航空自组网漫游接入认证方案

黄后彪，罗长远，宋玉龙
（解放军信息工程大学 电子技术学院，郑州 450004）

摘　要：当飞机节点漫游到外地空域通信时必须经过身份认证，而现有的认证方案无法同时满足认证的匿名性和高效率，因此针对航空自组网设计了一种基于身份的漫游接入认证方案。在本方案中飞机节点使用由认证服务器生成的部分私钥与用户生成的秘密值共同产生的签名私钥，与外地空域内的飞机节点进行身份认证。外地飞机节点使用的签名验证算法的验证结果是一个常量，在保证漫游接入认证安全性的同时实现了用户匿名性和不可跟踪性。而且本方案避免了复杂的双线性运算，提高了漫游接入认证的效率。分析表明，该方案同时具有安全性和效率上的优势。

关键词：航空自组网；漫游；基于身份的认证；匿名
中图分类号：TP393　　**文献标志码**：A　　**文章编号**：1001-3695(2013)02-0500-03
doi:10.3969/j.issn.1001-3695.2013.02.050

Authentication scheme for roaming in aeronautical Ad hoc networks

HUANG Hou-biao, LUO Chang-yuan, SONG Yu-long
(*Institute of Electronic Technology*, *PLA Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: Authentication is a crucial security requirement when one aircraft communicating with other aircrafts belong to another domain. For the existing scheme can not satisfied with user anonymity and high efficiency at the same time, this paper proposed a identity-based authentication scheme for roaming in aeronautical Ad hoc networks. It constructed the aircraft authenticate with aircrafts in other domain with the private key by partial private key and the secret value. The verification result of the signature was a constant with respect to the signer's identifier, which realized secure authentication and user anonymity. And this scheme avoided the pairing operation. It is shows that the proposed scheme has superiority in both security and efficiency.

Key words: aeronautical Ad hoc networks; roaming; identity-based authentication; anonymity

0　引言

航空自组网是一种具有高动态、大尺度、临时性、无中心节点等特点的无线自组织网络，用于飞机之间一跳或者多跳的数据通信。在航空自组织网络中，当飞机节点漫游到外地空域时，必须首先在外地认证服务器进行注册。当需要与外地空域中的其他飞机节点进行通信时，再利用外地认证服务器颁发的注册信息与通信对象进行身份认证，这样才能保证安全的会话通信。而在整个认证过程中，为了防止恶意的攻击者跟踪飞机节点的位置，漫游接入认证方案在实现安全认证和会话密钥建立的同时应满足匿名性和不可跟踪性，即外地空域内的认证服务器和其他飞机节点无法确定漫游飞机节点的真实身份，并且外地域中的飞机节点无法确定不同的会话来自相同的用户。其次，航空自组网中的飞机节点具有能量受限以及计算能力有限等特点，所以提高认证方案的效率也十分重要。图 1 为飞机节点漫游模型。

文献[1]提出了一种基于超立方体的跨域认证协议，减少了认证服务器的工作量，避免了网络瓶颈和单节点失效问题，具有较高的安全性和效率。但该方案无法实现用户的匿名认证。文献[2]设计了一种基于身份的部分盲签名方案，证明了该方案在随机预言机模型下具有自适应选择消息和身份攻击下存在不可伪造性，其安全性能够归约为计算 Diffie-Hellman 问题。但是该方案中用户需要进行多次双线性对运算，用户计算开销较大。文献[3]提出了一种新的基于身份的跨域匿名认证方案，方案通过减少双线性对运算次数提高了执行效率。但是方案在匿名性方面存在缺陷，因为当用户首次跨域认证后获得了一个临时证书，在之后的资源访问中，用户利用相同的临时证书作为认证凭证，这会使用户的会话被跟踪。文献[4]提出了一种基于身份的一次性跨域签名认证方案，该方案具有较高的效率，但是无法实现匿名认证，容易使得用户会话被跟踪。文献[5]解决了传统的基于身份的跨域两方密钥协商协议中固有的密钥托管问题，实现了跨域通信双方的身份验证，防止了主动攻击，有较好的安全性和认证性。但是该方案中用户需要进行多次双线性对运算，用户计算开销较大，效率较低。文献[6]提出一种基于身份的跨域认证方案，认证服务器只需在用户首次跨域认证时进行域间通信，在之后的跨域认证过程中，无须进行域间通信，避免了域间通信造成的过大时间延迟。但是该方案中用户需要进行多次双线性对运算，用户计算开销较大。

收稿日期：2012-06-21；**修回日期**：2012-07-28

作者简介：黄后彪(1986-)，男，江苏扬州人，硕士研究生，主要研究方向为无线网络安全(932430557@qq.com)；罗长远(1973-)，男，河南信阳人，副教授，硕导，博士，主要研究方向为装备工程、无线通信系统安全；宋玉龙(1988-)，男，黑龙江大庆人，硕士研究生，主要研究方向为无线网络安全.

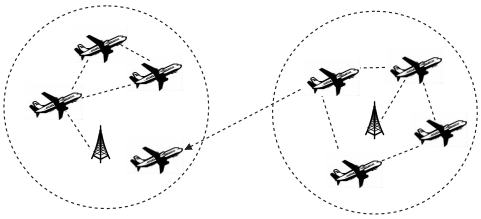

图 1　飞机节点漫游模型

本文在分析上述方案的基础上,设计了一种适用于航空自组网环境中基于身份的漫游接入认证方案。本方案在保证用户节点与外地空域中用户节点之间安全认证的前提下实现了认证的匿名性,并减少了用户节点的计算开销。经过分析,本方案可以满足航空自组网环境中漫游接入认证的安全性要求,并具有较高的效率。

1　漫游接入认证方案

1.1　系统结构

如图 2 所示,系统包括两个安全域 H 和 F,各个安全域中都有一个认证服务器对本域中的资源和用户节点进行管理,为访问本域资源的用户提供认证服务。用户节点 M 是属于安全域 H 的,安全域 H 中的认证服务器称为 HA(home authenticator);安全域 F 中的认证服务器称为 FA(foreign authenticator)。用户 M 事先在 HA 处进行注册,HA 为 M 签发基于身份的私钥,并为用户建立账户。当用户 M 访问安全域 H 中的资源时,可以直接通过 HA 的认证。但是,当用户 M 访问安全域 F 中资源时,FA 可以通过有线网络联合 HA 来对用户进行认证。本方案的安全性基于以下假设:HA 和 FA 都是诚实的,并互相信任对方作出的判断。

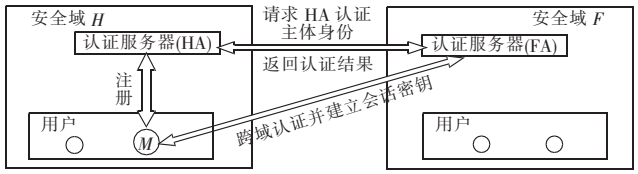

图 2　系统结构

1.2　系统初始化

1)系统建立

家乡认证服务器(HA)选择椭圆曲线$E(F_p)$上的 q 阶循环加法群 G,G 的生成元为 P。随机选择$k \in Z_q^*$ 作为系统主密钥,系统公钥为 $P_{\text{pub}} = kP \in G$。定义以下安全的哈希函数:

$$H_1:\{0,1\}^* \times G \to Z_q^*, H_2:\{0,1\}^* \to Z_q^*, H_3:G \to \{0,1\}^*$$

HA 公开系统参数$\{G,q,P,P_{\text{pub}},H_1,H_2,H_3\}$。外地认证服务器(FA)选择椭圆曲线 $E(F_p)$ 上的 q 阶循环加法群 G,G 的生成元为 P。随机选择 $k' \in Z_q^*$ 作为系统主密钥,系统公钥为 $P'_{\text{pub}} = k'P \in G$。定义相同的安全哈希函数 H_1、H_2、H_3,FA 公开系统参数$\{G,q,P,P'_{\text{pub}},H_1,H_2,H_3\}$。

2)用户注册

假设飞机节点 M 的身份标志为 ID_M。M 加入网络时,需要在家乡认证服务器 HA 处注册,该步骤可以在离线状态完成。其过程如下:

a)M 随机选择 $t_M \in Z_q^*$ 作为秘密数,计算 $R_1 = t_M P$,然后将 R_1 和 ID_M 发送给 HA。

b)HA 随机选择 $g_M \in Z_q^*$,计算 $R_2 = g_M P$,$R_M = R_1 + R_2$,计算 $s = H_1(\text{ID}_M, R_M)$,计算部分私钥 $d_M = g_M + ks$。HA 将 R_M 和 d_M 通过安全信道发送给 M。HA 为 M 建立账户$(\text{Ind}_M, \text{ID}_M, R_M)$,其中账户索引为 $\text{Ind}_M = R_M + H_1(\text{ID}_M, R_M)P_{\text{pub}}$。

c)M 通过检验$(d_M + t_M)P = R_M + H_1(\text{ID}_M, R_M)P_{\text{pub}}$是否成立来验证部分私钥的正确性,验证通过后 M 安全地保存 R_M 和 d_M。

1.3　全认证协议

当飞机节点 M 飞行到外地地面指挥站覆盖的区域,并与该区域的飞机节点首次进行通信时,需要运行如图 3 所示流程的全认证协议。

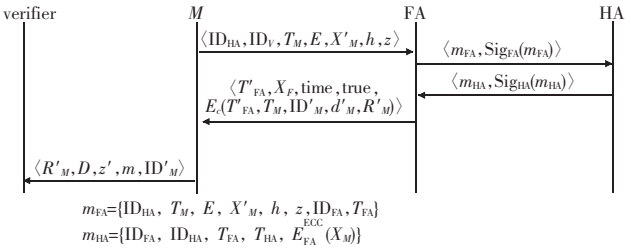

图 3　全认证协议流程

a)用户 M 随机选择 $e, x_M \in Z_q^*$,获取当前时戳 T_M,计算 $X_M = x_M P$,$E = eP$,$X'_M = X_M + eP_{\text{pub}}$,$h = H_2(\text{ID}_M, T_M, R_M, X_M)$,计算签名 $z = x_M + (d_M + t_M)h$。然后发送消息$\langle \text{ID}_{\text{HA}}, \text{ID}_V, T_M, E, X'_M, h, z, R_1 \rangle$给 FA,其中 ID_V 是 M 想与之通信的节点身份信息。

b)FA 收到消息后,检验 T_M 的新鲜性。若 T_M 新鲜,FA 获取当前时戳 T_{FA},构造消息 $m_{\text{FA}} = \{\text{ID}_{\text{HA}}, T_M, E, X'_M, h, z, \text{ID}_{\text{FA}}, T_{\text{FA}}\}$,计算消息的签名 $\text{Sig}_{\text{FA}}(m_{\text{FA}})$,FA 向 HA 发送消息$\langle m_{\text{FA}}, \text{Sig}_{\text{FA}}(m_{\text{FA}}) \rangle$。Sig()为椭圆曲线签名算法 ECDSA,生成签名算法需要一次点积、两次模乘和一次乘法逆元运算,时间复杂度为 $O(11n^2 \log n + n^2)$。签名验证算法过程需要两次点积、两次模乘和一次乘法逆元运算,时间复杂度为 $O(11n^2 \log n + 2n^2)$。FA 与 HA 整个认证过程的时间复杂度在航空自组网中是可以接受的。

c)HA 收到消息后,若 T_{FA}新鲜,且签名 $\text{Sig}_{\text{FA}}(m_{\text{FA}})$验证正确,则 HA 通过对 FA 的认证。HA 计算 $X_M = X'_M - kE$,计算 $\text{Ind}_M = h^{-1}(zP - X_M)$,然后在用户列表中检索 Ind_M。若存在以 Ind_M 为索引的账户,则取出账户信息验证 $h = H_2(\text{ID}_M, T_M, R_M, X_M)$是否成立,若成立则通过对用户 M 的认证。HA 获取当前时戳 T_{HA},构造消息 $m_{\text{HA}} = \{\text{ID}_{\text{FA}}, \text{ID}_{\text{HA}}, T_{\text{FA}}, T_{\text{HA}}, E^{\text{ECC}}_{P'_{\text{pub}}}(X_M)\}$,计算消息的签名 $\text{Sig}_{\text{HA}}(m_{\text{HA}})$。$E^{\text{ECC}}$为椭圆曲线加密算法,向 FA 发送消息$\langle m_{\text{HA}}, \text{Sig}_{\text{HA}}(m_{\text{HA}}) \rangle$。

d)FA 收到消息后,若 T_{HA}新鲜且签名验证正确,则通过对 HA 和 M 的认证,即相信用户 M 为 HA 中的合法用户。FA 查询用户列表,若节点 V 是它的合法用户,则输出 true,否则输出 false。FA 解密 $E^{\text{ECC}}_{P'_{\text{pub}}}(X_M)$获得 X_M,选择随机数 $x_F \in Z_q^*$,计算 $X_F = x_F P$,计算会话密钥 $c = H_3(x_F, X_M)$,并为用户 M 生成一个临时身份 ID'_M。FA 生成 M 基于身份的私钥:FA 随机选择 $g'_M \in Z_q^*$,计算 $R'_2 = g'_M P$,$R'_M = R_1 + R'_2$,计算 $s' = H_1(\text{ID}'_M, R'_M)$,计算临时部分私钥 $d'_M = g'_M + k's'$。FA 获取时戳 T'_{FA},向 M 发送消息$\langle T'_{\text{FA}}, X_F, \text{true/false}, \text{time}, E_c(T'_{\text{FA}}, T_M, \text{ID}'_M, d'_M, R'_M) \rangle$,time 为临时部分私钥的有效期,$E$ 为对称加密算法。

e)用户 M 收到消息后,若 T'_{FA}新鲜,则计算 $c = H_3(x_M,$

X_F),解密 $E_c(T'_{FA}, T_M, ID'_M, d'_M, R'_M)$,并核对 T'_{FA} 和 T_M,若一致则通过对 FA 的认证。M 通过检验 $(d'_M + t_M)P = R'_M + H_1(ID'_M, R'_M)P'_{pub}$ 是否成立来验证临时部分私钥的正确性,验证通过后 M 安全地保存 R'_M、d'_M 和 ID'_M。如果 FA 返回的查询信息是 false,则 M 放弃与节点 V 的通信;否则用户 M 对消息 $m \in \{0,1\}^*$ 的签名过程如下:

(a)用户 M 随机选择 $d \in Z_q^*$,计算 $D = dP$;

(b)计算 $l = H_2(ID'_M, m, R'_M, D)$,计算 $z' = d + l(d'_M + t_M)$,则 M 对 m 的签名为 $\sigma = (R'_M, D, z')$。

M 将签名 $\sigma = (R'_M, D, z')$、消息 m 和身份标志 ID'_M 发送给节点 V。

f)节点 V 对签名进行验证:

(a)V 计算 $b = H_1(ID'_M, R'_M)$ 和 $l = H_2(ID'_M, m, R'_M, D)$;

(b)验证等式

$$b^{-1}(l^{-1}(z'P - D)) - R'_M = P'_{pub} \quad (1)$$

是否成立,若成立则输出“真”,否则输出“假”。

2 安全性分析

1)提出的漫游接入认证方案满足以下安全特性:

a)双向身份认证

在全认证过程中,方案可实现各实体间的双向身份认证。

HA 对用户 M 的认证:在 1.3 节步骤 c)中 HA 完成了对用户 M 的认证,该认证过程实质上是对签名 (X'_M, h, z) 的验证过程。

HA 与 FA 之间的认证:它是通过验证对方的签名来实现的,由于所用的签名算法 ECDSA 是安全的,所以 HA 与 FA 之间的认证是安全的。

用户 M 对 FA 的认证:在 1.3 节步骤 e)中,用户 M 通过解密 $E_c(T'_{FA}, T_M)$ 并核对 T'_{FA} 和 T_M 完成对 FA 的认证。因为 HA 将密钥参数 X_M 利用 FA 的公钥加密传送,只有合法的 FA 可以利用私钥解密得到密钥参数 X_M,进而结合自己选择的密钥参数 x_F 计算出正确的密钥 c。

FA 对用户 M 的认证是通过 FA 认证 HA 和 HA 认证用户 M 间接实现的。

用户 M 对节点 V 的认证:FA 通过查询它的用户列表,返回节点 V 的身份是否合法。

节点 V 对 M 的认证:节点 V 通过 1.3 节步骤 f)对节点 M 的签名进行认证,从而得出节点 M 是否是合法节点。

b)安全的会话密钥协商和更新

在认证过程中,用户 M 和 FA 可以建立安全的会话密钥 $c = H_3(x_M, X_F)$。在 1.3 节步骤 e)中用户 M 通过解密 $E_c(T'_{FA}, T_M)$ 并核对 T'_{FA} 和 T_M 可以确认 FA 确实获得了正确的会话密钥 c。协商的密钥满足已知会话密钥安全、前向安全性和密钥控制安全。

c)用户身份匿名性

FA 中的飞机节点和 FA 无法确定用户 M 的真实身份。在全认证过程中,用户 M 提交的认证信息中没有身份信息,并且只有 HA 可以通过验证签名计算出用户的账户索引,因此除了 HA 以外,其他用户和 FA 无法确定用户 M 的真实身份。而且对于任何用户,其签名的验证结果 P'_{pub} 是一个确定的常量。因此,验证者无法确定不同的消息是否来自相同的用户,保证漫游接入认证中用户身份的匿名性。

2)安全性证明

文献[7]提出了一种无双线性对运算的基于身份的签名算法 T-IBS。该算法是基于椭圆曲线加法群实现的,不需要复杂的双线性对运算,具有较高的运行效率,并且在随机预言机模型下证明了该算法的安全性。但是该算法中提出的签名验证结果相对于签名者身份是变量,不能实现匿名认证。因此本文将文献[7]算法的验证等式 $l = H_2(ID'_M, m, R'_M, z'P - l(R'_M + H_1(ID'_M, R'_M)P'_{pub}))$ 进行了改进,提出了一种新的基于身份的签名算法。本验证算法的签名验证等式为 $b^{-1}(l^{-1}(z'P - D)) - R'_M = P'_{pub}$,验证结果是一常量,而且与原算法具有相同的安全性,并将该算法运用在了漫游接入认证方案的签名验证过程中(1.3 节步骤 f))。

定义攻击者 A:A 代表第三方攻击者,A 没有用户的秘密值,但是知道用户的部分私钥或系统主密钥。

文献[7]证明了其算法对于攻击者 A 是不可伪造的。下面证明本算法对于攻击者 A 是不可伪造的。

定理 1 如果算法 T-IBS 中对于攻击者 A 是不可伪造的,则本算法对于攻击者 A 同样是不可伪造的。

证明 假设攻击者 A 能够在时间 t 内以不可忽略的概率 α 伪造出 ID'_M 对消息 m 的有效签名 $\sigma = (R'_M, D, z')$,则攻击者 A 能够在时间 t 内以不可忽略的概率 α 伪造出 ID'_M 对消息 m 的有效 T-IBS 签名 (R'_M, l, z')。

若 A 能够伪造出 ID'_M 对消息 m 的有效签名 $\sigma = (R'_M, D, z')$,则 A 可计算 $l = H_2(ID'_M, m, R'_M, D)$,并输出 $\sigma' = (R'_M, l, z')$ 作为 ID'_M 对消息 m 的 T-IBS 签名。σ' 将是一个有效的伪造,若式(2)成立:

$$l = H_2(ID'_M, m, R'_M, z'P - l(R'_M + H_1(ID'_M, R'_M)P'_{pub})) \quad (2)$$

由于 $\sigma = (R'_M, D, z')$ 是一个有效的签名,则式(3)成立:

$$b^{-1}((l^{-1}(z'P - D)) - R'_M) = P'_{pub} \quad (3)$$

式(3)两边同乘以 b 得

$$l^{-1}(z'P - D) - R'_M = bP'_{pub} \quad (4)$$

式(4)两边同加上 R'_M 得

$$l^{-1}(z'P - D) = R'_M + bP'_{pub} \quad (5)$$

式(5)两边同乘以 l 得

$$z'P - D = l(R'_M + bP'_{pub}) \quad (6)$$

由式(6)得

$$D = z'P - l(R'_M + bP'_{pub}) \quad (7)$$

将式(7)代入 $l = H_2(ID'_M, m, R'_M, D)$ 得

$$l = H_2(ID'_M, m, R'_M, z'P - l(R'_M + H_1(ID'_M, R'_M)P'_{pub}))$$

因此,式(2)成立,定理 1 成立,本算法对于攻击者 A 是不可伪造的。

3 效率分析

该方案具有较小的通信开销,因为只在用户节点首次漫游接入时,FA 和 HA 联合对用户身份进行认证时需要域间通信。用户之后在有效期内进行跨域访问时不需要进行域间通信。

对方案的关键部分全认证协议的效率进行分析,并与文献[3,6]中的方案进行比较,如表 1 所示。在比较计算开销时,考虑的运算类型包括双线性对运算(P)、椭圆曲线加法群上的点乘运算(Pm)和映射到椭圆曲线上点的哈希运算(MtP)。相对于上述运算,其他运算(如椭圆曲线群上的点加运算、普通哈希运算)的开销可忽略不计。

(下转第 506 页)

d)公开验证性

当遇到纠纷时,接收组只需将(R,S,ch)提交给仲裁方,即可验证密文的真伪。整个验证过程不需要明文和接收者的私钥,方案满足公开验证性。

e)具有密钥短和安全性高优势

该方案充分发挥了 HECC 密钥短、安全性高的优点。如果所选超椭圆曲线亏格为 3,所基于的有限域为 60 bit,方案的安全性与 180 bit 的 ECC 等同,远远大于 1 024 bit 的 RSA。因此该方案特别适用于解决带宽受限网络的安全问题。

3 结束语

新方案同时具有(t,n)门限签密和(k,l)门限共享验证功能,在保留已有门限群签名方案优点的基础上,克服了 PLL 和 WR 方案的安全缺陷,对签密合成员合成的签密进行验证,在门限解签名阶段用先验证签密后解密的方式避免了恶意信息的攻击,满足可公开验证性。利用 Desmedt 等人的密钥重新分配协议的思想,密钥保存不变,成员或子密钥不断更新,建立在超椭圆曲线密码体制上,具有更高的安全性,其运算效率、操作数相对于其他公钥密码体制有较大的优势,具有很好的实用性。

参考文献:

[1] ZHENG Yu-liang. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption)[C]// Proc of the 17th Annual International Cryptology Conference on Advances in Cryptology. Berlin:Springer-Verlag,1997:165-179.

[2] WANG C T,CHANG C C,LIN C H. Generalization of threshold signature and authenticated encryption for group communications[J]. IEICE Trans on Fundamentals,2000,E83-A(6): 1228-1237.

[3] TSENG Y M,JAN J K,CHIEN H Y. On the security of generalization of threshold signature and authenticated encryption for group communication[J]. IEICE Trans on Fundamentals,2001,E84-A(10): 2606-2609.

[4] LEE N Y. The security of the improvement on the generalization of threshold signature and authenticated encryption[J]. IEICE Trans on Fundamentals of Electronics,Communications and Computer Sciences,2002,E85-A(10):2364-2367.

[5] WANG Shu-hong,WANG Gui-lin,BAO Feng,*et al*. Security notes on generalization of threshold signature and authenticated encryption for group communication[J]. IEICE Trans on Fundamentals,2004,E87-A(12):3443-3446.

[6] HSU C L,WU T S,WU T C. Improvements of generalization of threshold signature and authenticated encryption for group communications[J]. Information Processing Letters,2002,81(1):41-45.

[7] 彭长根,李祥,罗文俊. 一种面向群组通信的通用门限签密方案[J]. 电子学报,2007,35(1):64-67.

[8] WANG Xue-ming,REN Rui-fang. Design of generalization of threshold signcryption scheme based on ECC[C]//Proc of IEEE International Conference on Information Theory and Information Security. 2010:46-49.

[9] 刘丹妮,王兴伟,郭磊,等. 一种高效的(t,n)门限群签名方案[J]. 计算机科学,2011,38(1):110-112.

[10] MENEZES A J, WU Yi-hong, ZUCCHEZALO R J. An elementary introduction to hyperelliptic curve [EB/OL]. (1996). http://www.math. uwaterloo. ca/~ajmeneze/publications/hyperelliptic. pdf.

[11] NIZAMUDDIN,CHAUDHZY S A,NASAZ W,*et al*. Efficient signcryption schemes based on hyperelliptic curve cryptosystem[C]//Proc of the 7th International Conference on Emerging Technologies. 2011: 1-4.

[12] 陈逢林,胡万宝,孙广人. 基于超椭圆曲线的顺序多重盲签名[J]. 计算机工程,2011,37(9):160-162.

[13] DESMEDT Y,JAJODIA S. Redistributing secret shares to new access structures and its applications,TR-97-01[R]. Virginia:George Mason University,1997.

(上接第 502 页)其中,P 的计算开销约为 Pm 的 9.6 倍,MtP 的计算开销同 Pm 相当。由表 1 可以看出,本算法的计算开销为 7 Pm 加上四次公钥签名和两次公钥加/解密,微大于文献[6],小于文献[3],但是本方案的安全性都高于文献[3,6];而且本方案的计算开销对于航空自组网是完全可以接受的。因此本方案的整体性能优于文献[3,6]。另外,本方案中当用户节点在有效期内再次进行认证时,整个过程 M 与节点 V 之间消息交互次数为一次,只需两次点乘运算。综合以上分析,本方案具有更高的执行效率,更加适合在资源受限的航空自组网中应用。

表 1 各方案效率比较

比较项	文献[3]	文献[6]	本方案
双线性对(M/FA/HA)	4/4/4	0/0/1	0/0/0
公钥签名与验证(M/FA/HA)	0/1/1	0/2/2	0/2/2
公钥加/解密(M/FA/HA)	0/0/0	0/0/0	0/1/1
点乘(M/FA/HA)	7/6/4	5/1/2	3/2/2
消息交互数(M-FA/FA-HA)	3/2	2/2	2/2

4 结束语

在航空自组织网络环境下,对于漫游接入认证具有特殊的要求。本文提出的方案满足双向身份认证、安全的会话密钥建立以及用户身份匿名性等安全性要求。而且与现有的同类方案相比,本方案在满足安全性要求的基础上,用户节点的计算开销和总计算开销明显减少。因此该方案相比于其他漫游接入认证方案更适用于航空自组织网络环境。

参考文献:

[1] YAO Yao, WEI Wang-xing. A cross-domain authentication protocol based on hypercube[C]//Proc of Control and Decision Conference. 2011:3528-3532.

[2] SHIM K A. An ID-based aggregate signature scheme with constant pairing computations[J]. Journal of Systems and Software,2010, 83(10):1873-1880.

[3] 朱辉,李晖,苏万力. 基于身份的匿名无线认证方案[J]. 通信学报, 2009,30(4):130-136.

[4] WANG Yan-jiong, WEN Qiao-yan, ZHANG Hua. A single sign-on scheme for cross domain Web applications using identity-based cryptography[C]//Proc of the 2nd International Conference on Networks Security, Wireless Communications and Trusted Computing. Washington DC:IEEE Computer Society,2010:483-485.

[5] 刘小琼,潘进,李国朋. 基于无证书的两方跨域认证密钥协商协议[J]. 计算机应用研究,2012,29(2):646-649.

[6] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006,29(8):1271-1281.

[7] BELLARE M,NAMPREMPRE C,NEVEN G. Security proofs for identity-based identification and signature schemes[J]. Journal of Cryptology,2008,22(1):1-61.