

# 分布式 PKI 在移动 Ad Hoc 网中的应用

吴学成, 庄毅, 陈翔

(南京航空航天大学信息科学与技术学院计算机系, 江苏南京 210016)

**摘要:**介绍了一种基于椭圆曲线和门限算法的数字签名算法, 并提出了一个基于分布式 PKI 的移动 Ad Hoc 网络安全体系结构。该体系结构中主要采用了分布式 PKI 安全机制、门限密钥管理、椭圆曲线算法和动态网络分簇思想。分布式 PKI 和门限密钥管理的应用增加了系统的安全性、容错性, 椭圆曲线算法的应用减少了对移动节点的性能的要求, 分簇算法的应用减少了对节点容量的要求。

**关键词:**移动 Ad Hoc 网络; 门限算法; 分布式签名; 椭圆曲线算法

**中图分类号:** TP393.08

**文献标识码:** A

**文章编号:** 1005-3751(2006)02-0208-04

## Distributed PKI for Mobile Ad Hoc Networks

WU Xue-cheng, ZHUANG Yi, CHEN Xiang

(Computer Department, College of Information Science & Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

**Abstract:** In this paper, a digital signature scheme based on ellipse curve and threshold cryptography is introduced. And proposed a security framework based on distributed PKI for mobile Ad Hoc. The key elements of the framework are: (1) distributed PKI based on threshold cryptosystem which can provide a highly security and highly availability; (2) the use of elliptic curve cryptography (ECC) which is appropriate for mobile nodes with limited computational power; (3) a scheme for dynamically partitioning the network into smaller clusters of nodes based on nodal mobility which can reduce the storage of node.

**Key words:** mobile Ad Hoc network; threshold cryptography; distributed signature; elliptic curve cryptography

### 0 引言

移动 Ad Hoc 网络的安全问题是目前研究的热点。基于口令的认证策略: 一种是通过预先设置的密钥来完成认证, 它不需要专门的 CA (Certificate Authorities) 中心<sup>[1]</sup>; 另一种是和 PGP (Pretty Good Privacy) 类似的策略, 它的信任关系是用户自己建立的, 这种策略理论上非常适合应用到 Ad Hoc 网络中, 但是并不适合实际应用<sup>[2]</sup>; 另外一种重要的策略是基于门限算法的分布式认证, 它能避免传统 PKI 安全机制的单点 CA 易受攻击的缺点, 并且它具有很高的容错性<sup>[3]</sup>。

文中提出了一个多 CA 的、分布式 PKI 和传统 PKI 相结合的安全体系结构, 它适合应用到移动 Ad Hoc 网络中, 具有可扩展性, 并且易于实现。在这个体系结构中主要采用了以下几种重要策略:

- ①网络的动态分簇策略;
- ②基于门限的分布式 CA 策略;

③秘密共享恢复和多证书库策略;

④基于椭圆曲线算法签名的策略。

基于门限的分布式 CA 的应用提高了安全性, 因为任何对手要想攻破系统必须同时获得足够多的 CA 服务器。秘密共享和多证书库的应用提高了系统的容错性。网络的动态分簇和分布式密钥管理使得节点和服务所需存储容量减少。椭圆曲线的应用减少了节点的计算, 可有效地解决节点计算能力有限的缺点。

### 1 门限数字签名

#### 1.1 门限签名简介

所谓门限签名就是把对信息的签名能力分配给若干个机构。例如: 一个  $(t, n)$  签名体制中, 签署一份信息的能力由  $n$  个签名者  $p_1, p_2, \dots, p_n$ , 按如下方式分享: 对任意给定的  $t$  个或更多的签名者的子集可以协同产生一个合格的签名, 但是任意少于  $t$  个签名者的子集将无法伪造合法签名。它有如下优点:

①攻击者若想得到签名密钥, 必须得到  $t$  个子密钥, 这是很困难的;

②即使某些成员不合作, 不愿意出示子密钥, 泄露、篡改子密钥或子密钥丢失也不会影响签名消息的认证与恢复;

③实现权利分配, 避免滥用。

收稿日期: 2005-05-20

基金项目: 十五预研基金资助项目 (41801150201); 航空基金资助项目 (04c52009)

作者简介: 吴学成 (1978—), 男, 河南淮阳人, 硕士研究生, 研究方向为无线网络安全; 庄毅, 女, 副教授, 研究方向为网络安全。

## 1.2 基于椭圆曲线算法的 $(t, n)$ 门限签名方案

基于椭圆曲线密码体制的 $(t, n)$ 门限签名方案分为3个阶段:系统初始化阶段、签名阶段和签名验证阶段。

### 1.2.1 系统初始化阶段

初始化安全参数如下:

(1) 可信中心选取有限域 $F_q$ 上一条安全的椭圆曲线 $E(F_q)$ , 保证该椭圆曲线的离散对数问题是难解的。在 $E(F_q)$ 上选一基点 $G$ ,  $G$ 的阶数为 $p$  ( $p$ 是大于 $n$ 的一个大素数)。

(2)  $p_1, p_2, \dots, p_n$ 是 $n$ 个签名者。

(3) 可信中心随机选取 $d \in Z_q$ 作为签名的私钥, 与它对应的公钥 $Y = d \cdot G$  ( $Y \in E(F_q)$ ), 然后可信中心随机产生 $t-1$ 次多项式:  $f(x) = d + a_1x + \dots + a_{t-1}x^{t-1} \bmod q$ ,  $a_0 = d$ , 分别计算签名者 $P_i$ 的私钥与公钥对为:  $d_i = f(i)$ ,  $Y_i = d_i \cdot G$  ( $i = 1, \dots, n$ )。

(4) 可信中心通过安全信道发送 $d_i$  ( $i = 1, \dots, n$ ) 给 $p_i$ , 并且公开参数 $E(F_q)$ ,  $G$ ,  $n$ ,  $Y$ ,  $Y_i$ 。

(5) 每个 $p_i$ 接收到 $d_i$ 后, 可通过计算 $Y_i = Y + \sum_{j=0}^{t-1} p_j(a_j \cdot G)$ 是否成立来判断 $d_i$ 是否为有效密钥。如果不成立则拒绝 $d_i$ 并公开 $d_i$ 。

### 1.2.2 门限签名阶段

假设组 $Q = \{p_1, p_2, \dots, p_n\}$ 中有 $t$ 个签名者, 令 $B = \{i_1, i_2, \dots, i_t\}$ 。

签名步骤如下<sup>[4,5]</sup>:

(1) 选择 $t$ 个授权签名者 $S_i$  ( $i \in B, S_i \in Q$ )。

(2) 每个签名者 $S_i$ 计算 $e_{i,B} = b_{i,B}d_i$ 并向合成者公开 $Y_i = e_{i,B} \cdot G$ , 其中 $b_{i,B} = \prod_{h \in B, h \neq i} h(h-i)^{-1}$ 。

(3) 每个 $S_i$  ( $i \in B$ ) 选择随机数 $k_i \in Z_p \setminus \{0\}$ , 计算并公开 $R_i = k_i \cdot G$ 。

(4) 对每个 $S_i$  ( $i \in B$ ) 计算 $(x, y) = \sum_{i \in B} R_i$ ,  $r = x - h(m) \bmod q$ ,  $s_i = e_{i,B} + k_i \bmod q$ , 并公开 $s_i(h())$ 为哈希函数, 把 $(r, s_i)$ 发送给合成者。

(5) 合成者对所有 $(j \in B)$ 验证 $R_j = s_j \cdot G - rY_j$ , 如果成立则计算 $s = \sum_{j \in B} s_j \bmod q$ ,  $(r, s)$ 为消息 $m$ 的门限数字签名, 如果不成立, 则拒绝 $s_j$ 。

### 1.3 签名验证阶段

$(r, s)$ 是消息 $m$ 的合法签名当且仅当满足<sup>[6]</sup>  $x' = r + h(m) \bmod q$ , 其中 $(x', y') = s \cdot G - rY$ 。

## 2 Ad Hoc 网络中基于分布式 PKI 的体系结构

### 2.1 体系结构

文中结合 Ad Hoc 网络特点提出了一个分布式 PKI 和传统 PKI 相结合的体系结构(见图 1)。该体系结构主要分为两部分: 有线分布式 PKI 和无线分布式 PKI (签名方案采用上文提到的基于椭圆曲线算法的 $(t, n)$ 门限签名方案)。

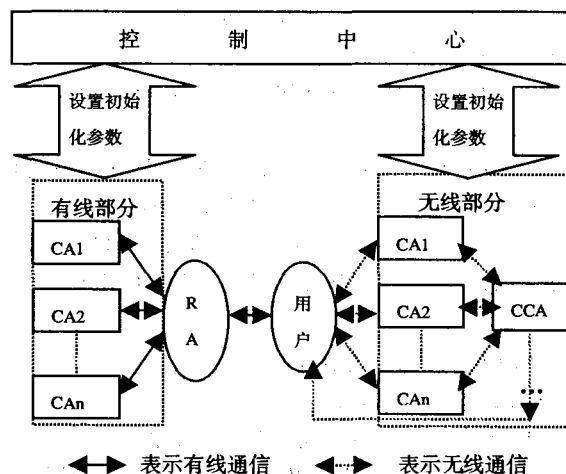


图1 分布式安全体系结构

图1中控制中心的主要任务是对有线分布式 PKI 和无线分布式 PKI 进行初始化参数设置。它是该体系结构中最关键的部分。有线分布式 PKI 主要任务是给要进入无线移动 Ad Hoc 网络的节点颁发证书, 节点只有具有合法的证书才允许接入无线移动 Ad Hoc 网络, 它保证网络的接入安全和路由安全。无线分布式 PKI 的主要任务是给节点颁发访问网络资源的证书, 只有具有合法的用户才能获得相应的信息, 它提供了网络资源访问的安全。RA (Registration Authority) 主要负责对用户身份的审查、有线分布式证书合并和向用户颁发入网证书。CCA (Combination Certification Authority) 合并证书服务器, 它负责无线分布式证书的合并, 它是经过多个 CA 服务器根据一定的算法选举产生的。

### 2.2 有线分布式 PKI 系统的工作流程

有线分布式 PKI 的证书颁发过程如下:

- (1) 用户向 RA 请求证书服务。
- (2) RA 核实用户信息。
- (3) 如果是合法用户, RA 向至少  $t+1$  个 CA 服务器发送签名请求。
- (4) CA<sub>i</sub> 验证 RA 身份, 如合法, 则用私钥  $d_i$  进行签名, 并把签名后的部分证书 CERT<sub>i</sub> 发送给 RA。
- (5) RA 对收到的部分证书 CERT<sub>i</sub> 进行验证和合并部分证书, 同时把合成的证书发送给用户。

### 2.3 无线分布式 PKI 系统的工作流程

#### 2.3.1 网络初始化

初始化网络的步骤如下:

- (1) 控制中心设置初始化参数和密钥对, 并把秘密密钥根据门限算法分配给各个 CA 服务器。
- (2) 每个 CA 服务器根据收到的私钥  $d_i$  计算它的公钥  $Y_i$ , 并对服务器组公开它们的公钥。
- (3) 配置一个初始化节点集合。

#### 2.3.2 节点的动态加入

N (一个新的节点) 节点的加入网络要执行如下步骤:

Step1 节点 N 获得证书  $c_N$  (节点 N 的证书)。

(1) N 获得接入证书后(有线分布式 PKI 签名产生的证书),进入无线网络;

(2) 节点 N 向所有 CA 服务器发送 CERTQ (Certificate Request);

(3) 收到 CERTQ 的 CA 服务器验证节点 N 的身份,如合法,则用私钥  $d_i$  进行签名,并发送 CERT<sub>i</sub> 给 CCA;

(4) CCA 对收到的 CERT<sub>i</sub> 进行验证,如果收到的合法的 CERT<sub>i</sub> 个数达到门限值,则把合法的 CERT<sub>i</sub> 合并成  $c_N$ ;

(5) CCA 把  $c_N$  发送给节点 N。

Step2 节点 N 加入簇  $i$ 。

(1) N 发送  $c_N$  给  $R_i$ (簇  $i$  中的证书库);

(2) N 从簇  $i$  中的证书库中请求  $C_i$ (簇  $i$  中节点的证书库集合)和 CRL;

(3)  $R_i$  广播  $c_N$  并存储  $c_N$ ;

(4) 簇  $i$  中的节点有选择地存储  $c_N$ 。

### 2.3.3 撤消证书

证书撤消的步骤如下:

Step1 如果簇  $i$  中的节点  $m$  请求节点  $w$  的  $cc_{i-w}$ (簇  $i$  中节点  $w$  的撤消证书)被颁发,则

(1) 簇  $i$  的节点  $m$  发送一个关于节点  $w$  的证书撤消请求给所有 CA 服务器;

(2) 至少  $t+1$  个 CA 服务器联合生成  $cc_{i-w}$  并给 CRL 增加  $cc_{i-w}$  的一个序列号;

(3)  $cc_{i-w}$  在网络中广播;

(4)  $R_i$ (簇  $i$  证书库),  $j_{i-w}$ (簇  $i$  中的节点  $w$ ) 存储  $cc_{i-w}$ ;

(5) CRL 被 CA 服务器周期性地更新;

(6) 簇  $i$  中的证书库和  $j_{i-w}$  存储 CRL。

Step2 若簇  $i$  中节点  $w$  请求撤消它自己的证书,则

(1) 节点  $w$  为  $cc_{i-w}$  的颁发向所有 CA 服务器发送一个证书撤消请求;

(2) 执行 Step1(2)到 Step1(6)。

### 2.3.4 节点的移动

跨簇节点的移动步骤如下:

Step1 簇  $i$  中的节点  $w$  离开原簇  $i$ 。

(1) 如果移动管理协议指出节点  $w$  永久地离开  $i$ , 节点  $w$  将删除簇  $i$  中节点的证书;

(2) 如果不是永久离开则执行 Step2。

Step2 簇  $i$  中的节点  $w$  加入目的簇  $d$ 。

(1) 节点  $w$  发送它的证书  $c_w$  到簇  $d$  的证书库  $u$  中;

(2) 节点  $w$  从簇  $d$  中的证书库  $u$  中请求簇  $d$  中的节点证书集合;

(3) 簇  $d$  中的证书库  $u$  广播  $c_w$  并存储  $c_w$ ;

(4) 簇  $d$  的节点有选择地存储  $c_w$ 。

## 2.4 体系结构的特点和安全性分析

### 2.4.1 技术特点

(1) 系统中应用了椭圆曲线算法。

椭圆曲线算法是现在研究的热点,它与 RSA 方法相比,有以下优点:

a. 安全性能更高, ECC 和其他几种公钥系统相比,其抗攻击性具有绝对的优势。如 160bit 的 ECC 与 1024bit 的 RSA, DSA 有相同的安全强度。

b. 计算量小, 处理速度快, 虽然在 RSA 中可以通过选取较小的公钥的方法提高公钥处理速度, 即提高加密和签名验证的速度, 使其在加密和签名验证速度与 ECC 有可比性, 但在私钥的处理速度上(解密和签名), ECC 远比 RSA, DSA 快得多。

c. 存储空间占用小, ECC 的密钥尺寸和系统参数与 RSA, DSA 相比要小得多, 意味着它所占的存贮空间要小得多。

d. 带宽要求低, 当对长消息进行加解密时, 三类密码系统有相同的带宽要求, 但应用于短消息时 ECC 带宽要求却低得多。带宽要求低使 ECC 在无线网络领域具有广泛的应用前景。

(2) 系统中应用了分布式 CA 签名算法。

基于门限签名的分布式签名算法, 具有密钥的分布式管理和抗攻击能力强的优点。它的应用能给网络提供较高的安全性。有线分布式 CA 签名算法的应用为移动 Ad Hoc 网络的物理层、数据链路层以及路由层的安全提供了保证。无线分布式 CA 的应用保证了网络的访问控制和应用层的安全。有线分布式 CA 具有不受地域限制、高安全性、签名权利分散、易扩展和易于实现的特点。

(3) 采用了基于分簇算法的 Ad Hoc 网络结构。

在移动 Ad Hoc 网络中, 整个网络逻辑上划分为不同的簇, 簇中服务器是负责分布式签名的移动节点, 它具有较强的处理能力和通信能力。分簇算法的应用有以下几个优点: ①减少了节点所需的存储容量; ②减少了通信量; ③增加了证书的管理效率; ④簇内通信效率高, 因为每个节点缓存区中都存放了最近使用的簇内的节点的证书、最新的 CRL, 这使得请求证书和 CRL (certificate revocation list) 的次数减少。

### 2.4.2 攻击模型和安全性分析

在移动 Ad Hoc 网中常用的攻击有对 CA 服务器、证书库以及证书服务的攻击。定义攻击的三元组表达式为  $(c, s, r)^{[7]}$ , 其中  $c$  表示网络中簇的数量,  $s$  和  $r$  分别表示网络中分布式 CA 服务器的数量和证书库数量。在实际应用中  $c, s, r$  都有可能受到攻击。

第一种攻击方法是对 CA 服务器的秘密密钥进行攻击。这种方法可攻破 CA 服务器。在文中提出的体系结构中, 应用了基于门限的分布式签名算法, 该算法采用了分布式密钥管理策略, 它可避免单节点 CA 服务器易受攻击的缺点, 提高对 CA 服务器的抗攻击能力。假定每个簇中只有一个 CA 服务器(实际情况中可能有多个), 基于门限算法的分布式 CA 使得  $(n, k, r)$  形式的攻击无效 ( $n = 2k + 1$ ),  $k$  表示受对手控制的最大 CA 服务器个数。

第二种攻击方法是对证书库的攻击,它使证书库不能提供服务。基于分簇的分布式 CA 策略,可以处理从  $(1, 0, r)$  到  $(1, s, r)$  形式的攻击( $r$  是簇中受到攻击的证书库的数量),设  $t$  是簇中证书库节点的数量( $t > r$ )。令  $b = t - r$ , 则簇中至少有  $b$  个证书库可以提供服务。这样只要簇中有一个证书库可以提供服务,就不会影响簇中的正常操作。这种增加证书库的冗余策略,提高了证书库的抗攻击能力,能有效地保证网络的正常运行。

第三种攻击方法是用户身份伪造,通过这种方法非法用户可以获得网络中的重要资源。系统中 RA 主要负责对用户身份的审查。用户只有通过 RA 才能获得入网证书。而 RA 是由控制中心指定,它具有较高的安全性。

### 3 结论

文中提出的分布式有线 PKI 和无线分布式 PKI 相结合的安全体系结构,解决了移动 Ad Hoc 网络中存在的一些安全问题,具有较高的安全性。基于门限算法的分布式 CA 签名的应用,解决了单点 CA 易受攻击的问题。有线分布式 CA 签名算法的应用为移动 Ad Hoc 网络的物理层、数据链路层以及路由层的安全提供了保证。无线分布式 PKI 保证了网络资源访问的安全性。分簇算法的应用减少了节点要存放证书所需的容量和网络中的通信流量。椭圆曲线算法的应用减少了节点计算的复杂度。

(上接第 207 页)

$A_r, B_1, \dots, B_s, r$  与  $s$  都是保密的。

### 2 注记

1) 第一部分中的原则可以用于多个加密算法的复合。此时,需要解形如:

$$\lambda_1 x_1 + \dots + \lambda_k x_k = E$$

的方程。由前面的定理可以得到确定上述方程解的条件,即对诸  $\lambda$  所需附加的条件。

2) 第一部分中的两个例子都用到简单背包向量,这并不是必要的。事实上,若有背包向量  $(a_1, \dots, a_n)$  使得方程

$$a_1 x_1 + \dots + a_n x_n = b$$

的求解总是容易计算的(当已知某些陷门信息时),就可用它代替例子中的简单背包向量,称这样的向量为易解背包向量。在文献[7]中所设计的背包向量就是易解背包向量。

3) 前面的两个例子中均取  $F_1$  与  $F_2$  为公钥密码系统的算法函数,这当然不是必要的。它们也可以是传统的加密算法函数。例如<sup>[8]</sup>,在例 1 中,若取  $F_2$  是用伪随机数列  $(\lambda_1, \dots, \lambda_s)$  对  $P_2 = p_{r+1} \dots p_n$  ( $n = r + s$ ) 加密的算法,即用二进制数  $a_1 \dots a_s$  作为  $E_2 = F_2(P_2)$ , 其中  $a_i \equiv p_{i+r} + \lambda_i \pmod{2}$ ,  $\lambda_i = 0$  或  $1, 1 \leq i \leq s$ , 那么,容易看出,在例 1

### 参考文献:

- [1] Asokan N, Ginzboorg P. Key Agreement in Ad-hoc Networks[EB/OL]. <http://citeseer.ist.psu.edu/cache/papers/cs/14830/>. <http://zSzzSzwww.semper.orgz/Szsirenez/Szpeoplez/Szasokanz/Szresearchz/Szccr.pdf/asokan99key.pdf>, 2005.
- [2] Capkun S, Buttyan L, Hubaux J P. Self-Organized Public-Key Management for Mobile Ad Hoc Networks[R]. Technical Report EPFL/IC/200234, Lausanne: Swiss Federal Institute of Technology, 2002.
- [3] Zhou L, Haas Z J. Securing Ad Hoc Networks[J]. IEEE Network, 1999, 13: 24-30.
- [4] 戴元军, 杨成. 基于椭圆曲线密码体制的  $(t, n)$  门限签名方案[J]. 计算机应用研究, 2004(9): 142-143.
- [5] 徐海霞, 李宝. 分布式密钥分发方案的安全性证明[J]. 软件学报, 2005, 16(4): 570-576.
- [6] 伍忠东, 谢维信, 喻建平. 一种安全增强的基于椭圆曲线可验证门限签名方案[J]. 计算机发展和研究, 2005, 42(4): 705-710.
- [7] Zouridaki C, Mark B L, Gaj K, et al. Distributed CA-based PKI for Mobile Ad Hoc Networks Using Elliptic Curve Cryptography[Z]. Lecture Notes in Computer Science[s. l.]: Springer-Verlag GmbH, 2004. 232-245.

中对  $F(P), F_1(P_1), F_2(P_2)$  所做的分析都仍是有效的, 只不过要将式(7)中的  $k'(m_1 + 1) < mL$  改为  $k'(2^{s+1} + 1) < mL$ 。

### 参考文献:

- [1] Salomaa A. Public-Key Cryptography[M]. New York: Springer-Verlag, 1990.
- [2] van Tilborg H C A. An Introduction to Cryptography[M]. Boston: Kluwer Academic Publishers, 1988.
- [3] 曹珍富. 公钥密码学[M]. 哈尔滨: 黑龙江教育出版社, 1993.
- [4] Koblitz N. A Course in Number Theory and Cryptography[M]. New York: Springer-Verlag, 1987.
- [5] Frieszetal A M. Reconstructing Truncated Integer Variables Satisfying Linear Congruences[J]. SIAM J. Comput, 1988, 17: 262-280.
- [6] Diffie W, Hellman M E. New Directions in Cryptography[J]. IEEE Trans. Informat. Theory, 1976, 22: 644-654.
- [7] Ben-Zion C. Two Issues in Public Key Cryptography[M]. ACM Distinguished Dissertations, MIT campus, USA: The MIT Press, 1985.
- [8] ElGamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm[J]. IEEE Trans. Informat. Theory, 1995, 31: 469-472.