适合 ad hoc 网络无需安全信道的密钥管理方案

李慧贤[1]，庞辽军[2]，王育民[2]
(1. 西北工业大学 计算机学院，陕西 西安 710072；2. 西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071)

摘 要：密钥管理问题是构建 ad hoc 安全网络系统首要解决的关键问题之一。针对 ad hoc 网络特点，提出了一个无需安全信道的门限密钥管理方案。该方案中，可信中心的功能由局部注册中心和分布式密钥生成中心共同实现，避免了单点失效问题；通过门限技术，网络内部成员相互协作分布式地生成系统密钥；利用基于双线性对的公钥体制实现了用户和分布式密钥生成中心的双向认证；通过对用户私钥信息进行盲签名防止攻击者获取私钥信息，从而可以在公开信道上安全传输。分析表明该方案达到了第 III 级信任，具有良好的容错性，并能抵御网络中的主动和被动攻击，在满足 ad hoc 网络安全需求的情况下，极大地降低了计算和存储开销。

关键词：ad hoc 网络；密钥管理；双线性对；门限密码
中图分类号：TP393 **文献标识码**：B **文章编号**：1000-436X(2010)01-0112-06

Key management scheme without secure channel for ad hoc networks

LI Hui-xian[1], PANG Liao-jun[2], WANG Yu-min[2]
(1. School of Computer Science and Engineering, Northwestern Polytechnical Univ., Xi'an 710072, China;
2. Key Lab of Computer Networks and Information Security of Ministry of Education, Xidian Univ., Xi'an 710071,China)

Abstract: Key management is one of the important issues for the ad hoc networks security. According to the characteristics of ad hoc networks, a threshold key management scheme without secure channel was proposed. In the proposed scheme, the role of the traditional certification authority (CA) is completed by a local register center and *n* distributed key generation centers, which can avoid the single point of failure. By using threshold cryptography, the ad hoc interior members collaborate to conduct the distributed generation the system private key. The mutual authentication between the user and distributed key generation centers was provided through the public cryptosystem based on the bilinear pairings. The user's private key is signed blindly to ensure that the private keys can be delivered securely in the public channel and cannot be eavesdropped. The analysis results show that the proposed scheme achieves the trust level III, has fault tolerance and is secure against the active and passive attacks. It is concluded that the proposed scheme satisfies the security requirements of ad hoc networks and reduces largely the cost of computation and storage.

Key words: ad hoc networks; key management; bilinear pairing; threshold cryptosystem

---

收稿日期：2009-06-08；**修回日期**：2009-11-21
基金项目：国家自然科学基金资助项目(60803151)；NSFC-广东联合基金重点资助项目(U0835004)；高等学校博士学科点专项科研基金新教师基金资助项目(20096102120045)；西北工业大学基础研究基金资助项目(NPU-FFR-JC200819)；教育部计算机网络与信息安全重点实验室(西安电子科技大学)开放基金资助项目(2008CNIS-07)
Foundation Items: The National Natural Science Foundation of China(60803151); The Key Program of NSFC- Guangdong Union Foundation of China(U0835004); The Research Fund for the Doctoral Program of Higher Education of China (20096102120045); NPU Foundation for Fundamental Research (NPU-FFR-JC200819); Open Foundation of the Key Laboratory of Network and Information Security in Xidian University, Ministry of Education of China(2008CNIS-07)

1　引言

Ad hoc 网络是一种由移动终端（也称作节点）通过无线通信技术构成的无基站、多跳、临时性的自组织网络系统，在军事战场、抢险救灾以及民用通信领域都有广泛的应用。作为一种新型的无线通信网络，ad hoc 网络具有拓扑结构动态变化、缺乏中心控制、无线网络易受攻击、无线通信带宽有限、主机能源有限等特点，这使其较传统固定网络面临更大的安全挑战。因此，ad hoc 网络的安全性受到了广泛关注，而其核心就是密钥管理问题[1]。

由于 ad hoc 网络的脆弱性，没有单个节点是可信赖的。如果采用一个可信中心管理密钥，容易产生单点失效问题[2, 3]，只要一个成员被攻破，就会暴露整个网络。因此，将信任分布化是解决 ad hoc 网络中密钥管理的一种有效手段，通过将多个节点组织为一个可信实体，能够满足即使部分节点失效或泄漏仍能保持网络的可用性和正确性。Zhou 和 Hatz[1]最先提出了基于(n, t)门限密码的分布化 ad hoc 密钥管理方案，将对一个节点的信任分散到对多个节点的信任。在该方案中，原来由一个证书机构（CA, certificate authority）掌管的系统密钥分成 n 个份额，分别交由 n 个分布式 CA 来掌管，其中任意 t 个可以重构系统密钥。但该方案没有实现完全分布化，因为仍需一个密钥产生中心来进行系统密钥的分发。后来，Luo 等[4]提出了自安全的 ad hoc 网络，无需第三方，仅依靠网络节点相互协作产生并分发系统私钥，实现了完全分布化的密钥管理。

然而，上述方案没有考虑 ad hoc 网络节点计算、存储能力有限、难以承受传统公钥的复杂计算任务等约束，于是 Khalili 等[5]提出了基于 ID 的 ad hoc 网络密钥管理思路，基于 ID 的密码体制[6]使用较短的密钥就能提供与传统公钥体制（如 RSA）相当的安全性，且无需证书，具有较高的计算和通信效率，适合于 ad hoc 网络中的应用。后来，Deng 等[7]给出了一种基于 ID 的 ad hoc 网络密钥管理的具体实现。但在上述 2 个方案中，都需要安全信道来传输用户私钥，而在 ad hoc 网络中预先建立和维护安全信道是十分困难的。需要安全信道也是基于 ID 的密码体制自身存在的一个弱点，Sui 等[8]提出了一个匿名密钥发送协议，用以提供安全的通信信道，但 Kwon 等[9]指出该协议不能抵御攻击者的伪造攻击，并给出了一个改进的协议。然而，这 2 个协议是针对传统网络提出的，不适用于 ad hoc 网络。

基于上述考虑，本文将基于 ID 的密码体制[6]和门限密码技术[10]相结合，提出了一个无需安全信道的 ad hoc 网络密钥管理方案。该方案通过门限技术，仅依靠 ad hoc 网络成员相互协作来分布式地生成节点密钥；采用基于 ID 的密码技术实现对用户和分布式可信机构的双向验证；通过盲签名[11]来实现私钥在公开信道上的安全传输。分析发现，该方案能够在满足 ad hoc 网络安全需求的情况下，有效地节省网络带宽和节点的计算能量。

2　预备知识

本文方案中的运算操作是基于 GDH (gap Diffie-Hellman) 群上双线性对(bilinear pairings)的特性，该方案的安全性是基于 GDH 群上的困难问题。关于双线性对的特性可以参考文献[6]，下面仅给出 GDH 群的定义。

定义 1　计算 DH 问题[6]。给定<P, aP, bP>，计算 abP，称为计算 DH 问题(CDHP，computational Diffie-Hellman problem)，其中 P 是 G_1^*中的随机元素，$a, b \in Z_q^*$。

一个概率多项式时间(PPT, probabilistic polynomial time)算法 A 在 G_1 群内解决 CDHP 的成功概率记为：Pr[A(<P, aP, bP>)]。

CDH 假设：对于任何 PPT 算法 A，Pr[A(<P, aP, bP>)]可以忽略。

定义 2　判定 DH 问题[6]。给定<P, aP, bP, cP >，判定 $c=ab \bmod q$ 是否成立，称为判定 Diffie-Hellman 问题（DDHP, decisional Diffie-Hellman problem），其中 P 是 G_1^*中的随机元素，$a, b, c \in Z_q^*$。

定义 3　GDH 群[6]。一个素数阶群 G_1 是 GDH 群，当存在一个有效的 PPT 算法在 G_1 上解决 DDHP，同时不存在 PPT 算法以不可忽略的概率成功解决 CDHP。

3　本文提出的密钥管理方案

在密钥管理中，一般需要一个可信中心，其主要作用是：1)鉴别用户身份；2) 发布用户私钥。由于可信中心的存在，使得网络容易存在单点失效问题，导致部分或整个网络不可用。因此，在本文方案中，为避免单点失效问题并减轻可信中心的负担，将其作用分离并分别由不同的实体来实现。由一个局部注册中心(LRA, local registration authority)

来实现鉴别用户身份的功能，由 n 个分布式密钥生成中心(DKGC, distributed key generation center)来完成产生并发送用户私钥的功能。本文提出的方案由 4 个阶段构成：系统初始化，用户注册，用户密钥发布，用户密钥恢复。

3.1 系统初始化

这个阶段可分为 2 个子阶段：1) 系统参数建立；2) 系统密钥分发。

1) 系统参数建立

系统选择 2 个阶同为素数 q 的群$(G_1, +)$和$(G_2, \bullet)$，构造双线性对映射 e: $G_1\times G_1\rightarrow G_2$，令 P 是 G_1的生成元。选择散列函数 H: $\{0, 1\}^*\rightarrow G_1^*$，$\{G_1, G_2, e, H, P\}$为系统公开参数。设 ad hoc 网络中每个节点 i 都有唯一的身份标识，记为 ID_i（$i\in\{1, 2, \cdots, N\}$，N 为网络节点总数）。LRA 节点选择一个随机整数 $s_0\in Z_q^*$作为私钥，其相应的公钥为 $P_{\mathrm{LRA}}=s_0P$。系统密钥和公钥分别为：s 和 $P_{\mathrm{pub}}=sP$。设参与系统密钥生成的节点为 n（$1\leqslant n\leqslant N$）个 DKGC 网络节点，门限值为 t（$t\leqslant n\leqslant 2t-1$）。

2) 系统密钥分发

在本文方案中，系统密钥 s 不是由可信中心来产生，而是由 ad hoc 网络中 n 个 DKGC 节点协作来产生，即每个 DKGC 节点产生私有密钥 d_i，然后通过分布式形式联合产生系统密钥 s 和每个 DKGC 节点秘密份额，具体步骤如下：

① 每个 DKGC 节点 $i(i=1, 2,\cdots, n)$选择一个秘密整数 $d_i\in Z_q^*$，然后建立一个$(t-1)$阶多项式：

$$f_i(x) = d_i+a_{i,1}x+a_{i,2}x^2+\cdots+a_{i,(t-1)}x^{t-1}\bmod q\ (a_{i,j}\in Z_q^*) \quad (1)$$

显然有 $f_i(0) = d_i$。

② 每个 DKGC 节点 i 计算并安全地发送其他 DKGC 节点 j（$j\neq i$）的部分秘密份额 $s_{i,j} = f_i(j)$。然后，计算并广播验证证据 $V_{i,0} = d_iP$，$V_{i,j} = a_{i,j}P(j=1, 2, \cdots, t-1)$。

③ DKGC 节点 j 收到来自 DKGC 节点 i 的部分秘密份额 $s_{i,j}$ 后，利用式(2)验证其真实性，

$$s_{i,j}P\overset{?}{=}V_{i,0}+\sum_{k=1}^{t-1}j^kV_{i,k} \quad (2)$$

真实则接受，否则拒绝。DKGC 节点 j 收到$(n-1)$个 $s_{i,j}$（$i\neq j$）后，再联合自身的秘密份额 $s_{j,j}$，计算其秘密份额 $s_j=\sum_{i=1}^{n}s_{i,j}$，然后计算并公布其公钥 $P_{sj} = s_jP$。

通过上述过程，安全地建立了系统的密钥 s 和公钥 $P_{\mathrm{pub}}=sP$，由任意 t 个秘密份额 s_i 就能恢复出系统密钥 $s=\sum_{i=1}^{n}d_i$。

3.2 用户注册

一个用户节点 h（其身份标识为 ID_h）首先要到局部最近的 LRA 处进行离线注册，用户 h 向 LRA 提供身份信息及盲因子，LRA 针对这些信息发给用户一个签名信息。具体注册过程如下：

1) 用户 h 选择一个秘密随机数 $r_h\in Z_q^*$，计算相应的盲因子 $R_h = r_hP$，然后将$\{ID_h, R_h\}$提交给 LRA。

2) LRA 收到用户 h 的信息后，计算用户的公开信息 $U_h = H(ID_h\|ID_{\mathrm{LRA}}\|T_h)+R_h$，这里 T_h 是盲因子 R_h 使用的一个合法期限，然后计算一个签名 $Sig_{IDh} = s_0U_h$ 作为注册证据。

3) LRA 将$\{Sig_{IDh}, T_h\}$发送给用户 h。

3.3 用户密钥发布

用户 h 要获得其密钥 y_h，需要向任意 t 个 DKGC 节点提出申请，设被选定的 t 个节点为 DKGC 节点 1，…，DKGC 节点 t。用户密钥的具体发布过程如下：

1) 用户 h 计算其公钥 $Y_{IDh} = H(ID_h)$以及盲公钥 $Y'_{IDh} = r_h\ H(ID_h)$，然后将$\{ID_h, ID_{\mathrm{LRA}}, R_h, Sig_{IDh}, T_h, Y'_{IDh}\}$发送给 DKGC 节点 $i(i=1, 2, \cdots, t)$。

2) DKGC 节点 i 收到用户 h 的申请信息后，计算 $U_h = H(ID_h\|ID_{\mathrm{LRA}}\|T_h)+R_h$，并通过式(3)检查盲因子的合法性：

$$e(Sig_{IDh}, P)\overset{?}{=}e(U_h, P_{\mathrm{LRA}}) \quad (3)$$

接着计算 $Y_{IDh} = H(ID_h)$，并通过式(4)验证盲公钥的有效性：

$$e(Y'_{IDh}, P)\overset{?}{=}e(Y_{IDh}, R_h) \quad (4)$$

上述验证通过后，接受用户 h 的请求，否则拒绝。

3) DKGC 节点 i 计算 $X_i = s_iY'_{IDh}$，并将 X_h 通过公开信道发送给用户 h。

4) DKGC 节点 i 将用户 h 的信息$\{ID_h, R_h, Sig_{IDh}, T_h\}$保存在一个数据库里。

3.4 用户密钥检索

用户 h 收到 DKGC 节点 i 发来的 X_i 后，通过式(5)验证其正确性：

$$e(X_i, P)\overset{?}{=}e(Y'_{IDh}, P_{si}) \quad (5)$$

验证通过则接受 X_i，否则拒绝。在收到 t 个来

自 DKGC 节点的 $X_i(i=1, 2, \cdots, t)$后，用户 h 通过 Lagrange 插值法得到盲化的密钥 y'_{IDh}，令 Lagrange 系数为 $l_i=\prod_{j=1,j\neq i}^{t}\frac{j}{j-i}$，计算 $y'_{IDh}=\sum_{i=1}^{t}l_iX_i=r_hsY_{IDh}$。然后用户 h 利用秘密值 r_h 解开盲密钥 y' 得到真正的密钥 y_{IDh}：$y_{IDh}=r_h^{-1}y'_{IDh}=r_h^{-1}r_hsY_{IDh}=sY_{IDh}=sH(ID_h)$。

4　方案正确性分析

定理 1　在系统密钥分发过程中，n 个 DKGC 节点协作，最后产生的共享系统密钥为 $s=\sum_{i=1}^{n}d_i$。

证明　在系统密钥分发过程中，每个 DKGC 节点 i 建立一个如式(1)的多项式 $f_i(x)$ (i=1, 2,…,n)，将这 n 个多项式 $f_i(x)$相加得到如下秘密多项式 $f(x)$：

$$\begin{aligned}f(x)&=\sum_{i=1}^{n}f_i(x)\bmod q\\&=\sum_{i=1}^{n}\left(d_i+a_{i,1}x+a_{i,2}x^2+\cdots+a_{i,(t-1)}x^{t-1}\right)\bmod q\\&=\sum_{i=1}^{n}d_i+\sum_{i=1}^{n}a_{i,1}x+\sum_{i=1}^{n}a_{i,2}x^2+\cdots+\\&\quad\sum_{i=1}^{n}a_{i,(t-1)}x^{t-1}\bmod q\end{aligned}$$

令 $s=\sum_{i=1}^{n}d_i$，$a_j=\sum_{i=1}^{n}a_{i,j}x^j$ (j=1, 2, …, t–1)，则有 $f(x)=s+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}\bmod q$，$f(x)$即为 n 个 DKGC 节点协作生成的秘密多项式，因此有 $s=\sum_{i=1}^{n}d_i$ 成立。

定理 2　任意 t 个 DKGC 节点 i 联合他们的秘密份额 s_i 可以重构系统密钥 $s=\sum_{i=1}^{n}d_i$。

证明　不失一般性，设 t 个 DKGC 节点 $i(i=1, 2, \cdots, t)$，通过 Lagrange 插值公式如下重构共享的密钥：

$$\begin{aligned}s&=\sum_{i=1}^{t}\left(s_i\prod_{k=1,k\neq i}^{t}\frac{k}{k-i}\right)\\&=\sum_{i=1}^{t}\left(\sum_{j=1}^{n}s_{i,j}\prod_{k=1,k\neq i}^{t}\frac{k}{k-i}\right)\\&=\sum_{j=1}^{n}\left(\sum_{i=1}^{t}s_{i,j}\prod_{k=1,k\neq i}^{t}\frac{k}{k-i}\right)\\&=\sum_{i=1}^{n}d_i\end{aligned}$$

定理 3　通过式(3)能够证明用户 h 对应的盲因子 R_h 的合法性。

证明　用户 h 在 LRA 处注册时，LRA 通过 R_h 计算公开信息 $U_h=H(ID_h\|ID_{\mathrm{LRA}}\|T_h)+R_h$，并对其进行签名得到 $Sig_{IDh}=s_0U_h$，签名信息 Sig_{IDh} 作为用户 h 的注册证据。如果不知道 LRA 的密钥 s_0，仅从 LRA 的公钥 $P_{\mathrm{LRA}}=s_0P$ 和用户的公开信息 $U_h=H(ID_h\|ID_{\mathrm{LRA}}\|T_h)+R_h$ 来计算 Sig_{IDh} 是一个 CDHP 问题，这在计算上是不可行的。另外，$Sig_{IDh}=s_0U_h$ 是可以被验证的。DKGC 节点可以通过判断<P, P_{LRA}, U_h, Sig_{IDh} >是否为一个有效 Diffie-Hellman 组来验证 Sig_{IDh} 的有效性。而且存在有效算法通过双线性对来解决 DDH 问题，即可以通过式(3)来证明盲因子的合法性：

$$\begin{aligned}\text{式(3)左}&=e(Sig_{IDh},P)=e(s_0U_h,P)\\&=e(U_h,s_0P)=e(U_h,P_{\mathrm{LRA}})=\text{式(3)右}\end{aligned}$$

定理 4　通过式(4)，在不揭露秘密值 r_h 的情况下，用户 h 能够向 DKGC 节点证明他是真正与盲因子 R_h 对应的用户。

证明　用户 h 可以计算盲公钥 $Y'_{IDh}=r_hH(ID_h)$ 提供给 DKGC 节点，这相当于对其公钥 $Y_{IDh}=H(ID_h)$ 进行了盲短签名[11]，而盲短签名的安全性已经在文献[11]中得到了证明。而在不知道 r_h 的情况下，想通过公开信息 Y_{IDh} 和 $R_h=r_hP$ 来计算盲公钥 Y'_{IDh} 等价于 CDHP 问题，在计算上是不可行的。另外，DKGC 节点可以通过判断<P, R_h, Y_{IDh}, Y'_{IDh}>是否为一个有效 Diffie-Hellman 组来验证 Y'_{IDh} 的合法性，即可以通过式(4)来进行如下计算：

$$\begin{aligned}\text{式(4)左}&=e(Y'_{IDh},P)=e(r_hY_{IDh},P)\\&=e(Y_{IDh},r_hP)=e(Y_{IDh},R_h)=\text{式(4)右}\end{aligned}$$

5　方案安全性分析

本文提出的密钥管理方案的安全性基于椭圆曲线上的离散对数问题的困难性，同时采用基于盲短签名[11]的传输方案，保证了用户私钥的安全发布。下面将具体分析本文方案的安全性。

定理 5　本文提出的密钥管理方案达到了第 III 级信任。

证明　在公钥密码系统中，信任在用户和可信第三方（TTP, trust third party）间具有重要作用。Girault[12]基于如下信任假设引入了 3 个信任等级：

第 I 级：TTP 知道（或易于计算）用户的私钥，因此可以随时假冒任何用户而不被发现，即存在密钥托管问题。

第 II 级：TTP 不知道（或难以计算）用户的私钥，但仍可以通过产生一个虚假公钥来假冒一个用户而不被发现。

第 III 级：TTP 不知道（或难以计算）用户的私钥，若 TTP 产生假的用户公钥，可以证明该公钥为假。

在本文方案中，每个 DKGC 节点 i 只发布了用户 h 的部分私钥，但不知道用户的完整私钥。如果一个恶意 DKGC 节点要假冒用户 h 欺骗其他的 DKGC 节点，首先他选择一个 $r'_h \in Z_q^*$，计算 $U'_h = H(ID_h \| ID_{\mathrm{LRA}} \| T_h) + r'_h P$，然后选择一个 $s'_0 \in Z_q^*$，伪造一个 LRA 的签名 $Sig'_{IDh} = s'_0 U'_h$。然后将伪造的信息发送给其他 t 个 DKGC 节点，请求用户私钥。由于 $s'_0 \neq s_0$，这些伪造的值将不能通过式(3)的验证，即 $e(Sig'_{IDh}, P) \neq e(U'_h, P_{\mathrm{LRA}})$，因此，恶意 DKGC 节点假冒用户无法成功。如果 LRA 要假冒用户 h，他选择一个 $r''_h \in Z_q^*$，计算 $R''_h = r''_h P$、$U''_h = H(ID_h \| ID_{\mathrm{LRA}} \| T_h) + R''_h$ 和签名 $Sig''_{IDh} = s_0 U''_h$，然后向 t 个 DKGC 节点发出申请信息。由于 $t+1 \leqslant n \leqslant 2t-1$，因此，至少有一个 DKGC 节点将收到了来自用户 h 和恶意 LRA 的申请信息，DKGC 节点通过其数据库里保存的用户 h 的信息 $\{ID_h, R_h, Sig_{IDh}, T_h\}$，比较 $R_h \stackrel{?}{=} R''_h$ 和 $Sig_{IDh} \stackrel{?}{=} Sig''_{IDh}$，就可以识别出恶意 LRA 假冒用户 h。另外，恶意节点想从 $R_h = r_h P$ 或 $P_{\mathrm{LRA}} = s_0 P$ 直接求取 r_h 或 s_0 的值将面临椭圆曲线离散对数计算的困难性。

定理 6 本文方案具有容错性，即使出错的 DKGC 节点达到了 $n-t$ 个，仍然能够正确执行用户密钥分发。

证明 由于采用(n, t)门限密码方案产生用户密钥，至少 t 个 DKGC 节点才能完成密钥发布功能，而 $t-1$ 个或更少的节点将不能产生用户密钥。当网络中出错的 DKGC 节点达到了 $n-t$ 个，仍然有 $n-(n-t) = t$ 个的节点是正确的，因此，能够正确执行用户密钥分发。当 $n = 2t-1$ 时，网络中允许出现 $t-1$ 个错误的 DKGC 节点，仍然能够正确执行用户密钥分发。同时，有效避免了网络中存在的单点失效问题。

定理 7 本文方案在用户密钥发布过程能够抵御主动攻击。

证明 在主动攻击中，攻击者通过伪造、重放、假冒等手段获取系统信息，从而欺骗诚实节点。本文方案在用户密钥发布过程能够抵御以下主动攻击：

1) 假冒攻击：在用户私钥发布过程中，攻击者不可能进行伪造，无法假冒诚实的节点，因为方案执行过程中进行双向认证，即 DKGC 节点对用户发来的信息进行认证，而用户对 DKGC 节点的回复也进行认证。另外，从 DKGC 节点的回复 $X_i = s_i Y'_{IDh}$ 中直接计算 r_h 将面临求解椭圆曲线离散对数问题的困难性。

2) 重放攻击：要计算用户的部分私钥需要使用秘密值 r_h，攻击者即使重放以前获得的回复，由于没有秘密值 r_h，也无法解盲得到用户的私钥。

3) 中间人攻击：如果攻击者更改了 DKGC 节点的回复或者部分私钥，那么在密钥恢复阶段中，用户能够通过式(5)进行验证，从而可以检测到攻击者的欺骗行为。

4) 内部攻击：本文方案中将注册功能和密钥发布功能完全分开，分别由 LRA 和 DKGC 来完成，这在减轻 2 个机构负担的同时，又可以有效地互相遏制对方的恶意行为。由 1)中的分析可知任何 DKGC 节点或 LRA 节点假冒一个用户都会被检测到。

定理 8 本文密钥发布过程能够抵御被动攻击。

证明 在被动攻击中，攻击者通过窃听信道从而获得用户与 DKGC 的会话记录。在本文方案中，由于采用了秘密值 r_h 对传输的用户密钥信息进行盲化，不需要通过安全信道就可以进行安全传输。因此，即使攻击者得到了会话记录，也无法得到用户的私钥。

6 性能分析

在本文提出的方案中，系统初始化部分采用分布式基于 Lagrange 差值的方法生成系统密钥，这一部分可以进行预处理，因此对系统的性能评价主要考虑新节点的密钥分发过程。

本文方案是基于身份的 ad hoc 网络密钥发布协议，节点的身份信息就可以作为它的公钥，不需要额外的公钥生成和传输过程。本文方案的实现主要基于椭圆曲线密码（ECC, elliptic curve cryptography）体制，该体制公钥短小，密钥长度为 160bit 的 ECC 密码的安全性相当于密钥长度 1024bit 的 RSA 的安全性[11]，而且计算量小。因此，本文方案相比于基于传统公钥算法（如 RSA、ElGamal 算法）的 ad hoc 密钥管理方案[1]具有更低的通信和计算代价，更适合于 ad hoc 网络。

在密钥分发过程中，本文的一个主要特点是在传输节点密钥时无需安全信道，这相比于需要安全信道的方案[5,7,13]节省了系统带宽和节点能量。在需要安全信道的方案中，一般需要在新节点与其直接通信的节点间建立安全信道。假设新节点 N_{new} 与系统中 t 个节点进行直接通信，这里新节点记为 N_{new}，t 个节点记为 $N_1, N_2, \cdots, N_t$。N_{new} 与每个 $N_i (i = 1, \cdots, t)$ 都要协商一个会话密钥，记为 $k_i (i = 1, \cdots, t)$。如

果采用 Diffie-Hellman 密钥协商协议，需要 2 次数据通信，这样产生 t 个会话密钥，需要进行 $2t$ 次数据通信，而且在后续的通信过程中，传输的数据需要用 k_i 进行加密。显然，这将增加系统的通信代价，占用系统带宽，而且也增加了节点的计算量，耗费节点能量。而在本文方案中无需安全信道，即不需要密钥协商，这就节省了该过程中的通信和计算代价，系统的安全性基于在新节点处引入秘密值 r_h 对传输的用户密钥信息进行盲化，不需要通过安全信道就可以进行安全传输。而且在本文方案中，在密钥分发过程中， t 个分布式密钥生成中心不需要发布任何公开信息，而是由新节点引入一个盲因子信息来保障安全性。而在现有方案如文献[13]中，在密钥分发过程中，为了增强安全性，t 个分布式授权节点每个都要选择一个随机数，并发布一个相应的公开信息，即要发布 t 个公开信息。显然本文方案节省了 t 次数据传输。

因此，本文方案与现有方案[5,7,13]相比，能够更好地节省带宽和节点的能量。

7　结束语

针对 ad hoc 网络这种新型无线通信网络，本文提出了一个无需安全信道的密钥管理方案。该方案将可信中心的功能分离，通过 LRA 和 DKGC 来实现，有效遏制了内部节点的恶意行为，避免了单点失效问题；通过引入盲因子，无需安全信道就可以安全地传送用户密钥信息；另外采用门限方案，增强了系统的健壮性。本文详细阐述了系统建立过程和用户密钥产生和发布过程，并证明了其正确性。然后分析了所提方案的安全性，结果表明本文提出的方案达到了第 III 级信任，具有良好的容错性，并能抵御网络中的主动和被动攻击，对于 ad hoc 网络中的应用具有较好的理论和实用价值。

参考文献：

[1] ZHOU L D, HASS Z J. Securing ad hoc networks[J]. IEEE Network, Special Issue on Network Security, 1999, 13(6): 24-30.

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

[3] 杜春来, 胡铭曾, 张宏莉. 在椭圆曲线域中基于身份认证的移动 ad hoc 密钥管理框架[J]. 通信学报, 2007, 28(12): 53-59.
DU C L, HU M Z, ZHANG H L. New group key management framework for mobile ad hoc network based on identity authentication in elliptic curve field[J]. Journal on Communications, 2007, 28(12): 53-59.

[4] LUO H, ZEFROS P, KONG J, *et al*. Self-securing ad hoc wireless networks[A]. Proceeding of the Seventh IEEE Symposium on Computers and Communications (ISCC'02)[C]. Taormina, Italy, 2002. 548-555.

[5] KHALILI A, KATZ J. Toward secure key distribution in truly Ad-Hoc networks[A]. Proceedings of the Symposium on Applications and the Internet Workshops (SAINT'03)[C]. Orlando, FL, USA, 2003. 342-346.

[6] BONEH D, FRANKLIN M K. Identity-based encryption from the Weil pairing[J]. SIAM Journal of Computing, 2003, 32(3): 586-615.

[7] DENG H, MUKHERJEE A, AGRAWAL D P. Threshold and identity-based key management and authentication for wireless ad hoc networks[A]. Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)[C]. Las Vegas, USA, 2004. 107-110.

[8] SUI A, CHOW S, HUI L, *et al*. Separable and anonymous identity-based key issuing without secure channel[A]. Proceedings of the 1st International Workshop on Security in Networks and Distributed Systems (SNDS'05)[C]. Fukuoka, Japan, 2005. 275-279.

[9] KWON S, LEE S H. Identity-based key issuing without secure channel in a broad area[A]. Proceedings of the 7th International Workshop on Information Security Applications (WISA'06)[C]. Jeju Island, Korea, 2006. 30-44.

[10] 庞辽军,王育民. 基于 RSA 密码体制(*t*, *n*)门限秘密共享方案[J]. 通信学报, 2005, 26(6): 70-73.
PANG L J, WANG Y M. (*t*, *n*) threshold secret sharing scheme based on RSA cryptosystem[J]. Journal on Communications, 2005, 26(6): 70-73.

[11] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[J]. J Cryptology, 2004, 17(4): 297-319.

[12] GIRAULT M. Self-certified public keys[A]. Proceedings of Advances in Cryptology (EUROCRYPT'91)[C]. Brighton UK, 1991. 490-497.

[13] 吕鑫,程国胜,许峰. 基于双线性对 ad hoc 网络门限身份认证方案[J]. 计算机工程, 2009, 35(1): 147-149.
LV X, CHENG G S, XU F. Threshold authentication scheme of ad hoc network based on bilinear pairings[J]. Computer Engineering, 2009, 35(1): 147-149.

作者简介：

李慧贤（1977-），女，内蒙古乌兰浩特人，博士后，西北工业大学副教授，主要研究方向为网络与信息安全、安全协议设计与分析、ad hoc 网络。

庞辽军（1978-），男，陕西渭南人，博士后，西安电子科技大学副教授，主要研究方向为密码学、安全协议设计与分析等。

王育民（1936-），男，北京人，西安电子科技大学教授、博士生导师，主要研究方向为信息论、密码学、编码学等。