第35卷 第10期 计 算 机 工 程 2009年5月
Vol.35 No.10 Computer Engineering May 2009
·安全技术· 文章编号：1000—3428(2009)10—0150—02 文献标识码：A 中图分类号：TP393

# 基于无证书密码学的移动自组网密钥管理

孙 磊，戴紫珊
(解放军信息工程大学电子技术学院，郑州 450004)

**摘 要：**在分析现有的Ad Hoc网络密钥管理方案存在的缺陷基础上，基于无证书密码学提出一个Ad Hoc网络密钥管理方案。将系统主密钥分发给一组预选节点，由其合作实现私钥生成中心PKG功能。该方案有效地克服密钥托管问题与恶意节点的合谋攻击，同时一次单播即可安全高效地实现节点私钥更新。分析与仿真结果表明其具有较高的安全性和实用性。

**关键词：**移动自组网；秘密共享；无证书的密码学；密钥管理；密钥托管

# Key Management Based on Certificate-less Cryptography in Mobile Ad Hoc Networks

SUN Lei, DAI Zi-shan
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

**【Abstract】** Based on the analysis of existing key management model to Ad Hoc networks, a key management scheme based on certificate-less cryptography is proposed, which employs the secret sharing technique to distribute system key among a pre-selected set of nodes, which offers a collaborative private-key-generator service. The scheme can strongly overcome the key escrow and resist coalition of adversaries. The construction method ensures secure and efficient network-wide key update by single broadcast. The analysis and simulation results show the scheme is secure and effective.

**【Key words】** mobile Ad Hoc networks; secret sharing; certificate-less cryptography; key management; key escrow

## 1 概述

移动自组网是一种新颖的移动通信网络，其自身特性使其具有巨大发展前景。但无线信道的脆弱性、网络拓扑结构的动态性以及无中心、无基础设施等移动自组网本身的特性很难部署集中式认证机构。

文献[1]基于门限密码学技术提出了URSA方案。该方案允许任何节点携带系统密钥的一个分量来公平地分配负荷，增强了服务可用性。但该系统易受Sybil攻击，这种攻击方式能够获得大量的身份从而收集足够多的分量重构系统密钥，且系统易受合谋攻击。URSA基于证书实现公钥与实体身份关联，这种方式在证书管理过程中需很高的计算与存储开销。

文献[2]提出的方案可以解决公开信道传输私钥的问题，但其缺点是方案中的所有网络节点必须参与生成用户私钥。同样，在新节点加入网络时，也必须保证所有节点在线，而且所有节点的私钥都需要更新，因此，该方案不能满足移动Ad Hoc网络动态性的要求，且通信开销过大。

文献[3]提出了基于身份密码学的AC-PKI方案。方案可以有效地应对Sybil攻击，但未讨论节点私钥更新，也未能解决基于身份密码学中的密钥托管问题，因而存在恶意节点合谋攻击。

本文基于无证书密码学[4]提出一个Ad Hoc网络密钥管理方案。方案引入离线PKG，其功能是实现网络初始化。PKG并不参与密钥更新、撤销等管理，因此与Ad Hoc网络自组特性并不违背。系统中主密钥由系统中初始化的预选节点(D-PKGs)集 $\Omega$ ($|\Omega|=n$, $n<N$, $N$ 为网络节点数)持有，节点持有的公私钥由用户获取的D-PKGs部分私钥与自己所选定的秘密值结合起来计算得出，这样可以有效解决基于身份的密码学中的密钥托管与网络恶意节点合谋。

## 2 基于无证书的密钥管理方案

### 2.1 双线性对

令 $G_1$ 为由 $P$ 生成的循环加法群，阶为 $q$，$G_2$ 是具有相同阶 $q$ 的循环乘法群，$a$, $b$ 是 $Z_q^*$ 中的元素，设 $G_1$ 和 $G_2$ 这2个群中的离散对数问题都是困难问题，双线性对是指满足下列性质的一个映射 $\hat{e}: G_1 \times G_1 \to G_2$：

(1)双线性性：$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$。

(2)非退化性：存在 $P,Q\in G_1$，使 $\hat{e}(P,Q)\neq 1$。

(3)可计算性：对所有的 $P,Q\in G_1$，存在有效的算法计算 $\hat{e}(P,Q)$。

双线性映射 $e$ 可通过有限域上的超椭圆曲线上的Tate对Weil对来构造。

### 2.2 系统初始化

考虑一个包含 $N$ 个节点的网络，节点集合标识为 $\Psi(|\Psi|=N)$，随着节点加入或离开，网络节点数 $N$ 动态可变。在初始化阶段，系统存在一个可信PKG为网络的节点分发密钥，节点 $A\in\Psi$ 有全网唯一标识 $ID_A$，通常可以是节点MAC地址或IP地址；将网络运行时间设为连续的，不相重叠的密钥更新时段 $p_i$ ($1\le p_i\le M$，任一更新时段 $p_i$ 与非零串 $phase_i$

**作者简介：**孙 磊(1973－)，男，讲师、博士，主研方向：无线网络安全；戴紫珊，副研究员、硕士

**收稿日期：**2008-10-28 **E-mail：**Sl0221@sina.com

相关，且 $phase_i = phase_{i-1}+1$， $i \in [2,M]$ )。

本文方案中所用到的相关标识符号有 $f(x)$ ：$t-1$ 次多项式； $G_1, G_2$ ： $q$ 阶循环群； $ID_A$ ：节点 $A$ 的身份标识； $\Omega$ ：密钥生成中心 D-PKGs 集合； $P$ ： $G_1$ 生成元； $s$ ：系统主密钥； $H_1, H_2$ ：安全的哈希函数； $s_V$ ：D-PKG $ID_V$ 对 $s$ 的共享份额；$\Psi$ ：网络节点集；$W_s^V$ ：验证参数 $W_s^V = s_V P \in G_1$ ；$P_{pub}$ ：系统公钥 $P_{pub} = sP$ ； $t,n$ ：秘密共享参数； $phase_i$ ：第 $i$ 个密钥更新时段非零串；$P_{ID}$ ：节点的公钥；$|X|$ ：集合元素个数； $S_{ID}$ ：节点的完整私钥； $D_{ID}$ ：节点的部分私钥； $\|$ ：消息串接操作。

PKG 选取系统参数，包括：阶为 $q$ 的由 $P$ 生成的循环加法群 $G_1$， $G_2$ 是具有相同阶 $q$ 的循环乘法群，双线性映射 $e: G_1 \times G_1 \to G_2$ ，定义 2 个安全的 Hash 函数：$H_1: \{0,1\}^* \to G_1$ ，$H_2: G_2 \to \{0,1\}^*$ 。

PKG 随机选取 $s \in Z_q^*$ 作为系统主密钥，计算公钥 $P_{pub} = sP \in G_1$ 。PKG 公开系统参数：

$$params = < P, P_{pub}, e, G_1, G_2, H_1, H_2 >$$

PKG 选取随机多项式： $f(x) = \sum_{i=0}^{t-1} a_i x^i \pmod q$ ，且 $f(0) = s$ ，任意选择包含 $n$ 个节点的子集 $\Omega \in \Psi$ 为方案中的预选节点 D-PKGs ($t \le n < |\Psi| = N$) ，对 $n$ 个 D-PKGs 节点 $ID_V \in \Omega (|\Omega| = n)$ ，PKG 计算并分发子密钥 $s_V = f(ID_V) \bmod q$ ，并广播参数 $W_s^V = s_V P \in G_1$ 。

对任意包含 $t$ 个或多于 $t$ 个节点的子集 $A \in \Omega$ 可以恢复多项式：

$$f(x) = \sum_{V \in A} \lambda_V(x) s_V \pmod q$$

其中， $\lambda_V(x) = \prod_{S \in A \setminus \{V\}} \frac{ID_S - x}{ID_S - ID_V}$ 为插值系数。

在初始化阶段，PKG 节点分发部分私钥：

$$D_V = sH_1(ID_V \| phase_0) = sQ_V$$

节点选取一个秘密数值 $x_V \in Z_q^*$ ，节点 $ID$ 的完整私钥为 $S_V = < D_V, x_V >$ ，节点公钥为 $P_V = x_V P$ 。

初始化完成，网络所有节点持有如下信息：

(1)公共参数： $params = < P, P_{pub}, e, G_1, G_2, H_1, H_2 >$ ；

(2)公私钥对： $< P_{ID}, S_{ID} >$ ；

(3)与时间段相关的非零字符串： $phase_0$ ；

(4)参数 $W_s^V$ ， $\{W_s^V = s_V P \in G_1 \mid V \in \Omega\}$ 。

除以上信息，预选节点 D-PKGs 持有系统共享子密钥 $s_V$ ，任何其他节点都不能通过 $W_s^V$ 获取 $s_V$ 。

### 2.3 节点密钥更新

为对抗移动对手攻击，网络节点需要定期更新节点公私密钥对 $< P_{ID}, S_{ID} >$ 。其算法与节点加入系统时类似，节点更新示意图如图 1 所示。

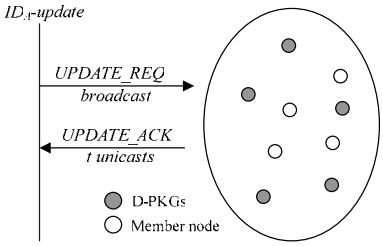


**图 1　节点私钥更新**

设网络运行至时间段 $phase_i$ ，节点 $ID_A$ 需要更新其公私密钥对 $< P_A, S_A >$ ， $ID_A$ 执行以下操作步骤：

**Step1** 选取随机数 $r_A \in Z_q^*$ ，计算：

$$R = r_A P \ , Q_A = H_1(ID_A \| phase_i)$$

**Step2** 节点 $ID_A$ 向网络预选 D-PKGs：

$$V \in \Omega (|\Omega| = n,\ t \le |V| \le n)$$

广播私钥更新请求消息：

$$REQ_{update} = \{Q_A, R\}$$

其中， $phase_i = phase_{i-1} + 1$ 。

收到此请求消息的预选节点 $ID_X$ 执行如下操作：

**Step3** 选取随机数 $r_x \in Z_q^*$ ；计算 $ID_A$ 的私钥信息 $m = s_x Q_A$ ， $s_x$ 为 $ID_X$ 的主密钥共享。

**Step4** $ID_X$ 对请求消息加密，向 $ID_A$ 返回部分更新应答消息密文对 $\sigma$ ，其中， $\sigma = < U, V > = < m + r_x R, r_x P >$ 。

节点 $ID_A$ 在收到更新应答密文消息后执行如下步骤：

**Step5** 解密消息得到 $ID_X$ 签发的部分私钥信息 $m$ ：

$$m = U - r_A V = s_x Q_A$$

**Step6** 根据参数 $W_s^V$ 及双线性性质验证其部分私钥的 $m$ 正确性，若 $\hat{e}(s_X Q_A, P) = \hat{e}(Q_A, W_s^x)$ 成立，则接受，否则认为 $\sigma$ 不合法。

**Step7** $ID_A$ 在收到 $t$ 个通过验证的解密消息后重构部分私钥：

$$D_A = \sum_{X \in V} \lambda_X(0) s_x Q_A = sQ_A$$

**Step8** 节点 $ID_A$ 的私钥是 $S_A = < D_A, x_A >$ ，公钥 $P_A = x_A P$ 保持不变。

方案中节点 $ID_A$ 只需一次单播即可实现私钥更新。

下面主要从密钥更新时请求节点与应答节点处理时间分析算法执行效率，这里处理时间包括对运算($P$)、映射到椭圆曲线上点的杂凑函数运算($MtP$)、群 $G_i$ 上的数乘运算($sM$)、群 $G_i$ 上的指数运算($Ei$)、群 $G_i$ 上的乘法运算($gM$)、群 $G_i$ 上的点加运算($pA$)。相对于上述操作，其他运算如异或运算、一般杂凑运算等可忽略不计。方案中节点间的密钥更新算法复杂度为：若请求更新节点为 $1sM+1Mtp+t(1sM+1pA+1P)+O(n)$，则 D-PKGs 节点为 $3sM+1pA$。

## 3　仿真实验

本文采用 NS-2 模拟器实现了方案的节点私钥更新算法。仿真环境链路可靠性为 90%，网络节点数 $N = 50$ ，预选节点 D-PKGs 数 $n = 20$ 。图 2 和图 3 分别是门限值 $t = 5$ 与 $t = 7$ 时的节点更新延迟与成功率性能对比。

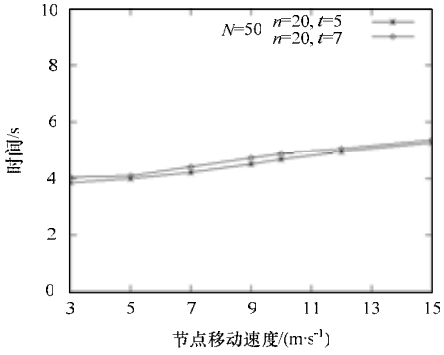


**图 2　单个节点密钥更新延迟**

(下转第 154 页)