一种新的基于椭圆曲线密码体制的 Ad hoc 组密钥管理方案

冯 涛[1,2],王毅琳[1],马建峰[2]
(1. 兰州理工大学计算机与通信学院,甘肃兰州 730050;
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: 在安全的组通信中,组密钥管理是最关键的问题.论文首先分析了组密钥管理的现状和存在的问题,然后基于椭圆曲线密码体制,针对 Ad hoc 网络提出了一种安全有效的分布式组密钥管理方案,并对其正确性和安全性进行了证明,由椭圆曲线离散对数困难问题保证协议的安全.针对 Ad hoc 网络节点随时加入或退出组的特点,提出了有效的组密钥更新方案,实现了组密钥的前向保密与后向保密.与其他组密钥管理方案相比,本方案更加注重组成员的公平性,没有固定的成员结构,并且还具有轮数少、存储开销、通信开销小等特点,适合于在 Ad hoc 网络环境中使用.

关键词: 组密钥管理; 椭圆曲线; 离散对数; 前向保密; 后向保密
中图分类号: TP301 **文献标识码**: A **文章编号**: 0372-2112 (2009) 05-0918-07

A New Ad hoc Group Key Agreement Scheme Based on ECC

FENG Tao[1,2], WANG Yi-lin[1], MA Jian-feng[2]
(1. *School of Computer and Communication, Lanzhou University of Technology, Lanzhou, Gansu 730050, China;*
2. *Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an, Shaanxi 710071, China*)

Abstract: In secure group communication, group key management is the most critical issue. Firstly, we analyze the state and the problem of existing group key management schemes, and then present a secure, efficient and contributory group key management scheme based on elliptic curve cryptosystems. The security, correctness and completeness of our scheme are discussed in this paper. The security of our scheme relies on the elliptic curve discrete logarithm problem (ECDLP). For the sake of the forward secrecy and backward secrecy of group key, new scheme supports group members to renew their group key when the external nodes join the group or the internal members leave the group. Compared with the known approaches, new scheme attaches more importance to impartiality, the group structure is unfixed, all participants only need two-rounds to generate the group key, the low memory cost is also the virtue of our scheme. The new scheme is suitable for application in Ad hoc network environment.

Key words: group key agreement; elliptic curves; discrete logarithm problems; forward secrecy; backward secrecy

1 引言

Ad hoc 网络是由一组带有无线信号收发装置的移动节点组成的无线通信系统,由于其快捷、灵活的组网方式,具有广泛的应用前景.与传统的无线网络不同,Ad hoc 网络是一种动态的缺乏基础设施支持的通信网络,其移动终端设备的计算能力和存储容量都有限,并且面临着无线通信带来的安全问题.Ad hoc 网络的安全组通信(SGC)是指组内成员之间可以安全地收发消息,这些消息通过事先协商好的组密钥加密来保证安全.组密钥管理协议(Goup Key Agreement)是指多个协议参与方相互协作共同协商一个组密钥,组外成员不能计算出该密钥.

目前,人们提出的组密钥管理协议有三种基本类型[1]:集中式组密钥管理(CGKD),分散式组密钥管理(DGKM)和分布式组密钥管理(CGKA).在 CGKD 方式中存在一个叫组协调员 GC(group controller)的中心机构,该机构负责为组内成员产生和分配组密钥.当成员事件(加入/离开)发生时,GC 负责更新和重新分发组密钥.CGKD 方式中,组密钥的安全性主要依赖于 GC,而要在

收稿日期:2008-04-01;修回日期:2008-12-03
基金项目:国家自然科学基金(No. 60573036,No. 60743005,No. 60702059,No. 60503012);国家 863 高技术研究发展计划(No. 2007AA01Z405,No. 2007AA01Z429);甘肃省自然科学基金(No. 2007GS04823,No. 2007GS04066)

Ad hoc 网络中找到一个可信任的中心机构是不现实的.在 DGKM 方式中,一个大的群组被划分成若干个子组,每个子组存在一个子组协调员 SC(subgroup controller)负责子组的密钥管理.DGKM 方式仍存在中心节点的问题,而且对消息的中继传输会给 SC 带来很大的负担.Ad hoc 网络环境下的动态对等群组中,通信各方身份完全平等,并且组成员关系经常发生变化,所以其群组密钥管理方案必须采用 CGKA 方式,该方式的特点是没有中心机构,成员节点的地位平等,分配到各节点上的计算量和通信开销也是相同的,组密钥由组成员协同运算产生.

BD[2]、CLIQUES[3]、STR[4]、TGDH[5]是比较典型的 CGKA 协议,它们最初都是针对有线局域网和广域网设计的.这几个协议都采用分布式的密钥协商机制,其安全需求和成员间的信任关系满足 Ad hoc 网络中组密钥协商的要求.但是,这些协议的计算量和存储开销比较大,而 Ad hoc 网络节点的计算和存储能力都有限,所以并不适合于在 Ad hoc 环境中使用.

基于椭圆曲线密码体制,Mark Manulis 在文献[6]中对这四个协议进行了改进,提出 μBD、μCLIQUES、μSTR 和 μTGDH 协议(上述协议具体描述见附录).由于椭圆曲线密码体制具有密钥短、安全性高等特点,所以改进后的协议在 Ad hoc 网络中更加适用.μBD 协议中每个组成员都有固定的邻居节点,并要求每个成员都知道与自己相邻的左右邻居节点,在发生节点加入/离开等动态事件时,需要重新发起组密钥协商协议以更新组密钥,造成极大的开销.另外,该协议没有提供可验证的信任关系,因为组成员不能验证其他成员在协商过程中广播出来的中间数据的正确性.μCLIQUES 协议中,所有组成员按照顺序依次参与计算组密钥,这将造成极大的时延,故影响了协议的效率.在理想的组密钥协商协议中,每个协议参与者所承担的计算量应该是一致的,而 μSTR 协议中分配给节点树最底层的成员的计算量最大,其余节点的计算量依层次由下往上递减,这种计算量分配不均的特点违背了公平性.μTGDH 协议较好地体现了成员的公平性,但是它所需的通信开销比较大.

Bresson 和 Catalano[7]在 PKC2004 会议上提出了一种基于 EL Gamal 密码系统的组密钥协商协议,其安全性基于离散对数的困难问题和 Shamir 密钥分享方案的安全性,但该方案多次用到赋值和插值运算,增大了各参与方的通信开销和计算量.文献[8～14]都是基于门限密码(秘密共享)体制的密钥管理方案,这些方案仍需要在移动自组网内通过可信第三方(TTP)提供服务,这种门限方法只不过是把传统 PKI 中由单个节点承担的 CA 的功能分散到了多个节点上,由这些节点共同承担原来单个 CA 的功能.

基于椭圆曲线密钥体制,本文提出了一种安全有效的组密钥管理方案,它具有以下特点:(1)协议建立在椭圆曲线密钥体制基础上,具有安全强度高、密钥短、计算量小、速度快等特点.(2)强调组成员的公平协商,轮数少,仅需两轮就可完成组密钥的协商.存储开销小,并行计算组密钥效率高.(3)无固定的群组结构和成员依赖关系.(4)支持节点动态事件组密钥更新.

2　研究基础

椭圆曲线是一个具有两个变元及系数的方程.有限域 F_P 上的椭圆曲线是具有形式 $E: y^2 = x^3 + ax + b \pmod p$ 的方程,并表示为 $E_p(a, b)$,其中,a 和 b 是满足 $4a^3 + 27b^2 \neq 0 \pmod p$ 的 $F_P(p > 3)$ 中的常数.为了使 E 上的点构成一个群,还需要另外包含一个记为 O 的点,称这个点为无穷远点.

本节将讨论已知 $E_p(a, b)$ 内某点 G 的阶为素数 r 时,根据正整数 k 及其与 G 的标量乘结果 Q,如何求解点 G.其计算方法将被应用到下一节群组密钥协商过程中.

定理 1[15]　若群中元素 G 的阶是 r,则 $|G^k| = r/\gcd(k, r)$.

由于 $|G| = r$,则根据定理 1,$|Q| = |kG| = r/\gcd(k, r)$,由于 r 是素数,此时:(1)当 $k = nr$ 时,$|Q| = 1$,n 是任意正整数.此时,Q 是无穷远点 O,G 可以是群内的任何一点;(2)当 $k \neq nr$ 时,$|Q| = r$.此时,G 是群内确定的点,下面讨论这种情况下 G 的求解方法.

定理 2[16]　如果 k 和 r 是互素的,则存在唯一的整数 $x < r$ 满足 $kx \equiv 1 \pmod r$.

由于 k 和 r 互素,即 $\gcd(k, r) = 1$,则由定理 2,必存在唯一的 $x < r$ 使得 $kx \equiv 1 \bmod r$ 成立,也就是说 $kx - 1$ 是 r 的倍数,假设 $kx - 1 = ry$,其中 y 是正整数.$kx - ry = 1$ 是一次不定方程,该方程有解的充要条件是 $\gcd(k, r) = 1$,而由已知条件 k 和 r 互素,所以该方程必有解.运用 Euclid 算法确定 x 的值.

对等式 $Q = kG$ 两边同时做倍标量乘运算:$xQ = (kx)G = (ry + 1)G = ryG + G = G$,即 $G = xQ$.

3　基于 ECC 的组密钥管理方案

本文提出了一种安全有效的分布式群组密钥管理方案.分布式组密钥协商必须满足三个条件:(1)群组成员都必须贡献自己的秘密值,并能通过自己的秘密值和其他成员的公共信息计算出组密钥;(2)即使攻击者知道组密钥协商协议的运行过程,也不可能得到组密钥;(3)每个成员贡献的秘密值是秘密的,即使其他所有成员联合起来也不可能计算出该秘密值.

3.1 密钥协商协议模型

群组结构:每个组成员都有自己的公私钥对(PK_i, k_i),以及相应的签名方案 Sign(·)和验证方案 Verf(·).在协议开始执行之前,每个成员 M_i 都知道组内所有成员的公开信息,如成员 M_j 的身份信息 ID_j 和公钥信息 PK_j,以及群组的成员构成情况等.并且在协议执行过程中,这些成员信息保持不变.密钥协商的任务标识为 SID.

攻击者能力:假设外部攻击者 A 知道组成员的构成以及协议的运行过程,知道组内所有公开信息,比如公钥信息等.攻击者 A 能够截获并读取组成员之间的消息,也可以伪造消息,但是 A 不能控制组成员,也不能读取他们的秘密信息,比如私钥信息等.

3.2 主要参数选择

系统的主要参数包括:定义在有限域 F_P 上的椭圆曲线 E、G 是 E 上选择的基点,G 的阶为 r,r 是大于 160 位的素数.由 G 产生的子群表示为$\langle G\rangle = \{O, G, 2G, \cdots, (r-1)G\}$,组密钥管理方案中所有 E 上的运算都是在群$\langle G\rangle$内的运算.组内成员记为 $M_1, M_2, \cdots, M_n$,组成员 M_i 从$[1, 2, \cdots, r-1]$随机选择 k_i 作为自己的私钥,计算并公布公钥 $PK_i = k_iG$.签名和验证密钥对为(SK_i, VK_i),ID_i 是成员身份标识,SID 是本次密钥协商的任务标识,$H(\cdot)$是无碰撞的单向散列函数.

3.3 组密钥协商协议

第一轮:每个组成员 M_i:

(1) 从$[1, 2, \ldots, r-1]$随机选取 m_i.

(2) 对每个 $j = 1, 2, \cdots, n$ 且 $j \neq i$,计算 $A_{ij} = m_i PK_j$,$S_{ij} = \mathrm{Sign}_{SK_i}(X_{ij} \| Y_{ij} \| ID_i)$,其中 X_{ij} 和 Y_{ij} 分别是 A_{ij} 的 x 和 y 坐标.

(3) 向组内成员广播 $A_i = \{(A_{ij}, S_{ij}) \mid 1 \leq j \leq n$ 且 $j \neq i\}$.

第二轮:组成员 M_j 收到所有其他组成员 $M_i(i = 1, 2, \cdots, n$ 且 $i \neq j)$ 在第一轮发来的 A_i 后:

(1) 对收到的数据及其签名(A_{ij}, S_{ij})进行验证,若验证通过则执行下一步.

(2) 计算 $Q_j = \sum_{i \neq j} A_{ij} = \sum_{i \neq j} m_i k_j G = k_j((\sum_{i \neq j} m_i)G)$,根据第 2 节计算$(\sum_{i \neq j} m_i)G$,令 $B_j = (\sum_{i \neq j} m_i)G$.

(3) 利用自己的秘密值 m_j 计算 $C_j = m_j G + B_j$.

(4) 计算并广播 $H_j = H(U_j \| V_j \| \mathrm{SID})$,其中 U_j 和 V_j 分别是 C_j 的 x 和 y 坐标.

(5) 比较所有 $H_i(i = 1, 2, \cdots, n)$,若全部相等,则组密钥协商成功.计算组密钥 $GK = H(U_j \| V_j)$.

3.4 节点加入事件的组密钥更新协议

组外成员 M_{n+1} 在加入组之前,首先产生公私钥对(k_{n+1}, PK_{n+1})以及签名验证密钥对(SK_{n+1}, VK_{n+1}),并向组内广播自己的公钥信息和身份标识 ID_{n+1}.组内确定 M_n 为 Sponsor,由 M_n 发起组密钥更新协议;

(1) M_n 从$[1, 2, \cdots, r-1]$随机选择 m_n',计算 $Rn = Bn + m_n'G$ 以及签名 $S_n = \mathrm{Sign}_{SK_n}(R_x \| R_y \| ID_n)$.其中 R_x 和 R_y 分别是 R_n 的 x 和 y 坐标,M_n 向组内广播$\{R_n, S_n\}$.

(2) M_{n+1} 从$[1, 2, \cdots, r-1]$随机选择 m_{n+1},对每个 $j = 1, 2, \cdots, n$,计算 $A_{n+1j} = m_{n+1} PK_j$ 及 $S_{n+1j} = \mathrm{Sign}_{SK_{n+1}}(X_{n+1j} \| Y_{n+1j} \| ID_{n+1})$,其中 X_{n+1j}、Y_{n+1j} 分别是 A_{n+1j} 的 x 和 y 坐标.

(3) M_{n+1} 向组内广播 $A_{n+1} = \{(A_{n+1j}, S_{n+1j}) \mid 1 \leq j \leq n\}$.

(4) $M_j(j = 1, 2, \cdots, n)$ 收到 A_{n+1} 后对(A_{n+1j}, S_{n+1j})进行验证,若验证通过则根据第 2 节计算 $m_{n+1}G$.

(5) $M_j(j = 1, 2, \cdots, n+1)$ 验证 M_n 的消息$\{R_n, S_n\}$(M_n 不需要验证),验证通过则计算 $C_j = R_n + m_{n+1}G$.然后,M_j 计算并广播 $H_j = H(U_j \| V_j \| \mathrm{SID})$,其中 U_j 和 V_j 分别是 C_j 的 x 和 y 坐标.

(6) M_j 比较所有 $H_i(i = 1, 2, \cdots, n+1)$,若全部相等则组密钥更新成功,$M_j$ 计算组密钥 $GK = H(U_j \| V_j)$.

3.5 成员离开事件的组密钥更新协议

设组成员 $M_L(1 \leq L \leq n)$ 离开组,M_L 离开后剩余组成员集合为 S.组内确定 S 中具有最大编号的成员为 Sponsor,这里设为 M_k,由 M_k 发起组密钥更新协议:

Sponsor M_k:

(1) 从$[1, 2, \cdots, r-1]$随机选择 m_{k1},对每个 $M_j \in S$,计算 $A_{kj} = m_{k1} PK_j$,$S_{kj} = \mathrm{Sign}_{SK_k}(X_{kj} \| Y_{kj} \| ID_k)$,其中 X_{kj} 和 Y_{kj} 分别是 A_{kj} 的 x 和 y 坐标.

(2) 向 S 内成员广播$\{(A_{kj}, S_{kj}) \mid 1 \leq j \leq n$ 且 $j \neq L\}$;每个 $M_j \in S$.

(3) 验证 M_k 的消息(A_{kj}, S_{kj}),验证通过则根据第 2 节计算 $m_{k1}G$.

(4) 计算 $C_j' = C_j + m_{k1}G$.

(5) 计算并广播 $H_j = H(U_j \| V_j \| \mathrm{SID})$,其中 U_j 和 V_j 分别是 C_j' 的 x 和 y 坐标.

(6) 比较 S 内所有成员在上一步广播的散列值,若全部相等则组密钥更新成功,计算组密钥 $GK = H(U_j \| V_j)$.

4 方案的正确性分析

本方案由组密钥协商协议和节点加入/退出事件组密钥更新协议三部分组成,这些协议都是正确的.

命题 1 在组密钥协商协议中,只要每个组成员的计算过程没有错误,则最后计算出来的 GK 就是组密钥.

证明 $Q_j = \sum_{i \neq j} A_{ij} = \sum_{i \neq j} m_i PK_j = \sum_{i \neq j} m_i k_j G = k_j((\sum_{i \neq j} m_i)$

$G)$. 令 $B_j = (\sum_{i\neq j} m_i)\ G$,设其阶为 r',则 $Q_j = k_j B_j$. 因为 G 的阶是大素数 r,由定理 1 知,r 的值有两种可能:(1) $r' = 1$ 时,$B_j = O$,所以 $C_j = m_j G$. (2) $r' \neq r$,由 k_j 是 M_j 的私钥,Q_j 是确定的值,所以根据第 2 节,M_j 可以计算出 B_j,最后 $C_j = m_j G + B_j = \sum_{i=1}^{n} m_i G$.

由于 M_j 可以是组内任意一个节点,所以每个成员根据 C_j 的坐标计算出来的散列值都是相同的,也就是组密钥 GK.

命题 2　外部节点加入事件组密钥更新协议中,只要每个组成员的计算过程没有错误,则最后计算出来的 GK 就是组密钥.

证明　$A_{n+1j} = m_{n+1} PK_j = m_{n+1} k_j G = k_j (m_{n+1} G)$,与命题 1 中的分析完全类似,$M_j$ 可以计算出 $m_{n+1} G$. 再由 $R_n = B_n + m_n' G = (\sum_{i=1}^{n-1} m_i + m_n')\ G$,$M_j$ 计算 $C_j = R_n + m_{n+1} G = (\sum_{i=1}^{n-1} m_i + m_n' + m_{n+1})\ G$. 由于 M_j 可以是组内任意一个节点,所以每个成员根据 C_j 的坐标计算出来的散列值都是相同的,也就是组密钥 GK.

命题 3　成员离开事件组密钥更新协议中,只要每个组成员的计算过程没有错误,则最后计算出来的 GK 就是组密钥.

证明　$A_{kj} = m_{k1} PK_j = m_{k1} k_j G = k_j (m_{k1} G)$,与命题 1 中的分析完全类似,$M_j$ 可以计算出 $m_{k1} G$,然后再计算 $C_j' = C_j + m_{k1} G = (\sum_{i}^{n} m_i + m_{k1})\ G$. 由于 M_j 可以是组内任意一个节点,所以每个成员根据 C_j'的坐标计算出来的散列值都是相同的,也就是组密钥 GK.

5　方案的安全性分析

本方案基于椭圆曲线密码体制,其安全性建立在有限域上椭圆曲线离散对数问题的难解性(ECDLP)上. 基于椭圆曲线离散对数问题的难解性是指:对于方程 $Q = kP$,其中 Q、$P \in E_p(a, b)$,k 是整数且 $k < p$,对于给定的 Q 和 P 计算 k 是困难的. 与建立在一般有限域上离散对数的难解问题相比,椭圆曲线上离散对数难解问题的计算将更加困难. 目前最好的求解 ECDLP 的算法是 Pollard-p 方法和 Pohlig-Hellman 方法,当椭圆曲线点加群的阶 r 含有长度不小于 160bit 的大素因子时算法就会失效.

命题 4　组密钥协商协议是安全的.

证明　设外部攻击者 A 在组密钥协商协议的第一轮收集到所有发给 M_j 的消息 $A_{ij}(i = 1, 2, \cdots, n$ 且 $i \neq j)$,A 可以计算它们累加值 Q_j. 但 A 不知道 M_j 的私钥 k_j,所以它不能根据第 2.2 节解出 B_j. 另一方面,如果 A 能通过 Q_j 计算出组成员秘密值累加和 $\sum_{i\neq j} M_i'$,则显然违背了椭圆曲线离散对数问题的难解性质. 所以,攻击者 A 要求解 B_j 是困难的. 同理,攻击者 A 要从 $A_{ij} = m_i PK_j$ 计算 m_i 也是不可行的,即 A 不能求解每个组成员贡献的秘密值 m_i. 因此,攻击者 A 不能计算 C_j 和组密钥 GK.

在第二轮中,攻击者 A 可以得到所有组成员广播的消息 $H_j, j = 1, 2, \cdots, n$. 由于 $H_j = H(U_j \| V_j \| \mathrm{SID})$,根据散列函数的单向性,即使攻击者 A 知道任务标识 SID,也不可能从 H_j 得到 C_j(或 C_j')的坐标值(U_j, V_j),从而无法计算组密钥 GK. 而且根据散列函数的无碰撞性,A 也无法伪造能通过验证的 U_j 和 V_j.

综上所述,本方案的组密钥协商协议是安全的.

命题 5　组密钥管理方案是后向保密的.

证明　外部节点加入时,Sponsor M_n 改变自己贡献的秘密值为 M_n',C_j 变化为 $R_n = B_n + m_n' G$. 对加入事件之前的组密钥 GK,新成员 M_{n+1}所能得到的信息和攻击者所能得到的信息是完全相同的,即 R_n. 而 m_n 与 m_n'都是 M_n 贡献的秘密值,由椭圆曲线离散对数困难问题可保证新成员和攻击者 A 不能得到该秘密值. 所以,M_{n+1}和攻击者 A 都不能从 R_n 中得到 C_j 的任何信息,因此也不能计算新节点加入前的任何组密钥. 由散列函数的单向性和抗碰撞性可保证 R_n 的坐标值在广播消息时不被泄露,即组密钥管理方案的后向保密性得到了保证.

命题 6　组密钥管理方案满足前向保密性.

证明　当组内成员 M_L 离开组后,Sponsor M_k 立即改变自己贡献的秘密值为 m_{k1},并对集合 S 内的所有剩余组成员 M_j 计算 $A_{kj} = m_{k1} PK_j$. 由于 k_j 是 M_j 的私钥,所以 M_L 和攻击者 A 不能根据第 2 节计算出 $m_{k1} G$. 另外,由椭圆曲线离散对数困难问题可保证离开节点和攻击者都不能从 A_{kj}计算出 m_{k1}. 而 C_j 变化为 $C_j' = C_j + m_{k1} G$,因此 M_L 和 A 都不能从 C_j 中得到 C_j'的任何信息. 由散列函数的单向性和抗碰撞性可保证 C_j'的坐标值在广播消息时不被泄露,即我们的方案提供了前向保密性.

6　性能比较与分析

下面从通信开销、计算量和存储开销等几方面将本方案与文献[6]中的方案进行比较,如表 1 所示. 其中,S 表示组密钥协商协议,J 表示节点加入事件的组密钥更新协议,L 表示节点离开事件的组密钥更新协议,n 表示组成员数,i 是组成员编号,s 是密钥更新协议的发起人 Sponsor,h 是节点树高度,M_i 表示第 i 个节点,l_i 表示节点 M_i 在其节点树中的层次数,v_i 是 M_i 在其节点树上的编号. k 是使 $\lfloor v_i / 2^k \rfloor$ 为偶数的最小整数,M_s 表示 Sponsor 节点. odd 表示节点编号 v_i 为奇数,even

表示节点编号 v_i 为偶数.

轮数方面,为了减少计算量和通信代价,群组密钥管理协议中成员之间的消息交互次数应尽可能少. 新方案中组密钥协商协议只需 2 轮,这表明成员间的消息交互次数与群组成员个数无关,所以协议的操作可以并行执行,这减少了组密钥的交换时间,提高了协议的执行效率. 而 μCLIQUES 组密钥协商协议需要 $n+1$ 轮的消息交互,其轮数随节点规模的增加而增加. μTGDH 组密钥协商协议需要的轮数与节点树高度 h 成正比. 由于 μCLIQUES 与 μTGDH 密钥协商协议的轮数均与群组规模有关,所以,我们的方案实现了更好的并行性与效率,减少了节点的计算量和通信开销.

单播总次数方面,μCLIQUES 密钥协商协议中组成员消息单播总次数为 $2n-3$ 次,其成员加入事件组密钥更新协议需要 1 次消息单播,而新方案的组密钥协商协议、更新协议的单播次数均为 0. 由于群组规模增大时,群组成员间的消息交换会引起非常大的延时,因此应尽量减少协议执行过程中的消息数量. 显然,对于较大的群组,新方案的单播次数远低于 μCLIQUES 方案. 另外,μCLIQUES 方案的单播次数与组内成员规模有关,其单播次数随成员数量的增加而增加.

广播总次数方面,新方案与 μSTR 组密钥协商协议均需要 $n+1$ 次消息广播,这低于 μBD 的 $2n$ 次消息广播以及 μTGDH 的 $2n-2$ 次消息广播. 与 μBD 等其他四个方案一样,新方案的组密钥更新协议所需的广播总次数为常量,这表明群组成员间的消息广播次数与群组规模无关,从而避免了因消息交换引起的大的延时.

表 1 不同方案的比较

CGKA 协议		Communication			Computation	Memory
		Rounds	Unicast	Broadcast	Scalar-Point Multiplication	
μBD	S	2	0	$2n$	3	1
μCLIQUES	S	$n+1$	$2n-3$	2	$i<n-1$:3; $i=n-1$:2, $i=n$:n	$n+1$
	J	2	1	1	$i=n$, $i=n+1$:$n+1$; $i<n$:1	
	L	1	0	1	$i=s$:$n-1$; $i\neq s$:1	
μSTR	S	2	0	$n+1$	$i=1$:2$n-1$; $i>1$:$n-i+2$	$i=1$:2n $i>1$:2$(n-i+2)$
	J	1	0	2	$i=s$:4, $i\neq s$:2	
	L	1	0	1	$i<s$:$n-s$; $i=s$:2$(n-s)$, $i>s$:$n-i$	
μTGDH	S	h	0	$2n-2$	v_i is odd:l_i+k, v_i is even:l_i+1	$li+1$
	J	2	0	2	M_s:2l_s, M_i:$f(i,s)$	
	L	1	0	1	M_s:2l_s, M_i:$f(i,s)$	
Our Scheme	S	2	0	$n+1$	$n-1$	sponsor:3 other:2
	J	2	0	3	1	
	L	1	0	2	$i=k$:n, $i<k$:1	

说明:(1) 部分数据参考了文献[6]. (2) S:setup; J:join; L:leave (3) s:Sponsor 节点号; n:节点数; h:节点树的高度; i:节点编号; k:$\in[1,2,\cdots,h-1]$,是使 $\lfloor v_i/2^k\rfloor$ 为偶数的最小整数; l_i:节点树中的层次数. (4) $l_i\leq l_s$:$f(i,s)=l_i-\lfloor\log(v_s-\lfloor v_s/2^{l_s-l_i}\rfloor)\rfloor$; $l_i>l_s$:$f(i,s)=l_s-\lfloor\log(v_s-\lfloor v_i/2^{l_s-l_i}\rfloor)\rfloor$.

标量乘计算量方面,在组密钥协商协议中,μBD 协议里每个成员的标量乘计算量均为 3,而由表 1 知,其余方案的成员标量乘计算量均与成员规模有关,所以,对于较大的群组 μBD 协议的组成员计算量最少. 节点加入事件组密钥更新协议中,新方案的成员标量乘计算量为 1,低于其余四个方案的组成员标量乘计算量. 在成员离开事件的组密钥更新协议中,新方案除了发起人 M_k 的标量乘计算量等于组成员数 n 外,其余成员的标量乘计算量均为 1,这明显少于 μSTR 等协议的成员标量乘计算量. μSTR 协议在每个节点上分配的计算量不一致,这将导致节点树底层节点计算量过大、顶层节点计算量过小的问题,而 Ad hoc 网络强调公平性,μSTR 协议显然是有悖公平的. 新方案里所有组成员平等协商,并进行同样的运算,因此更好地体现了成员的计算公平性.

存储开销方面,新方案中组成员的存储开销为常量,这表明成员的存储开销与群组规模无关,这对于存储资源受限的 Ad hoc 网络节点显得尤其重要,而其余方案(μBD 除外)中组成员的存储开销均随群组规模增大而增加. 因此,对于较大的群组,新方案表现出更好的存储性能. 另外,μSTR 协议在每个节点上分配的存储开销不一致,即组成员的存储开销随节点树层次由上到下逐次增加,这显然违背了 Ad hoc 网络群组成员的公平性. 新方案除了 Sponsor 为处理动态事件而额外存储少量辅助信息(如 Bn)外,其余成员的存储开销基本一致. 新方案在计算量、通信开销以及存储开销等方面都有较好的性能表现.

7　结论

随着 Ad hoc 网络技术的发展,出现了大量分布式、动态协作组的应用,相应地产生了一种新的密钥管理形式 —组密钥管理. 本文提出了一种有效的基于椭圆曲线的组密钥管理方案,新方案的安全性建立在椭圆曲线离散对数难解问题上. 方案强调成员之间的公平性,轮数少,算法简单,所需的存储开销、通信开销小,安全性和效率都比较高,适合于在 Ad hoc 这种没有固定基础设施且资源受限的网络环境中应用.

附录:

(一) μBD 组密钥协商协议

组内成员 $M_i, i \in \{1, \cdots, n\}$:

(1) 从 $\{1, \cdots, t-1\}$ 随机选择 r_i,计算并广播 $Z_i = r_i G$. 其中,t 是基点 G 的阶.

(2) 计算并广播 $X_i = r_i (Z_{i+1} - Z_{i-1}) = r_i (r_{i+1} - r_{i-1}) G$. 其中,$Z_i = r_i G$.

(3) 最后计算出组密钥 $K = nr_i Z_{i-1} + (n-1) X_i + \cdots + X_{i+n-2} = (r_1 r_2 + r_2 r_3 + \cdots + r_{n-1} r_n) G$.

(二) μCLIQUES 组密钥协商协议

(1) $M_i (1 \leq i \leq n-2)$ 从 $\{1, \cdots, t-1\}$ 随机选择 r_i,并向 M_{i+1} 单播 $Z_i = r_i Z_{i-1}$. 其中,$Z_1 = r_1 G$,t 是基点 G 的阶.

(2) M_{n-1} 从 $\{1, \cdots, t-1\}$ 内随机选择 r_{n-1},并广播 $Z_{n-1} = r_{n-1} Z_{n-2}$.

(3) M_i 向 M_n 发送 $X_i = Z_{n-1} / r_i$.

(4) M_n 广播 $S = \{S_i = r_n X_i \mid 1 \leq i \leq n\}$.

(5) M_i 计算组密钥 $K = r_i S_i = r_1 r_2 \cdots r_n G$.

(三) μSTR 组密钥协商协议

(1) M_i 从 $\{1, \cdots, t-1\}$ 随机选择 r_i,计算并广播 $R_i = r_i G$. 其中,t 是基点 G 的阶.

(2) M_1 和 M_2 计算 $(k_2, \cdots, k_n)$. 然后,M_1 计算并广播 $(K_1, \cdots, K_{n-1})$. 其中,$k_i = r_i k_{i-1} G$,$k_1 = r_1$,$K_1 = R_1$.

(3) M_i 计算 $(k_i, \cdots, K = k_n)$,其中,$i \neq \{1, 2\}$. K 即是组密钥.

(四) μTGDH 组密钥协商协议

(1) M_i 从 $\{1, \cdots, t-1\}$ 随机选择 $k_{\langle li, vi \rangle}$,计算并广播 $K_{\langle li, vi \rangle}$,然后计算 $l := l_i - 1$ 和 $v := \lfloor v_i / 2 \rfloor$.

(2) M_i 更新节点树结构,计算密钥 $k_{\langle l, v \rangle}$ 和公钥 $K_{\langle l, v \rangle}$. 然后 M_i 所在子树的 Sponsor 广播 $K_{\langle l, v \rangle}$.

(3) 反复执行第(2)和第(3)步,同时执行 $l := l - 1$ 和 $v := \lfloor v / 2 \rfloor$,直到每个组成员都计算出组密钥 $K = k_{\langle 0,0 \rangle}$.

参考文献:

[1] Adusumilli P, Xukai Zou, Ramamurthy B. DGKD: distributed group key distribution with authentication capability[A]. Information Assurance Workshop, IAW '05[C]. Proceedings from the Sixth Annual IEEE SMC. 2005. 286 - 293.

[2] M Burmester, Y Desmedt. A secure and efficient conference key distribution system[A]. In Advances in Cryptology (EUROCRYPT '94)[C]. Lecture Notes in Computer Science, Springer-Verlag Berlin, 1994. 275 - 286.

[3] M Steiner, G Tsudik, M Waidner. Key agreement in dynamic peer groups[J]. IEEE. Transactions on Parallel and Distributed Systems, 2000, 11(8): 769 - 780.

[4] Y Kim, A Perrig, G Tsudik. Communication-efficient group key agreement[A]. Proceedings of the 17th International Information Security Conference[C]. Paris, Kluwer, 2001. 10 - 18.

[5] Y Kim, A Perrig, G Tsudik. Tree-based group key agreement [J]. ACM Transactions on Information and System Security, 2004, 7(1): 60 - 96.

[6] Mark Manulis. Contributory group key agreement protocols, revisited for mobile ad-hoc groups[A]. In Proceedings of 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS 2005), International Workshop on Wireless and Sensor Networks Security (WSNS 2005)[C]. Washington, USA, 2005. 811 - 818.

[7] Emmanuel Bresson, Dario Catalano. Constant round authenticated group key agreement via distributed computation[A]. Public Key Cryptography-PKC 2004[C]. Springer-Verlag, 2004. 115 - 129.

[8] 王志伟,谷大武. 基于树结构和门限思想的组密钥协商协议[J]. 软件学报. 2004, 15(6): 924 - 927.
Wang Zhi-wei, Gu Da-wu. A group key agreement protocol based on tree and threshold idea[J]. Journal of Software. 2004, 15(6): 924 - 927. (in Chinese)

[9] 况晓辉,胡华平,卢锡城. 移动自组网络组密钥管理框架[J]. 计算机研究与发展. 2004, 41(4): 704 - 710.
Kuang Xiao-hui, Hu Hua-ping, Lu Xi-cheng. A new group key management framework for mobile ad-hoc networks[J]. Journal of Computer Research and Development. 2004, 41(4): 704 - 710. (in Chinese)

[10] Deng Hongmei, Mukherjee, Anindo Agrawal, Dharma P. Threshold and identity-based key management and authentication for wireless ad hoc networks[A]. International Conference on Information Technology: Coding Computing, ITCC 2004[C]. 2004. 107 - 111.

[11] Lin Hua-Yi, Huang Yueh-Min. Clustering-organized key management for mobile ad hoc networks[A]. Proceedings of the Fourth IASTED International Multi-Conference on Wireless and Optical Communications[C]. 2004. 472 - 477.

[12] Guo Wei, Xiong Zhong-Wei, Li Zhi-Tang. Complex threshold key management for ad hoc network[J]. Wuhan University Journal of Natural Sciences, 2005, 10(1): 132 - 136.

[13] L Zhou, Z J Haas. Securing ad hoc networks[J]. IEEE Network Magazine Special Issue on Network Security, 1999, 13(6): 24 - 30.

[14] Claude Castelluccia, Nitesh Saxena, Jeong Hyun Yi. Self-configurable key pre-distribution in mobile Ad Hoc Networks[J]. Lecture Notes in Computer Science. 2005, 3462: 1083 - 1095.

[15] 杨子胥. 近世代数[M]. 北京: 高等教育出版社, 2004. 41.
Yang Zi-xu. Modern Algebra[M]. Beijing: Higher Education Press, 2004, 41. (in Chinese)

[16] Wenbo Mao 著, 王继林, 伍前红等译. 现代密码学理论与实践[M]. 北京: 电子工业出版社, 2004. 117.
Wenbo Mao. Modern Cryptography-Theory and Practice[M]. Beijing: Publishing House of Electronics Industry, 2004. 117. (in Chinese)

作者简介:

冯 涛 男, 1970 年出生于甘肃临洮, 博士, 兰州理工大学计算机与通信学院研究员, 主要研究兴趣为安全协议组合理论、无线传感器网络安全. E-mail: fengt@lut.cn

王毅琳 男, 1980 年出生于重庆, 兰州理工大学硕士生, 主要研究方向为无线网络安全.

马建峰 男, 1963 年出生于陕西西安, 西安电子科技大学教授、博导, 主要研究领域为计算机安全、密码学、移动与无线网络安全.