抉择。与中央目录相比较, 对等网络独立于中央管理机制, 与因特网的自治特性非常相符。

## 1 Chord 协议

通常, 一个 PKI 用集中目录服务器来检索和存取证书。本文描述了一个基于 Chord 协议的对等网络, 作为证书的分布式数据库的方法。以 Chord 协议为基础的网络是由联机系统的节点组成, 节点提供自己的资源 (比如: 文件) 给其他节点, 并利用其他节点的资源。Chord 协议是由 MIT 提出的一种分布式查找协议, 采用了相容哈希的一种变体来为节点分配关键字。在 Chord 协议中, 实现了这样一种操作: 给定一个关键字 (key), 将 key 映射到某个节点。

与非结构化的 P2P 协议如 Gnutella 相比, 这使得结构化的 P2P 协议能实现一个更有效的查找算法。设节点标识 ID 的二进制位数为  $m$ , 每个节点维持着最多  $m$  条记录, 该记录表被称为 finger 表。该协议中, 每个节点和数据都赋予一个特定名字空间中唯一的一个  $m$  bit 的标识号 ID, 所有可能的  $2^m$  个 ID 号构成一个一维环。在模  $2^m$  算术运算辅助下, 标识符在标识符环上排序。为实现高效路由, 每个节点的本地仅仅维护环中其后第  $2^0, 2^1, \dots, 2^{m-1}$  位共计  $m$  ( $m < b$ ) 个虚拟点的

收稿日期: 2006-04-29; 修订日期: 2006-06-14 基金项目: 中国矿业大学科技基金资助项目 (2005A045; F200405)

作者简介: 毕方明 (1974-), 男, 江苏徐州人, 讲师, 博士研究生, 主要研究方向: 信息安全和 GIS; 张虹 (1942-), 女, 山东济南人, 教授, 博士生导师, 主要研究方向: 图像处理和信息安全等; 闫大顺 (1974-), 男, 河北邯郸人, 讲师, 硕士, 主要研究方向: 信息安全和异常处理等。

后继节点的位置信息。这样,每个节点只需要维护其他  $O(\log N)$  个节点的信息,同样,每次查找只需要  $O(\log N)$  条消息。当节点加入或者离开网络时,Chord 需要更新路由信息,每次加入或者离开需要传递  $O(\log N)$  条消息。Chord 如果给对等网络应用的每个数据都分配一个 key,那么对等网络中的数据查找问题就可以用 Chord 很容易地解决了。

如下的映射规则具有特殊的重要性,每个键(Key)被分配给现有的第一个标识符大于或等于键的标识符的节点。这个节点被称为键 K 的后继节点,用  $\text{Successor}(k)$  表示。例如,在图 1 中,具有标识符 53 的键被分配给标识符为 56 的节点。因为,没有节点的标识符在 53 到 56 之间。如有一个标识符为 55 的节点存在,这个键就定位到那里。

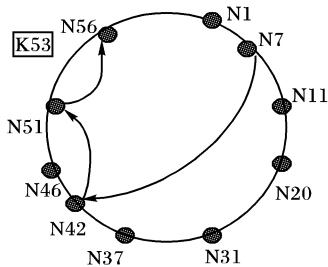


图 1 Chord 环

根据 Chord 环的关键值分配方法,某个关键字只能出现在相应的后继节点上,这个后继节点是唯一的。因此,键查找的目的是确定节点的标识符和 IP 地址。每个节点拥有一个  $m$  条的路由表,即 finger 表。存储在 finger 表中信息的特殊结构,是用来进行一个有效的关键字查询。图 1 展示了一个标识符长度  $m=6$  的 Chord 环,那么每一个节点的 finger 表存储 6 个条目。这个 Chord 环为  $2^6=64$  个节点提供标识符 ID。假设节点 7 启动了一个查询,要查询具有标识符 ID 为 53 的关键字,过程如下:在节点 7 的 finger 表中,53 之前最大的节点的 ID 是 42,那么节点 7 将让这个节点(42)来回答这个查询。依次,具有 ID 为 42 的节点将在它自己的 finger 表中查找小于 53 的最大 ID,结果在指针号为 4 的指向了 ID 为 51 的节点。这个节点(51)发现它的直接后继节点 ID 为 56,是在所要查询键 53 之后。最后,查询结果“节点 56”被返回到节点 7。

## 2 信任模型

这部分描述了一些过程和消息,它们形成了基于对等网络的 PKI 的协议。这部分的目的是定义相应的过程,它能够让一个节点去检查一些推荐信任的等级,最终确定一个公钥和给定身份之间的绑定的真实性。

### 2.1 信任关系的分类

实体之间的信任关系可以分为直接信任和推荐信任两类。

**定义 1** 直接信任是指两个实体之间曾经有过直接的交易,它们之间建立了一种直接信任关系,信任值来源于根据双方的交易情况得出的直接经验。

**定义 2** 推荐信任是指两个实体之间没有进行过直接的交易,而是根据其他实体的推荐建立的一种信任关系,它们之间的信任值是根据其他实体的评估得出的结果。

在公钥基础设施的内容中,当做出这样的假定,即第二个

实体将完全按照第一个实体期望的那样表现时,就可以说第一个实体能相信第二个实体。而以 Chord 协议为基础的 PKI 实现了一个以用户为中心的信任模型,每个节点直接并且完全负责地决定相信哪个其他节点。

### 2.2 两类消息的引入

根据如上的信任关系,引入两类公共消息,它们代表以 Chord 协议为基础的 PKI 节点之间进行交流的信息,假定每个节点都能产生一致的公共消息。在 Chord 中,这些消息与值(values)(e.g. files)相应。这些值都有一个键(key(e.g. filename)),并被依次哈希到相应的 Chord 标志符。

**定义 3** 在这个基于对等网络系统中,有两类在 PKI 中数字签名的公共消息。

#### 1) 证书消息类型

语法:  $\text{Cert}(X, \text{PX}, Y, \text{PY})$

语义: 这个消息描述了由节点 X 进行签名并发布的数字证书。该证书证明了节点 Y(证书的主体)是与公钥 PY 绑定的。假如节点 X 是公钥 PX 可信的拥有者,那么这个消息的数字签名是有效的,即数字签名能够通过公钥 PX 进行验证。

#### 2) 推荐消息类型

语法:  $\text{Rec}(X, \text{PX}, Y, i)$

语义: 这个消息类型用来为节点 Y(主体)传递一个  $i$  等级的推荐。它是由节点 X 进行签名并发布的推荐。假如节点 X 是公钥 PX 可信的拥有者,那么这个消息的数字签名是有效的,即数字签名能够通过公钥 PX 进行验证。一个推荐消息有一定的等级  $i$ 。这个等级的目的是将在后面的描述里阐述。

在基于 Chord 协议的 PKI 中,节点使用信任声明去确定其他节点的权利。每个节点产生这些声明是按照这个节点对其他节点的信任,用来表示其他节点对这个节点访问的特权。信任声明被放在节点的 privateView 里。如果一个节点乐于接受由节 X 发行的证书,它把  $\text{Trust}(X, 1)$  声明安置在它的 privateView 里。注意,要选择合适的信任声明需考虑如下的五条规则:

1)  $\text{Trust}(X, 1)$  表示在它的 privateView 里拥有这条声明的节点,将承认由节点 X 发布的证书信息,但不是承认由节点 X 发布的推荐信息。

2)  $\text{Trust}(X, i)$  当  $i > 1$  时,表示在它的 privateView 里拥有这条声明的节点,将在等级  $i$  上承认由节点 X 发布的推荐信息。

3) 一条信任声明  $\text{Trust}(X, i)$  中,隐含着接受所有的信任声明  $\text{Trust}(X, j)$  (其中,  $j < i$ ),尤其隐含  $\text{Trust}(X, 1)$ 。

4) 有一条推荐信息  $\text{Rec}(X, \text{PX}, Y, i)$ ,如果这个节点拥有声明  $\text{Trust}(X, j)$  ( $j > i$ ),并且推荐信息的数字签名是有效的,那么,这条推荐信息就被当作类似声明  $\text{Trust}(Y, i)$ 。

5) 有一条推荐信息  $\text{Rec}(X, \text{PX}, Y, i)$  ( $i > 1$ ),隐含所有的  $j < i$  的推荐信息  $\text{Rec}(X, \text{PX}, Y, j)$ 。

**规则 1** 把信任模型和证书验证的处理联系了起来。在一个特定节点上,要承认另一个节点发布的证书,第 1 等级的信任是必须的。推荐信息是在其他节点上建立新的信任的基

础,他们被用来两个节点的通信,其中有一个确定节点是值得信任的。

### 2.3 确定信任等级的过程

每一个节点能够表示它个体对其他节点的信任关系和它的信任锚。这样,检查公钥真实性的过程的基础就有了。

这个过程确认当前节点是否对另外一个节点有一个明确的信任等级。这个结果是基于上面描述的信任模型,在图 2 中定义。过程的变量是节点的名字和最小的信任等级  $tlevel$ 。它将检验,是否当前节点在至少  $tlevel$  上信任节点  $name$ ,即  $Trust(name, tlevel)$  是否被包含在  $privateView$  中,或者,能够按照上面提到的信任模型中的规则 4 推得。

```

if_trusted( name, tlevel)
if ( if_trust_contained( name, tlevel))
    // if adequate Trust is contained in privateView
    return true;
else
    ...
    rec[ ] = n.retrieve( k);
    for i = 0 till length_of( cert[ ] )
        encPubMsg = get_encPubMsg( rec[ i] );
        ...
        rec_level = get_rec_level( pubMsg );
        // recommendation verification
        if ( rec_level > = tlevel )
            if ( if_trusted( issuer, issuer_pkey ) )
                if ( if_trusted( issuer, tlevel + 1 ) )
                    return true;
        // if Aut is not in privateView and not deriveable
    return false;

```

这个过程的第一步是在当前节点的  $privateView$  中查找合适的信任声明。如果发现这个节点  $name$  的一个信任声明,它的等级等于或大于需要的  $tlevel$ ,那么,过程的结果为  $true$ 。这意味着,信任节点  $name$  具有足够的信任等级让当前节点直接信任。

如果没有直接的信任,节点有可能通过一个推荐信息(规则 4)来建立对节点  $name$  的信任。出于这个目的,过程  $n.retrieve(k)$  发现并传递所有的具有索引键为  $k = h(h(name))$  的消息。如果没有这样的消息被发现,这个检索过程将交付一个空数组。在这种情况下,  $if\_trusted$  交付结果  $false$ 。如果有这样的消息被发现,这个过程就开始以一定的顺序,来验证它们。另外,发布者的名称  $issuer$  和公钥  $issuer\_pkey$ ,以及推荐的等级  $rec\_level$  也都被提取出来。

最后,要进行三个检验,实现信任模型中描述的第 2~5 条规则。

1) 如果当前的推荐等级  $rec\_level$  是小于所需的信任等级  $tlevel$ ,当前推荐不被使用,然后检查下一条推荐。

2) 推荐信息的数字签名必须是有效的。要证实  $issuer$  和  $issuer\_pkey$  之间绑定的真实性。

3) 过程被递归地调用来证实,当前节点是否在最小  $tlevel + 1$  的登记上信任推荐信息的发布者。对一个推荐的发布者的信任必须要超过对节点  $name$  所需的信任。

只要对一条推荐信息这三个实验都成功地通过,过程  $if\_trusted$  的回答是  $true$ 。如果所有检索到的推荐信息都没有通

过这些检验,结果就是  $false$ 。

## 3 基于 Chord 协议的 PKI 的优点

1) 操作组织的独立性:与集中目录的公共信息发布相比,基于 Chord 协议的 PKI 本质上是独立于一个操作组织的。这正好与网络的自我管理特性相匹配。一个应用于 Internet 的广泛的 PKI 系统为了能够被更多的 Internet 用户接受,必须满足独立性的需求。

2) 负载均衡:理想情况下,一个 hash 函数均匀地分发它的结果。那么消息就能够均匀地在对等网络的节点上传播,因为它们的寻址和路由是基于一个 hash 函数。这个特性为消息发布、检索、存储实现了负载平衡。

3) 可扩展性:消息的检索或发布花费随着整体节点的数量  $N$  以  $\log(N)$  增长。那么具有许多消息和节点的大系统就具有可行性。

4) 可用性和自我管理、容错性:Chord 功能可以自动调整  $finger$  表适应新加入的节点和失败的节点。这种分布的方式提供了内在的错误抵抗的优点,而不是依靠与一个单一的目录或数据库系统的特定功能。

## 4 结语

如上的过程实现了一个分布式的 PKI,这个 PKI 基于一个 Chord 协议的网络,这个网络的有效性是基于证书和推荐的发布、检索的机制。在一个具有  $N$  个节点的网络中,每一个节点仅维护  $\log(N)$  个其他节点的路由信息。消息发布和检索任务通过少于  $\log(N)$  个其他节点就实现。并且具有一个重要的特性,就是自治的特性,这个特性与 Internet 的自我管理范例很好匹配,会促进 PKI 技术获得更高的认可。可能的应用案例是私有的和专业的 Internet 应用,比如确保电子邮件安全,及在线商场(eBay)的用户鉴定。

### 参考文献:

- [1] ABERER K, DATTA A, HAUSWIRTH M. A decentralized public key infrastructure for customer-to-customer ecommerce [J]. International Journal of Business Process Integration and Management, 2004, 10(10).
- [2] ADAMS C, LLOYD S. Understanding PKI [M]. Boston: Addison-Wesley, 2003.
- [3] KARGER D, LEHMAN E, LEIGHTON T, *et al.* Distributed Caching Protocols for Relieving Hot Spots on the World Wide Web [A]. In Proceedings of the 29<sup>th</sup> Annual ACM Symposium on Theory of Computing (STOC 97) [C]. EL PASO, May 1997. 654-663.
- [4] KOHLHAS R, MAURER U. Reasoning about Public-key Certification-on Bindings Between Entities and Public Keys [A]. In Proceedings of Financial Cryptography 99, Lecture Notes in Computer Science [C]. Berlin: Springer, 1999. 86.
- [5] MAURER U. Modelling a public-key infrastructure [A]. In Proceedings of the 1996 European Symposium on Research in Computer Security (ESORICS96), Lecture Notes in Computer Science [C]. Berlin: Springer, 1996, 1146. 325-350.
- [6] BISHOP M. Computer Security: Art and Science [M]. 北京:清华大学出版社, 2004, 5.
- [7] PKI 基础. 中国金融认证中心(CFCA) [EB/OL], <http://www.cfca.com.cn/zhishi/pki-1.htm>, 2006.