doi:10.3969/j.issn.1000-436X.2012.10.004

移动 ad hoc 网络预分配非对称密钥管理方案

韩磊[1]，刘吉强[2]，韩臻[2]，魏学业[1]
（1. 北京交通大学 电子信息工程学院，北京 100044；2. 北京交通大学 计算机与信息技术学院，北京 100044）

摘 要：为了降低移动 ad hoc 网络非对称密钥管理中的通信开销，基于组合公钥思想，将 ElGamal 方案与预分配密钥方式相结合，提出一种基于身份的预分配非对称密钥管理方案(PAKMS)。该方案通过私钥生成中心为节点预分配主密钥子集及基于时间获得节点密钥更新的方式，从方法上降低了移动 ad hoc 网络非对称密钥管理中的通信开销；私钥生成中心为节点预分配主密钥子集的方式也使节点在网络运行阶段不再依赖私钥生成中心为节点分配和更新密钥。由此，弱化了基于身份密钥管理中存在的私钥托管问题对网络安全的影响。与典型方案对比分析表明，该方案在提供节点密钥更新服务的情况下能够有效降低网络通信开销。此外，对方案的安全性进行了详细证明。

关键词：移动 ad hoc 网络；安全；预分配；基于身份的密钥管理；通信开销
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2012)10-0026-09

Pre-distribution asymmetric key management scheme for mobile ad hoc networks

HAN Lei[1], LIU Ji-qiang[2], HAN Zhen[2], WEI Xue-ye[1]
(1. School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China;
2. School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China)

Abstract: In order to reduce communication overhead of the asymmetric key management in mobile ad hoc networks, an identity-based pre-distribution asymmetric key management scheme (PAKMS) was presented based on combined public key (CPK) framework, ElGamal public key cryptosystem and key pre-distribution mode. This scheme essentially reduced communication overhead of the asymmetric key management in mobile ad hoc networks by the private key generation (PKG) distributing a subset of master key for every node beforehand and a time-based key update approach. The method that PKG pre-distributed a subset of master key also made the nodes obtain their keys and key update services, which did not need to rely on online PKG. Thus, the inherent key escrow problem existing in identity-based asymmetric key management was avoided to some degree. Compared with typical schemes, this scheme needed much less communication overhead to accomplish node key update service. Furthermore, security proof of the scheme was described in detail.

Key words: mobile ad hoc network; security; pre-distribution; identity-based key management; communication overhead

1 引言

移动 ad hoc 网络（MANET, mobile ad hoc network）是一种由移动节点组成的无固定网络基础设施和中心信任机构的自组织网络，广泛应用于军事通信和灾难救援等没有固定网络基础设施的环

收稿日期：2011-08-19；**修回日期**：2011-12-16
基金项目：国家自然科学基金资助项目（60973112）；中央高校基本科研专项基金资助项目（2011JBM031）
Foundation Items: The National Natural Science Foundation of China (60973112); The Fundamental Research Funds for the Central Universities (2011JBM031)

境。MANET 具有如下特点[1]：移动性、网络拓扑结构动态变化、有限的节点计算资源、多跳无线通信、无固定网络基础设施等。这些特点在保障 MANET 灵活应用的同时也使 MANET 面临诸多挑战[2]，尤其随着 MANET 组网技术的发展及应用环境对网络安全需求的提高，增强 MANET 安全已经成为一个亟待解决的问题。

基于身份的加密(IBE, identity-based encryption)思想[3]由 Shamir 于 1984 年提出，主要目标是寻找一种非对称加密算法使得公钥可以为任意的字符串以简化密钥管理过程。2000 年，Boneh 和 Franklin 提出了使用 Weil 来实现 IBE 的一个实用方案[4]。此后，在 MANET 中出现了大量基于 IBE 的密钥管理方案[5~9]。在基于 IBE 的 MANET 密钥管理方案中，公钥是标识节点身份的信息(如地址、名字等)，不依赖可信认证机构(CA, certification authority)为节点颁发公钥证书。所以，从方法上简化了 MANET 中节点的密钥管理过程，但基于 IBE 的 MANET 密钥管理方案还存在以下主要问题。1)现有基于 IBE 的非对称密钥管理方案主要采用分布式私钥生成(PKG, private key generation)中心结合门限密码学的方式，将 PKG 的功能分散到网络的多个节点中，这种方式从本质上改善了传统非对称密钥管理中基于 CA 或分布式 CA 系统的复杂性，也有效避免了密钥服务的单点失败。但是，网络中需要密钥服务的节点需要和多个节点通信，带来了大量的网络带宽和节点能量损耗。因此，在 MANET 中设计高效、低能耗的密钥管理方案是增强 MANET 安全性和可用性的一个重要问题。2)密钥托管问题。基于 IBE 的密钥管理方案由于 PKG 能够计算出节点的私钥，所以 PKG 可以解密发向节点的密文或冒充该节点。因此，密钥托管是 MANET 中增强网络安全的另一个需要考虑的问题。

本文从以上 2 个问题着手，借鉴组合公钥(CPK, combined public key)思想[10]在 MANET 中提出一种基于身份的预分配非对称密钥管理方案(PAKMS, identity-based pre-distribution asymmetric key management scheme)。该方案通过私钥生成中心为节点预分配主密钥子集及通过基于时间获得节点密钥更新的方式，从方法上降低了移动 ad hoc 网络中非对称密钥管理的通信开销；私钥生成中心为节点预分配主密钥子集的方式也使节点在网络运行阶段不再依赖私钥生成中心为节点分配和更新密钥。由此，弱化了基于身份密钥管理中的私钥托管问题对网络安全的影响。与 MANET 中典型基于对称加密系统的预分配密钥管理方案比较[11,12]，只需每个节点预分配一个向量密钥，避免了通过提高预分配密钥数量提高对偶密钥建立概率的缺陷，减少了预分配密钥的存储空间；同时，由于采用了基于身份的密钥管理方案，在源节点能获得目标节点身份标识的前提下保证了密钥的成功建立。与典型基于身份的分布式门限 PKG 密钥管理方案[5,6]比较，减小了密钥服务中的通信次数，从而降低了节点获得密钥服务的通信开销和能量损耗。

2　基于身份的预分配非对称密钥管理方案的定义及安全模型

2.1　方案描述

定义 1　基于身份的预分配非对称密钥管理方案 Γ 由 Setup、Predistribute、Extract、Encrypt 和 Decrypt 5 部分组成，构成一个关于算法的五元组 $\Gamma = (Gen, Pre, Ext, Enc, Dec)$，具体描述如下。

1) 算法 *Gen*：在 Setup 阶段 PKG 运行算法 *Gen*，输入安全参数生成系统参数 *Params* 和主密钥 X_{Pri}。

2) 算法 *Pre*：在 Predistribute 阶段 PKG 运行算法 *Pre*，在主密钥 X_{Pri} 矩阵中输出子集 $\boldsymbol{X}_{ID}$，预分配到节点集合 I 中。

3) 算法 *Ext*：在 Extract 阶段节点运行算法 *Ext*，输入节点密钥标识 $Str = (ID \,|\, Time) \in \{0,1\}^*$，输出对应节点的公钥 y_{Str} 和私钥 x_{Str}。

4) 算法 *Enc*：在 Encrypt 阶段节点运行算法 *Enc*，输入待加密的消息 M，公钥 y_{Str} 和系统参数 *Params*，输出关于明文 M 的密文 C。

5) 算法 *Dec*：在 Decrypt 阶段节点运行算法 *Dec*，输入密文 C 和私钥 x_{Str}，输出密文 C 所对应的明文消息 M。

2.2　安全模型与假设

定义 2　在基于身份的预分配非对称密钥管理方案中，根据方案基于身份和预分配主密钥子集的特点，定义 2 种类型的敌手模型。

类型Ⅰ：在攻击过程中敌手具有适应性选择身份及查询节点私钥的能力，以获取待攻击节点之外的节点私钥。

类型Ⅱ：敌手除了具有类型Ⅰ敌手具有的能力外，还具有查询节点预分配主密钥子集的能

力，以获取待攻击节点之外的节点预分配主密钥子集。

定义 3 一个函数 $f:R\to R$ 是可忽略的，对于 $\forall d\geqslant 0$，d 为常数，都存在一个整数 N，使得对于 $\forall k\geqslant N$，有 $\left|f(k)\right|\leqslant\frac{1}{k^d}$。

定义 4 如果任何多项式时间 IND-ID-CPA 敌手 A(类型Ⅰ)赢得 IND-ID-CPA 游戏的优势概率 $Adv_{\Gamma,A(k)}$ 是可忽略的，则称基于身份的预分配非对称密钥加密方案在适应性选择身份和明文的攻击下是安全的。

IND-ID-CPA 游戏[4,13]由 5 个步骤构成。

1) Setup：挑战者 B 运行算法 *Gen* 产生系统参数和主密钥，并将系统参数发送给敌手 A。

2) Phase1：敌手 A 通过节点 *ID* 向 B 发起提取私钥请求，B 向 A 返回对应节点 *ID* 的私钥。

3) Challenge：A 向 B 发送在 Phase1 阶段没有请求过的节点 ID_0 及明文 M_0、M_1，B 随机选取 $b\in\{0,1\}$ 运行算法 *Enc* 加密明文 M_b 得到密文 C，并将 C 发送给 A。

4) Phase2：A 继续发起除 ID_0 外的私钥提取请求，B 向 A 返回对应节点的私钥。

5) Guess：A 输出 $b'\in\{0,1\}$ 猜测明文 M_b。如果 $b'=b$ 输出 1，否则输出 0，敌手攻击成功的优势概率为 $Adv_{\Gamma,A(k)}=\left|\mathrm{pr}[b'=b]-\frac{1}{2}\right|$。

定义 5 在基于身份的预分配非对称密钥管理方案中，对于能够适应性提取 x 个节点主密钥预分配子集的敌手(类型Ⅱ)能以概率 $p(x)$ 获得待攻击节点密钥的方式，称为选择节点概率攻击，攻击成功的概率为 $p(x)$。

本文假设节点具有 GPS(global position system)模块，能够通过 GPS 模块获得精确的时间信息并且敌手只具有定义 2 中描述的攻击能力。

3 基于身份的预分配非对称密钥管理方案

3.1 具体方案

基于身份的预分配非对称密钥管理方案由以下 5 个部分构成。

1) Setup 阶段

由 PKG 生成系统参数和主密钥对。

S-Step1 PKG 生成阶数为素数 q 的循环群 G，任意选择生成元 $g\in G$。

S-Step2 选取 $x_{ij}\in Z_{q-1}$，$1\leqslant i\leqslant m$，$1\leqslant j\leqslant n$，$m,n\in Z^+$，令 $y_{ij}=g^{x_{ij}}$，构造主密钥对 $(\boldsymbol{X}_{\mathrm{Pri}},\boldsymbol{Y}_{\mathrm{Pub}})$，其中，$Z_{q-1}$ 为模 $q-1$ 的整数集合，Z^+ 为正整数集合。

$$\boldsymbol{X}_{\mathrm{Pri}}=\begin{pmatrix}x_{11}&x_{12}&\cdots&x_{1n}\\x_{21}&x_{22}&\cdots&x_{2n}\\\vdots&\vdots&&\vdots\\x_{m1}&x_{m2}&\cdots&x_{mn}\end{pmatrix}$$

$$\boldsymbol{Y}_{\mathrm{Pub}}=\begin{pmatrix}y_{11}&y_{12}&\cdots&y_{1n}\\y_{21}&y_{22}&\cdots&y_{2n}\\\vdots&\vdots&&\vdots\\y_{m1}&y_{m2}&\cdots&y_{mn}\end{pmatrix}$$

S-Step3 选择强密码杂凑函数 $H:\{0,1\}^*\to\{0,1\}^{l\times n}$，其中，$l$ 满足 $m=2^l$。

S-Step4 公开系统参数 $(G,g,q,\boldsymbol{Y}_{\mathrm{Pub}},H)$。

2) Predistribute 阶段

PKG 根据节点的身份为节点预分配主密钥子集后离线。

P-Step1 $I=\{ID_1,ID_2,\cdots,ID_N\}$ 为节点身份集合，其中，ID_u $(0<u\leqslant N)$由节点唯一身份标识 id_u 和物理地址 MAC_u 构成，$ID_u=(id_u\,|\,MAC_u)$。计算 ID_u 的散列值 $H(ID_u)=h_1^{ID}h_2^{ID}\cdots h_n^{ID}$，其中，$h_j^{ID}$ $(1\leqslant j\leqslant n)$ 是长度为 l 的二进制串。

P-Step2 对于每个 h_j^{ID}，从 $\boldsymbol{X}_{\mathrm{Pri}}$ 中选择第 j 列的第 i_j+1 个值 $x_{i_j j}$，其中，i_j $(0\leqslant i_j<m)$为 h_j^{ID} 的十进制表示。设 $\boldsymbol{X}_{\boldsymbol{ID_u}}=\{x_{i_1 1},x_{i_2 2},\cdots,x_{i_n n}\}$，将 $\boldsymbol{X}_{\boldsymbol{ID_u}}$ 预先分配到节点 ID_u 中。

3) Extract 阶段

节点通过预分配的主密钥子集生成节点私钥，通过公开的系统参数生成目标节点公钥。

X-Step1 节点身份标识 ID_u 与当前密钥时间 *Time* 构成节点密钥生成标识 $Str_u=\{ID_u\,|\,Time\}$ $(0<u\leqslant N)$。计算 Str_u 散列值 $H(Str_u)=h_1^{Str}h_2^{Str}\cdots h_n^{Str}$，由 $\boldsymbol{X}_{\boldsymbol{ID_u}}$，$H(Str_u)$ 生成节点私钥 x_{Str_u}。

$$x_{Str_u}=\sum_{j=1}^{n}h_j^{Str}x_{i_j j}\bmod q,\quad 0\leqslant i_j<m \tag{1}$$

X-Step2 设目标节点为 ID_u(目标节点可以为任意节点，只需通过应用获得其节点身份信息)，通过 $H(ID_u)=h_1^{ID}h_2^{ID}\cdots h_n^{ID}$ 中的 h_j^{ID} $(1\leqslant j\leqslant n)$ 从 $\boldsymbol{Y}_{\mathrm{Pub}}$ 中选择第 j 列的第 i_j+1 个值 $y_{i_j j}$，其中，i_j

($0 \leqslant i_j < m$)为 h_j^{ID} 的十进制表示。设 $\boldsymbol{Y}_{\boldsymbol{ID}_u}=\{y_{i_1 1}, y_{i_2 2},\cdots,y_{i_n n}\}$，由 $\boldsymbol{Y}_{\boldsymbol{ID}_u}$，$H(Str_u)$ 生成节点公钥 y_{Str_u}。

$$y_{Str_u}=\prod_{j=1}^{n}(y_{i_j j})^{h_j^{Str}} \bmod q=\prod_{j=1}^{n} g^{x_{i_j j}h_j^{Str}} \bmod q=g^{x_{Str_u}},$$
$$0 \leqslant i_j < m \tag{2}$$

4) Encrypt 阶段

任意节点 ID_v ($0<v\leqslant N, v\neq u$)需要向节点 ID_u 发送秘密消息时，利用节点 ID_u 的公钥 y_{Str_u} (在密钥更新后，ID_v 加密需要利用 X-Step2 阶段计算节点 ID_u 的公钥)，随机数 $r\in Z_{q-1}$ 及 ElGamal 算法[14]计算明文 $M\in G$ 的密文 $C=(c_1,c_2)$ 并发送给节点 ID_u，其中，$c_1=M(y_{Str_u})^r$，$c_2=g^r$。

5) Decrypt 阶段

给定密文 $C=(c_1,c_2)$，节点 ID_u 计算私钥 x'_{Str_u} (x'_{Str_u} 通过 X-Step1 阶段所述方法计算)解密密文 C，当且仅当节点 ID_u 具有与其身份对应的合法预分配主密钥子集时(此时生成的私钥满足 $x'_{Str_u}=x_{Str_u}$)，能够解密得到明文 M。

$$M=c_1/c_2^{x_{Str_u}}=M(y_{Str_u})^r/(g^r)^{x_{Str_u}}$$
$$=M(y_{Str_u})^r/(g^{x_{Str_u}})^r=M \tag{3}$$

3.2　节点密钥更新

密钥更新的目标是变换节点在 Extract 阶段为节点使用而生成的公私钥。该过程能够更新节点当前使用的密钥而无需改变节点中预分配的主密钥子集。若系统当前时间 t ($t_i\leqslant t<t_{i+1}$)时刻节点 ID_u 公私钥对为 (y_{Str_u},x_{Str_u})，节点密钥生成标识为 $Str_u=\{ID_u\,|\,Time\}$，其中，$Time=t_i$，节点 ID_u 需要在 t_{i+1} 时刻更新节点密钥对 $(y_{Str_u}^{\text{new}},x_{Str_u}^{\text{new}})$，密钥更新时间间隔为 Δt，满足 $t_{i+1}=t_i+\Delta t$，其中，Δt 可以根据系统不同的应用需求来设定(如 24h、12h、2h 等)，则节点 ID_u 需要如下过程。

R-Step1　由节点身份标识 ID_u 与更新密钥时间 $Time=t_i+\Delta t$ 构成节点新的密钥生成标识 $Str_u=\{ID_u\,|\,Time\}$ ($0<u\leqslant N$)。计算 Str_u 散列值 $H(Str_u)=h_1^{Str}h_2^{Str}\cdots h_n^{Str}$，由 $\boldsymbol{X}_{\boldsymbol{ID}_u}$，$H(Str_u)$ 生成节点更新的私钥 $x_{Str_u}^{\text{new}}$。

$$x_{Str_u}^{\text{new}}=\sum_{j=1}^{n}h_j^{Str}x_{i_j j} \bmod q,\quad 0\leqslant i_j<m \tag{4}$$

R-Step2　通过 $H(ID_u)=h_1^{ID}h_2^{ID}\cdots h_n^{ID}$ 中的 h_j^{ID} ($1\leqslant j\leqslant n$)从 Y_{Pub} 中选择第 j 列的第 i_j+1 个值 $y_{i_j j}$，其中，i_j ($0\leqslant i_j<m$)为 h_j^{ID} 的十进制表示。设 $\boldsymbol{Y}_{\boldsymbol{ID}_u}=\{y_{i_1 1}, y_{i_2 2},\cdots,y_{i_n n}\}$，由 $\boldsymbol{Y}_{\boldsymbol{ID}_u}$，$H(Str_u)$ 生成节点更新的公钥 $y_{Str_u}^{\text{new}}$。

$$y_{Str_u}^{\text{new}}=\prod_{j=1}^{n}(y_{i_j j})^{h_j^{Str}} \bmod q=\prod_{j=1}^{n} g^{x_{i_j j}h_j^{Str}} \bmod q=g^{x_{Str_u}^{\text{new}}},$$
$$0\leqslant i_j<m \tag{5}$$

4　方案分析

4.1　安全性分析

分析方案的安全性之前，先回顾一下本文方案基于的困难假设。

定义 6　判定 Diffie-Hellman 假设(DDH 假设)：在阶数为素数 q 的循环群 G 中，g 为 G 的任意生成元，随机选择 $a,b,c\in Z_q^*$，$\tau\in\{0,1\}$。如果 $\tau=1$ 输出四元组 (g,g^a,g^b,g^{ab})；否则 $\tau=0$，输出四元组 (g,g^a,g^b,g^c)。输出 $\tau'\in\{0,1\}$ 猜测 τ 成功的概率是可忽略的，即在 G 中解决 DDH 问题是困难的，其成功的优势概率定义为 $\varepsilon=\left|\text{pr}[\tau'=\tau]-\frac{1}{2}\right|$。

定理 1　在 DDH 假设和随机预言机模型下，本文方案对于类型Ⅰ敌手 A 在选择身份和明文攻击下是安全的。

证明　假设存在敌手 A 在 k ($0<k<n$)次请求后，能够以 ε 的优势攻破方案，则构建算法 B 调用敌手 A 的攻击能力，在概率多项式时间内解 DDH 问题。B 模拟 A 的挑战者以四元组 $(g,G_a=g^a,G_b=g^b,Z)$ 作为输入与 A 进行 IND-ID-CPA 游戏。

1)Setup：B 模拟算法 *Gen* 利用四元组 $(g,G_a=g^a,G_b=g^b,Z)$ 构建系统参数 *Params* 和主密钥 $\boldsymbol{X}_{\text{Pri}}$。

S-Step1　生成阶数为素数 q 的循环群 G，任意选择生成元 $g\in G$。

S-Step2　选择 $m\times n$ 矩阵 $\boldsymbol{U}_{m\times n}$，$\boldsymbol{V}_{m\times n}$，其中，$u_{ij}\in\{0,1\}^*$，$v_{ij}\in\{0,1\}^*$。

$$\boldsymbol{U}_{m\times n}=\begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ u_{21} & u_{22} & \cdots & u_{2n} \\ \vdots & \vdots & & \vdots \\ u_{m1} & u_{m2} & \cdots & u_{mn} \end{pmatrix}$$

$$\boldsymbol{V}_{m\times n}=\begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix}$$

从 $\boldsymbol{U}_{m\times n}$ 中选择元素构成向量 $\boldsymbol{u}=(u_{i_1 1},u_{i_2 2},\cdots,u_{i_n n})$ $(0\leqslant i_j<m,1\leqslant j\leqslant n)$，从 $n\times n$ 矩阵族 $\boldsymbol{H}_{n\times n}^{u}$ 中选择矩阵

$$\boldsymbol{H}_{n\times n}=\begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & & \vdots \\ h_{n1} & h_{n2} & \cdots & h_{nn} \end{pmatrix}$$

$h_{ij}\in\{0,1\}^{l}$，使 $\boldsymbol{u}$ 和 $\boldsymbol{H}_{n\times n}$ 满足 $\boldsymbol{u}\boldsymbol{H}_{n\times n}=0$，$\boldsymbol{H}_{n\times n}\in\boldsymbol{H}_{n\times n}^{u}$。

S-Step3 B 构建主密钥对 $(\boldsymbol{X}_{\text{Pri}},\boldsymbol{Y}_{\text{Pub}})$，其中，B 已知 G_a $(G_a=g^a)$。

$$\boldsymbol{X}_{\text{Pri}}=\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix}$$

$$\boldsymbol{Y}_{\text{Pub}}=\begin{pmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2n} \\ \vdots & \vdots & & \vdots \\ y_{m1} & y_{m2} & \cdots & y_{mn} \end{pmatrix}$$

设其中 $x_{ij}=au_{ij}+v_{ij}$，则 $y_{ij}=g^{au_{ij}+v_{ij}}=G_a{}^{u_{ij}}g^{v_{ij}}$。

S-Step4 B 向敌手公开系统参数 $(G,g,q,\boldsymbol{Y}_{\text{Pub}})$。

2)Random Oracle 请求：敌手 A 以 ID_u，Str_u $(Str_u=\{ID_u\,|\,Time\}$，为了方便描述假设 *Time* 为定值，这样的假设与一个密钥更新周期内 *Time* 为定值是一致的)向 B 提出 Random Oracle 请求，B 为了回答 A 的 Random Oracle 请求需要维持一个列表 $H_{\text{list}}=(ID_u,Str_u,H(ID_u),H(Str_u))$，$0<u<k$，列表初始为空。*B* 做出以下回答：

如果 ID_u，Str_u 在 H_{list} 中，B 向 A 返回 $H(ID_u)$，$H(Str_u)$；

如果 ID_u，Str_u 不在 H_{list} 中，B 选择 $H(ID_u)=h_1^{ID_u}h_2^{ID_u}\cdots h_n^{ID_u}$，$H(ID_u)\in\{0,1\}^{l\times n}$，对于 $H(ID_u)$ 中每个 $h_j^{ID_u}$ 从 $\boldsymbol{U}_{m\times n}$ 中选择第 j 列的第 i_j+1 个值 $u_{i_j j}$，其中，i_j $(0\leqslant i_j<m$，$1\leqslant j\leqslant n)$为 $h_j^{ID_u}$ 的十进制表示，构成 $\boldsymbol{u}=(u_{i_1 1},u_{i_2 2},\cdots,u_{i_n n})$，从 $\boldsymbol{H}_{n\times n}$ 中选择列元素使 $H(Str_u)=h_{1j}h_{2j}\cdots h_{nj}$，将 $H(ID_u)$，$H(Str_u)$ 返回给 A，并把 $H(Str_u)$，$H(ID_u)$ 加入 H_{list}。

3) Phase1: 敌手 A 发起提取私钥请求 Str_1，$Str_2,\cdots,Str_u$ $(0<u<k)$。B 从 Str_u 中得到 ID_u，如果 ID_u，Str_u 不在 H_{list} 中，以 Random Oracle 请求中 b) 方式选择 $H(ID_u)$ 和 $H(Str_u)$，将 $H(ID_u)$，$H(Str_u)$ 返回给 A，并把 $H(Str_u)$，$H(ID_u)$ 加入 H_{list}。对于 $H(ID_u)$ 中每个 $h_j^{ID_u}$ 从 $\boldsymbol{X}_{\text{Pri}}$ 中选择第 j 列的第 i_j+1 个值 $x_{i_j j}$，其中，i_j $(0\leqslant i_j<m)$为 $h_j^{ID_u}$ 的十进制表示。则

$$\begin{aligned}\boldsymbol{X}_{\boldsymbol{ID}_u}&=\{x_{i_1 1},x_{i_2 2},\cdots,x_{i_n n}\}\\&=\{au_{i_1 1}+v_{i_1 1},au_{i_2 2}+v_{i_2 2},\cdots,au_{i_n n}+v_{i_n n}\}\end{aligned}\tag{6}$$

由 $\boldsymbol{X}_{\boldsymbol{ID}_u}$，$H(Str_u)$ 生成节点私钥为

$$\begin{aligned}x_{Str_u}&=\sum_{r=1}^{n}h_{rj}x_{i_r r}\bmod q=\sum_{r=1}^{n}h_{rj}(au_{i_r r}+v_{i_r r})\bmod q\\&=(\sum_{r=1}^{n}au_{i_r r}h_{rj}\bmod q+\sum_{r=1}^{n}h_{rj}v_{i_r r}\bmod q)\bmod q\\&=0+\sum_{r=1}^{n}h_{rj}v_{i_r r}\bmod q\end{aligned}\tag{7}$$

4) Challenge：敌手 A 选择在 Phase1 阶段没有查询过的 ID，$Str=\{ID\,|\,Time\}$ 及明文消息 M_0，$M_1\in G$，B 随机选择 $H(Str)=h_1^{Str}h_2^{Str}\cdots h_n^{Str}$，$H(ID)=h_1^{ID}h_2^{ID}\cdots h_n^{ID}$，其中，$H(Str)$，$H(ID)\notin H_{\text{list}}$，$h_j^{Str}$，$h_j^{ID}\in\{0,1\}^{l}$，$1\leqslant j\leqslant n$。利用 $H(ID)=h_1^{ID}h_2^{ID}\cdots h_n^{ID}$ 中的 h_j^{ID} $(1\leqslant j\leqslant n)$从 $\boldsymbol{Y}_{\text{Pub}}$ 中选择第 j 列的第 i_j+1 个值 $y_{i_j j}$，其中，i_j $(0\leqslant i_j<m)$为 h_j^{ID} 的十进制表示。设 $\boldsymbol{Y}_{\boldsymbol{ID}}=\{y_{i_1 1},y_{i_2 2},\cdots,y_{i_n n}\}$，由 $\boldsymbol{Y}_{\boldsymbol{ID}}$，$H(Str)$ 生成节点公钥 y_{Str}。

$$\begin{aligned}y_{Str}&=\prod_{j=1}^{n}(y_{i_j j})^{h_j^{Str}}\bmod q=\prod_{j=1}^{n}g^{x_{i_j j}h_j^{Str}}\bmod q\\&=g^{\sum_{j=1}^{n}(au_{i_j j}+v_{i_j j})h_j^{Str}}=g^{a\sum_{j=1}^{n}u_{i_j j}h_j^{Str}+\sum_{j=1}^{n}v_{i_j j}h_j^{Str}}\\&=g^{au+v}=G_a{}^{u}g^{v}\end{aligned}\tag{8}$$

其中，$u=\sum_{j=1}^{n}u_{i_j j}h_j^{Str}$，$v=\sum_{j=1}^{n}v_{i_j j}h_j^{Str}$。B 选择 $b\in\{0,1\}$，将密文 $C=(c_1,c_2)$ 发送给敌手 A，其中，$c_1=M_bZ^{u}G_b{}^{v}$，$c_2=G_b$。如果 $H(Str)=h_1^{Str}h_2^{Str}\cdots h_n^{Str}$ 是 H_{list} 中所有 $H(Str_u)$ $(0<u<k)$的线性组合，则 B 出错。

5) Phase2：敌手继续发起提取私钥请求。

6) Guess：B 根据 A 对 M_b 的猜测 b'，输出四元组 $(g, G_a = g^a, G_b = g^b, Z)$ 是否为 DH 元组的猜测 τ'。如果 $b' = b$，则 $\tau' = 1$；否则 $\tau' = 0$。

假设 *Error* 是 B 在仿真挑战 A 过程中出错的事件，则 B 调用 A 的能力解决 DDH 问题的成功概率为

$$\begin{aligned}\Pr[Suc] &= \Pr[Suc \wedge Error] + \Pr[Suc \wedge \overline{Error}] \\ &= \Pr[Suc \mid Error]\Pr[Error] + \\ &\quad \Pr[Suc \mid \overline{Error}]\Pr[\overline{Error}]\end{aligned} \tag{9}$$

其中，仿真过程出错后，B 猜测成功概率 $\Pr[Suc \mid Error]$ 为 $\frac{1}{2}$；仿真过程顺利进行，B 调用 A 的能力解决 DDH 问题成功的概率 $\Pr[Suc \mid \overline{Error}]$ 等于 A 攻破方案的概率 $\Pr[b' = b] = \frac{1}{2} + \varepsilon$，这与假设是一致的。

$$\Pr[Suc] = \frac{1}{2}\Pr[Error] + (\frac{1}{2} + \varepsilon)\Pr[\overline{Error}] \tag{10}$$

B 在仿真挑战 A 过程中出错概率 $\Pr[Error]$ 为挑战过程中 $H(Str)$ 是 H_{list} 中所有 $H(Str_u)\,(0 < u < k)$ 的线性组合。在挑战前，敌手 A 通过提取私钥请求已经拥有一个包括 $H(Str_u)$ 的规模不超过 $k \times n$ 的矩阵 $\boldsymbol{M}_{k\times n}$，由此可知矩阵 $\boldsymbol{M}_{k\times n}$ 的秩 $\text{rank}_{\boldsymbol{M}_{k\times n}} \leqslant \min(k, n)$。在 $k < n$ 的条件下，$\boldsymbol{M}_{k\times n}$ 的秩 $\text{rank}_{\boldsymbol{M}_{k\times n}} \leqslant k$，即在 $\boldsymbol{M}_{k\times n}$ 中最多有 k 个向量线性无关，则线性相关的概率最大为 $\frac{1}{2^{l(n-k)}}$，即出错概率 $\Pr[Error]$ 满足：

$$\Pr[Error] \leqslant \frac{1}{2^{l(n-k)}} \tag{11}$$

由式(10)和式(11)可知：

$$\Pr[Suc] \geqslant \frac{1}{2} + \varepsilon\left(1 - \frac{1}{2^{l(n-k)}}\right) \tag{12}$$

如果存在敌手能够以 ε 的优势攻破方案的假设成立，则构建算法 B 调用敌手 A 的攻击能力，在概率多项式内解决 DDH 问题的概率为 $\Pr[Suc] \geqslant \frac{1}{2} + \varepsilon\left(1 - \frac{1}{2^{l(n-k)}}\right)$，其优势概率 $\varepsilon\left(1 - \frac{1}{2^{l(n-k)}}\right)$ 不可忽略，由此，定理 1 得证。

在选择节点概率攻击过程中，类型Ⅱ敌手除了具有类型Ⅰ敌手具有的能力外，还具有查询节点预分配主密钥子集的能力，能够获取待攻击节点之外的节点预分配主密钥子集。由此，类型Ⅱ敌手可以通过捕获其他节点来获取待攻击节点的预分配主密钥子集。例如，当主私钥 $\boldsymbol{X}_{\text{Pri}} = \begin{pmatrix} x_{11} & x_{12} & x_{13} & \boxed{x_{14}} \\ \boxed{x_{21}} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & \boxed{x_{33}} & x_{34} \\ x_{41} & \boxed{x_{42}} & x_{43} & x_{44} \end{pmatrix}$，$(m = 4, l = 2, n = 4)$，节点身份标识为 ID_0 及其散列值为 $H(ID_0) = 01\ 111\ 000$ 时，节点 ID_0 预分配主密钥子集为 $\boldsymbol{X}_{ID_0} = \{x_{21}, x_{42}, x_{33}, x_{14}\}$，敌手为了获得 ID_0 的预分配主密钥子集 $\boldsymbol{X}_{ID_0}$，可以通过查询 ID_1，ID_2，ID_3，ID_4 的预分配主密钥子集得到。其中，ID_1，ID_2，ID_3，ID_4 的预分配主密钥子集为

$$\begin{pmatrix} \boldsymbol{X}_{ID_1} \\ \boldsymbol{X}_{ID_2} \\ \boldsymbol{X}_{ID_3} \\ \boldsymbol{X}_{ID_4} \end{pmatrix} = \begin{pmatrix} \boxed{x_{21}} & x_{32} & x_{43} & x_{24} \\ x_{11} & \boxed{x_{42}} & x_{13} & x_{34} \\ x_{31} & x_{32} & \boxed{x_{33}} & x_{34} \\ x_{41} & x_{12} & x_{43} & \boxed{x_{14}} \end{pmatrix} \tag{13}$$

假设类型Ⅱ敌手已经查询到 k 个节点预分配主密钥子集，则该敌手获取节点 ID_0 预分配主密钥子集的概率为

$$P_{ID_0}(k, l, n) = \left(1 - \left(\frac{2^l - 1}{2^l}\right)^k\right)^n \tag{14}$$

通过图 1 分析式(14)可以看出随着主密钥规模的增大，类型Ⅱ敌手查询 k 个节点预分配主密钥子集以获取特定节点预分配主密钥子集的概率会逐渐减小。如果类型Ⅱ敌手要以 80%以上的概率获得待攻击节点的预分配主密钥子集，当主密钥规模为 $(2^l \times n, l = 8, n = 20)$ 时，类型Ⅱ敌手至少查询 1 150 个节点的预分配主密钥子集；当主密钥规模增加到 $(2^l \times n, l = 10,\ n = 64)$ 时，类型Ⅱ敌手查询的节点预分配主密钥子集个数增加到 5 851 个。由此，类型Ⅱ敌手查询 k 个节点预分配主密钥子集获取特定节点预分配主密钥子集的攻击在实际 MANET 中是不可行的。

4.2　节点密钥更新对比分析

在典型的基于身份的 MANET 密钥管理中，节点密钥更新过程产生的通信开销主要与分布 PKG 的门限值和网络规模有关。以 n 表示 PKG 主私钥分布到网络中节点的个数，$t(t<n)$表示分布 PKG 的门限值，以 N 表示网络规模，将本文方案 PAKMS 和 2 种典型方案进行分析对比(如表 1 所示)。

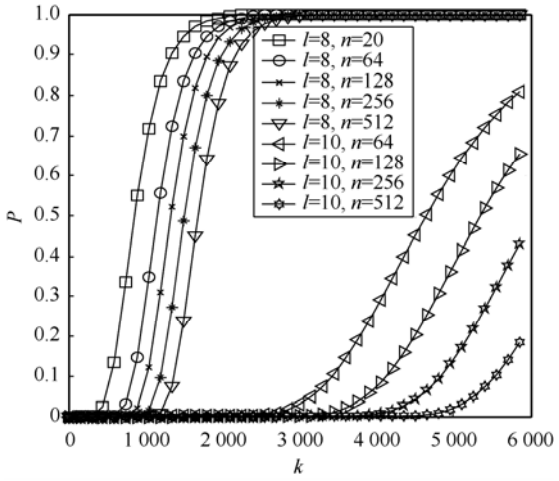

图 1　类型Ⅱ敌手查询 k 个节点预分配主密钥子集获取特定节点预分配主密钥子集的概率

从表 1 中可以看出以上 3 种方案在节点密钥更新过程中网络通信开销与门限值和网络规模的关系，Khalili[5]和 TIDS[6]方案密钥更新过程中的通信次数相同且与 PKG 分布门限值与网络规模的乘积有关，并会随着门限值的提高和网络规模的增大而增多，如图 2 所示。本文方案 PAKMS 在节点密钥更新过程中与 PKG 分布门限值和网络规模无关，仅依赖于时间参数，在能够获得系统精确时间的条件下，不会产生通信开销，从根本上节省了节点能量的消耗。

从表 1 和图 2 综合分析可以得出，网络中的所有节点获得一次密钥更新服务时，PAKMS 方案比 Khalili 和 TIDS 方案在节点间通信次数方面少 $2\times tN$ 次。例如，当 t=51，n=100，N=1 000 时，Khalili 和 TIDS 方案中所有节点通过分布式门限 PKG 更新一次密钥的通信次数为 102 000 次，网络能量开销为 28 743.6W(其中节点收发一次所需的能量消耗以 NS2[15]中 MANET 节点能量模型的典型值 281.8mW 计算)，平均单节点消耗能量为 28.7W。由此，网络中所有节点获得一次密钥更新服务，本文 PAKMS 方案中节点消耗功率比以上 2 种典型方案中节点消耗功率少 28.7W。

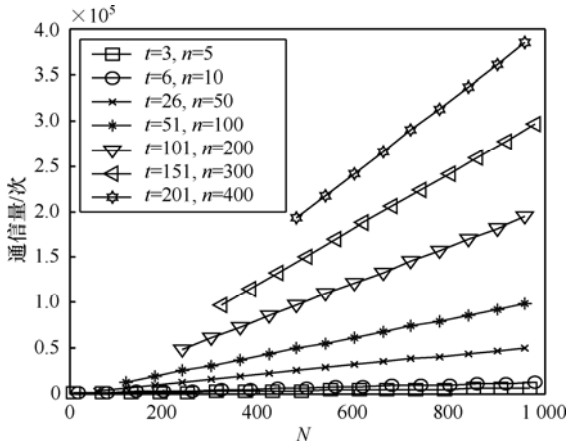

图 2　节点密钥更新中网络所有节点的通信次数

4.3　移动 ad hoc 网络密钥管理方案综合比较

从表 2 可以看出 PAKMS 方案结合了移动 ad hoc 网络密钥管理中基于身份和预分配密钥的方式，在密钥更新、节点密钥存储空间方面更具有优势。与典型的移动 ad hoc 网络中基于身份的分布式门限 PKG 方案[5,6]相比较，在密钥更新方面的优势可以从 4.2 节得出，而与典型对称预分配密钥管理方案[11,12]比较，本文方案采用预分配主密钥子集不变而更新节点当前使用密钥的非对称密钥管理方

表 1　PAKMS 与典型基于身份的密钥管理方案节点密钥更新对比

密钥管理方案	密钥更新		通信量	时间同步
	预分配密钥	节点密钥		
PAKMS	固定	更新	N/A	是
TIDS	N/A	更新	$2\times tN$	否
Khalili	N/A	更新	$2\times tN$	否

表 2　密钥管理方案综合比较分析

密钥管理方案	类型	理论基础	时间同步	密钥更新及撤销	通信量	存储需求
Khalili[5]	基于身份&门限	基于身份密码学&门限密码学	否	有	大	大
TIDS[6]	基于身份&门限	基于身份密码学&门限密码学	否	有	大	大
E-G[12]	预分配	对称密码体制&概率论	否	无	N/A	大
HARPS[13]	预分配	对称密码体制&概率论	否	无	N/A	大
PAKMS	基于身份&预分配	基于身份密码学&ElGamal 加密方案	是	有	小	小

式，在密钥功能和节点密钥更新方面具有优势。在密钥存储空间方面，本文方案具有基于身份密钥管理的优点，即无需存储所有节点公钥，只需存储系统参数和获得节点的身份，同时每个节点预分配一个主密钥子集的方式也改善了对称预分配密钥中需要大量存储对偶密钥的缺陷。

4.4　方案局限性及下一步工作

1) 本文方案中节点密钥更新过程相对典型基于身份的分布式 PKG 密钥管理方案降低了网络整体的通信开销，这种性能上的改善是由于密钥更新过程中保持了预分配主密钥子集不变而仅根据时间参数变化节点密钥的方式。由此，本文所提的密钥管理方案需要节点在时间上满足密钥更新需要，由此需要节点能够通过 GPS 模块获得精确的时间信息。同时，节点预分配主密钥子集是节点密钥的基础，当敌手具有超过类型 II 敌手能力直接能够读取节点预分配主密钥子集时(比如节点被捕获时)，节点预分配主密钥子集的安全性受到威胁。这时可以采用 PTPM[16,17]硬件来存储节点预分配主密钥子集，通过 PTPM 的安全存储能力保护节点预分配主密钥子集的安全性，这种方法是可信计算技术在移动 ad hoc 网络中的一种应用，是下一步工作中的第一个着眼点。

2) 本文方案最多允许敌手获取某一节点更新密钥产生的 $n-1$ 个私钥，以保证该节点预分配主密钥子集的安全。如果敌手能够获取某一节点更新密钥产生的 n 个节点私钥，该节点的预分配主密钥子集可以由式(1)计算出来，但此时根据 4.1 节对选择节点概率攻击的分析可知，敌手获得一个节点预分配主密钥子集几乎不会影响到其他节点预分配主密钥子集的安全性。同时因为敌手已经能够获得节点私钥来解密消息，也就没有再获得节点预分配主密钥子集的意义。由此，这个问题回归到了所有加密系统私钥安全性这个基本问题上来。为了从根本上解决这个问题，可以利用 PTPM 构建密钥链式结构，通过节点密钥的父密钥加密节点密钥并存储于 PTPM 中，通过 PTPM 来增加方案的私钥安全性，这将是下一步工作的另一着眼点。

5　结束语

本文提出了基于身份的预分配非对称密钥管理方案，方案利用私钥生成中心为节点预分配主密钥子集的方式及通过基于时间获得节点密钥更新的方法解决了现有基于身份的密钥管理过程带来的大量通信开销；同时也通过私钥生成中心为节点预分配主密钥子集的方式使节点在网络运行阶段不再依赖私钥生成中心为节点分配和更新密钥，弱化了基于身份密钥管理中存在的私钥托管问题对网络安全的影响。文中详细描述了基于身份的预分配非对称密钥管理方案，并给出了方案的安全性证明，由此表明：1)本文方案在 DDH 和随机预言机模型假设下，关于选择身份和明文攻击(IND-ID- CPA)是安全的；2)选择节点概率攻击在实际 MANET 中是不可行的。同时本文通过对比分析给出了方案的性能评价及下一步的工作重点。

参考文献：

[1] 易平, 蒋嶷川, 张世永. 移动 ad hoc 网络安全综述[J]. 电子学报, 2005, 33(5):893-899.
YI P, JIANG N C, ZHANG S Y. A survey of security for mobile ad hoc networks[J]. Acta Electronica Sinica, 2005, 33(5):893-899.

[2] 华平,胡光明,董攀. 大规模移动自组网络安全技术综述[J]. 计算机研究与发展, 2007, 44(4):545-552.
HUA P, HU G M, DONG P. Survey of security technology for large scal manet[J]. Journal of Computer Research and Development, 2007, 44(4):545-552.

[3] SHAMIR A．Identity-based cryptosystems and signature schemes[A]. Proceedings of the Advances in Cryptology-CRYPTO'84[C]. Berlin: Springer, 1984.47-53.

[4] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[J]. SIAM Journal of Computing, 2000, 32(3): 586-615.

[5] KHALILI A, KATZ J, ARBAUGH W A. Toward secure key distribution in truly ad hoc networks[A]. International Symposium on Applications and the Internet[C]. Orlando,USA, 2003. 342-346.

[6] DENG H, AGRAWAL D. TIDS: threshold and identity-based security scheme for wireless ad hoc networks[J]. Ad Hoc Networks, 2004, 2(3): 291-307.

[7] SILVA E, SANTOS A L, ALBINI L C P. Identity-based key management in mobile ad hoc networks: techniques and applications[J]. IEEE Wireless Communications, 2008, 15(5):46-52.

[8] CHIEN H Y, LIN R Y. Improved ID-based security framework for ad hoc network[J]. Ad Hoc Networks, 2008, 6(1):47-60.

[9] SUN J Y, ZHANG C, ZHANG Y C. An identity-based security system for user privacy in vehicular ad hoc networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2010, 21(9):1227-1239.

[10] 南湘浩. CPK 密码体制与网际安全[M]. 北京：北京国防工业出版社, 2008.
NAN X H. CPK-Crypotosystem and Cyber Security[M]. Beijing: National Defence Industry Press, 2008.

[11] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[A]. Proceedings of the 9th ACM Conference on Computer and Communication Security[C].Chicago, USA, 2002. 41-47.

[12] RAMKUMAR M, MEMON N. An efficient key predistribution scheme for ad hoc network security[J]. IEEE Journal on Selected Areas in Communications,2005, 23(3):611-621.

[13] 胡亮, 刘哲理, 孙涛. 基于身份的密码学的安全性研究综述[J]. 计算机研究与发展, 2009, 46(9):1537-1548.
HU L, LIU Z L, SUN T. Survey of security on identity-based cryptography[J]. Journal of Computer Research and Development, 2009, 46(9): 1537-1548.

[14] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4):469-472.

[15] The NS manual (formerly ns notes and documentation)[EB/OL]. http://www.isi.edu/nsnam/ ns/doc/, 2011.

[16] HAN L, LIU J Q, ZHANG D W. A portable TPM scheme for general-purpose trusted computing based on EFI[A]. MINES'09: International Conference on Multimedia Information Networking and Security[C]. Wuhan, China, 2009.140-143.

[17] HAN L, LIU J Q, HAN Z. Design and implementation of a portable TPM scheme for general-purpose trusted computing based on EFI[J]. Frontiers of Computer Science in China, 2011,5(2):169-180.

作者简介：

韩磊（1983-），男，内蒙古呼伦贝尔人，北京交通大学博士生，主要研究方向为移动自组织网络安全。

刘吉强（1973-），男，山东烟台人，博士，北京交通大学教授、博士生导师，主要研究方向为网络安全、安全协议设计与分析和可信计算。

韩臻（1962-），男，浙江宁波人，北京交通大学教授、博士生导师，主要研究方向为信息安全体系结构和可信计算。

魏学业（1963-），男，山东潍坊人，北京交通大学教授、博士生导师，主要研究方向为无线传感器网络和信号检测。