文章编号:1000 - 582X(2004)11 - 0063 - 03

基于移动 Ad Hoc 网络的分布式 RSA 密钥生成机制*

沈　颖[1],杨 天 怡[1],刘 益 良[2]
(1. 重庆大学 自动化学院,重庆　400030;2. 重庆工学院 信息安全研究所,重庆　400050)

摘　要:移动 Ad Hoc 网络(MANET)是一种具有全新概念的无线网络,不依赖于任何固定物理基础设施和集中式组织管理机构,通过无线信道实现移动节点之间的通信。然而 Ad Hoc 网络的固有特性使其更易遭受各种安全威胁,在基于分布式 PKI/CA 体制的安全解决方案中如何生成和分发 CA 密钥将是一个具有挑战性的问题。对现有的几种方案进行了分析讨论,指出了其中存在的问题,并就此提出了一种基于门限 RSA 密码体制的分布式 CA 密钥共享生成机制,提高了系统的安全性和鲁棒性。

关键词:移动 Ad Hoc 网络;密钥生成;自组织;RSA;安全
中图分类号:TP393.08　　**文献标识码**:A

移动 Ad Hoc 网络(MANET,以下简称 Ad Hoc 网络)是由若干无线移动节点组成的不依赖于任何固定基础设施和集中式组织管理机构而通过节点间的相互协作进行网络互联的一种多跳自组织临时性自治系统。主要用于军事战术通信、紧急情况下的快速组网及其它对安全敏感环境。相对于传统网络,其具有动态的拓扑结构、有限的无线链路带宽、分布式控制及安全性差等特性[1-2]。由于自身的特点和特殊应用使得 Ad Hoc 网络成为当前网络研究的热点,具有重要的战略意义和潜在的广阔的商业应用前景。

Ad Hoc 网络自身所固有的大部分特性也正成为其潜在的脆弱点,使其更易遭受各种安全威胁,面临日益严重的安全问题[3]。类似于传统有线网络,为保障 Ad Hoc 网络敏感信息的安全需要利用适当的安全机制如加密、认证、数字签名来提供网络所需的各种安全服务(如身份认证、机密性、完整性、不可否认和可用性)。基于公钥密码机制的 PKI/CA 体系在提供各种基本安全服务以解决目前的网络安全问题方面已成为一种有效的完善的安全解决方案,但如何将其应用于 Ad Hoc 网络环境中是一个具有挑战性的问题。目前在国外已有学者对此提出了几种安全模型方案,主要解决认证和密钥管理这两个基本安全要素。Zhou 和 Hass[3]首先提出了基于门限密码学的局部分布式 CA 模型,由一组服务器节点共同实现 CA 功能。此后 Yi 和 Kravets[4]也提出了类似的方案,进一步阐明了服务器节点的选择标准。由 Kong、Luo[5]等人提出的一种全分布式 CA 模型,类似于前面的方案,只是由网络所有节点共同承担 CA 职责。上述这些方案共同之处在于均假设 CA 的签名私钥共享由一可信管理机构 dealer 预先分发给各 CA 节点,然而这种方式存在以下问题:1)由于单个 dealer 拥有 CA 的完整私钥信息,其被暴露将危及 CA 系统安全;2)忽视了 Ad Hoc 网络的自组织特性,即由节点自发的构建网络并提供各种服务,而不依赖于或无法确保具有任何基础设施和管理机构。鉴于此,笔者提出了基于门限 RSA 密码体制的分布式密钥共享生成机制,即在网络形成时由各 CA 节点协作完成 CA 的 RSA 私钥共享的生成和分发。

1　门限 RSA 公钥密码体制

1.1　RSA 公钥密码体制

RSA 体制是由 MIT 的 Ronald Rivist、Adi Shamir 和 Len Adlemar 于 1978 年提出并开发的第一个可逆的公钥密码体制,可用于加密和数字签名,其算法成为目前被广泛接受且被实现的通用公钥加密方法。

RSA 算法是基于群 Z_N 中大整数因子分解的困难性。其过程如下:选取两个保密的大素数 p 和 q,计算 $N=pq$(公开)和 $\Phi(N)=(p-1)(q-1)$(保密),随机选取公钥 e,且满足 $1<e<\Phi(N)$ 和 $\gcd(e,\Phi(N))=1$,计

* 收稿日期:2004 - 06 - 18
作者简介:沈颖(1968 -),男,重庆人,重庆科技学院讲师,重庆大学硕士研究生,主要研究方向为计算机控制及信息安全。

算私钥 $d \equiv e^{-1} (\mathrm{mod}\ \Phi(N))$。设消息明文为 m,密文为 c,则加密为 $c = m^e (\mathrm{mod}\ N)$,解密为 $m = c^d (\mathrm{mod}\ N)$。若用于数字签名,对消息 m 的签名为 $s = m^d (\mathrm{mod}\ N)$,签名验证为 $m = s^e (\mathrm{mod}\ N)$。

1.2 Shamir[6]的(k,n)门限方案

设 r 是一个素数,$s \in Z_r$ 是由 n 个参与者 $i(i = 1, \cdots, n)$ 所共享的秘密,且 $r > \max(s,n)$,随机选取 $k-1$ 阶多项式 $f(x) \in Z_r[x]$,使得 $f(0) = s$,每个秘密共享者 i 分配一个 s 的多项式秘密共享 $s_i = f(i) (\mathrm{mod}\ r)$。由任意 k 个秘密共享 $s_1, s_2, \cdots, s_k$,利用 Lagrange 插值公式可重构多项式:$f(x) = \sum_{i=1}^{k} (s_i \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{x-j}{i-j} (\mathrm{mod} r))$,则可恢复秘密 $s = f(0)$,而少于 k 个秘密共享无法恢复秘密。

结合 RSA 体制和(k,n)门限秘密共享方案,可得到门限 RSA 公钥密码体制。在该体制中由 n 个参与者共享原本由单个实体拥有的 RSA 私钥 d,使得每个参与者拥有一个 d 的多项式私钥共享 $d_i (i = 1,2,\cdots,n)$。在进行数字签名时,由任意 k 个参与者可形成对消息 m 的完整签名 $s = \prod_{i=1}^{k} m^{(d_i \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{-j}{i-j})} (\mathrm{mod} N) = m^d (\mathrm{mod} N)$,而少于 k 个参与者则无法形成对消息 m 的完整签名。

2 分布式 RSA 密钥共享的生成方案

假设 Ad Hoc 网络的 CA 由 n 个 CA 节点组成,作为整体 CA 需要有一对 RSA 公钥/私钥(pk/sk),其中私钥 sk 由全体 CA 节点共享,利用(k,n)门限方案实现 CA 的各种功能,如数字签名等。此外假设各 CA 节点存在点对点的私有秘密通道,同时 CA 节点也共享一个广播通道。该方案由 4 个部分组成:

1)素数共享选择。每个 CA 节点秘密的随机生成两个整数 p_i、$q_i (i = 1,2,\cdots,n)$。

2)计算RSA模N。利用私有通道n个CA节点分布式计算 $N = (\sum_{i=1}^{n} p_i)(\sum_{i=1}^{n} q_i = pq$ 并公开。

3)素性测试。n 个 CA 节点通过分布式计算以测试 N 确实是两个素数之积$(N = pq)$,若测试失败,则返回 1)。

4)密钥生成。给定一个公钥 pk,n 个 CA 节点通过私有通道分布式计算以产生私钥 sk 的共享 $sk_i (i = 1,2,\cdots,n)$。

以下就 2) -4)部分进行描述。

2.1 模 N 的分布式计算

运用 BGW[7]方法,取 r 为一素数,且 $r > N$,则过程如下:

1)取 $m = \left\lfloor \frac{n-1}{2} \right\rfloor$,每个 CA 节点 i 随机选择两个 m 阶多项式 $f_i(x)$、$g_i(x) \in Z_r[x]$,且满足 $f_i(0) = p_i$ 和 $g_i(0) = q_i$,而多项式其余系数可任意选择。此外再选择一个 $2m$ 阶多项式 $h_i(x) \in Z_r[x]$,且满足 $h_i(0) = 0$。

2)每个节点 $i(i = 1,2,\cdots,n)$ 计算:$\forall j = 1,2,\cdots, n$,$p_{i,j} = f_i(j)$,$q_{i,j} = g_i(j)$,$h_{i,j} = h_i(j)$,其中 $p_{i,j} (j = 1,2,\cdots,n)$ 是 p_i 的(m,n)Shamir 秘密共享,其余类同。然后节点 i 通过私有通道将三元组$\langle p_{i,j}, q_{i,j}, h_{i,j} \rangle$发送给节点 $j (j = 1,2,\cdots,n$,且 $j \neq i)$。

3)每个节点 i 有 n 组三元组$\langle p_{j,i}, q_{j,i}, h_{j,i} \rangle$,计算 $N_i = (\sum_{j=1}^{n} p_{j,i})(\sum_{j=1}^{n} q_{j,i}) + \sum_{j=1}^{n} h_{j,i} (\mathrm{mod}\ r)$,然后通过广播通道传送给其余所有的 CA 节点。

4)每个 CA 节点 j 拥有所有的 $N_i (i = 1,2,\cdots,n)$,取多项式 $\alpha(x)$ 有 $\alpha(x) = (\sum_{j=1}^{n} f_j(x))(\sum_{j=1}^{n} g_j(x)) + \sum_{j=1}^{n} h_i(x) (\mathrm{mod}\ r)$,则 $\alpha(i) = N_i$,由 $f_i(x)$、$g_i(x)$ 和 $h_i(x)$ 的定义,于是得到 $\alpha(0) = N (\mathrm{mod}\ r)$,由于 $N < r$,则每个CA节点获得了正确的 N。

2.2 分布式素性测试

每个 CA 节点 i 拥有两个秘密整数 p_i 和 q_i,并且知道了 $N = pq = (\Sigma p_i)(\Sigma q_i)$,随后要求判断 N 是否是两个素数之积,同时又不能暴露关于 N 的因子分解的任何信息。在此采用 Fermat 定理来进行素性测试,过程如下:

1)假定由 CA 节点 1 随机选取 $g \in Z_N^*$,并通过广播通道由所有的 CA 节点共知。

2)节点 1 计算 $v_1 = g^{N-p_1-q_1+1} (\mathrm{mod} N)$,而其余 CA 节点 $i(i = 2,3,\cdots,n)$ 计算 $v_i = g^{p_i+q_i} (\mathrm{mod} N)$,然后所有 CA 节点彼此交换各自的 v_i 值,并验证是否满足 $v_1 = \prod_{i=2}^{n} v_i (\mathrm{mod} N)$,若是,则各 CA 节点确信 N 是两个素数之乘积,否则测试失败。

2.3 CA 私钥共享生成

CA 节点选取公钥 $pk > n$,对于构建的模 N,要求计算私钥 $sk = pk^{-1} (\mathrm{mod}\ \Phi(N))$ 的多项式共享 $sk_i (i = 1,2,\cdots,n)$,其过程如下:

1)假定由 CA 节点 1 本地计算 $\Phi_1 = N - p_1 - q_1 + 1$,其余 CA 节点计算 $\Phi_i = -p_i - q_i (i = 2,3,\cdots,n)$,显然有 $\Phi(N) = \sum_{i=1}^{n} \Phi_i$。通过私有通道各 CA 节点可构建

一 k 阶多项式 $f(x) = \Phi(N) + a_1x + \cdots + a_kx^k$，其中 $\forall j, a_j \in [-N, N]$。

2）每个 CA 节点 $i(i = 1,2,\cdots,n)$ 随机选择两个 k 阶多项式 $g_i(x) = \lambda_i + b_{i,1}x + \cdots + b_{i,k}x^k$，$h_i(x) = r_i + c_{i,1}x + \cdots + c_{i,k}x^k$，以及 $2k$ 阶多项式 $\rho_i(x) = 0 + \rho_{i,1}x + \cdots + \rho_{i,2k}x^{2k}$，且要求 $\lambda_i \in_R [0, N^2]$，$r_i \in_R [0, N^3]$；$\forall j$，$b_{ij} \in_R [-N^3, N^3]$，$c_{ij} \in_R [-N^4, N^4]$，$\rho_{ij} \in_R [-N^5, N^5]$。随后给每个节点 $j(j = 1,2,\cdots,n, j \neq i)$ 发送 $g_i(j)$、$h_i(j)$、$\rho_i(j)$。

3）每个节点 $j(j = 1,2,\cdots,n)$ 计算 $g_j = \sum_{i=1}^{n} g_i(j)$，$h_j = \sum_{i=1}^{n} h_i(j)$，$\rho_j = \sum_{i=1}^{n} \rho_i(j)$。然后通过广播通道广播 $F_j = f(j) \cdot g_j + pk \cdot h_j + \rho_j$。

4）每个节点 i 利用收到的 $F_j(j = 1,2,\cdots,n)$ 重构 $2k$ 阶多项式 $F(x) = f(x)g(x) + pk \cdot h(x) + \rho(x)$，其中 $g(x) = \Sigma g_i(x)$，$h(x) = \Sigma h_i(x)$，$\rho(x) = \Sigma \rho_i(x)$。然后运用 gcd 算法，寻找 a、b 使得 $a \cdot F(0) + b \cdot pk = 1$，如果 a、b 不存在，则返回 2）。否则，有 $sk = a \cdot h(0) + b = pk^{-1} (\mathrm{mod}\ \Phi(N))$，因此每个 CA 节点可得 CA 私钥的多项式共享 $sk_i = a \cdot h(i) + b$ $(i = 1,2,\cdots,n)$。

2.4　方案的几点讨论

1）关于素性测试。在第 2.2 节中采用了 Fermat 测试来判断数 N 是否两个素数 p 和 q 之乘积，其本质上是判断是否满足 $g^{N-p-q+1} = 1 \ (\mathrm{mod}\ N)$。需注意的是这种方法存在这样一种情况，即整数 N 不是两素数之积但却能够通过 Fermat 测试，出现这种整数的概率[8]一般小于 $1/10^{40}$。一种改进的方法是采用由 Boneh 等人提出的完备概率性素性测试方法，在通过 Fermat 测试基础上，运用该法可确保 N 是两素数之积。

2）关于 CA 私钥共享的正确性。通过分布式计算各 CA 节点得到了 CA 的私钥共享 $sk_1, sk_2, \cdots, sk_n$，若这些共享能构成 CA 私钥 $sk = pk^{-1} (\mathrm{mod}\ \Phi(N))$ 的 (k, n) 多项式秘密共享，则认为该生成方案是正确的。

从第 2.3 节可知多项式 $F(x)$ 具有整数系数，因此 $F(0) = \lambda \cdot \Phi(N) + R \cdot pk$ 是一个整数，其中 $\lambda = \sum_{i=1}^{n} \lambda_i$，$R = \sum_{i=1}^{n} r_i$，一旦得到等式 $a \cdot F(0) + b \cdot pk = 1$，则可写成 $a(\lambda \cdot \Phi(N) + R \cdot pk) + b \cdot pk = 1$，两边取 $\mathrm{mod}\Phi(N)$，可得 $(a \cdot R + b)pk = 1 \ (\mathrm{mod}\Phi(N))$，即 $sk = a \cdot R + b = pk^{-1} (\mathrm{mod}\Phi(N))$，由此可知 k 阶多项式 $a \cdot h(x) + b$ 构成了私钥 sk 的 (k, n) 多项式，各 CA 节点的私钥共享 $sk_i(i = 1,2,\cdots,n)$ 就完全包含在该多项式之中。

3　结束语

对于移动 Ad Hoc 网络这样一种具有自组织特性的分布式网络环境，安全问题正逐渐成为被关注的焦点。其中基于门限公钥密码学的分布式 PKI/CA 体制是一种可行的安全解决方案，针对这种解决方案，笔者提出了一种基于门限 RSA 公钥密码体制的分布式 CA 密钥共享生成机制，在 CA 的 RSA 私钥共享生成过程中，除了公共模 N 和其它不需保密的公开信息外，各 CA 节点仅拥有自己的私有秘密，并运用分布式算法在本地生成其 CA 的私钥共享，由此排出了对单点集中式管理机构的需要，充分考虑到了 Ad Hoc 网络的自组织特性，同时避免了由于该机构拥有完全的 CA 私有秘密而带来的安全隐患，提高了系统的安全性和鲁棒性。

参考文献：

[1] MACKER J, CORSON M. Mobile ad hoc networking and the IETF[J]. Mobile Computing and Communications Review, 1998,2(1):9 - 14.

[2] RFC 2501,Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations[S].

[3] ZHOU L, HAAS Z. Securing Ad Hoc Networks[J]. IEEE Network Magazine, 1999,13(6):24 - 30.

[4] YI S, KRAVETS R. Practical PKI for Ad Hoc Wireless Networks[R]. Urbana : University of Illinois, 2002.

[5] KONG J, ZERFOS P,LUO H,et al. Providing robust and ubiquitous security support for MANET[A]. Proceedings of 9th International Conference on Network Protocols (ICNP) [C]. California: IEEE Computer Society Press,2001.251 - 260.

[6] SHAMIR A. How to Share a Secret[J]. Communications of the ACM, 1979,22(11):612 - 613.

[7] BEN - OR M, GOLDWASSER S, WIGDERSON A. Completeness theorems for non - cryptographic fault tolerant distributed computation[A]. Proc. 20th Annual ACM Symposium on Theory of Computing(STOC)[C]. New York:ACM Press ,1988.1 - 10.

[8] RIVEST R. Finding four million large random primes[A]. Proceedings of Crypto'91[C]. London: Springer - Verlag,1991.625 - 626.

（下转第 70 页）

Application of Multivector Algebra in Real Space-time to Set Pair Analysis

DUAN Shao-guang

(College of Mathematics and Science, Chongqing University, Chongqing 400030, China)

Abstract: The contact number is an important mathematical tool of systems theory and methods in the monograph *Set Pair Analysis and Its Preliminary Applications* written by Zhao Keqin for unitizedly processing the uncertainties due to the fuzzy, stochastic, intermediate and information uncomplete about something. The article applies the multivector algebra which is isomorphism with the real Dirac algebra in the real space-time adopted by Venzo de Sabbata to the contact number of set pair analysis, and consequently, the contact number is generalized correspondingly.

Key words: real space-time; multivector; algebra; set pair analysis; contact number; spinor; manifold

(编辑 张 苹)

(上接第65页)

Distributed Generation of Shared RSA Keys in Mobile Ad Hoc Networks

SHEN Ying[1], *YANG Tian-yi*[1], *LIU Yi-liang*[2]

(1. College of Automation, Chongqing University, Chongqing 400030, China;
2. Information Security Research Institute, Chongqing Institute of Technology, Chongqing 400050, China)

Abstract: Mobile Ad hoc NETworks(MANET) is a totally new concept in which mobile nodes are able to communicate together over wireless links in an independent manner, without needing any fixed physical infrastructure and centralized organizational/administrative infrastructure. However, the nature of ad hoc networks makes them very vulnerable to security threats. Generation and distribution of shared keys for CA(Certification Authority) is challenging in security solution based on distributed PKI/CA. Those solutions that have been proposed in the literature and some issues are discussed. This paper propose the solution of distributed generation of shared CA keys based on threshold RSA cryptosystems, with which the security and robustness of system is enhanced.

Key words: Mobile Ad Hoc Networks; keys generation; self - organization; RSA; security

(编辑 张 苹)