无可信中心的门限追踪 ad hoc 网络匿名认证

刘方斌[1]，张琨[1]，李海[2]，张宏[1]
(1. 南京理工大学 计算机科学与技术学院，江苏 南京 210094；2.南京炮兵学院 计算机教研室，江苏 南京 211132)

摘 要：为解决 ad hoc 网络中的匿名认证问题，将民主签名与无中心的秘密分享方案相结合，提出一种无可信中心的门限追踪 ad hoc 网络匿名认证方案。方案的无中心性、自组织性很好地满足了 ad hoc 网络的特征，从而解决了传统网络中匿名认证方案由于需要可信中心而不适合 ad hoc 网络的问题；方案中认证者的匿名性、可追踪性和完备性（不可冒充性）满足了匿名认证的安全需求。

关键词：匿名认证；无可信中心；ad hoc 网络；追踪性；门限性
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2012)08-0208-06

Threshold traceability anonymous authentication scheme without trusted center for ad hoc network

LIU Fang-bin[1], ZHANG Kun[1], LI Hai[2], ZHANG Hong[1]
(1. Institute of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China;
2. Computer Department, Nanjing Artillery Academy, Nanjing 211132, China)

Abstract: In order to provide anonymous authentication for ad hoc network, democratic group signatures with centerless secret sharing scheme and proposed a threshold traceability anonymous authentication scheme without trusted center for ad hoc network were combined. The scheme was centerless and self-organized, which was well suited to the characters of ad hoc network and had solved the problem that those schemes of traditional network were not suited to the ad hoc network. The prover of the scheme was anonymous, traceable, and complete, which well satisfied the security of anonymous authentication.

Key words: anonymous authentication; without trusted center; ad hoc network; traceability; threshold

1 引言

Ad hoc 网络由于具有不需要基础设施、自组织、自管理等特点，使其在军事战场、抢险救灾等环境中得到越来越多的应用。但由于 ad hoc 网络自身的特性，如使用无线信道作为传输介质，使其安全性面临很大的威胁，其中节点身份的匿名性（私密性），得到越来越多的关注，如 ANODR[1]、A3RP[2]等协议。在 ad hoc 网络环境下，通信中节点身份的匿名性研究比较多，如 ANODR[1]等匿名路由协议，而在认证中节点身份的匿名性研究较少；且由于 ad hoc 网络的自组织性、无中心性，使传统网络中的基于可信中心的匿名认证方案不再适合，所以提出新的适合 ad hoc 网络的匿名认证方案非常有必要。

Jung 等[2]提出的 A3RP 协议，以及田子健等[3]提出的动态可追踪的匿名认证方案，虽能提供匿名认证，但它们都需要一个可信中心 TA 参与匿名认证，导致权利过于集中以及单点失效等问题，这与 ad hoc 网络的无中心性相违背；Zhimin 等[4]将可信计算及 One-Way Accumulator 引入匿名认证中，降低了协议计算量，且不需要可信第三方参与，但示

收稿日期：2011-04-01；修回日期：2012-05-08

证者（被认证者）身份无法追踪；为了解决 ad hoc 网络中节点匿名认证及示证者追踪问题而又不引入可信第三方，本文提出一种无可信中心的门限追踪 ad hoc 网络匿名认证方案。方案提供对任意节点合法性的认证，而不暴露示证者身份；通过门限机制实现任意 k 个合法节点可联合追踪示证者身份，而不需要管理员等可信第三方参与，亦不会导致任意合法节点都可追踪示证者身份的过于自由、随意性等问题；方案的整个执行过程，不需要可信第三方参与，完全符合 ad hoc 网络的无中心、自组织、自管理等特性。

2　无可信中心的门限追踪匿名认证模型及安全要求

定义 1　认证方案的匿名性：示证者不暴露自己的身份而能向验证者证明自己身份的合法性。

定义 2　认证方案的可追踪性：在需要的情况下，能够根据陷门信息及验证者提供的信息，恢复出示证者的身份。

定义 3　无可信中心性：从方案的初始化开始，整个方案不涉及可信中心。

Ad hoc 网络中一群体组织 $U=\{u_1,u_2,\cdots,u_n\}$，U 中无任何可信中心，其中，u_i 是此组织的成员节点，且为图灵机。群组织为一连通网络（可以弱化为：群组织中的任意 2 个节点，借助于网络中的其他节点（非群组织成员亦可）实现连通即可）。网络初始化结束后，各节点已分配合法公钥，且各合法节点互相知道对方的公钥。（公钥的管理，可使用文献[5,6]中的方案，此类方案使用门限机制实现密钥管理，与本协议相结合使用，可节省通信管理代价。）假设系统中各节点使用不同的公钥实现签名和加密。

匿名认证阶段，任意节点 u_P 向任意节点 u_V（u_V 可以不属于 U）证明它属于组织 U，但不透露 u_P 的身份。若想知道已通过匿名认证的节点 u_P 的身份，则必须经 U 中至少 k 个节点同意，方可恢复出 u_P 的身份，实现 u_P 身份的追踪。

整个模型包括如下过程。

1) 初始化：群组织中各成员生成自己的签名公私钥对，并相互协作建立群公钥及群共享秘密（匿名认证中的追踪陷门信息）。

2) 匿名认证过程：示证者利用自己的签名私钥及群公钥生成一个签名，验证者对示证者的签名进行验证，整个过程不暴露示证者的身份信息。

3) 追踪算法：k 个成员联合利用追踪陷门等信息恢复出示证者身份。

4) 新成员加入算法：新成员与群组织中各成员相互协商，以更新群公钥、群追踪陷门等信息。

5) 成员撤销算法：节点离开后，剩余节点相互协商以更新群公钥、群追踪陷门等信息。

一个无可信中心的陷门追踪 ad hoc 网络匿名认证方案是安全的，若满足以下条件。

1) 正确性：群组织中任意一个成员执行匿名认证中的签名算法后，输出的签名都能通过匿名认证中的签名验证算法。

2) 匿名性：任意一个匿名认证过程中，验证者不能以大于 $\frac{1}{n}$ 的概率识别示证者的真实身份，其中，n 为组织中成员个数。

3) 可追踪性：群组织中任意 k 个合法成员，可联合恢复出已通过认证的示证者身份。

4) 完备性：任何不属于组织 U 的节点，皆不能通过匿名认证。

5) 追踪的(k, n)门限性：必须至少 k 个合法成员联合，方可追踪示证者身份。

6) 无可信中心性：从系统建立至匿名认证及身份追踪，皆不需要可信第三方的参与。

3　相关技术介绍

3.1　假设

离散对数假设：设 G 为 g 生成的一个阶为 q 的循环群。不存在概率多项式时间算法 A，其能以不可忽略的概率从 g^a 计算出 a。

确定的 Diffie-Hellman(DDH）假设：设 G 为 g 生成的一个阶为 q 的循环群。不存在概率多项式时间算法 A，其能以不可忽略的概率区分出分布 D 和 R，$D=(g,g^a,g^b,g^c)$，$R=(g,g^a,g^b,g^{ab})$，$a,b,c\in_R Z_q$。

3.2　民主签名

使用群签名实现匿名认证是最直接的方法。群签名概念最初由 Chaum 和 Heyst 提出[7]，目前较好的群签名方案由 Ateniese[8]等提出。群签名实现匿名认证，群管理员可以实现示证者身份的追踪。由于群管理员的特殊身份，将会导致权利过于集中、权利滥用以及单点失效等问题，所以必须对群管理员加以约束。

民主签名[9]由 Manulis 于 2006 年提出，其中任

意成员可代表群进行签名，群内任意成员可从给定的有效群签名中恢复出签名者的身份。若使用民主签名实现匿名认证方案，则群中任意成员可恢复出示证者的身份，追踪示证者。这种追踪能力过于自由必将导致不受控制的滥用，所以必须对群成员的这种追踪能力加以控制。

将群签名中管理员权利过于集中与民主签名中成员追踪能力过于自由进行折衷，提出具有门限追踪能力的匿名认证方案，使得至少 k 个群成员同意恢复示证者身份时，方能追踪到示证者身份。

3.3 秘密共享

(k, n)门限秘密共享是指将一个秘密 s 分成 n 个份额 $s_1, s_2, \cdots, s_n$，并将这些秘密份额秘密地分发给 n 个用户，使得发生如下情况。

1) 由 k 个或多于 k 个用户拥有的秘密份额 s_i 可以恢复出秘密 s。

2) 由少于 k 个用户持有的秘密份额 s_i 不能获得关于秘密 s 的任何信息。这里 k 称为门限，且 $1 \leqslant k \leqslant n$。

Shamir[10]于 1979 年提出的基于多项式拉格朗日插值的(k, n)门限方案。该方案有如下 2 个缺点：1)不能检测可信中心分发假的份额给用户；2)该方案需要一个可信的中心。随后 Feldman 提出了可验证秘密共享方案，Pedersen[11]提出了无可信中心的秘密共享方案。由于 ad hoc 网络的无中心性、自组织性等特点，本文选用 Pedersen 的无可信中心的秘密共享方案，并将其应用于匿名认证方案中，从而实现本方案的门限追踪能力。

4 匿名认证协议

借助群签名、民主签名以及无可信中心的秘密共享思想，实现了无可信中心的门限追踪 ad hoc 网络匿名认证方案。本方案主要包括系统初始化、匿名认证、示证者追踪、新成员加入以及成员吊销等过程。

4.1 系统初始化

系统初始化的目的是建立各节点签名公私钥对、群共享秘密 S（匿名认证中的追踪陷门）、群公钥 P_U。

1) 选取素数 q，G 为 q 阶循环群，其上离散对数问题是困难的，g 为生成元；k 是门限值，n 是用户数；散列函数 $H: \{0,1\}^* \to \{0,1\}^{k_0}$，$k_0$ 为安全参数。

2) 节点 u_i 选取 $S_i \in Z_q$ 作为自己的签名私钥，计算对应的签名公钥为 $P_i = g^{S_i}$。

3) u_i 在 Z_q 上选择 $k-1$ 次多项式 $f_i(x) = a_{i0} + a_{i1}x + \cdots + a_{i,k-1}x^{k-1}$。

4) u_i 计算 $y_{ij} = f_i(j) \bmod q, 1 \leqslant j \leqslant n$, 并将 y_{ij} 秘密发送给节点 u_j，节点 u_i 保留 y_{ii}。

5) 节点 u_i 收到其他所有节点的 y_{ji}，并计算 $y_i = \sum_{j=1}^{n} y_{ji}$，$y_i$ 即是节点 u_i 的秘密份额。

6) 群共享秘密 S 的计算方法。

任意 k 个节点可利用自己的秘密份额通过拉格朗日插值法计算出群共享秘密 S，群秘密 S 即为匿名认证中的追踪陷门。

任选 k 个节点 $\{u_{1'}, u_{2'}, \cdots, u_{k'}\} \subset U = \{u_1, u_2, \cdots, u_n\}$，计算群共享秘密 $S = \sum_{i=1'}^{k'} y_i c_i$，$c_i = \prod_{j=1, j\neq i}^{k} \frac{-x_j}{x_i - x_j}$。

7) 群公钥计算方法。

任选 k 个节点 $\{u_{1'}, u_{2'}, \cdots, u_{k'}\} \subset U = \{u_1, u_2, \cdots, u_n\}$，计算 $P_0 = \prod_{i=1'}^{k'} g^{y_i c_i} = g^{\sum_{i=1'}^{k'} y_i c_i} = g^S$，则群公钥 $P_U = \{P_0, P_1, \cdots, P_n\}$。

初始化结束后，每个节点拥有自己的公私钥对 (S_i, P_i)、自己的秘密份额 y_i 以及群公钥 P_U。

4.2 匿名认证过程

节点 u_P 想向节点 u_V 证明自己属于组织 U，则 u_P 使用自己的签名私钥及群公钥生成一群签名，并把此签名交给 u_V 验证，若验证通过则说明 u_P 属于组织 U，否则 u_P 不属于组织 U。匿名认证过程主要包括签名生成算法和签名验证算法。

1) 示证者 u_P 签名的生成算法

参照民主签名[9]，给出如下签名算法，算法的输入为 u_P 的私钥 S_p、群公钥 P_U，待签名消息为 $m \in \{0,1\}^*$，u_P 执行如下计算。

①选择随机数 $r \in_R Z_q$，计算 $x_0 = g^r$，$y_0 = P_0^r P_P$。

②选择随机数 $r_{1i} \in_R Z_q$，$r_{2i} \in_R Z_q$，$1 \leqslant i \leqslant n$，$c_1, c_2 \cdots c_{P-1}, c_{P+1}, \cdots c_n \in_R \{0,1\}^k$。

③ $x_P = P_0^{r_{1P}}, y_P = g^{r_{2P}}, z_P = g^{r_{1P}}$。

④ $j \neq P$ 时，$x_j = y_0^{c_j} P_0^{r_{1j}} g^{r_{2j}}$，$y_j = P_j^{c_j} g^{r_{2j}}$，$z_j = x_0^{c_j} g^{r_{1j}}$。

⑤ c_P 满足：

$c_1 \oplus c_2 \oplus \cdots \oplus c_n = H(g, P_0, x_0, y_0, x_1, \cdots, x_{P-1}, x_P y_P, x_{P+1}, \cdots x_n, y_1, \cdots, y_n, z_1, \cdots, z_n, m)$;

⑥ $s_{1P} = r_{1P} - c_P r$, $s_{2P} = r_{2P} - c_P S_P$。

⑦ $j \neq P$ 时， $s_{1j} = r_{1j}, s_{2j} = r_{2j}$。

⑧生成对消息 m 的签名： $\text{sign}(m) = (x_0, y_0, c_1, \cdots, c_n, s_{11}, \cdots, s_{1n}, s_{21}, \cdots, s_n)$，并将 $\text{sign}(m)$ 发送给 u_V。

2) 签名验证算法

u_V 接收到 $\text{sign}(m)$ 后，利用群公钥 P_U 以及消息 m，验证如下等式是否成立：

$$c_1 \oplus c_2 \oplus \cdots \oplus c_n = H(g, P_0, x_0, y_0, y_0^{c_1} P_0^{s_{11}} g^{s_{21}}, \cdots, y_0^{c_n} P_0^{s_{1n}} g^{s_{2n}}, P_1^{c_1} g^{s_{21}}, \cdots, P_1^{c_n} g^{s_{2n}}, x_0^{c_1} g^{s_{11}}, \cdots, x_0^{c_n} g^{s_{1n}}, m)$$

如果成立，则签名认证通过，说明 u_P 是 U 中合法节点；否则认证不通过。在此身份认证过程中，验证者只能确定示证者是群中的某个成员，而不能确定是哪一个成员，即实现了示证者身份的匿名性。

4.3 示证者身份追踪算法

为了在必要情况下实现示证者身份的追踪，组织 U 中的任意 k 个成员 $\{u_{1'}, u_{2'}, \cdots, u_{k'}\} \subset U = \{u_1, u_2, \cdots, u_n\}$，可联合利用群追踪陷门恢复出示证者的身份，具体步骤如下。

1) k 个节点使用自己的秘密份额 $y_{1'}, y_{2'}, \cdots, y_{k'}$， x_0 以及对应的 $c_{1'}, c_{2'}, \cdots, c_{k'}$ 联合计算出 $T = x_0^S = \prod_{i=1'}^{k'} x_0^{y_i c_i}$ 。

2) $P_P = \dfrac{y_0}{T}$。

3) 输出示证者的签名公钥，即可得到示证者身份。

4.4 节点加入算法

新节点的加入，将导致群公钥、追踪陷门以及各节点秘密份额的更新。假设节点 u_x 想加入到组织 U 中，且组织 U 中目前节点数为 n，则执行如下步骤。

1) 节点 u_x 选取 $S_x \in Z_q$ 作为自己的签名私钥，计算对应的签名公钥为 $P_x = g^{S_x}$； u_x 在 Z_q 上选择 $k-1$ 次多项式 $f_x(x) = a_{x0} + a_{x1} x + \cdots + a_{x,k-1} x^{k-1}$，并计算 $y_{xj} = f_x(j) \bmod q, 1 \leqslant j \leqslant n+1$, 并将 y_{xj} 秘密发送给节点 u_j ,节点 u_x 保留 y_{xx}。

2) 组织 U 中原有节点 u_i 计算 $y_{ix} = f_i(x) \bmod q$, $1 \leqslant i \leqslant n$, 并将 y_{ix} 秘密发送给节点 u_x。

3) 节点 u_x 收到其他所有节点的 y_{ix}，并计算 $y_x = \sum_{i=1}^{n+1} y_{ix}$， y_x 即是节点 u_x 的秘密份额。

4) U 中原有节点更新自己的秘密份额，且新的秘密份额 $y_i' = y_i + y_{xi}, 1 \leqslant i \leqslant n$。

5) k 个节点联合利用拉格朗日插值算法，计算新的追踪陷门，进而得到新的群公钥。

4.5 节点吊销算法

由于节点的移动性等原因，致使节点离开组织 U，将导致群公钥、追踪陷门以及各节点秘密份额的更新。假设节点 u_j 离开组织 U，且 u_j 离开前 U 中的节点数为 n，则执行如下步骤。

1) 组织 U 中各节点计算新的秘密份额，且新的秘密份额为 $y_i' = y_i - y_{ji}$， $i \neq j$，且 $1 \leqslant i \leqslant n$。

2) k 个节点通过拉格朗日插值算法，计算新的追踪陷门，以及新的群公钥。

5 协议分析

5.1 协议性质分析

定理 1 匿名性：本方案在确定的 Diffie-Hellman (DDH)假设的前提下，可保证示证者的匿名性。

以下论证皆在 DDH 假设的前提下进行。r 的随机性，可保证 y_0 与示证者公钥 P_P 的无关联性。由 r_{1i}、r_{2i}（$1 \leqslant i \leqslant n$）以及 $c_1, c_2 \cdots c_{P-1}, c_{P+1}, \cdots c_n$ 的随机性，决定了 x_i、 y_i 及 z_i 的随机性。由于 c_P 由 x_i， y_i 及 z_i 决定，因此不能从 S_{1P}、 S_{2P} 中推导出示证者的公私钥，亦找不出 S_{1P}、 S_{2P} 与示证者身份的关联性，所以无法从消息 m 的签名中判断出签名者的身份。匿名性的形式化数学证明可参照文献[9]。

定理 2 可追踪性：任意 k 个合法群组织成员，可联合恢复出通过认证的示证者身份。

k 个节点使用自己的秘密份额 $y_{1'}, y_{2'}, \cdots, y_{k'}$， x_0 以及对应的 $c_{1'}, c_{2'}, \cdots, c_{k'}$ 联合计算出：

$$T = \prod_{i=1'}^{k'} x_0^{y_i c_i}$$

$$T = \prod_{i=1'}^{k'} x_0^{y_i c_i} = \prod_{i=1'}^{k'} g^{r y_i c_i} = x_0^{r \sum_{i=1'}^{k'} y_i c_i} = g^{rS} = P_0^r$$

$$\frac{y_0}{T} = \frac{P_0^r P_P}{P_0^r} = P_P$$

其中， P_P 即为示证者的公钥，根据公钥即可找到示

证者身份。

定理 3 正确性：群组织中任意一合法成员，可通过匿名认证。

生成算法及签名验证算法中的 u_P 为随机选取的，故对群中任意成员 u_X 及其对消息 m 的签名 $\text{sign}(m)$，都存在一多项式时间算法 $Verify$，使得 $Verify(S_X, P_U, m.\text{sign}(m)) = 1$（1 表示签名有效，通过匿名认证；0 表示无效）。

定理 4 完备性（不可冒充性）：非群组织成员，不能通过匿名认证。

由于匿名认证中签名算法的第 6 步需要签名者私钥的参与，而非组织成员没有合法的私钥，从而导致生成的签名不能通过验证者的验证。

定理 5 无中心性：本方案不需要可信第三方参与。

本方案各阶段皆不需要可信第三方参与。系统初始化阶段，各节点生成自己的签名公私钥，并使用无可信中心的秘密分享方案协商生成群追踪陷门及群公钥；匿名认证阶段，示证者选择相应随机数并生成签名，而验证阶段只需验证者参与；新节点加入及节点吊销阶段，只需群内各节点相互协作更新群追踪陷门及群公钥即可，所以方案这个过程没有可信第三方的参与。

定理 6 追踪的（k, n）门限性：若要追踪示证者身份，则必须至少 k 个合法节点同意参与方可。

若想恢复示证者身份，则必须得到群陷门信息。群陷门信息则由 k 个节点的秘密份额通过拉格朗日插值法方能得出。若少于 k 个节点，则不能恢复出群陷门信息，亦不能恢复出示证者的身份。示证者身份追踪的(k, n)门限性，既避免了群签名中的管理员权利过大而导致的各种问题，又避免了民主签名中各节点追踪能力过于自由而导致不受控制的滥用等问题。

定理 7 签名的无关联性：本方案中示证者 2 次提供的签名具有无关联性，可抵抗对签名的一致性攻击。

观察示证者的签名 $\text{sign}(m) = (x_0, y_0, c_1, \cdots, c_n, s_{11}, \cdots, s_{1n}, s_{21}, \cdots, s_n)$，由于每次示证者选择不同的随机数 r，使得 x_0 和 y_0 具有不可关联性；由于每次签名中 r_{1i}，r_{2i} 及 $c_1, c_2, \cdots, c_{P-1}, c_{P+1}, \cdots, c_n$ 的不同，使得 c_P 具有无关联性，进而使得 c_i，s_{1i} 及 s_{2i}（$1 \leqslant i \leqslant n$）具有无关联性，最终可以保证每次的签名具有无关联性。故不能判断 2 次签名是否出自同一示证者。

5.2 节点移动性分析

第 4.4 节及第 4.5 节的节点加入、吊销算法，很好地满足了 ad hoc 网络节点的移动性。节点加入（或者离开）群组织，将激活节点加入算法（节点吊销算法）更新群公钥、追踪陷门以及各节点秘密份额，从而保证后续的匿名认证及追踪的成功性。特别地，

1) 节点的大量离开，导致 $n<k$，此时已打破 Pedersen 的秘密共享方案，故需从新选取 k；

2) 节点的大量加入，导致 k 远小于 n，安全性下降，由于节点的大量加入，恶意节点个数超过 k 的可能性增加，而 k 个节点联合可恢复出示证者的身份，故需从新选取 k，k 的选取方式可参照 Pedersen 的秘密共享方案。

5.3 协议比较

与现有匿名认证协议相比较，本协议同时具有示证者身份的匿名性、无中心性、门限可追踪性，结果如表 1 所示。

表 1 协议性质比较

协议名	身份匿名性	无中心性	可追踪性	是否陷门可追踪
ANODR	×	√	×	×
A3RP	√	×	√	×
田等[3]协议	√	×	√	×
Zhimin 等[4]协议	√	√	×	×
本协议	√	√	√	√

5.4 匿名认证阶段计算量分析

签名算法中，计算量主要是计算 x_i、y_i 和 z_i 的指数运算，复杂度与普通的公钥运算相同，且随着群组织中成员数的增加，计算量成线性增加。分析可知，验证阶段的计算量与签名过程相同。

5.5 建立可检测秘密共享方案

系统建立阶段，若群组织内有恶意节点，发送虚假秘密 y_{ij} 以破坏秘密共享机制的建立，可通过建立可检测秘密共享方案抵制恶意节点，具体实现方案可在 4.1 节系统建立阶段，加入以下 2 步。

1) u_i 计算 $v_{ij} = g^{a_{ij}} \bmod p$，$j$=0,1,⋯,$k$−1，并广播 $\{v_{ij}\}_{j=0,1,\cdots,k-1}$。

2) u_j 验证从 u_i 处收到的秘密 y_{ij}：

$$g^{y_{ij}} = \prod_{l=0}^{k-1} b_{il}^{j^l} \bmod p$$

若等式成立，则秘密 y_{ij} 有效，否则 y_{ij} 无效。若 y_{ij} 无效，则 u_j 可广播一个对 u_i 的抱怨。

等式正确性分析：

$$\prod_{l=0}^{k-1} b_{il}^{j^l} = \prod_{l=0}^{k-1} (g^{a_{il}})^{j^l} = \prod_{l=0}^{k-1} g^{a_{il} j^l} = g^{\sum_{l=0}^{k-1} a_{il} j^l} = g^{f_i(j)} = g^{y_{ij}}$$

6　结束语

由于 ad hoc 网络的无中心性、自组织性，使传统网络中的匿名认证方案不再适合。本文提出一种适合 ad hoc 网络的匿名认证方案，本方案将民主签名与无中心的秘密分享方案应用到匿名认证中，实现了在不需要可信中心的参与下，示证者身份的匿名性、可追踪性及不可冒充性，并给出了相应的匿名认证算法、追踪算法、节点加入算法及节点吊销算法。

参考文献：

[1] KONG J J, HONG X Y, GERLA M. An identity-free and on-demand routing scheme against anonymity threats in mobile ad hoc networks[J]. IEEE Transactions on Mobile Computing, Frequency,2007, 6:888-902

[2] PAIK J H, KIM B H, LEE D H. A3RP: anonymous and authenticated ad hoc routing protocol[A]. Information Security and Assurance[C]. 2008.

[3] 田子健, 王继林, 伍云霞. 一个动态可追踪匿名认证方案[J]. 电子与信息学报, 2005,27(11): 1737-1740.
TIAN Z J, WANG J L, WU Y X. A dynamic anonymous authentication scheme with identity escrow[J]. Journal of Electronics & Information Technology, 2005,27(11): 1737-1740.

[4] XU Z M, TIAN H, LIU D S, *et al*. A ring-signature anonymous authentication method based on one-way accumulator[A]. Communication Systems, Networks and Applications[C]. 2010. 56-59.

[5] ZHOU L, HAAS Z. Securing ad hoc networks[J]. IEEE Network, 2000, 13(6): 24-30.

[6] KONG J, ZERFOS P, LUO H, *et al*. Providing robust and ubiquitous security support for mobile ad hoc networks[A]. Washington: IEEE Computer Society[C]. 2001.251-261.

[7] CHAUM D, HEYST E. Group signatures[A]. Cryptology-EUROCRYPT'91[C]. 1991. 257-265.

[8] ATENISES G, CAMENISCH J, JOYE M, *et al*. A practical and provably secure coalition-resistant group signature[A]. Cryptology-CRYPTO 2000[C]. Santa Barbara, California, USA, 2000. 255-270.

[9] MANULIS M. Democratic group Signature: on example of joint ventures[A]. Proceedings of ACM Symposium on Information[C]. 2006. 191-196.

[10] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(1):612-613.

[11] PEDERSEN T P. Non-interaetive and information-theoretic secure verifiable secret sharing[A]. Cryptology-CRYPTO'91[C]. Berlin, 1992. 129-140.

作者简介：

刘方斌（1985），男，江苏连云港人，南京理工大学博士生，主要研究方向为网络安全和路由。

张琨（1977），女，河北昌黎人，博士，南京理工大学副教授、博士生导师，主要研究方向为网络安全、网络通信和自主计算。

李海（1973），男，湖北公安人，硕士，南京炮兵学院讲师，主要研究方向为计算机网络。

张宏（1956），男，上海人，南京理工大学教授、博士生导师，主要研究方向为数据挖掘和信息安全。