自组网环境下基于组合公钥的分布式密钥管理

张玉臣 王亚弟 韩继红 范钰丹
(信息工程大学电子技术学院 郑州 450004)

摘 要 结合组合公钥密码体制和秘密共享思想,针对移动自组网环境,提出了一种分布式密钥管理方案。从系统初始化、管理平台构建、节点公私钥生成、私钥矩阵份额更新等4个方面进行了详细描述,并给出了具体实施方法。分析表明,该方案具有安全性高、扩展性强、计算量小、适用性好的特点,特别适合移动自组网环境。

关键词 组合公钥,门限方案,ECC复合定理,种子矩阵

中图法分类号 TP309 **文献标识码** A

Distributed Key Management for Ad-hoc Network Based on CPK

ZHANG Yu-chen WANG Ya-di HAN Ji-hong FAN Yu-dan
(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)

Abstract A distributed key Management scheme for Mobile Ad-hoc Networks(MANETS) was proposed, which combines Combined Public Key(CPK) cryptography with secret sharing threshold cryptography. Four aspects were depicted detailedly including initializing system, designing management platform, obtaining nodes' private/public key and updating private matrix sharing. Analysis shows that this project is secure, distensible, concise and applicable. So it is especially suitable for the characteristics of MANETS.

Keywords Combined public key, Threshold scheme, ECC composed principle, Seed matrix

1 引言

移动自组网(Mobile Ad-hoc Networks)是由若干无线移动节点构建的不依赖于任何固定基础设施或集中组织管理机构的一种多跳自组织临时性自治系统[1],不仅具有极高的军用价值,也可广泛应用于紧急救援、移动会议、家庭网络、传感器网络、无线个域网等民用领域。

安全问题始终是制约移动自组网发展的核心问题之一,而密钥管理又是诸多安全问题中最核心、最重要、最难以解决的问题。针对移动自组网的无固定基础设施、无中心节点、节点资源受限等特点,分布式密钥管理研究受到青睐。Zhou等在文献[1]中提出了基于门限密码体制的部分分布式CA密钥管理,这是关于部分分布密钥管理最早的提法。文献[2]给出了部分分布式算法的具体实现,称为MOCA,并用网络模拟器检测了其算法性能。文献[3]提出了一种基于身份的门限密钥管理方法,重点给出了密钥产生、密钥分配和密钥更新的具体方法。文献[4-6]分别从不同角度就分布式密钥管理进行了描述。

本文基于椭圆曲线密码系统的组合公钥体制(Combined Public Key,CPK)和门限密码技术,提出了一种无证书的分布式密码管理方案,并对该密钥管理方案进行了分析。

2 组合公钥密码体制

组合公钥密码体制是构建在椭圆曲线密码体制(Elliptic Curve Cryptography,ECC)上的基于标识的密码体制,采用有限域 F_q 上的椭圆曲线密码,以 (a,b,G,n,p) 定义[5]。其中,a,b 定义三次方程 $y^2\equiv(x^3+ax+b) \bmod p$,$G$ 为加法群的基点,n 是以 G 为基点的群的阶。令任意小于 n 的整数 r 为私钥,则 $rG=R$ 为对应公钥。

ECC复合定理描述如下,任意多对公、私钥,其私钥之和、公钥之和构成新的公私钥对。

如果,私钥之和:$(r_1+r_2+\cdots+r_m) \bmod n=r$,则,对应公钥之和:$R_1+R_2+\cdots+R_m=R$,那么,$R$ 和 r 将形成新的公、私钥对。因为,

$$R=R_1+R_2+\cdots+R_m=r_1G+r_2G+\cdots+r_mG$$
$$=(r_1+r_2+\cdots+r_m)G=rG$$

由ECC复合定理可知,组合公钥密码体制具有超大规模的密钥管理优势,能够由少量的种子矩阵通过组合的方法产生大量的密钥,对于资源受限的移动自组网,无疑有着应用的现实意义。

到稿日期:2010-11-10 返修日期:2011-03-03 本文受国家高新技术研究发展计划(863)项目(2008AA01Z404)资助。

张玉臣(1977-),男,博士生,讲师,主要研究方向为计算机网络安全,E-mail:zycxz@sohu.com;王亚弟(1953-),男,教授,博士生导师,主要研究方向为计算机网络安全、信息系统安全;韩继红(1966-),女,教授,博士生导师,主要研究方向为计算机网络安全、信息系统安全;范钰丹(1982-),女,硕士生,讲师,主要研究方向为信息安全。

3 基于组合公钥的分布式密钥管理

3.1 系统初始化

将网络中的节点分成两类：服务节点和普通节点，服务节点构成系统分布式管理中心。网络中的每个节点 P_k 都拥有一个唯一的标识符 ID_k，它可以唯一地代表节点 P_k，并且对外公开。

步骤 1　可信第三方选取安全椭圆曲线 E 的各种参数 $T=\{a,b,G,q,p\}$，其中，G 为加法群的基点，q 为以 G 为基点的群的阶。

步骤 2　选取 h 个单项映射函数 $F_i(i=1,2,\cdots,h)$。

步骤 3　产生系统的私钥种子矩阵 $SSK=[r_{ij}]_{m\times h}$，其中，r_{ij} 为任意小于 n 的整数；产生对应的公钥种子矩阵 $PSK=[R_{ij}]_{m\times h}$，且 $r_{ij}G=R_{ij}$。SSK 必须严格保密。

3.2 管理平台的构建

分布式管理平台的构建采用 Shamir 提出的基于 Lagrange 插值的门限方案，具体描述如下：

F_q 是一个有限域，其中 q 是一个大于 n 的素数之幂，设 α 是 F_q 的一个本原元。设秘密 s 属于 F_q，在 F_q 中随机选取 k 个元素 $a_1,a_2,\cdots,a_{k-1}$，其中 $a_{k-1}\neq 0$，构造一个 $k-1$ 次多项式：

$$f(x)=s+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1}$$

那么将秘密份额的集合$\{s_i:s_i=f(\alpha^i),1\leqslant i\leqslant n\}$分配给 n 个参与者，即构成一个(k,n)门限方案。

秘密恢复描述如下，先假设 k 个参与者提供了关于 s 的秘密份额 $s_{i_j}(j=1,2,\cdots,k)$，其中 i,j 互异，则由拉格朗日插值公式可得到：

$$f(x)=\sum_{j=1}^{k}s_{i_j}\prod\frac{x-\alpha^{i_j}}{\alpha^{i_j}-\alpha^{i_i}}$$

式中，$s=f(0)$。

分布式管理平台由网络中的服务节点构成，假设共有 n 个服务节点。利用 Shamir 门限方案，假设私钥种子矩阵 SSK 的门限参数为(t,n)，对于 $SSK=[r_{ij}]_{m\times h}$，每个元素 r_{ij} 都被相应地分成 n 份。

步骤 1　可信第三方随机选取 $m\times h$ 个 $t-1$ 次多项式：

$$f_{ij}(x)=r_{ij}+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}$$

式中，$i=1,2,\cdots,m,j=1,2,\cdots,h$，且满足 $f_{ij}(0)=r_{ij}$。

步骤 2　计算 $f_{ij}^{(k)}(ID_k),k=1,2,\cdots,n$。这样，私钥矩阵 $SSK=[r_{ij}]_{m\times h}$ 被分为 n 个 $m\times h$ 矩阵，即 $SSK_1,SSK_2,\cdots,SSK_n$，其中 $SSK_k=[f_{ij}^{(k)}(ID_k)]_{m\times h}$ 不难证明，$(SSK_1,SSK_2,\cdots,SSK_n)$构成系统私钥矩阵 SSK 秘密份额。

步骤 3　可信第三方通过安全通道向服务节点分发以下参数：(1) 椭圆曲线 E 的参数值 T；(2) 映射函数 $F_i(i=1,2,\cdots,h)$；(3) 公钥种子矩阵 PSK；(4) 私钥种子矩阵 SSK_k。

步骤 4　可信第三方通过安全通道向普通节点分发以下参数：(1) 椭圆曲线 E 的参数值 T；(2) 映射函数 $F_i(i=1,2,\cdots,h)$；(3) 公钥种子矩阵 PSK。

步骤 5　可信第三方完成上述操作后退出系统。

3.3 节点公私钥的生成

假设节点 P_0 要获取自己的私钥，首先选取 t 个邻居服务节点 $P_1,P_2,\cdots,P_t$，按以下步骤获取自己的私钥。

步骤 1　将自己的身份信息 ID_0 在单项映射函数 $F_i(i=1,2,\cdots,h)$的作用下映射为 h 个映射值，即 $m_i=F_i(ID_0)\bmod m$，其中 $i=1,2,\cdots,h$，然后将 m_i 传送给 t 个邻居服务节点。

步骤 2　各邻居服务节点 $P_k(k=1,2,\cdots,t)$收到 $m_i(i=1,2,\cdots,h)$后，将 m_i 作为行号，从自己的私钥种子矩阵份额 SSK_k 中依次取出相应矢量 $r_{m_1,1}^{(k)},r_{m_2,2}^{(k)},\cdots,r_{m_h,h}^{(k)}$ 计算 $sk_0^{(k)}=(r_{m_1,1}^{(k)}+r_{m_2,2}^{(k)}+\cdots+r_{m_h,h}^{(k)})\bmod p$，并把 $sk_0^{(k)}$ 传至 P_0 节点。

步骤 3　节点 P_0 将接收到的 t 个私钥矩阵秘密份额：$sk_0^{(1)},sk_0^{(2)},\cdots,sk_0^{(t)}$，利用 Lagrange 插值公式，计算节点 P_0 的私钥为：

$$sk_0=\sum_{k=1}^{k=t}l_k(0)sk_0^{(k)}$$

步骤 4　节点 P_0 的公钥为 $pk_0=(R_{m_{1,1}}+R_{m_{2,2}}+\cdots+R_{m_{h,h}})$。

3.4 种子矩阵份额的更新

合谋攻击是分布式密钥管理密钥的最大威胁，潜在的攻击对手始终存在，且很难发现，极有可能与退出系统的服务节点进行联合攻击，恢复并窃取系统的私钥矩阵。可以采用两种方法来解决这一问题：1)定期更新系统的公、私钥矩阵，需要重新将系统进行初始化，并再次进行管理中心的构建。从实用的角度来说，这个方法不可取；2)更新服务节点拥有的私钥矩阵份额 $SSK_1,SSK_2,\cdots,SSK_n$，并不改变系统私钥矩阵 SSK 和公钥矩阵 PSK。这里针对第二种方法分析私钥矩阵更新的过程。

选择某一服务节点定期向其它服务节点发送新的私钥矩阵来更新份额参数，所有服务节点利用新的私钥矩阵更新份额参数，将各自的私钥矩阵份额更新为新的私钥矩阵份额，具体步骤如下：

步骤 1　假设发起更新节点 P_u 是服务节点中的任意一个。首先，节点 P_u 秘密、随机地构造 $k-1$ 次多项式：$f_u(x)=(b_1x+b_2x^2+\cdots+b_{t-1}x^{t-1})\bmod p$，满足 $f_u(0)=0$；然后计算各服务节点的私钥矩阵份额更新参数 $f_u(ID_k),k=1,2,\cdots,n$；最后将 $f_u(ID_k)$传至除 P_u 以外的各服务节点。

步骤 2　节点 P_k 接收到 $f_u(ID_k)$后，重新计算新的私钥矩阵份额 $SSK_k'=[f_u(ID_k)+f_{ij}^{(k)}(ID_k)]_{m\times h}$。

步骤 3　节点 P_k 更新完私钥矩阵份额后，向节点 P_u 发送更新完毕回执，节点 P_u 删除秘密、随机的参数 $b_1,b_2,\cdots,b_{t-1}$。

上述步骤完成了服务节点的私钥矩阵份额的更新，但并未改变系统的私钥矩阵 SSK，因此系统的公钥矩阵 PSK 也无需改变。

4 方案分析

4.1 特点分析

无中心：系统充分考虑移动自组网的自身特点，融入分布式密钥管理的思想，采用 Shamir 的(t,n)秘密共享门限方案，

构建由 n 个服务节点组成的相互配合、相互制约的密钥管理平台。可信第三方在系统运行之前退出，不再参与具体的密钥生成、分发和更新。

无证书：系统基于组合公钥密码体制构建，摆脱了基于CA密钥管理的局限性，实现了节点身份与节点公钥的方便绑定，省去了证书生成、证书分发、证书更新和证书销毁等处理环节，减少了系统的消耗，提高了系统的实用性。

大容量：系统私钥矩阵为 $SSK=[r_{ij}]_{m\times h}$，根据 ECC 复合原理，可以构建 m^h 个组合私钥，能够以较小的密钥空间实现海量密钥的管理，具有很强的实用性。

可扩展：拓扑结构的动态性是移动自组网的主要特点之一，节点的加入和退出具有随机性。个别服务节点的退出不会影响系统的安全性和可用性，经过可信第三方注册的新的服务节点可快速融入系统参与运行。支持普通节点的加入和退出。

4.2 安全分析

攻击 1：攻击节点 P_a 试图通过截获节点 P_k 发送的私钥矩阵份额 $sk_0^{(k)}$ 推出节点 P_k 的私钥矩阵：$SSK_k=[r_{ij}^{(k)}]_{m\times h}$。

分析：因为节点 P_k 的私钥矩阵份额为：

$$sk_0^{(k)}=(r_{m_1,1}^{(k)}+r_{m_2,2}^{(k)}+\cdots+r_{m_h,h}^{(k)}) \bmod p$$

若想从该式中推出 $[r_{ij}^{(k)}]_{m\times h}$ 中的所有元素，显然是不现实的。

攻击 2：在生成节点公私钥阶段，攻击节点 P_a 试图发送假的私钥矩阵份额 $sk_0^{(a)}$ 来欺骗节点 P_k。

分析：节点 P_k 收到节点 P_a 的私钥份额后，会对其有效性进行验证。首先检查节点 P_a 的身份 ID_a 在系统节点 ID 列表中是否存在，若不存在，则删除 $sk_0^{(a)}$；然后通过 $sk_0^{(a)}G=R_{m_e,1}+R_{m_e,2}+\cdots+R_{m_e,h}$ 来验证 $sk_0^{(a)}$ 的真实性，若 $sk_0^{(a)}$ 是假冒的，上面等式肯定不成立。

攻击 3：攻击节点 P_a 试图通过截获 t 个服务节点发送给节点 P_k 的私钥矩阵份额 $sk_0^{(k)}$，$k=1,2,\cdots,t$，恢复出节点 P_k 的私钥 sk_0。

分析：假设节点 P_a 接收到 $sk_0^{(1)}$，$sk_0^{(2)}$，$\cdots$，$sk_0^{(t)}$ 共 t 个私钥矩阵秘密份额，而 $sk_0=\sum_{k=1}^{k=t} l_k(0)sk_0^{(k)}$，因为节点 P_a 无法得到 $\sum_{k=1}^{k=t} l_k(0)$，所以 P_a 不能恢复节点 P_k 的私钥 sk_0。

攻击 4：在私钥矩阵份额更新过程中，攻击节点 P_a 通过截获私钥矩阵份额更新参数，获取新的私钥矩阵份额。

分析：攻击节点 P_a 截获更新服务节点发送的私钥矩阵份额更新参数 $f_u(ID_k)$，$k=1,2,\cdots,n$ 后，需要联合自己旧的私钥矩阵份额才能获取新的私钥矩阵份额。

$$SSK_k'=[f_u(ID_k)+f_{ij}^{(k)}(ID_k)]_{m\times h}$$

因为 P_a 没有旧的私钥矩阵份额，所以无法得到新的私钥矩阵份额。

4.3 效率分析

椭圆曲线密码体制相对于 RSA、DSA 等公钥密码体制，具有单位比特较高强度的安全性，这意味着椭圆曲线密码体制可以使用较短的密钥满足较高的安全性需求。同时，短密钥将有助于提升系统性能，降低对系统存储空间和传输带宽的需求。

节点公钥的生成依托 ECC 复合原理，因为系统公钥矩阵 SPK 和单项映射函数 $F_i(i=1,2,\cdots,h)$ 是公开的，所以节点公钥的生成方便、快捷，且无需存储，若需要即可随时生成。

服务节点私钥种子矩阵份额的更新是在不改变系统私钥矩阵的情况下进行的，发起更新节点只需将更新参数传递给其它服务节点即可，整个过程计算量小，更新方便。

私钥种子矩阵份额更新在 NS-2 模拟器下做如下测试：100 个移动节点在边长 800m 的正方形区域内，以(0～20)m/s 的速度自由移动，节点停留时间在 0～100s 之间，门限阈值为(5,10)，仿真运行时间为 15min。

测试表明：只要节点的移动速度适中，方案提出的私钥矩阵份额更新的成功率接近 100%，而文献[3]与文献[5]提出的私钥份额更新的成功率相对低一些，且随着节点数量的增加而降低。图 1 比较了节点移动速度在 10m/s 的情况下 3 种方案各自的私钥份额更新成功率。

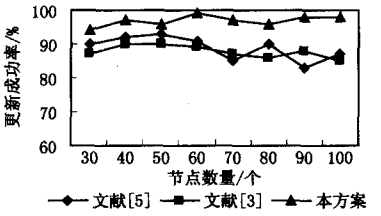

图 1 节点移动速度 10m/s 的更新成功率

结束语 针对移动自组网的特点，本文结合组合公钥密码体制提出了一种分布式密钥管理方案。方案没有集中的管理中心，无需以证书的形式绑定节点公钥，安全性高、扩展性强、计算量小，特别适用于移动自组网环境。下一步需实现方案的原型系统以进一步检验可用性、安全性和适用性。

参 考 文 献

[1] Zhou L, Hass Z J. Securing Ad-hoc networks[J]. IEEE Network Magazine, 1999, 13(6): 24-30

[2] Yi S, Naldurg P, Kravets R. Security-aware Ad hoc routing for wireless networks[R]. UIUCDCS-R-2002-2290. U. S., UIUCDCS, 2002

[3] Zhang Yu-chen, Liu Jing, Wang Ya-di, et al. Identity-based threshold key management for Ad hoc networks [C]// Proceedings of PACIIA 2008. U. S: IEEE Computer Society, 2008: 797-780

[4] Zhang Yu-chen, Liu Jing, Wang Ya-di, et al. Distributed key management based on elliptic curve cryptography for Mobile Ad-hoc network[C]// Proceedings of ICCSE 2008. Xiamen: Xiamen University Press, 2008: 779-782

[5] 张玉臣，刘璟，马自堂，等. Ad hoc 网络环境下基于 ECC 的分布式密钥管理[J]. 武汉大学学报，2009，55(1)：85-88

[6] Wang G, Chao G. Compromise-resistant pairwise key establishment for mobile Ad hoc networks[J]. ETRI Journal, 2006, 28(3): 375-378