P2P – PKI 中节点信任模型研究

Research on Peers Trust Models in P2P – PKI

陶世忠 史清华 王亚敏 (山东大学计算机科学与技术学院 山东 济南 250061)

摘要:近年来对等网络(Peer – Peer)架构得到迅速发展,针对这种架构提出了 P2P – PKI 的安全机制模型。P2P – PKI 实现了高效的搜索以及证书和信任推荐的传输,它基于一个可升级的 Chord 查找协议,并且网络中的节点能够依据给出的数学模型和算法计算"建议"值,从而确定节点间的信任关系。依据这个"建议"值,本地节点选择与信任度高的其他节点进行通信,更好地保证了网络的安全性和避免恶意攻击。

关键词:P2P – PKI Chord 信任模型

1 引言

公开密钥基础设施 PKI(Public – Key – Instucture)是一个用公钥概念与技术来实施和提供安全服务的具有普适性的安全基础设施。PKI 提供了包括身份证书、密钥管理、机密性、完整性、身份认证和数字签名等一系列的安全服务。而近年来迅速发展的 P2P(Peer – Peer)是指由物理上分散的主机不经过服务器等中继设备而实现节点之间资源共享(包括文件、存储空间及计算能力等等)的技术模式。与集中式地址目录的方法比较,P2P 网络在差错容忍、负载均衡和自适应管理等方面有着本质上的优点。P2P – PKI 模型是由德国雷根斯堡大学 Thomas Woelfl 在 2005 年提出的。顾名思义,这是一个建立在 P2P 网络上的公开密钥基础设施,它的一个至关重要的好处就是运行机制上的独立性。本文在介绍 P2P – PKI 模型的基础上,提出了两个节点之间如何建立可靠的信任关系,这种信任关系是由节点给出的"建议"值来确定的,一个"建议"值表示了一个节点拥有另一个节点的信任级别。如果一个指定节点的信任值小于我们给定的最小信任值极限,则该节点就是可信的。

2 P2P – PKI 模型介绍

2.1 Chord 协议

Chord 协议在 2001 年由麻省理工学院提出,主要用于解决如何在 P2P 网络中找到存有特定数据的节点。Chord 算法中每个节点需要存储 m 个其它节点的信息,这些信息的集合被称为查询表(Finger Table),表格中的节点不再是直接相邻的节点,它们的间距(ID 间隔)将成 2i 的关系排列(i 表示查询表中的数组下标)。在查询的过程中,查询节点将请求发送到与键值最接近的节点上。收到查询请求的节点如果发现自身存储了被查询的信息,可以直接回应查询节点;如果被查询的信息不在本地,就根据查询表将请求进一步转发到与键值最接近的节点上,直到找到相应的节点为止。

2.2 公共消息(Public messages)

P2P – PKI 模型中定义了三种公共消息:

(1) 证书消息类型。Cert(X, PX, Y, PY),由 X 签名颁发的证书,用于证明节点 Y 和公钥 PY 之间的绑定关系。该证书有效性可以通过公钥 PX 来证明。

(2) 推荐消息类型。Rec(X, PX, Y, i),用于传送对于节点 Y 的推荐,推荐值为 i,该消息同样由节点 X 签名颁发,有效性可以通过公钥 PX 来证明。

(3) 密文形式。MessageToken(encPubMsg, msgKey):该消息包含了被加密的 PublicMessge(加密密钥为 C)和索引密钥 Key。注意,加密密钥 C 和索引密钥 K 是不同的,其中 C = h(name ∪ pkey),K = h(C)。

2.3 私有声明(Private Statements)

私有声明用来描述一个节点对于 P2P – PKI 模型中其他节点的信任,共有两种类型的私有声明:

(1) 真实性声明。Aut(X, PX),用于表示本地节点信任节点 X 为公钥 PX 的真实所有者。

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

(2) 信任声明。Trust(X, i),表示本地节点根据自身安全的需要,确定对节点 X 的信任值为 i。

2.4 数据存储与访问

每个节点具有两个集合:PrivateView 集合,包括 Private Statements 信息,不允许其他节点访问;PublicView 集合,包括 MessageToken 等,反映了一个节点共享的存储空间。每个节点具有以下四个基本功能:n. get_message(msgKey);n. set_message(msgToken);is_trust_contained(name,tlevel);is_authenticity_contained(name,pkey)。

3 节点信任值的计算

3.1 信任值计算遵循的原则

对于上面提到的 Trust(X, i) 与 Rec(X, PX, Y, i) 中 i 值的计算是本节我们要讨论的主要内容。基于 Dempster – Shafer 原理(简称 D – S 原理)利用下面给出的两条基本原则来求得信任值。

(1) 信任传递原则。如果两个对等节点是间接连通的,则它们之间的信任是由路径中的其他节点传递得到的。在图 1 中,节点 X 对节点 Y 的信任值大小为 S(X,Y),节点 Y 对节点 Z 的信任值大小为 S(Y,Z),由此可以推断出 X 和 Z 之间的信任关系值为 SY(X,Z) = S(X,Y)S(Y,Z)。

这里 $S_Y(X,Z) \leq \min\{S(X,Y), S(Y,Z)\}$。

(2) 信任聚合原则。如图 2 所示,若对等节点 X 到 Y 之间有 n 条不重合的路径,这 n 条路径分别给出了它们的信任值 $S_1(X,Y)$、$S_2(X,Y)$、…$S_n(X,Y)$,由此可以推断 X 和 Y 之间的信任关系值 $S(X,Y) = S_1(X,Y) \oplus S_2(X,Y) \cdots \oplus S_n(X,Y)$。

这里 $S(X,Y) \geq \max\{S_1(X,Y), S_2(X,Y), \cdots S_n(X,Y)\}$。

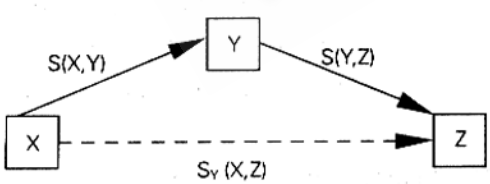

图 1 信任的传递

在实际问题中,人们对命题 A 的相信程度并不能反映出对 A ~ 的相信程度,即 P(A) + P(A ~) ≤ 1。根据这一特性,D – S 原理定义了证据区间的概念,即[Spt(A), Pls(A)],信任(Support)函数 Spt(A) 为证据区间的下限,它表示对命题支持程度的下限估计(悲观估计);似真度(Plausibility)函数 Pls(A) 为该区间的上限,它表示对命题支持程度的上限估计(乐观估计)。为保证足够的安全和便于计算,我们规定节点的综合信任值等于该区间的下限信任值。

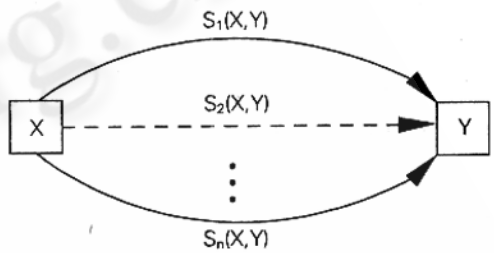

图 2 信任的聚合

(1) 定义 1。信任辨识框架 Θ 为集合{T(信任), D(不信任)},Θ 的幂集合 2^Θ 为{Φ,{T},{D},{T, D}}。

(2) 定义 2。基本概率分配 m 为幂集合 2^Θ 的函数,$m: 2^\Theta \to [0,1]$,并满足:① $m(\Phi) = 0$;② $\sum_{B \subseteq 2^\Theta} m(A) = m(\{T\}) + m(\{D\}) + m(\{T,D\}) = 1$,而 m({T, D}) 的直观含义为"不知道"如何处理。

(3) 定义 3。称映射 $Spt(A): 2^\Theta \to [0,1]$ 为信任函数,它是包含在 A 中的所有子集的基本概率分配之和,即 $Spt(A) = \sum_{B \subseteq A} m(B)$,$A \subseteq 2^\Theta$,$B \subseteq 2^\Theta$,可以推出 $Spt(\{T\}) = \sum_{B \subseteq \{T\}} m(B) = m(\{T\})$。Spt({T}) 的含义为 X 认可 Y 的程度,即是我们要求的下限值。

3.2 传递后信任值的计算

下面我们来看一下信任值进行传递的计算方法。如图 1 所示,节点 X 对 Y 的信任值为 SptXY({T}),节点 Y 对 Z 的信任值为 $Spt_{YZ}(\{T\})$,需要导出 X 对 Z 的 $Spt_{XZ}(\{T\})$,根据信任传递衰减原则可以定义:

$$Spt_{XZ}(\{T\}) = \sum_{B \subseteq \{T\}} m_{XZ}(B) = \sum_{B \subseteq \{T\}} (m_{XY}(B) \times m_{YZ}(B))$$

$$= \sum_{B \subseteq \{T\}} (m_{XY}(B) \times \sum_{B \subseteq \{T\}} m_{YZ}(B)$$

$$= Spt_{XY}(\{T\}) \times Spt_{YZ}(\{T\})$$

显然,$Spt_{XZ}(\{T\}) \leq \min\{Spt_{XY}(\{T\}), Spt_{YZ}(\{T\})\}$

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

3.3 合成后信任值的计算

如图 2 所示，在 X 与 Y 之间存在 n 条建议路径，这就存在把这些不同的信任值进行合成的问题。在进行信任值的合成时，建议路径数越多，得出的合成信任值的可靠性就越高。

设 $m_1, m_2, \cdots, m_n$ 为 2^Θ 上的 n 个基本概率分配（m_i 为 m_{XYi} 的简写），它们的正交和表示为 $m_{XY} = m_1 \oplus m_2 \oplus \cdots \oplus m_n$，且定义

$$\begin{cases} m(\Phi) = 0 \\ m(A) = \frac{1}{K} \sum_{\cap A_i = A \, 1 \le i \le n} \prod m_i(A_i) \end{cases}$$

$A \subseteq 2^\Theta, A_i \subseteq 2^\Theta, A \neq \Phi$。

其中 $K = \sum_{\cap A_i \neq \Phi \, 1 \le i \le n} \prod m_i(A_i)$，参数 K 起着将合成后的基本概率分配归一化的作用。当证据之间存在冲突（即证据支持的假设有不相交的部分）时，冲突部分的基本概率分配设置为零，而剩下部分的基本概率分配则通过因子 K^{-1} 归一化。

例如，当 $n = 2$，即 $m = m_1 \oplus m_2$，可以推出：

$$K = \sum_{A \cap B \neq \varphi} m_1(A) m_2(B) = m_1(\{T\}) \times m_2(\{T\}) + m_1(\{T\}) \times m_2(\{T,D\}) + m_1(\{D\}) \times m_2(\{D\}) + m_1(\{D\}) \times m_2(\{T,D\}) + m_1(\{T,D\}) \times m_2(\{T\}) + m_1(\{T,D\}) \times m_2(\{D\}) + m_1(\{T,D\}) \times m_2(\{T,D\})$$

$$Spt_{XY}(\{T\}) = m(\{T\}) = K^{-1} \times \left(\sum_{A \cap B = \{T\}} m_1(A) m_2(B) \right) = K^{-1}(m_1(\{T\}) \times m_2(\{T\}) + m_1(\{T\}) \times m_2(\{T,D\}) + m_1(\{T,D\}) \times m_2(\{T\}))$$

4 节点信任值的计算方法

在这一节中我们给出信任值计算的完整算法。节点 x 在计算信任值之前先赋予自己一个完全的信任值（Complete_trust），然后，再用 Best_node( ) 函数确定的次序计算出与 X 节点相连的、并经前任节点计算出了信任值的节点，最后利用传递和聚合原则通过循环计算出 X 的信任值 Trust(X)。{done} 为已计算节点集合，{remaining} 表示剩下节点集合。

```
//计算节点 x 的信任值 Trust(x)
calculating_Trust(x)
  {done} = myself;
  {remaining} = {nodes} - myself;
  //在 myself 中有完全信任
  Trust(myself) = complete_trust;
  While {remaining} ≠ φ do
    Current = best_node(remaining);
    Trust(current) = uncertainly;
    if T(x,current) ≠ uncertainly
      //通过节点 x 计算传播信任值
      Tm(current) = Trust(x)      T(x,current);
      //通过节点 x 计算合成信任值
      Trust(current) = Trust(current) Tm(current);
      Trust(x) = Trust(current);
    else
      {remaining} = {remaining} - current;
    {done} = {done} + current;
  return best_node(remaining);
end
```

5 结论

P2P 网络建立了计算机系统之间灵活而有效的联系，但增加了网络安全的控制和管理复杂性。在 P2P－PKI 模型中引入 Trust(X, i) 与 Rec(X, PX, Y, i) 消息类型，虽然不能完全地避免欺骗节点对通信的影响，但信任值 i 的引入，使得节点之间通信具有更高的安全性。基于 D－S 理论的信任模型给出了对等节点之间信任值计算的数学模型，并且考虑了信任关系本身的不确定性，为该模型的广泛应用提供了基础，具有极大的推广价值。

参考文献

1 Thomas Wolfl, Public－Key－Infrastructure Based on Peer－to－Peer Network[J], Proceeding of the 38th Hawaii International Conference on System Sciences－2005.

2 Ion Stoica, Robert Morris, David Liben－Nowell, "Chord:A Scalable Peer－to－Peer Lookup Protocol

（下转第 91 页）

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

(上接第 75 页)

for Internet Application[J]. IEEE/ACM TRANSACTION ON NETWORKING, VOL,11, FEBRUARY 2003.

3 A. P. Dempster, Upper and lower probabilities induced by a multivalued mapping[J], Annals of Mathematical Statistics, Vol,38,1967.

4 G. Shafer, A Mathematical Theory of Evidence[M], Princeton University Press, Princeton, NJ,1976.

5 R Perlman, "An Overview of PKI Trust Models"[J], IEEE Network,1999,13(6):38 -43.

6 Carlisle Adams Steve Lloyd. 公开密钥基础设施 - 概念、标准和实施[M],冯登国等,北京:人民邮电出版社,2001,5 -12.

7 张键红、伍前红、王育民,基于代理签名链的安全移动代理[J],西安电子科技大学学报,2003,30(6):784 -791.

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn