ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.8, August 2006, pp.1811−1817
DOI: 10.1360/jos171811

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于口令认证的移动 Ad Hoc 网密钥协商方案*

王晓峰+, 张 璟, 王尚平, 张亚玲, 秦 波

(西安理工大学 密码理论与网络安全研究室,陕西 西安 710054)

A Key Agreement Scheme for Mobile Ad Hoc Networks Based on Password Authentication

WANG Xiao-Feng+, ZHANG Jing, WANG Shang-Ping, ZHANG Ya-Ling, QIN Bo

(Laboratory of Cryptography Theory and Network Security, Xi'an University of Technology, Xi'an 710054, China)

+ Corresponding author: Phn: +86-29-82066369, Fax: +86-29-82066369, E-mail: wang-xf66@sohu.com, http://www.xaut.edu.cn

Wang XF, Zhang J, Wang SP, Zhang YL, Qin B. A key agreement scheme for mobile Ad Hoc networks based on password authentication. *Journal of Software*, 2006,17(8):1811−1817. http://www.jos.org.cn/1000-9825/17/1811.htm

Abstract: As a new type of wireless mobile networks, Ad Hoc networks do not depend on any fixed infrastructure, and have no centralized control unit and so its computation capabilities are limited by mobile nodes. In this paper, a novel multi-party key agreement scheme with password authentication and sharing password evolvement for Ad Hoc networks is proposed based on ECC (elliptic curves cryptography). One of the functions of passwords is used as sharing information to authenticate the mobile node's secret keys, and the other is used as a symmetrical key to encrypt alternating information between mobile nodes. The freshness and security of passwords are guaranteed by sharing password evolvement every time in mobile node's secret keys authentication and key agreement. Consequently, the computational overheads and the store load of mobile nodes are lessened, moreover, secret keys authentication and information encryption between mobile nodes are provided. The new scheme enjoys many secure properties such as against man-in-the-middle attack, against replay attack, key independence, forward security, etc.
Key words: Ad Hoc network; elliptic curve; key agreement; key authentication

摘 要: Ad Hoc 网是一种不依赖于任何固定基础设施、没有中心控制节点、计算资源受限的新型无线移动网络.基于 ECC(elliptic curves cryptography),提出了一个新的适用于 Ad Hoc 网的具有口令认证和共享口令进化的多方密钥协商方案.口令的一个功能是作为共享信息认证移动节点的密钥,另一个功能是作为对称密钥加密移动节点间的交互信息.共享口令进化机制保证每次认证节点密钥和协商会话密钥时口令的新鲜性和安全性,从而既减轻了移动节点的计算量和存储负担,又实现了移动节点之间的密钥认证和信息加密.新方案具有抗中间人攻击、抗重放攻击、密钥独立和前向安全等多种安全特性.

* Supported by the National Natural Science Foundation of China under Grant No.60273089 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2003AA1Z2560 (国家高技术研究发展计划(863)); the Shanxi Province Natural Science Foundation Research Plan of China under Grant No.2005F02 (陕西省自然科学基础研究计划); the Science and Technology Innovation Foundation of Xi'an University of Technology of China under Grant No.108210402 (西安理工大学科技创新基金)

Received 2005-06-02; Accepted 2005-10-10

关键词: Ad Hoc 网;椭圆曲线;密钥协商;密钥认证
中图法分类号: TP309 文献标识码: A

移动自组网络(mobile Ad Hoc network)[1]是一种不依赖于任何固定基础设施的新型无线网络,是由移动节点组成的临时性自治系统.Ad Hoc 网通过移动节点之间的相互协作来进行网络互联.由于它支持节点间的多跳通信,并采用无中心的分布式控制方式,因而具有很强的自组性、鲁棒性、抗毁性和容易构建的特点.这些特点使得 Ad Hoc 网的安全问题[2,3]尤为突出.由于不依赖固定基础设施并采用无线通信,用于传统网络的安全解决方案不能直接应用于 Ad Hoc 网,现存的用于 Ad Hoc 网的大多数协议和提案也没有很好地解决安全问题.随着 Ad Hoc 网进入商用领域,对 Ad Hoc 网的安全体系结构提出了新的挑战.如何在 Ad Hoc 网中提供认证、数据的机密和完整性保护、与服务相关的匿名性或隐私保护等是亟待解决的主要安全问题.其中,在不依赖固定基础设施的情况下,如何在这种对等网络中的移动节点之间协商会话密钥,成为研究的热点[4−8].

关于会话密钥协商,从传统的 Diffie-Hellman 密钥协商协议到椭圆曲线密码体制(elliptic curves cryptography,简称 ECC)下的认证密钥协商方案,国内外学者已经做了大量工作,如文献[9–11]中的方案等,都各有其特点.但这些方案中,多数需要多轮通信,安全性不够高,尤其是不具有认证功能,不适用于 Ad Hoc 网.M. Aydos 在文献[12]中提出了用于无线通信的可认证密钥协商协议——该协议采用证书机制来实现可认证的密钥交换,虽然能防止中间人攻击,但由于需要 CA,不适用于 Ad Hoc 网这种没有任何公共设施的环境.Xinjun Du 在文献[13]中提出一个基于身份的两轮多方密钥协商方案,并在文献[14]中进行了改进,但这两个方案都需要有公钥基础设施,也不适用于 Ad Hoc 网环境.另一类提供可认证的密钥协商的方法是假设双方拥有预共享的秘密口令.Jonathan Katz 在文献[15]中提出的方案就是用口令实现密钥协商的,但文献[15]不支持交互认证,且只支持两方密钥协商.之后,文献[16]对文献[15]进行了改进,增加了认证功能,但仍为仅适用于两方协商的协议.文献[17]提出一种用于三方协商的口令认证的密钥协商协议,隋爱芬在文献[18]中提出一种基于 ECC 的口令认证的密钥协商协议,但也是仅适用于两方协商的密钥协商协议.

根据人类记忆特点,口令不能太长.所以,若用共享口令协商会话密钥,难以避免字典攻击,很难达到预期的安全要求.本文基于 ECC,针对 Ad Hoc 网密钥协商提出了一个基于共享口令进化认证机制的具体方案.本文的主要贡献是采用共享口令进化机制实现 Ad Hoc 网中的节点密钥认证和会话密钥协商.口令的作用一是作为节点的共享信息,认证节点的密钥;二是相当于一个对称密钥,加密移动节点间的交互信息.口令的安全性由进化机制来保证.口令进化机制的优点和必要性在于:首先,保证每次协商会话密钥时口令新鲜.这样,即使攻击者获得了以前某次的口令,因为不知道口令已进化了多少次,所以仍然无法获得本次的密钥协商信息.其次,我们用单向函数进化口令,保证从本次的共享口令无法获得上次的共享口令,保证了前向安全性.这样,既减轻了节点的计算量和存储负担,又实现了密钥认证的功能;另外,我们的方案用 ECC 实现 Ad Hoc 网的密钥协商.移动通信设备本身由于体积较小,只有较低的运算能力和有限的存储空间,因此,相应的密码算法应该具有计算数据量小、运算速度快的特点.ECC 算法密钥短和效率高的优点是非常明显的[7,8],非常适用于移动 Ad Hoc 网环境.

1 Co-Gap-Diffie-Hellman 群和双线性映射

我们的方案基于一个强有力的密码学工具——Co-Diffie-Hellman 群对[19],简称为 Co-DH 群对.Co-DH 群对可以用椭圆曲线上的点来构造.下面我们来描述 Co-DH 群对上的 Gap-Diffie-Hellman 问题和双线性映射.

(1) 令 $E(F_q)$为椭圆曲线,$S\in E(F_q)$是阶为素数 p 的点,满足:① $p\neq q$;② $p\nmid q$;③ $p^2\nmid |E(F_q)|$.

(2) 令 $\alpha>1$ 是$\langle S\rangle$的安全乘数,则存在点 $Q\in E(F_{q^\alpha})$ 与 S 是线性无关的(参见文献[20]).

(3) 令 $G_1=\langle S\rangle, G_2=\langle Q\rangle$.

(4) 由于 S 与 Q 线性无关,Weil 对 $\hat{e}: G_1\times G_2\to F_{q^\alpha}^*$ 即为一个非退化的双线性映射.

基于以上定义的椭圆曲线 $E(F_q)$上的子群对(G_1,G_2),讨论以下问题:

定义 **1**(计算性 **Co-Diffie-Hellman** 问题和判定性 **Co-Diffie-Hellman** 问题).

(1) (G_1,G_2)上的计算性 Co-Diffie-Hellman 问题(Co-CDH):给定 $Q,aQ\in G_2,R\in G_1$,计算 $aR\in G_1$.

(2) (G_1,G_2)上的判定性 Co-Diffie-Hellman 问题(Co-DDH):给定 Q 和 $R,aQ\in G_2,bR\in G_1$,判断是否 $a=b$,如果等式成立,则称(Q,aQ,R,bR)为一个有效的 Co-Diffie-Hellman 四元组.

当 $G_1=G_2$ 时,上述问题即为标准计算性 Diffie-Hellman 问题和判定性 Diffie-Hellman 问题.

定义 **2**(**Co-Gap-Diffie-Hellman**(**Co-GDH**)群). Co-GDH 群是一个群对(G_1,G_2),在这个群对上求解 Co-DDH 问题容易,而求解 Co-CDH 问题较难.

一个可有效计算的双线性映射 $\hat{e}$ 提供了解决 Co-DDH 问题的算法[21]:对于(Q,aQ,R,bR),其中 $R\in G_1$, $Q\in G_2$, $a,b\in Z_p^*$,有: $a=b \bmod p \Leftrightarrow \hat{e}(R,aQ)=\hat{e}(bR,Q)$.

2 Ad Hoc 网密钥协商协议模型及其安全模型

下面以一个单一对等群组为例,定义 Ad Hoc 网密钥协商模型.假设系统中有 n 个节点$\{U_1,U_2,\ldots,U_n\}$.

2.1 Ad Hoc网密钥协商协议模型

定义 **3**. Ad Hoc 网密钥协商协议是多项式时间四元组

$$(\text{Setup}(1^k),\text{UkeyGen}(1^k),\text{UKeyAuth}(\cdot),\text{KeyAgreement}(\cdot)).$$

(1) 系统设置算法 Setup(1^k):输入安全参数 k,生成系统公共参数 M;

(2) 节点密钥生成算法 UkeyGen(1^k):输入公共参数 M,输出第 i 个节点的私钥/公钥对$(SK_i,PK_i)(1\le i\le n)$;

(3) 节点密钥认证算法 UkeyAuth(PK_i,PW_j):输入第 i 个节点的公钥 PK_i 和第 j 次密钥协商的口令 PW_j,输出 1 或 0;

(4) 密钥协商算法 KeyAgreement(PW_j,SK_i,r_{j_i},PK_t):输入第 j 次密钥协商的口令 PW_j,第 i 个节点的私钥 SK_i 和随机数 r_{j_i},群组中除节点 i 之外的其他节点 t 的公钥 $PK_t(1\le t\le n,t\ne i)$,输出 j 时段的会话密钥 K_j.

2.2 安全模型

在移动 Ad Hoc 网中,每个移动节点身份对等,网络中不存在任何一个完全可信的实体,移动节点间的会话密钥必须由通信各方自行产生.考虑以下安全需求:

(1) 节点密钥认证:保证通信各方身份的真实性.我们采用口令进化认证机制,口令由一个离线的口令服务器产生,欲参加通信的节点需要先向口令服务器申请一个口令;

(2) 会话密钥协商:节点之间通过协商确定会话密钥,不能单独由一方确定;

(3) 一次一密:每次协商密钥时得到的会话密钥不同,防止由于旧的会话密钥泄露引发的重放攻击;

(4) 会话密钥认证:节点间通信时,要首先认证会话密钥,以保证对方和自己拥有相同的会话密钥;

(5) 当群组成员发生变化(加入或退出)时,不需要复杂的计算就能更新群组中各个成员的密钥;

(6) 前向安全和后向安全:即使本次会话密钥泄露,攻击者也无法从本次会话密钥中获得以前和以后的会话密钥的任何信息.

根据这些安全性需求,我们定义 Ad Hoc 网密钥协商协议的安全模型由下述定义 4~定义 9 组成.

定义 **4**(完备性). 如果所有参与者 $U_i\in\{U_1,U_2,\ldots,U_n\}(1\le i\le n)$都诚实地执行协议,则在第 j 次密钥协商运行 KeyAgreement(PW_j,SK_i,r_{j_i},PK_t)后,每个参与者 U_i 得到的第 j 次会话密钥 K_j 都是相同的.

定义 **5**(封闭性). 在第 j 次密钥协商中,对于任意 $U_i\notin\{U_1,U_2,\ldots,U_n\}$和任意多项式时间算法 $A(\cdot)$,概率 $\Pr[A(PK_1,\ldots,PK_i,\ldots,PK_n)=K_j]<\varepsilon$,其中$\varepsilon$是一个关于 k 的可忽略的量.

定义 **6**(公平性). 在第j次密钥协商中,如果所有参与者 $U_i\in\{U_1,U_2,\ldots,U_n\}(1\le i\le n)$都诚实地执行协议,则每个 U_i 的地位和提供的密钥份额大小相同,即每个参与者想要控制会话密钥 K_j 的决定权在计算上是不可行的.

定义 **7**(会话密钥独立性). 任意多项式时间攻击者 A,从第 j 次会话密钥 K_j 求得第 m 次$(m\ne j)$会话密钥 K_m 的任何信息在计算上不可行.

定义 **8**(抗中间人攻击性). 在第 j 次密钥协商中,对任意多项式时间攻击者 $A\notin\{U_1,U_2,\ldots,U_n\},U_a,U_b\in\{U_1,$

$U_2,\ldots,U_n\}$,A 要向 U_a 假冒 U_b 在计算上不可行.

定义 **9**(抗重放攻击性). 任意多项式时间攻击者 A,用非本次密钥协商生成的密钥份额来获得本次的会话密钥在计算上不可行;用非本次密钥协商所得的会话密钥获得本次会话的秘密消息,在计算上不可行.

3 新的 Ad Hoc 网密钥协商方案

3.1 方案构造

我们以一个单一对等群组为例,在 Co-GDH 群对(G_1,G_2)上构造 Ad Hoc 网密钥协商方案.假设群组中有 n 个节点$\{U_1,U_2,\ldots,U_n\}$,其中任意两个节点间都有一个公开的通信信道,n 个节点希望协商共享的会话密钥.

(1) 系统设置 Setup(1^k)

令 k,l 为安全参数,$p\geq 2^k$ 为素数,G_1 和 G_2 是第 1 节中定义的 p 阶加法循环群,即(G_1,G_2)是 Co-GDH 群对.$G_1=\langle S\rangle,G_2=\langle Q\rangle,\hat{e}:G_1\times G_2\to G_T\in F_{q^*}^*$是双线性映射.其中 G_T 为乘法循环群.令 G_1,G_2 和 G_T 中的元素的长度(即表示为二进制时的位数)为 l.设 $H_1(\cdot),f_1(\cdot),f_2(\cdot)$是抗碰撞的密码学单向 Hash 函数,定义为 $H_1(\cdot):\{0,1\}^*\to G_1$, $f_1(\cdot):G_1\to G_1$, $f_2(\cdot):G_1\to G_T$.我们用 $f_1(\cdot)$作为口令进化函数,公开$(G_1,G_2,G_T,Q,p,q,\hat{e},H_1(\cdot),f_1(\cdot),f_2(\cdot))$.

(2) 节点密钥生成 UkeyGen(1^k)

① 每个节点 $U_i\in\{U_1,U_2,\ldots,U_n\}(1\leq i\leq n)$事先秘密向公共的口令服务器申请一个共享秘密初始口令 $PW_0\in G_1$;

② U_i 运行算法 UkeyGen(1^k):随机选取 $x_i\in_R Z_p^*$,计算 $y_i=x_iQ\in G_2$,生成$\{SK_i,PK_i\}=\{x_i,y_i\}$.

(3) 节点密钥认证 UkeyAuth(PK_i,PW_j)

该算法是在每次协商会话密钥之前,每个节点 $U_i\in\{U_1,U_2,\ldots,U_n\}(1\leq i\leq n)$首先要认证其他节点的密钥而必须执行的算法,目的是为了保证参加协商的各方密钥的真实性和可靠性.

在第 1 次协商会话密钥之前,每个节点 $U_i\in\{U_1,U_2,\ldots,U_n\}(1\leq i\leq n)$按照下列步骤认证其他节点的密钥:

① U_i 计算:$R_1=H_1(PW_0)$,$PW_1=f_1(PW_0)$, $\sigma_{1_i}=x_iR_1\oplus PW_1$,广播 (y_i,σ_{1_i}), 并删除 PW_0;

② U_i 收到其他节点的 $(y_k,\sigma_{1_k})(1\leq k\leq n,k\neq i)$后,计算 $R_1=H_1(PW_0)$,验证 $\hat{e}\left(\sum_{i=1}^{n}(\sigma_{1_i}\oplus PW_1),Q\right)=\prod_{i=1}^{n}\hat{e}(R_1,y_i)$ 是否成立:若成立,则返回 1,通过认证;否则,返回 0,终止协议.

⋮

在第 j 次协商会话密钥之前,每个节点 $U_i\in\{U_1,U_2,\ldots,U_n\}(1\leq i\leq n)$按照下列步骤认证其他节点的密钥:

① U_i 计算:$R_j=H_1(PW_{j-1})$,$PW_j=f_1(PW_{j-1})$, $\sigma_{j_i}=x_iR_j\oplus PW_j$,广播 (y_i,σ_{j_i}),并删除 PW_{j-1};

② U_i 收到其他节点的 $(y_k,\sigma_{j_k})(1\leq k\leq n,k\neq i)$后,计算 $R_j=H_1(PW_{j-1})$,验证 $\hat{e}\left(\sum_{i=1}^{n}(\sigma_{j_i}\oplus PW_j),Q\right)=\prod_{i=1}^{n}\hat{e}(R_j,y_i)$ 是否成立:若成立,则返回 1,通过认证;否则返回 0,终止协议.

讨论:在①中,用 U_i 的私钥 x_i 对 R_j 产生一个短签名[22] x_iR_j,然后用口令 PW_j 对 x_iR_j 加密得到 $\sigma_{j_i}=x_iR_j\oplus PW_j$,在②中解密并验证.口令的作用之一是作为节点的共享信息认证节点密钥,保证节点密钥的真实性和可靠性;其次相当于一个对称密钥,对 x_iR_j 加密,保证其完整性.每次协商会话密钥后,用抗碰撞的密码学单向 Hash 函数 $PW_j=f_1(PW_{j-1})$作为口令进化函数,进化口令,并删除上次的口令 PW_{j-1}.口令进化机制的优点在于:保证每次协商会话密钥时口令新鲜,这样,即使攻击者得到了以前某次的口令,但因为不知道口令已经进化了多少次,所以仍然无法得到本次密钥协商的信息.由口令进化函数 $f_1(\cdot)$的单向性,保证从本次的共享口令 PW_j,无法获得上次的共享口令 PW_{j-1},从而无法获得上次的密钥协商信息.由 $f_1(\cdot)$的抗碰撞性,保证在口令进化过程中得到相同口令的概率是可忽略的.移动 Ad Hoc 网的节点由于只有较低的运算能力和有限的存储空间,节点之间采用无线通信和分布式控制,口令进化机制的这些优点,既减轻了节点的计算量和存储负担,又实现了密钥认证.这正是本方案的特点.

(4) 密钥协商和提取 KeyAgreement(PW_j,SK_i,r_{j_i},PK_t)

在(3)中,若每个节点的计算结果都返回 1,则每个节点的密钥都得到了认证.此时,可按下列步骤计算自己的密钥份额并提取会话密钥(所有指数运算都在模 p 下进行):

考虑第 j 次密钥协商,节点 U_1 随机选取 $r_{j_1} \in_R Z_p^*$,计算自己的密钥份额 $w_{j_1}=\hat{e}(y_n,y_2)^{r_{j_1}x_1}\oplus PW_j$,广播 w_{j_1}. 节点 U_n 随机选取 $r_{j_n} \in_R Z_p^*$,计算自己的密钥份额 $w_{j_n}=\hat{e}(y_{n-1},y_1)^{r_{j_n}x_n}\oplus PW_j$,广播 w_{j_n}. 节点 $U_i\in\{U_1,U_2,\ldots,U_n\}(1<i<n)$ 随机选取 $r_{j_i} \in_R Z_p^*$,计算自己的密钥份额 $w_{j_i}=\hat{e}(y_{i-1},y_{i+1})^{r_{j_i}x_i}\oplus PW_j$,广播 w_{j_i}.

节点 $U_i\in\{U_1,U_2,\ldots,U_n\}(1\le i\le n)$提取自己的会话密钥: $K_j=\prod_{i=1}^{n}(w_{j_i}\oplus PW_j)$.

讨论:在此,口令 PW_j 的作用相当于一个对称密钥,用于加密每个节点的密钥份额的秘密信息,确保秘密信息在传输过程中没有被篡改;另一方面,只有拥有口令 PW_j 的合法节点,才能恢复出其他节点的正确的密钥份额.

3.2 方案分析

3.2.1 安全性

结论 **1**(完备性). 如果合法节点诚实地执行协议,则合法节点计算得出的会话密钥是相同的.

分析(以第 j 次协商会话密钥为例):参与协商的每个节点 $U_i\in\{U_1,U_2,\ldots,U_n\}(1\le i\le n)$可以计算出同样的 K_j;

$$\begin{aligned}K_j&=\prod_{i=1}^{n}(w_{j_i}\oplus PW_j)\\&=(w_{j_1}\oplus PW_j)(w_{j_2}\oplus PW_j)\ldots(w_{j_n}\oplus PW_j)\\&=\hat{e}(y_n,y_2)^{r_{j_1}x_1}\ldots\hat{e}(y_{i-1},y_{i+1})^{r_{j_i}x_i}\ldots\hat{e}(y_{n-1},y_1)^{r_{j_n}x_n}\\&=\hat{e}(Q,Q)^{x_nx_1x_2r_{j_1}+x_1x_2x_3r_{j_2}+\ldots+x_{i-1}x_ix_{i+1}r_{j_i}+\ldots+x_{n-1}x_nx_1r_{j_n}}.\end{aligned}$$

结论 **2**(封闭性). 新的密钥协商方案是封闭的.

分析:攻击者 $A\notin\{U_1,U_2,\ldots,U_n\}$想要冒充任意合法节点 $U_i\in\{U_1,U_2,\ldots,U_n\}(1\le i\le n)$,利用公开数据计算 K_j,A 必须知道 U_i 的私钥 x_i,而从 $y_i=x_iP$ 求解 x_i 是椭圆曲线离散对数问题,在计算上不可行,所以计算出 K_j 的概率可忽略.

封闭性保证不合法用户根据公开的数据不能提取会话密钥的任意信息.

结论 **3**(公平性). 新的密钥协商方案是公平的.

分析:考虑第 j 次密钥协商,每一个合法节点 U_i 的密钥份额为 $w_{j_i}=\hat{e}(y_{i-1},y_{i+1})^{r_{j_i}x_i}\oplus PW_j$,由求 K_j 的算法可知:每一个合法节点 U_i 在求 K_j 时的地位是均等的,所提供的密钥份额的长度均为 l,即对 K_j 的决定权是均等的.

结论 **4**(会话密钥独立性). 新的密钥协商方案所产生的会话密钥是独立的.

分析:因为每一个合法节点 U_i 在计算自己的密钥份额时都选择了一个一次性随机数,所以每一次协商的会话密钥不相等.两次会话密钥相等的概率为 $1/p$.

结论 **5**(抗中间人攻击). 新的密钥协商方案是抗中间人攻击的.

分析:考虑第 j 次密钥协商,对任意攻击者 $A\notin\{U_1,U_2,\ldots,U_n\},U_i,U_t\in\{U_1,U_2,\ldots,U_n\}$,假定 A 要向 U_t 假冒 U_i.攻击者必须伪造 σ_{j_i} 满足 $\hat{e}((\sigma_{j_i}\oplus PW_j),Q)=\hat{e}(R_j,y_i)$.而伪造 σ_{j_i} 相当于伪造对 PW_j 的签名,其难度相当于求解椭圆曲线离散对数问题,由签名方案的安全性(见文献[22])可知,成功伪造 σ_{j_i} 的概率是可以忽略的.

结论 **6**(抗重放攻击性). 任意多项式时间攻击者 A,用非本次会话密钥获得本次会话的秘密消息,在计算上不可行.

分析:因为用 Hash 函数 $f_1(\cdot)$作为密钥进化函数,并采用口令进化机制 $PW_j=f_1(PW_{j-1})$,所以每次得到的口令都不同.根据 Hash 函数的抗碰撞性,得到相同口令的概率可忽略.再由会话密钥独立性,以保证新协议抗重放攻击.

结论 **7**(前向安全性). 由会话密钥独立性和 Hash 函数的单向性可以得到.

3.2.2 效 率

为了方便比较,我们统一用$|l|$表示运算域中元素的长度,分别用 T_m,T_E,T_c,T_e 表示一次模乘(除)运算、模指数运算、逆运算和对运算所需的时间.表 1 给出在 n 个节点的对等网络中,每进行一次密钥协商,几个方案的计算

量和所需时间以及通信轮数和通信开销的比较(其中忽略了 G_1 中的加法运算和“⊕”运算的计算量).

Table 1 Efficiency comparison of key agreement schemes

表 1 密钥协商方案的效率比较

Scheme	Model multiplication or division (times)	Model Exponentiation (times)	Reversion operation (times)	$\hat{e}$ (times)	Operation time	Communication rounds	Communication cost
Ref.[4]	n	$n^2/2-n/2+4$	0	0	$nT_m+(n^2/2-n/2+4)T_E$	5	$5(n-1)\|l\|$
Ref.[5]	n	$n^2/2+n/2$	0	0	$nT_m+(n^2/2+n/2)T_E$	n	$2n^2\|l\|$
Ref.[6]	$3n-1$	$3n+2$	n	0	$(3n-1)T_m+(3n+2)T_E+nT_m$	3	$2\|l\|$
Ref.[10]	$n-1$	n^2+n+1	0	0	$(n-1)T_m+(n^2+n+1)T_E$	3	$2(n-1)\|l\|$
Ref.[11]	$n^2/2+5n/2-6$	$2n+4$	2	0	$(n^2/2+5n/2-6)T_m+(2n+4)T_E+2T_c$	n	$2n^2\|l\|$
Our scheme	$n(n-1)$	n	0	$2n+1$	$n(n-1)T_m+nT_E+(2n+1)T_e$	2	$3\|l\|$

由表 1 可见:本方案的计算量小,通信开销小;由于对运算所需的时间较长,所以,所需时间与其他方案相当.由此可见,本方案的效率较高.

4 结束语

本文提出了一个适用于 Ad Hoc 网的可认证多方密钥协商方案.新方案基于 ECC,采用共享口令进化认证机制认证节点的密钥,既减轻了节点的计算量和存储负担,又实现了密码认证的功能.本文的方案简单,具有较全面的安全性,效率较高,计算量较低,适合应用在 Ad Hoc 网这种没有固定公共设施并且计算资源受限的环境.

本文中的口令进化认证机制保证所认证的私钥确实是对应于某个特定公钥的私钥,但不能避免下述特定攻击:例如合法节点 A 有意把口令泄露给非法节点 B,B 用自己的公钥和私钥参与到与其他合法节点的密钥协商中.要避免这种攻击,需要用到基于身份的认证机制,即把口令与身份绑定,这将是我们下一步要研究的问题.

References:

[1] McDonald AB, Znati T. A mobility-based framework for adaptive clustering in wireless Ad-Hoc networks. IEEE Journal on Selected Areas in Communication, 1999,17(8):1466−1487

[2] Zhou LD, Haas ZJ. Securing Ad Hoc networks. IEEE Network, 1999,13(6):24−30.

[3] Wang HT, LIU XM. The summary of Ad Hoc network security. Network and Computer Security, 2004,(7):26−30 (in Chinese with English abstract).

[4] Asokan N, Ginzboorg P. Key agreement in Ad-Hoc networks. Computer Communications, 2000,23(17):1627−1637.

[5] Hietalahti M. Efficient key agreement for Ad-Hoc networks [MS. Thesis]. Espoo: Helsinki University of Technology, 2001.

[6] Nam JY, Lee JW, Kim SJ, Won DH. DDH-Based group key agreement for mobile computing. Cryptology ePrint Archive, Report 2004/127, 2004. http://eprint.iacr.org/2004/127

[7] Ertaul L, Chavan N. Security of Ad Hoc networks and threshold cryptography. IEEE, 2005. http://www.mcs.csuhayward.edu/~lertaul/MA2-6.pdf

[8] Ertaul L, Lu WM. ECC based threshold cryptography for secure data forwarding and secure key exchange in MANET (I). In: Boutaba R, Almeroth K, Puigjaner R, Shen S, Black JP, eds. Networking 2005. LCNS 3462, Canada: University of Waterloo, Springer-Verlag GmbH, 2005. 102−113.

[9] Kim YD, Perrig A, Tsudik G. Simple and fault-tolerant key agreement for dynamic collaborative groups. In: Jajodia S, ed. Proc. of the 7th ACM Conf. on Computer and Communications Security. Athens: ACM Press, 2000. 235−244.

[10] Burmester M, Desmedt Y. A secure and efficient conference key distribution system. In: Santis AD, ed. Advances in Cryptology–EUROCRYPT'94. LNCS 950, Berlin: Springer-Verlag, 1995. 275−286.

[11] Horng G. An efficient and secure protocol for multi-party key establishment. The Computer Journal, 2001,44(5):463−470.

[12] Aydos M, Sunar B, Koc CK. An elliptic curve cryptography based authentication and key agreement protocol for wireless communication. In: Proc. of the 2nd Int'l Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications. Dallas, 1998. http://www.crypto.wpi.edu/Publications/Documents/ask_98_an.pdf

[13] Du XJ, Wang Y, Ge JH, Wang YM. An ID-based authenticated two round multi-party key agreement. Cryptology ePrint Archive, Report 2003/247, 2003. http://eprint.iacr.org/

[14] Du XJ, Wang Y, Ge JH, Wang YM. An improved ID-based authenticated group key agreement scheme. Cryptology ePrint Archive, Report 2003/260, 2003. http://eprint.iacr.org/

[15] Katz J, Ostrovsky R, Yung M. Efficient password-authenticated key exchange using human-memorable passwords. In: Pfitzmann B, ed. Proc. of the EUROCRYPT 2001. LNCS 2045, Innsbruck: Springer-Verlag, 2001. 475–494.

[16] Jiang SQ, Gong G. Password based key exchange with mutual authentication. Cryptology ePrint Archive, Rert 2004/196, 2004. http://www.jablon.org/passwordlinks.html#JG04

[17] Kwon T. Practical authenticated key agreement using passwords. In: Zhang K, Zheng Y, eds. Proc. of the 7th Information Security Conf. LNCS 3225, Palo Alto: Springer-Verlag, 2004. 1–12.

[18] Sui AF,Yang YX, Niu XX, Luo SS. Research on the authenticated key agreement protocol based on elliptic curve cryptography. Journal of Beijing University of Posts and Telecommunications, 2004,27(3):28–32 (in Chinese with English abstract).

[19] Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham E, ed. Proc. of the Eurocrypt 2003. LNCS 2656, Warsaw: Springer-Verlag, 2003. 416–432.

[20] Shikata J, Zheng YL, Suzuki J, Imai H. Optimizing the Menezes-Okamoto-Vanstone (MOV) algorithm for non-supersingular elliptic curves. In: Lam KY, Okamoto E, Xing CP, eds. Proc. of the Cryptology-ASIACRYPT'99. LNCS 1716, Singapore: Springer-Verlag, 1999. 86–102.

[21] Joux A, Nguyen K. Separating decision diffie-hellman from diiffie-hellman in crypto-graphic groups. Cryptology ePrint Archive, Report 2001/003, 2001. http://eprint.iacr.org/

[22] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. In: Boyd C, ed. Proc. of the Cryptology—ASIACRYPT 2001. LNCS 2248, Gold Coast: Springer-Verlag, 2001. 514–532.

附中文参考文献:

[3] 王海涛,刘晓明.Ad Hoc 网络的安全问题综述.计算机安全,2004,(7):26–30.

[18] 隋爱芬,杨义先,钮心忻,罗守山.基于椭圆曲线密码的可认证密钥协商协议的研究.北京邮电大学学报,2004,27(3):28–32.

王晓峰(1966－),女,河南新乡人,博士生,副教授,主要研究领域为密码理论,网络安全.

张亚玲(1966－),女,博士生,副教授,主要研究领域为计算机网络.

张璟(1952－),男,博士,教授,博士生导师,主要研究领域为计算机网络,网络安全.

秦波(1977－),女,博士生,讲师,主要研究领域为密码理论,网络安全.

王尚平(1963－),男,博士,教授,主要研究领域为密码理论,网络安全.