基于身份密码的机载自组织网络动态密钥管理

王 宏*①② 李建华① 赖成喆③
①(空军工程大学信息与导航学院 西安 710077)
②(国防科技大学信息通信学院 西安 710106)
③(西安邮电大学 西安 710121)

摘 要：针对现有机载自组织网络密钥管理存在的预分配密钥更新困难、公钥证书传递开销大、分布式身份密钥传递需要安全信道的问题，该文提出一种无需安全信道的基于身份密码体制的动态密钥管理方案。该方案包括系统密钥自组织生成和用户私钥分布式管理两个算法；采取遮蔽密钥的办法，确保私钥在公共信道中全程安全传递，使得密钥管理易于部署、方便扩展；最后分析了方案的正确性与安全性。结果证明方案理论正确，能够抵抗假冒、重放、中间人攻击。

关键词：机载网络；身份密码体制；密钥管理；自组织；分布式
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2018)08-1985-07
DOI: 10.11999/JEIT171148

Identity Based Dynamic Key Management of Airborne Ad Hoc Network

WANG Hong①② LI Jianhua① LAI Chengzhe③
①(*Information and Navigation College, Air Force Engineering University, Xi'an* 710077, *China*)
②(*Information and Communication College, National University of Defense Technology, Xi'an* 710106, *China*)
③(*Xi'an University of Posts & Telecommunications, Xi'an* 710121, *China*)

Abstract: Because of nowadays airborne network's updating difficulty of pre-allocated symmetrical key, high communication cost of public key certificate and the requirement of security channel for distributed identity-based key management, identity-based dynamic key management of airborne network is proposed. It is composed of two algorithms: self-organized generation of master key without the trusted third party and distributed management of user's private key. Moreover, the master key share and user private partition can be delivered without the pre-established security channel by blinding them so that the scheme is easy to develop and flexible to extend. Finally, the correctness and security of the proposed scheme are proved, it is shown that it can provide the ability to resist the impersonation attack, replay attack and man-in-the-middle attack.

Key words: Airborne network; Identity-based cryptography; Key management; Self-organized; Distributed

1 引言

机载网络是以一定范围内的空中飞行平台为网络节点，通过无线链路互连而成的，用于保障飞行平台之间敌我身份识别、战场信息共享以及战术行动协同等任务的基础支撑环境[1]。随着自组网技术与数据链技术在航空领域的创造性应用，机载自组织网络以其抗毁性好、适应性强、灵活性大等优势，已经发展成为机载网络的重要组网形式[2]。机载自组织网络(以下简称机载自组网)由于部署环境复杂、无线信道开放、网络节点分散等原因，其安全管理面临严峻的挑战[3]。构建安全的机载自组网环境，需要提供机密性、完整性和抗抵赖性等安全服务，安全的密钥管理策略是提供这些服务的先决条件。传统的密钥管理方案多采用基于可信第三方的集中式管理模式，始终需要一个在线中心完成节点的密钥生成、密钥分发、密钥更新等服务，如对称密钥体制需要密钥分发中心(Key Distribution Center, KDC)，非对称密钥体制需要证书中心(Certificate Authority, CA)。但是在机载自组网中难以实施基于可信第三方的集中式密钥管理模式。首先，机载网络节点移动速度快、相对位置变化大造成网络各连接边时通时断，网络成员分散聚合频繁，难以找到完全可靠的第三方可信节点来实施集

收稿日期：2017-12-06；改回日期：2018-05-02；网络出版：2018-06-07
*通信作者： 王宏 whongger2017@163.com
基金项目：国家自然科学基金(61401499, 61502386)
Foundation Items: The National Natural Science Foundation of China (61401499, 61502386)

中式密钥管理；其次，在拓扑动态变化的机载自组网设置集中式的密钥管理中心容易导致单点失效和拒绝服务攻击。因此研究“无可信中心”的密钥管理策略，对机载自组网安全应用具有重要的现实意义。

围绕“无可信中心”的机载网络密钥管理问题，文献[3～16]做了深入的探索研究，归纳起来主要集中在以下3个方面，它们虽然解决了不同应用场景的密钥管理问题，但都不能直接照搬到机载自组网中。一是采取对称密码算法的密钥离线预分配方案[4]。全网共享一个密钥，初始化时密钥管理中心为每个网络节点离线安全分发共同的密钥，网络中不部署在线的密钥管理中心，这个全网共享的密钥既作为认证密钥，又作为节点之间的会话密钥的加密密钥。这种解决办法虽然简便易行，然而由于密钥的全网公用，如果有一个节点叛变，便会造成全网密钥的泄露，造成不可挽回的损失，存在很大的安全隐患。二是基于公钥证书的密钥管理。按照组织方式的不同，基于证书的密钥管理可以区分为分布式证书密钥管理和自组织证书密钥管理。分布式证书密钥管理[5–7]是利用门限秘密共享方案，将传统的公钥证书中心CA的功能进行分散化、分布式、扁平化处理，原来由单一证书中心承担的责任，转变为由n个分布式证书中心CA的其中至少m个共同承担。自组织证书管理认证[8–11]由节点自己生成一对公私钥，并通过节点之间互相信任关系的传递构成一个有向图$G(V,E)$，节点集合V代表公钥，有向边集合E代表证书颁发关系，G_u表示节点u更新的证书集合，G_v表示节点v更新的证书集合，当用户u验证用户v的公钥K_v时，在$G_u \cup G_v$中寻找K_u到K_v的证书链。基于公钥证书的密钥管理，证书传递需要消耗大量通信资源。三是分布式身份密钥管理。基于身份密码体制[12,13](Identity-Based Encryption, IBE)的密钥管理不需要证书参与，可以直接使用用户的身份信息(如IP地址、MAC地址、邮件地址等)作为公钥。但是，IBE的用户不能自己生成私钥，由可信的私钥生成中心(Private Key Generation center, PKG)生成私钥，然后经过安全信道传送给用户。PKG掌握着全网用户的私钥信息，易于导致密钥单点失效和私钥托管问题[14]，因此文献[15～20]提出了分散PKG功能的分布式密钥生成方案，将PKG的私钥生成分散部署到n个节点，把系统私钥碎片化，在n个节点之间托管共享，有效地缓解了集中式PKG所面临的安全性威胁，但在上述方案中，未研究系统私钥共享分配的安全传输问题，在系统私钥分片化共享的过程中，只能采取安全信道传输，而在机载网络中利用无线媒介建立安全信道是非常困难的。在机载网络中这样的设计，要求分布式系统私钥持有节点只能在地面通过有线传输完成系统私钥的共享分发，势必造成升空后机载网络系统密钥份额更新困难的问题。

为解决机载自组网密钥管理存在的预分配密钥更新困难、公钥证书传递开销大、分布式身份密钥传递需要安全信道的问题，通过分析上述密钥管理方案优缺点，本文从机载自组网的环境特殊性出发，基于以下4个方面考虑，提出一种机载自组网动态密钥管理方案：(1)密钥生成实现自组织、无中心化；(2)密钥更新实现动态化；(3)密钥管理过程的各个环节无需提前建立安全信道，与其它分布式密钥管理方案相比需要较少的通信和计算消耗；(4)密钥分发能够抵抗几种常见的攻击，如假冒攻击、中间人攻击和重放攻击等。

以下首先对机载自组网动态密钥管理方案进行系统分析；第3节详细阐述机载自组网动态密钥管理方案的具体实现过程；第4节对机载自组网动态密钥管理实现的关键技术进行正确性、安全性分析，第5节将本文方案与其它方案进行通信和计算量消耗比较，最后给出结论。

2 机载自组网动态密钥管理方案

鉴于IBE在解决“无可信中心”网络密钥管理方面所具有的特殊优势，选取其作为机载自组网动态密钥管理的基础密码体制。首先，基于IBE的密码体制没有繁琐的证书管理。基于身份的密码体制以用户的身份识别信息直接作为公钥，不需要公钥证书，使得加密密钥的管理更加简单，有利于提高机载自组网密钥管理的工作效率；其次，IBE的PKG是一个天然的密钥托管中心。从保护用户的隐私性角度出发，密钥的托管是身份密码体制的缺点，但在军事保密通信方面，私钥的托管备份有利于系统的信息管控；第三，IBE的密钥撤销简单灵活。机载自组网主要为了遂行战术行动或信息共享等特殊任务而临时组网，当训练或作战任务完成后网络随即解散，等待下一次重新组网，网络生存期往往较为短暂，随机性大，要求网络密钥的生成与撤销灵活机动。IBE在用户身份信息中加入时间元素再生成相应私钥，便可以使得用户的密钥具有时效性，到期后密钥自动撤销。

如图1所示，采取身份识别和密钥生成相分离的原则，注册中心(Registration Authority, RA)对用户进行离线身份审核，分布式PKG(Distributed

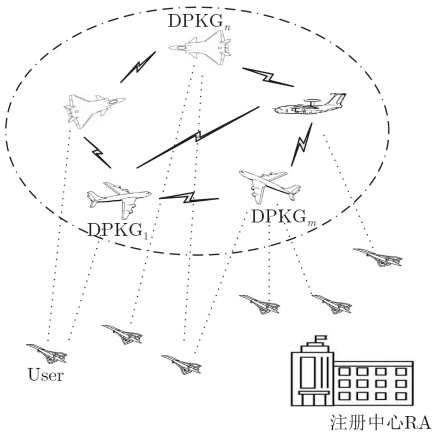

图 1 机载自组网密钥管理结构图

PKG, DPKG)自组织在线生成系统密钥[18]，多于门限个数的DPKGs共同生成用户密钥，并引入遮蔽因子，通过公开信道传递遮蔽的私钥份额，进行密钥的分发、更新。具体方案包括一个RA, n个DPKGs节点和许多用户User，各个部分承担的主要任务分别为：(1)RA：验证审核申请入网用户身份，并提供证明，由绝对安全的地面指挥中枢承担；(2)DPKG：利用自己的部分私钥计算用户部分私钥，并发送给用户，由机载网络中比较可信的空中节点(如预警机、指通机、编队长机等空中控制指挥平台)构成；(3)User：收集多个DPKG节点生成的部分私钥，生成自己的私钥，代表机载网络中大量的普通节点。

3　基于身份密码的机载自组网密钥管理实现

首先选择椭圆曲线$E(F_p)$上的阶为素数q的加法群$(G_1, \hat{+})$和乘法群$(G_2, \cdot)$, P为G_1的一个生成元，构造双线性映射$e: G_1 \times G_1 \to G_2$，杂凑函数$H_1: \{0,1\}^* \to G_1^*$, $H_2: G_2 \to Z_q^*$，系统公开参数为$\langle G_1, G_2, P, e, H_1, H_2\rangle$。RA选择$s_0 \in_{\text{rnd}} Z_q^*$，计算$P_{\text{RA}} = s_0 P$，并公开$P_{\text{RA}}$。

3.1　系统密钥自组织生成算法

每个DPKG随机选择$r_{\text{DPKG}_i} \in_{\text{rnd}} Z_q^*$，计算遮蔽因子$R_{\text{DPKG}_i} = r_{\text{DPKG}_i} P$；并与RA取得联系进行离线注册，节点$\text{DPKG}_i$向RA提交身份信息$\text{ID}_{\text{DPKG}_i}$和遮蔽因子$R_{\text{DPKG}_i}$, RA进行审核；审核通过后RA发送给节点：$(\text{Sig}_{\text{ID}_{\text{DPKG}_i}}, T_{\text{DPKG}_i})$，其中$\text{Sig}_{\text{ID}_{\text{DPKG}_i}} = s_0 H_1(\text{ID}_{\text{DPKG}_i} \| T_{\text{DPKG}_i})$, T_{DPKG_i}为节点DPKG_i的合法期限；空中组网阶段，n个DPKG相互协同，自组织完成系统密钥的生成，以其中DPKG_i与DPKG_j联系过程为例，说明系统密钥的具体生成过程，如图2所示。

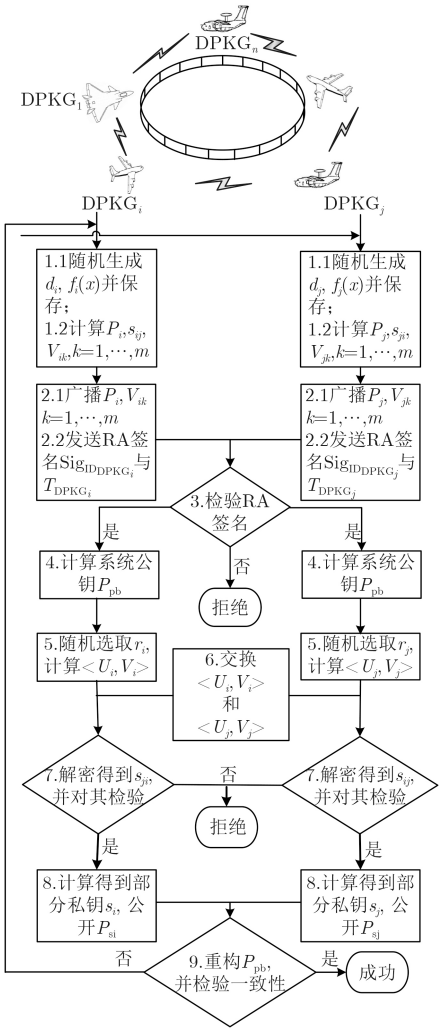

图 2 机载网络自组织系统密钥生成

第i个DPKG_i随机选择$d_i \in_{\text{rnd}} Z_q^*$，在有限域GF($q$)上随机选取$m-1$次多项式，

$$f_i(x) = d_i + \sum_{k=1}^{m-1} a_{ik} x^k \bmod q \tag{1}$$

计算$P_i = d_i P$和$V_{ik} = a_{ik} P(k = 1, 2, \cdots, m-1)$，并向其他$\text{DPKG}_j(j \neq i)$公开$P_i$和$V_{ik} = a_{ik} P(k = 1, 2, \cdots, m-1)$, DPKG_i以d_i为临时私钥，P_i为临时公钥，其中$i = 1, 2, \cdots, n$, m为门限值。

DPKG_i计算$f_i(j)$，并记为$s_{ij} = f_i(j)$，其中$j \neq i$，并计算

$$C = \langle U, V \rangle \tag{2}$$

其中$r_i \in_{\text{rnd}} Z_q$, $U = r_i P$, $V = s_{ij} \oplus H_2(g_j^{r_i})$, $g_j = e(P_j, P_{\text{pub}})$，并将$C$发送给$\text{DPKG}_j$。

DPKG_j对DPKG_i的有效期T_{DPKG_i}进行检查并验证式(3)是否成立。

$$e(\text{Sig}_{\text{ID}_{\text{DPKG}_i}}, P) = e(H_1(\text{ID}_{\text{DPKG}_i} \| T_{\text{DPKG}_i}), P_{\text{RA}}) \tag{3}$$

那么系统公钥为$P_{\text{pb}} = \sum_{i=1}^{n} P_i$，系统私钥为

$s=\sum_{i=1}^{n} d_i$，公钥P_{pb}可以由P_i相加得到，下面对私钥s的分配进行阐述。

DPKG$_j$收到C后，计算

$$V\oplus H_2(e(U,d_jP_{\mathrm{pub}}))=s_{ij} \tag{4}$$

并验证式(5)是否成立。

$$s_{ij}P=P_i+\sum_{k=1}^{m-1}V_{ik}j^k \tag{5}$$

验证通过后，待收到所有$s_{ij},(i=1,2,\cdots,j-1,j+1,\cdots,n)$后，结合自己持有的$s_{jj}=f_j(j)$，则DPKG$_j$分到的部分系统私钥$s_j=\sum_{i=1}^{n} s_{ij} \bmod q$，计算并公开$P_{\mathrm{sj}}=s_jP$，并以它为DPKG$_j$的公钥，丢弃临时公钥$P_i$。

DPKG$_j$任意选择m个DPKG的公钥$P_{\mathrm{sk}},k=1,2,\cdots,m$，验证

$$P_{\mathrm{pb}}=\sum_{k=1}^{m}\lambda_k(0)P_{\mathrm{sk}} \tag{6}$$

其中，$\lambda_k(x)=\prod_{l=1,l\neq k}^{m}\frac{x-k}{l-k}$，$\lambda_k(0)=\prod_{l=1,l\neq k}^{m}\frac{-k}{l-k}$。

如果正确，表示系统密钥的初始化成功，P_{pb}为系统公钥，系统私钥s为DPKG$_j(j=1,2,\cdots,n)$所共享，共享私钥为$s_j=\sum_{i=1}^{n} s_{ij} \bmod q$，公钥为$P_{\mathrm{sj}}=s_jP$。

3.2 用户密钥分布式管理算法

如图3所示，新入网节点h选择$r_h\in_{\mathrm{rnd}}Z_q^*$，计算遮蔽因子$R_h=r_hP$，然后联系RA进行离线注册，节点$h$向RA提交身份信息ID$_h$和遮蔽因子$R_h$, RA进行审核；审核通过后RA发送给节点$h$: $(\mathrm{Sig}_{\mathrm{ID}_h},T_h)$，其中$\mathrm{Sig}_{\mathrm{ID}_h}=s_0H_1(\mathrm{ID}_h\parallel T_h)$, T_h为节点h的合法期限。

新入网节点h收到RA的签名后，需要向至少m个DPKG提出私钥申请，计算公钥$Q_h=H_1(\mathrm{ID}_h\parallel T_h)\in G_1^*$，向DPKG$s$发送密钥申请REQ$=\{\mathrm{ID}_h,R_h,\mathrm{Sig}_{\mathrm{ID}_h},T_h\}$。

DPKG$_k(k=1,2,\cdots,m)$收到节点h的密钥申请后，检查T_h，并验证

$$e(\mathrm{Sig}_{\mathrm{ID}_h},P)=e(H_1(\mathrm{ID}_h\parallel T_h),P_{\mathrm{RA}}) \tag{7}$$

验证通过后DPKG$_k$选择$\mathrm{rr}_k\in_{\mathrm{rnd}}Z_q^*$，计算

$$\mathrm{REP}=\{Y,\mathrm{RR}_k,V_k\} \tag{8}$$

其中，$X_k=s_kH_1(\mathrm{ID}_h\parallel T_h)$, $Y=X_k\hat{+}\mathrm{rr}_kR_h$, $\mathrm{RR}_k=\mathrm{rr}_kP$, $V_k=s_kP_{\mathrm{pb}}$，并发送REP。

节点h收到REQ后，验证

$$e(V_k,P)=e(P_{sk},P_{\mathrm{pb}}) \tag{9}$$

若不成立，丢弃应答消息；若成立，通过

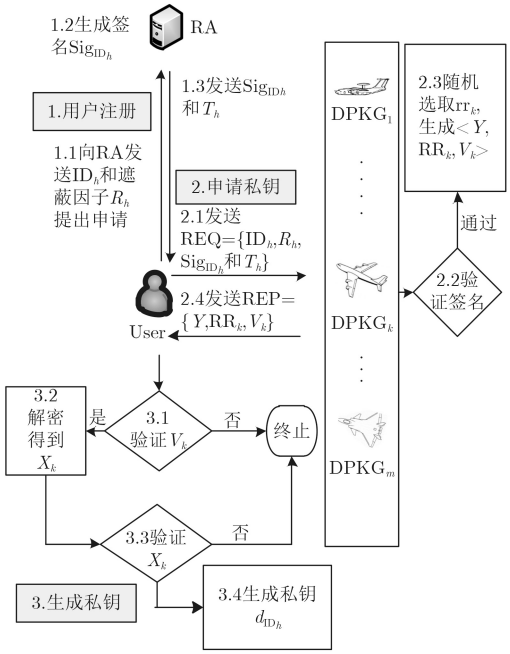

图 3 机载网络用户密钥管理

$$Y\hat{-}r_h\cdot\mathrm{RR}_k=X_k \tag{10}$$

解密得到DPKG$_k$签发的私钥份额X_k(其中$\hat{-}$表示G_1的加法$\hat{+}$的逆运算)。

节点h继续验证

$$e(X_k,P_{\mathrm{pb}})=e(H_1(\mathrm{ID}_h\parallel T_h),V_k) \tag{11}$$

若成立，则接受X_k；否则丢弃该节点签发的私钥份额X_k。

节点h在收到m个DPKG$_k$通过验证的私钥份额后$X_k(k=1,2,\cdots,m)$，利用式(12)的插值公式构建自己的私钥：

$$d_{\mathrm{ID}_h}=\sum_{k=1}^{m}\lambda_k(0)X_k \tag{12}$$

其中，$\lambda_k(0)=\prod_{l=1,l\neq k}^{m}\frac{-k}{l-k}$。

4 关键技术可行性分析

密钥管理方案的可行性分析的内容主要包括：方案中算法的正确性与协议的安全性两个方面分析。

4.1 正确性分析

定理 1 n个DPKG生成的密钥共享多项式为

$$F(x)=\sum_{i=1}^{n}f_i(x)=\sum_{i=1}^{n}\left(d_i+\sum_{k=1}^{m-1}a_{ik}x^k \bmod q\right) \tag{13}$$

系统私钥$s=\sum_{i=1}^{n} d_i=F(0)$，每个DPKG分到的部分系统私钥$s_j=F(j)$，公钥为$P_{\mathrm{sj}}=s_jP$，任意DPKG收集$m$个DPKG的公钥可以检验系统密钥

是否成功生成。

证明　在系统密钥自组织生成过程中，采用DPKG相互协同生成系统密钥的方法，以第j个DPKG为例，每个DPKG在有限域GF(q)上随机选取$m-1$次多项式$f_i(x)=d_i+\sum_{k=1}^{m-1}a_{ik}x^k \bmod q$，计算$s_{ij}=f_i(j),(j\neq i)$后，经过加密传输给其它DPKG，收到所有$s_{ij},(i=1,2,\cdots,j-1,j+1,\cdots,n)$后，结合自己持有的$s_{jj}=f_j(j)$，求和：

$$\begin{aligned}s_j&=\sum_{i=1}^{n}s_{ij} \bmod q=\sum_{i=1}^{n}f_i(j) \bmod q\\&=\sum_{i=1}^{n}\left(d_i+\sum_{k=1}^{m-1}a_{ik}j^k\right) \bmod q=F(j)\end{aligned}\tag{14}$$

$$F(x)=\sum_{i=1}^{n}f_i(x)=\sum_{i=1}^{n}\left(d_i+\sum_{k=1}^{m-1}a_{ik}x^k\right] \bmod q\Big),$$

则系统私钥$s=F(0)=\sum_{i=1}^{n}d_i$。

由于$F(x)$为$m-1$次多项式，m个以上DPKG通过拉格朗日插值公式恢复$m-1$次多项式，$F(x)\cdot P=\sum_{k=1}^{m}\lambda_k(x)P_{\rm sk}$，其中$\lambda_k(x)=\prod_{l=1,l\neq k}^{m}\frac{x-k}{l-k}$，则得到系统公钥$F(0)P=sP=P_{\rm pb}=\sum_{k=1}^{m}\lambda_k(0)P_{\rm sk}$，因此每个DPKG可以利用任意$m$个以上DPKG的公钥为$(k,P_{\rm sk})$检验系统密钥生成是否成功。　　证毕

定理 2　在系统密钥自组织生成过程中，每个DPKG通过式(2)，式(4)能够正确地传递s_{ij}。

证明　为了使用公开信道传递s_{ij}, DPKG之间利用达到选择明文安全的Boneh-Franklin方案[13]对s_{ij}进行加密传递，DPKG$_i$采用式(2)计算并传递$C=\langle U,V\rangle$, DPKG$_j$接收到后，通过式(4)计算$V\oplus H_2(e(U,d_jP_{\rm pb}))$。实际上$H_2(e(U,d_jP_{\rm pb}))=H_2(e(r_iP,d_jP_{\rm pb}))=H_2(e(P_j,P_{\rm pb})^{r_i})=H_2(g_j^r,V\oplus H_2(e(U,d_jP_{\rm pb}))=s_{ij}\oplus H_2(g_j^{r_i})\oplus H_2(e(U,d_jP_{\rm pb}))=s_{ij}$。　　证毕

定理3　在用户密钥分布式生成过程中，通过式(8)，式(10)用户和DPKG可以正确传递部分私钥生成元X_k，通过式(9)，式(11)可以验证DPKG的合法性。

证明　用户h收到DPKG的式(8)回复REP后，计算式(10)的$Y\hat{-}r_h\cdot{\rm RR}_k$得到$X_k$，实际上$r_h\cdot{\rm RR}_k=r_h\cdot{\rm rr}_k\cdot P={\rm rr}_kR_h$, $Y\hat{-}{\rm rr}_kR_h=X_k\hat{+}{\rm rr}_kR_h\hat{-}r_h{\rm RR}_k=X_k$，式(9)中$e(V_k,P)=e(s_kP_{\rm pb},P)=e(s_kP,P_{\rm pb})=e(P_{\rm pb},P_{\rm sk})$，式(11)中，$e(X_k,P_{\rm pb})=e(s_kH_1({\rm ID}_h\parallel T_h),P_{\rm pb})=e(H_1({\rm ID}_h\parallel T_h),s_kP_{\rm pb})=e(H_1({\rm ID}_h\parallel T_h),V_k)$，因此，用户可以通过两个双线性对分别验证DPKG发送的Y和X_k的合法性。　　证毕

4.2 安全性分析

(1)系统主密钥的机密性：攻击者企图利用公开的P和$P_{\rm pb}$，以及在系统密钥生成过程中攻击者可以监听到与主密钥有关的参数$P_i,P_{\rm si}$，通过n个P_i，求和可以得到$\sum_{i=1}^{n}P_i=\sum_{i=1}^{n}d_iP=\left(\sum_{i=1}^{n}d_i\right)P=sP$，由$m$个$P_{\rm sk}$, $k=1,2,\cdots,m$，通过拉格朗日插值可以得到$sP=\sum_{k=1}^{m}\lambda(0)P_{\rm sk}$，窃取主密钥需要面对求解离散对数问题的困难。

(2)用户私钥的机密性：在用户密钥分布式生成过程中，DPKG利用掌握的部分系统私钥生成$X_k=s_kH_1({\rm ID}_h)$，经过遮蔽因子R_h加密后，和恢复消息${\rm REQ}=\{Y,{\rm RR}_k,V_k\}$一起发送给用户$h$。攻击者通过监听可以收集到REQ, $Y=X_k\hat{+}{\rm rr}_kR_h$，要知道$X_k$，必须得到${\rm rr}_kR_h$，攻击者还可能监听到${\rm RR}_k={\rm rr}_kP$和$R_h=r_hP$，得到${\rm rr}_kR_h$需要面对计算双线性Diffie-Hellman(CBDH)困难问题。

(3)抗假冒攻击：在系统密钥自组织生成过程中，假冒DPKG的节点无法通过RA审查，所以只能伪造RA的签名${\rm Sig}'_{{\rm DPKG}_i}$。在系统密钥产生过程中自主生成$d'_i$和$f'_i(x)$，计算$P'=d'_iP$, $f'_i(j)$和${\rm Sig}'_{{\rm DPKG}_i}$发送给DPKG$_j$，显然无法通过$e({\rm Sig}'_{{\rm DPKG}_i},P)=$验证，因为伪造RA的签名需要求解离散对数问题(DLP)。在用户密钥分布式生成过程中，同样设置了双线性对验证进行检验。

(4)抗重放攻击：在系统密钥自组织生成过程中，DPKG之间传输s_{ij}时，通过随机选取r_i，计算$U=r_iP$, $V=s_{ij}\oplus H_2(g_j^{r_i})$, $g_j=e(P_j,P_{\rm pb})$，通过加密传输，其中加密体制达到了随机预言模型下的选择明文安全[12]。随机数r_i的选取可以防止攻击者重放以前获得的信息，由于每次选择的r_i不同，攻击者重放以前的$<U,V>$，收到后DPKG会比较$<U,V>$，如果发现相同，则可断定对方在重放消息。在用户密钥分布式生成过程中，${\rm REQ}=\{Y,{\rm RR}_k,V_k\}$的$Y=X_k\hat{+}{\rm rr}_kR_h$, ${\rm RR}_k={\rm rr}_kP$，同样选择了随机数${\rm rr}_k$，保证了REQ的不同。

(5)抗中间人攻击：在系统密钥自组织生成过程中，攻击者在DPKG$_i$和DPKG$_j$之间传递$<U,V>$前，首先进行RA的签名验证，即使DPKG$_i$发生叛变生成不正确的s'_{ij}，发送给DPKG$_j$，从而阻止系统密钥的生成，最后DPKG$_j$也能通过选择任意m个$P_{\rm sk}$, $(k=1,2,\cdots,m)$，生成系统公钥并验证$P_{\rm pb}=\sum_{k=1}^{m}\lambda_k(0)\cdot P_{\rm sk}$，可以发现是否有人阻止密钥的生成。

5　性能分析

为适应机载自组网的无中心特征，本文的系统

密钥采用基于Lagrange内插公式秘密共享理论的自组织生成方式，且可以事先预处理完成，因此性能分析主要考虑用户密钥的分布式生成产生的开销。基于身份密码的机载自组网密钥管理方案与其它分布式密钥管理方案性能比较分析，如表1所示，文献[17]的用户私钥采用在线分布式更新对用户身份进行验证，但是在系统密钥份额的分发过程中需要建立安全的私有信道；文献[18]中系统私钥的生成采取完全自组织方式，需要节点的完全配合，适用于普通无线自组网环境，但容错率低是其不足之处；文献[19]将用户私钥的生成进行外包处理，不仅降低了中心服务器的运算开销，而且促成了密钥的分布式生成，但其节点间的通信量较多，容易加大时延；文献[20]对用户密钥份额进行加密处理，无需安全信道保障便可完成用户密钥的管理任务，但没有对系统密钥份额的更新进行研究；本文方案采取部分自组织方式生成系统密钥，分布式管理用户私钥，虽然增加了一些计算量和通信开销，和其它文献的计算量和通信开销相比并没有优势，增加的开销对于像无线传感器网络这样的低开销网络或许难以承受，但对于机载网络则不成问题。综合比较分析，本文方案在增加少量计算量和通信量的情况下，确保机载自组网的密钥管理自组织、分布式进行，有利于安全性的提升，同时由于其全程无需安全信道，使该方案易于以后的具体实施。

表 1 性能比较

方案	F1	F2	F3	F4	F5	F6
文献[17]	是	否	否	$(m-1)/n$	$4P+(7+m)M$	$2m$
文献[18]	是	是	否	$1/n$	$3P+(3+m)M$	$3m$
文献[19]	否	否	是	$(m/2)/n$	$2P+7M$	$4m$
文献[20]	是	是	否	$(m-1)/n$	$6P+(3+m)M$	$2+2m$
本文方案	是	是	是	$(m-1)/n$	$6P+(4+m)M$	$2+2m$

表1中F1：身份验证；F2：自组织生成系统密钥；F3：系统密钥加密处理；F4：容忍度(m表示门限，n表示用户数量)；F5：用户密钥生成的计算开销(P表示双线性对运算，M表示数乘运算)；F6：用户密钥生成的通信开销。

6 结束语

密钥管理是机载自组网安全管理最薄弱却又最关键的环节，本文提出了一种无需安全信道的机载自组网动态密钥管理方案，仅依靠节点的相互协作自组织生成系统公私钥，并由系统私钥持有节点分布式生成用户密钥，使用遮蔽因子加密系统私钥分片和用户私钥分片，实现公开信道传递私钥，最后对其正确性、安全性进行了分析证明，结果表明该方案能够抵抗假冒攻击、重放攻击、中间人攻击。另外，分布式密钥管理一直以来都是机载网络的研究重点与热点，下一步将着力研究会话密钥协商。

参 考 文 献

[1] 李杰, 宫二玲, 孙志强, 等. 下一代机载网络技术评述[J]. 指挥与控制学报, 2015, 1(3): 351–356. doi: JCC.CN.2015.00351.
LI Jie, GONG Erling, SUN Zhiqiang, *et al*. An overview of next generation airborne networks[J]. *Journal of Command and Control*, 2015, 1(3): 351–356. doi: JCC.CN.2015.00351.

[2] 梁一鑫, 程光, 郭晓军, 等. 机载网络体系结构及其协议栈研究进展[J]. 软件学报, 2016, 27(1): 96–111. doi: 10.13328/j.cnki.jos.004925.
LIANG Yixin, CHENG Guang, GUO Xiaojun, *et al*. Research progress on architecture and protocol stack of the airborne network[J]. *Journal of Software*, 2016, 27(1): 96–111. doi: 10.13328/j.cnki.jos.004925.

[3] SHANTHI K and MURUGAN D. Pair-wise key agreement and hop-by-hop authentication protocol for MANET[J]. *Wireless Networks*, 2016, 23(4): 1–9. doi: 10.1007/s11276-015-1191-x.

[4] PHUNG P H and MINH Q T. DASSR: A distributed authentication scheme for secure routing in wireless ad-hoc networks[C]. International Conference on Future Data and Security Engineering. Can Tho, Vietnam, 2016: 219–236. doi: 10.1007/978-3-319-48057-216.

[5] DONG Ying, SUI Aifeng, YIU S M, *et al*. Providing distributed certificate authority service in cluster-based mobile ad hoc networks[J]. *Computer Communications*, 2007, 30(11/12): 2442–2452. doi: 10.1016/j.comcom.2007.04.011.

[6] 韩磊, 刘吉强, 赵佳, 等. 移动ad hoc网络分布式轻量级CA 密钥管理方案[J]. 四川大学学报(工程科学版), 2011, 43(6): 133–139. doi: 10.15961/j.jsuese.2011.06.021.
HAN Lei, LIU Jiqiang, ZHAO Jia, *et al*. Distributed lite CA key management scheme in mobile ad hoc networks[J]. *Journal of Sichuan University (Engineering Science Edition)*, 2011, 43(6): 133–139. doi: 10.15961/j.jsuese.2011.

06.021.

[7] DATKO B. Supporting secure, ad hoc joins for tactical networks[R]. Maryland: United States Naval Academy Trident Scholar Project Report, 2002.

[8] CAPKUN S, NUTTYAN L, and HUBAUX J P. Self-organized public-key management for mobile ad hoc networks[J]. *IEEE Transactions on Mobile Computing*, 2003, 2(1): 52–64. doi: 10.1109/TMC.2003.1195151.

[9] RAFSANJANI M K and SHOJAIEMEHR B. Improvement of self-organized public key management for MANET[J]. *Journal of American Science*, 2012, 8(1): 197–202.

[10] JANANI V S and MANIKANDAN M S K. Trust-based hexagonal clustering for efficient certificate management scheme in mobile ad hoc networks[R]. Sadhana, 2016. doi: 10.1007/s12046-016-0545-0.

[11] OMAR M, BOUFAGHES H, MAMMERI L, *et al*. Secure and reliable certificate chains recovery protocol for mobile ad hoc networks[J]. *Journal of Network & Computer Applications*, 2016, 62(C): 153–162. doi: 10.1016/j.jnca.2016.01.007.

[12] SHAMIR. Identity-based cryptosystems and signature schemes[J]. *LNCS*, 1984, 21(2): 47–53. doi: 10.1007/3-540-39568-75.

[13] BONEH D and FRANKLIN M. Identity-based encryption from the weil pairing[C]. International Cryptology Conference on Advances in Cryptology. Santa Barbara, USA, 2001: 213–229. doi: 10.1007/3-540-44647-8_13.

[14] 曹丹, 王小峰, 王飞, 等. SA-IBE: 一种安全可追责的基于身份加密方案[J]. 电子与信息学报, 2011, 33(12): 2922–2928. doi: 10.3724/SP.J.1146.2011.00399.

CAO Dan, WANG Xiaofeng, WANG Fei, *et al*. SA-IBE: A secure and accountable identity-based encryption scheme[J]. *Journal of Electronics & Information Technology*, 2011, 33(12): 2922–2928. doi: 10.3724/SP.J.1146.2011.00399.

[15] ZHANG Tao, YUE Kang, and YAN Jinkui. A distributed anonymous authentication scheme for mobile ad hoc network from bilinear maps[C]. International Conference on Mechatronic Science, Electric Engineering and Computer. Jilin, China, 2011: 314–318. doi: 10.1109/mec.2011.6025464.

[16] NARAYANA V L and BHARATHI C R. Identity based cryptography for mobile ad hoc networks[J]. *Journal of Theoretical and Applied Information Technology*, 2017, 95(5): 1173–1182.

[17] 罗长远, 李伟, 邢洪智, 等. 空间网络中基于身份的分布式密钥管理研究[J]. 电子与信息学报, 2010, 32(1): 183–188. doi: 10.3724/SP.J.1146.2009.00461.

LUO Changyuan, LI Wei, XING Hongzhi, *et al*. Research on identity-based distributed key management in space network[J]. *Journal of Electronics & Information Technology*, 2010, 32(1): 183–188. doi: 10.3724/SP.J.1146.2009.00461.

[18] XIA Pengrui, WU Meng, WANG Kun, *et al*. Identity-based fully distributed certificate authority in an OLSR MANET[C]. International Conference on Wireless Communications, Networking and Mobile Computing. Dalian, China, 2008: 1–4. doi: 10.1109/wicom.2008.614.

[19] 任艳丽, 蔡建兴, 黄春水, 等. 基于身份加密中可验证的私钥生成外包算法[J]. 通信学报, 2015, 36(11): 61–66. doi: 10.11959/j.issn.1000-436x.2015233.

REN Yanli, CAI Jianxing, HUANG Chunshui, *et al*. Verifiable outsourcing private key generation algorithm in an identity-based encryption scheme[J]. *Journal of Communications*, 2015, 36(11): 61–66. doi: 10.11959/j.issn.1000-436x.2015233.

[20] 李慧贤, 庞辽军, 王育民. 适合ad hoc网络无需安全信道的密钥管理方案[J]. 通信学报, 2010, 31(1): 112–117.

LI Huixian, PANG Liaojun, and WANG Yumin. Key management scheme without secure channel for ad hoc networks[J]. *Journal of Communications*, 2010, 31(1): 112–117.

王　宏：男，1979年生，博士生，讲师，研究方向为航空自组网信息安全.

李建华：男，1965年生，博士，教授，博士生导师，研究方向为空天信息网络建设.

赖成喆：男，1985年生，博士，副教授，硕士生导师，研究方向为车载网络信息安全.