# 一种基于身份的移动自组网认证机制

陈 炜 龙 翔 高小鹏

(北京航空航天大学 计算机学院, 北京 100083)

**摘 要**: 针对移动自组网无公钥基础设施的特点,采用基于身份的密码学算法、分布式秘密共享算法和椭圆曲线加密算法,实现安全高效的移动节点认证. 简单讨论基于身份的数字签名算法;介绍如何使用 Lagrange 插值公式,实现分布式的系统主密钥;然后给出节点密钥安全分发的模型,并在此模型的基础上,基于椭圆曲线加密算法实现安全的分布式节点密钥签发;给出算法安全性和效率分析;根据双线性对的特点,讨论会话密钥的产生和更新. 给出的认证方法,具有分布式实现和安全高效的特点,同时可以非交互式产生一次性会话密钥,适用于分布式移动网络环境.

**关 键 词**: 移动自组网; 秘密共享; 公钥密码学; 基于身份的密码学; 椭圆曲线密码学

**中图分类号**: TP 393.08

**文献标识码**: A **文 章 编 号**: 1001-5965(2006)07-0869-04

# Identity-based authentication scheme for mobile ad hoc networks

Chen Wei Long Xiang Gao Xiaopeng

(School of Computer Science and Technology, Beijing University of Aeronautics and Astronautics, Beijing 100083, China)

**Abstract**: In order to realize secure and efficient mobile node authentication in mobile ad hoc networks (MANET) which have no traditional public key infrastructure (PKI), a scheme consisting of identity-based cryptograph, distributed secrete sharing algorithm and elliptic curves encryption was proposed. Identity-based digital signature algorithm was briefly discussed. Lagrange interpolating polynomial was used to distribute master secret key among system nodes. A model describing secure node key issue was given, and a distributed procedure based on the given model was presented to securely issue node key by using elliptic curves encryption. The security and efficiency of the proposed algorithm was analyzed. According to the property of the bilinear pairing, the generation and update of session keys was discussed. The proposed authentication scheme could be used to realize efficient and secure authentication in distributed mobility scenarios, and to generate non-interactive one time session keys between two mobile nodes.

**Key words**: manet; secret sharing; public key cryptography; identity-based cryptography; elliptic curves cryptography

移动自组网(MANET, Mobile Ad Hoc Networks)[1]是一种无网络基础设施的无线自组织网络. 与传统有线网络相比较,MANET 网络具有以下突出的特点:①自组织性. 所有的移动节点都具有路由器和终端节点的双重身份,节点之间通过分布式算法实现互联互通;②没有中心认证机构. 在 MANET 网络中,没有认证中心(CA, Certificate Authority)和公钥基础设施(PKI, Public Key Infrastructure);③网络拓扑动态变化. 网络中的节点具有移动特性,且节点可能在任意时刻关机或离开网络;④节点的带宽和能源有限. MANET 网络自组织的组网方式,有限的网络带宽和能源,无线通信的特点,都使得传统有线网络中基于 PKI 的认证方法不适用于 MANET 网络.

文献[2]提出使用基于身份的认证方法和门限算法实现高效的身份认证,但没有讨论认证私

**收稿日期**: 2005-07-21

**作者简介**: 陈 炜(1977-),男,四川自贡人,博士生, buaa_chen@yahoo.com.cn.

钥的安全签发,也没有讨论会话密钥的协商和更新. 文献[3]提出的方案和本文的方案很相似,都采用基于身份的分布式认证算法,都使用基于身份的算法产生会话密钥. 但根据 Dolev 和 Yao 的网络安全模型[4], 文献[3]存在2个不足:①直接使用已有的主密钥分量产生新的主密钥分量. 已有主密钥分量的泄露,可能直接威胁到主密钥的安全;②会话密钥不可更新.

本文在上述文献的基础上,进行了如下改进:①基于 Shamir 的门限算法[5],实现 Cha 和 Cheon 的基于身份的认证算法[6];②使用椭圆曲线加密算法实现安全高效的认证私钥签发;③基于身份和单向函数实现非交互式的会话密钥产生和更新.

# 1 基于身份的签名算法

1984年,Shamir[7]提出基于身份构建密码学算法,以简化证书的管理. 2001年,Boneh 和 Franklin 首先实现实用的基于身份和双线性对(bilinear pairing)的加密方案[8]. 不久,基于身份和双线性对进行认证的方法也提了出来. 基于身份实现加密和认证的系统中,每个通信实体拥有一个<公钥,私钥>对:公钥是通信实体的身份,私钥由通信双方都信任的第三方 KGC(Key Generation Center)生成. 本节首先简要介绍 Cha 和 Cheon 的基于身份的签名算法[6],最后讨论该算法的优缺点.

## 1.1 基于身份的签名算法

令 $G$ 是阶为素数 $p$ 的循环群,$P$ 是 $G$ 的生成元. 假设 $G$ 是加法群,且 $a$,$b$ 和 $c$ 是 $F_p$ 的元素. 定义下面2个数学问题:① CDHP(Computational Diffie-Hellman Problem)问题. 给定$(P,aP,bP)$,计算 $abP$;② DDHP(Decisional Diffie-Hellman Problem)问题. 给定$(P,aP,bP,cP)$,如果在有限域 $F_p$ 中,有 $c=ab$ 成立,则称$(P,aP,bP,cP)$为有效 Diffie-Hellman 组. 称 $G$ 为 GDH(Gap Diffie-Hellman)群,如果 DDHP 问题可以在多项式时间内求解,CDHP 问题不可在多项式时间内求解.

Cha 和 Cheon 的基于身份的签名算法如下:

1) Steup:定义2个密码学哈希函数:$H_1:\{0,1\}^*\times G\rightarrow F_p$ 和 $H_2:\{0,1\}^*\rightarrow G$. 选 $G$ 的生成元 $P$,随机选取 $s\in F_p$,计算 $P_{\text{pub}}=sP$. 系统参数是$(P,P_{\text{pub}},H_1,H_2)$,主密钥是 $s$;

2) Extract:给定身份 $I_{\text{ID}}$,计算 $D_{\text{ID}}=sH_2(I_{\text{ID}})$,公钥为 $I_{\text{ID}}$,对应的私钥为 $D_{\text{ID}}$. 记$Q_{\text{ID}}=H_2(I_{\text{ID}})$;

3) Sign:给定私钥 $D_{\text{ID}}$ 和消息 $m$,随机选择 $r\in F_p$,计算签名 $\sigma=(U,V)$. 其中 $U=rQ_{\text{ID}}$,$h=H_1(m,U)$,$V=(r+h)D_{\text{ID}}$;

4) Verify:检查$(P,P_{\text{pub}},U+hQ_{\text{ID}},V)$是否为有效的 Diffie-Hellman 组. 如果通过验证,则 $\sigma=(U,V)$是对应于身份 $I_{\text{ID}}$和消息 $m$ 的有效签名.

## 1.2 算法讨论

基于身份的认证方法以通信实体的身份作为公钥,避免了证书的传递,极大地减少了网络带宽的占用,很适合带宽有限且网络拓扑动态变化的 MANET 网络. 例如,根据现在计算机的处理能力,使用1 024 ~ 2 048 bit 公钥的 RSA 签名算法是安全的[9]. 这样,为传送证书,基于证书的 RSA 签名算法至少需要1 024 ~ 2 048 bit 的带宽,而基于身份的认证方法则不需要这些带宽. 另一方面,基于身份的认证方法不能简单应用到 MANET 网络. 基于身份的认证方法要求有可信的 KGC 为通信实体签发私钥,而 MANET 网络无网络基础设施的特点,使得集中式的 KGC 难以实现.

# 2 认证私钥的安全签发

在 MANET 网络中,使用基于身份的认证算法实现通信实体的认证,需要解决2个问题:①主密钥的分布式实现;②通信实体认证私钥的安全签发.

本节首先讨论基于拉各朗日(Lagrange)插值公式产生分布式主密钥 $s$;然后介绍基于椭圆曲线加密算法,使用 Cha 和 Cheon 的基于身份的认证算法,实现认证私钥的安全签发;最后分析该算法的安全性和效率.

## 2.1 分布式主密钥 $s$

从1.1节的介绍可知,通信实体的认证私钥由下式产生:. $D_{\text{ID}}=sH_2(I_{\text{ID}})$ 显然,为了生成 $D_{\text{ID}}$,需要主密钥 $s$. 为了解决 MANET 网络无集中式 KGC 的问题,根据 Shamir 的$(t,n)$门限密钥方案[5],可以将 $s$ 分解成 $n$ 个 $s$ 分量$(s_1,s_2,\cdots,s_n)$,由 $n$ 个节点分别保存. 需要恢复 $s$ 时,可由任意 $t$ 个 $s$ 分量$(s_1,s_2,\cdots,s_t)$重构,而少于 $t$ 个分量则不能重构 $s$. 基于拉格朗日插值公式产生 $s$ 分量和重构 $s$ 的过程如下.

设 $p$ 为素数,$F_p$ 为有限域,其中 $p\geqslant n+1$,随机选取 $s\in F_p\backslash\{0\}$,随机选取 $t-1$ 个系数 $a_1,a_2,\cdots,a_{t-1}\in F_p\backslash\{0\}$,在 $F_p$ 上构建 $t-1$ 次多项式$f(x)=s+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}$. 取 $F_p^*$ 的生成元 $g$,计算由第 $i$ 个节点保存的 $s$ 分量 $s_i$,$s_i=f(g^i)$ $i=1,2,$

…,$n$.

根据 Lagrange 插值公式,任选 $t$ 个 $s_i$,可以重构 $t-1$ 次多项式

$$f(x)=\sum_{i=1}^{t}s_i l_i(x)=\sum_{i=1}^{t}s_i\prod_{\substack{j=1\\ j\neq i}}^{t}\frac{x-g^i}{g^i-g^j}$$

其中 $l_i(x)=\prod_{\substack{j=1\\ j\neq i}}^{t}\frac{x-g^j}{g^i-g^j}$ 为 Lagrange 插值基函数. 计算

$$s=f(0)=\sum_{i=1}^{t}s_i l_i(0)=\sum_{i=1}^{t}s_i\prod_{\substack{j=1\\ j\neq i}}^{t}\frac{g^j}{g^j-g^i}$$

通过上述 Lagrange 插值公式,可以安全地把 KGC 的主密钥 $s$ 分成 $n$ 个分量,并由任意 $t$ 个分量重构 $s$.

### 2.2　认证私钥签发

通信实体认证私钥的签发需要满足以下要求:①拥有 $s$ 分量的通信实体不应该泄漏其拥有的 $s$ 分量;②主密钥 $s$ 不应该被任何通信实体获得;③任何通信实体不应该了解其他通信实体的认证私钥.

如果简单地按照 Shamir 的$(t,n)$门限密钥方案恢复 $s$,并由第 $t$ 个节点签发认证私钥,则认证私钥签发过程有以下缺陷:①$s$ 分量以明文形式传输,容易被攻击者截获;②第 $t$ 个节点在获得了 $s$ 的 $t$ 个分量后,可以重构 $s$;③第 $t$ 个节点可以了解申请私钥节点的认证私钥.

为解决上述问题,本文提出基于椭圆曲线加密算法实现认证私钥的安全签发. 假设拥有 $s$ 分量的节点为 $N_i,i=1,2,\cdots,n$,申请认证私钥的节点为 $V$. 下面介绍本文提出的认证私钥产生算法.

1) 根据文献[8]产生系统参数. 随机选择素数 $2<q\in Z$,求出满足下列条件的最小素数 $p$:①$p>3$;②$p=2\bmod 3$;③$q\mid(p+1)$;④$q^2$ 不能被$(p+1)$整除. 椭圆曲线 $E:y^2=x^3+1$ 定义在有限域 $F_p$ 上;群 $G_1$ 是 $E/F_p$ 上阶为 $q$ 的子群;群 $G_2$ 是 $F_{p^2}^*$ 上阶为 $q$ 的子群;$e$ 是 $G_1\times G_1\rightarrow G_2$ 的有效双线性映射(bilinear map). 选取曲线 $E/F_p$ 的基点 $P$,随机选取 $s\in F_p$,令 $P_{\text{pub}}=sP$,公开系统参数:$(P,P_{\text{pub}},H_1,H_2)$;

2) 按 2.1 节算法产生 $s_i$,并销毁 $s$;

3) 节点 $V$ 申请认证私钥. 节点 $V$ 首先随机选取私钥 $n_A\in F_p$,并以 $P_v=n_AP$ 作为公钥. 节点 $V$ 随机选取 $t$ 个 $N_i$,并给每个 $N_i$ 发送$<I_{\text{ID}},P_v>$;

4) 节点 $N_i$ 计算认证私钥分量. 节点 $N_i$ 根据来自申请节点的消息$<I_{\text{ID}},P_v>$,计算认证私钥分量 $D_{\text{IDi}}=s_i l_i(0)H_2(I_{\text{ID}})=s_i\prod_{\substack{j=1\\ j\neq i}}^{t}\frac{g^j}{g^j-g^i}H_2(I_{\text{ID}})$;

5) 节点 $N_i$ 对认证私钥分量进行签名,并加密消息. 节点 $N_i$ 首先使用基于身份的签名算法对认证私钥分量 $D_{\text{IDi}}$ 签名,得到消息 $m=D_{\text{IDi}}\parallel\sigma$,其中 $\parallel$ 代表载荷链接;然后随机选取正整数 $k\in F_p$,产生密文对$<kP,m+kP_v>$;最后将签名后的密文对发送给节点 $V$;

6) 节点 $V$ 产生认证私钥. 节点 $V$ 在收到来自不同 $N_i(i=1,2,\cdots,t)$的密文对后,首先根据密文对计算 $m$:$m+kP_v-n_AkP=m+kn_AP-n_AkP=m$,然后根据基于身份的签名算法对密文对进行验证,即判断 $e(P,V)=e(P_{\text{pub}},U+hQ_{\text{ID}})$;最后由 $t$ 个 $D_{\text{IDi}}(i=1,2,\cdots,t)$,计算签名私钥 $D_{\text{ID}}$:

$$\begin{aligned}D_{\text{ID}}&=D_{\text{ID1}}+D_{\text{ID2}}+\cdots+D_{\text{IDt}}=\\&s_1l_1(0)H_2(I_{\text{ID}})+s_2l_2(0)H_2(I_{\text{ID}})+\cdots+\\&s_tl_t(0)H_2(I_{\text{ID}})=(s_1l_1(0)+s_2l_2(0)+\cdots+\\&s_tl_t(0)H_2(I_{\text{ID}})=sH_2(I_{\text{ID}})\end{aligned}$$

### 2.3　算法讨论

系统初始化时,集中式的控制中心产生 $n$ 个主密钥分量,并分发到各个通信实体,各个通信实体只以 $s_i$ 的某种单向变形使用 $s_i$,如 $D_{\text{IDi}}=s_il_i(0)\cdot H_2(I_{\text{ID}})$,因此有较好的安全性. 文献[3]采用分布式算法产生主密钥,并直接使用 Lagrange 插值公式为新节点产生主密钥分量. 该算法虽然有较好的可扩展性,但存在主密钥分量的泄露问题,由此可能泄露主密钥,因此存在安全隐患.

本文使用椭圆曲线加密算法保护节点 $V$ 的认证私钥分量,从而保证只有节点 $V$ 可以产生认证私钥. 同时,由 2.2 节的算法可知,通过认证私钥求解主密钥 $s$ 的问题是椭圆曲线离散对数问题,因此节点 $V$ 计算上不可能获得主密钥 $s$,也不可能获得任何 $s$ 分量.

椭圆曲线加密算法与传统的 RSA 算法相比,在相同的密钥长度下,计算量差别不大. 但是在安全性相同的情况下,椭圆曲线加密算法的密钥长度比 RSA 算法要小的多[9],因此本文给出的基于椭圆曲线加密认证私钥分量的方案效率较高.

每个通信实体 $N_i$ 在将认证私钥分量发送给节点 $V$ 时,都会对消息进行基于身份的签名,保证了消息的完整性和不可否认性. 为了保证消息的新鲜性,可以在产生签名时,将一次性随机数 $N_{\text{nonce}}$ 也作为产生签名的材料.

## 3　会话密钥的产生和更新

设通信实体 $A$ 的密钥为$<D_{\text{IDA}},I_{\text{IDA}}>$,通信实

体 $B$ 的密钥为 $<D_{\mathrm{IDB}}, I_{\mathrm{IDB}}>$，$e$ 是双线性映射. 令 $K_{AB}=e(D_{\mathrm{IDA}}, I_{\mathrm{IDB}})=e(sI_{\mathrm{IDA}}, I_{\mathrm{IDB}})=e(I_{\mathrm{IDA}}, I_{\mathrm{IDB}})^s$，$K_{BA}=e(D_{\mathrm{IDB}}, I_{\mathrm{IDA}})=e(sI_{\mathrm{IDB}}, I_{\mathrm{IDA}})=e(I_{\mathrm{IDB}}, I_{\mathrm{IDA}})^s$. 由对的双线性性质(bilinear property of the pairing)[10]可知，$K_{AB}=K_{BA}$. 文献[4]直接使用 $K_{AB}$ 作为会话密钥，由于 $K_{AB}$ 不可更新，长期使用 $K_{AB}$ 作为会话密钥，存在 $K_{AB}$ 被攻击者破解的安全隐患.

本文使用单向 Hash 函数(如 SHA1[11])非交互式产生和更新会话密钥，产生过程如下：$N_{\mathrm{key}}=H(N_{\mathrm{nonce}} \| K_{AB})$，其中 $N_{\mathrm{nonce}}$ 是由通信发起方产生的随机数. 通信实体 $A$ 使用 $N_{\mathrm{key}}$ 加密消息，并以明文的方式将 $N_{\mathrm{nonce}}$ 传递给通信实体 $B$. 通信实体 $B$ 根据公式 $N_{\mathrm{key}}=H(N_{\mathrm{nonce}} \| K_{AB})$ 计算会话密钥，并解密消息. 由于 $N_{\mathrm{nonce}}$ 的随机性，$N_{\mathrm{key}}$ 也是一个不可预测的随机数. 根据单向函数的性质，即使 $N_{\mathrm{key}}$ 被攻击者破解，由 $N_{\mathrm{key}}$ 破解 $K_{AB}$，计算上也是不可能的，即 $K_{AB}$ 总是安全的. 会话密钥的更新可以通过重新选择 $N_{\mathrm{nonce}}$ 来实现，如果每次选择不同的 $N_{\mathrm{nonce}}$，则可实现理想的“一次性”会话密钥.

## 4 结束语

MANET 网络的分布式组网方式，动态的网络拓扑和有限的带宽资源，使得传统有线网基于证书的认证方法不适合 MANET 网络. 本文首先分析基于身份的认证方法；然后讨论如何使用 Lagrange 插值公式，椭圆曲线加密算法实现安全的基于身份的分布式身份认证；最后给出实现非交互式会话密钥协商和更新的方法. 本文给出的身份认证方法，不但具有分布式实现和安全高效的特点，还实现了非交互式的会话密钥协商和更新.

## 参考文献（References）


[1] IETF MANET work group [EB/OL]. http://www.ietf.org/html.charters/manet-charter.html

[2] Khalili A, Katz J, Arbaugh W, et al. Toward secure key distribution in truly ad hoc networks[C]// Proceedings of the 2003 Symposium on Application and the Internet Workshops. [S.l.]: IEEE Computer Society, 2003: 1-5

[3] Deng Hongmei, Mukherjee A, Agrawal D P. Threshold and identity-based key management and authentication for wireless ad hoc networks [C]// Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 2004). [S.l.]: IEEE Computer Society, 2004: 107-111

[4] Dolev D, Yao A C. On the security of public-key protocols[J]. IEEE Trans on Information Theory, 1983, 29(2): 198-208

[5] Shamir S. How to share a secret[J]. Communications of the ACM, 1979, 22(11), 612-613

[6] Cha J, Cheon J H. An identity-based signature from gap diffie-hellman groups[C]// Proc of the PKC 2003. [S.l.]: Springer-Verlag, 2003, 18(30): 18-30

[7] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of Crypto'84, Lecture Notes in Computer Science. [S.l.]: Springer-Verlag, 1984: 47-53

[8] Boneh D, Franklin M. Identity based encryption from the Weil pairing [C]// Extended Abstract in Proceedings of Crypto '2001, Lecture Notes in Computer Science. [S.l.]: Springer-Verlag, 2001: 213-229

[9] Stallings W. Cryptography and network security: principles and practice [M]. 3rd ed. Upper Saddle River NJ: Prentice Hall, 2003

[10] Mao Wenbo. Modern cryptography: theory and practice [M]. Upper Saddle River, NJ: Prentice Hall PTR, 2004

[11] Eastlake D, Jones P. US secure hash algorithm 1 (SHA1) [EB/OL]. IETF RFC3174, 2001. http://www.ietf.ore/rfc/rfc3174.txt? number=3174


(责任编辑：娄 嘉)