用于无线自组织网络的属性加密算法

高昂，李增智，赵季中
（西安交通大学电子与信息工程学院，710049，西安）

摘要：针对在无线自组织(ad hoc)网络中难以高效地加密和传输敏感消息的问题，提出了一种基于属性的无线自组织网络加密算法.该算法的阈值访问策略使得只有属性超过一定阈值的用户才能够解密消息，从而实现了群组加密；利用离散傅里叶变换分割密钥，使得密钥的分享值可以通过公开信道发布给用户；利用离散傅里叶逆变换还原密钥，使得解密过程具有一定的容错性且降低了解密的时间复杂度.实验结果表明，该算法不仅能有效降低无线自组织网络节点的能耗，而且使用该算法传输消息时延很小，适合在无线自组织网络中使用.

关键词：属性加密；阈值访问策略；离散傅里叶变换；无线自组织网络
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2012)08-0033-04

An Efficient Attribute-Based Encryption Algorithm for Ad Hoc Networks

GAO Ang, LI Zengzhi, ZHAO Jizhong
(School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: An efficient attribute-based encryption algorithm is proposed to solve the problem that it is inefficient to encrypt and transmit sensitive message in ad hoc networks. The use of the access control policy that only allows users with the attributes above one threshold to decrypt message results in group decryption. The discrete Fourier transform is used to share secret key, such that the shares of the secret key are issued to users over open channel; Users use the inverse discrete Fourier transform to recover the secret key, such that decryption has a fault tolerance and the time complexity of decryption is reduced. Experimental results show that the proposed algorithm not only reduces the energy consumption of the node in ad hoc networks, but also has an ignorable delay in transmitting message, thus it is suitable for application to ad hoc networks.

Keywords: attribute-based encryption; threshold access control; discrete Fourier transform; ad hoc networks

在公钥加密体系中，用户的生物特征如指纹、人脸和虹膜等是唯一的且不易被伪造，自然可以作为公钥使用，Shamir 等[1]首先提出了基于身份的加密(Identity-Based Encryption，IBE).与 ID 有关的私钥由一个私钥生成中心(Private Key Generator，PKG)生成，通过秘密信道发送给用户.然而，由于生物特征数据一般包含噪声，即同一个生物特征值的两个测量值不完全相同，所以将公钥与生物特征值绑定就具有了模糊性，从而导致解密失败.为了解决这个问题，Sahai 等[2]提出了具有容错性的 IBE 机制，其生物特征信息是具有某些特定属性的集合.这样，IBE 就发展成为基于属性的加密(Attribute-Based Encryption，ABE).近年来，国内外学者提出了很多 ABE 方案[3-7]，其中针对 ABE 容易遭受共谋

收稿日期：2012-01-09. 作者简介：高昂(1978—)，男，博士生；李增智(通信作者)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60873262).
网络出版时间：2012-05-18 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20120518.0557.001.html

攻击的问题，Chase[6]提出了具有多个 PKG 的 ABE 机制；Chase 等[7]改进了 Chase 的 ABE 方案，提出了一种匿名 ABE 机制，从而保护了加密过程的隐私性.

但是，目前的 ABE 机制主要用于有线网络. 对于缺少通信网络基础设施的无线网络，尤其是移动自组织网络(又称 ad hoc 网络)，由于其节点可以不断地随意运动，网络的拓扑结构总是处于动态变化中，加上无线自组织网络中的节点一般兼具主机和路由器功能的无线终端，其计算能力、存储能力和电源能量都十分有限，且无线访问介质处于公共开放区域，使得节点间的通信易遭到窃听. 因此，无线自组织网络所面临的安全问题比传统有线网络复杂得多.

本文提出了一种适合无线自组织网络应用的基于属性的加密算法，设计了一个阈值访问策略以限定具有某种属性的用户才能够解密消息，分别利用离散傅里叶变换及其逆变换分割密钥和解密，在无线自组织网络环境中对该算法的有效性进行了验证.

1 ABE 的基本原理

ABE 是利用双线性映射构建的加密方案. 该双线性映射可表示为 $\hat{e}:\boldsymbol{G}_1\times\boldsymbol{G}_1\rightarrow\boldsymbol{G}_2$，其中 $\boldsymbol{G}_1$ 和 $\boldsymbol{G}_2$ 均是阶为素数 q 的循环群，且 g_1 和 g_2 分别为 $\boldsymbol{G}_1$ 和 $\boldsymbol{G}_2$ 的生成元. 对于 $\forall u,v\in\boldsymbol{G}_1$ 以及 $\alpha,\beta\in\boldsymbol{Z}_q$，$\hat{e}$ 有以下 3 条性质：①双线性，$\hat{e}(u^\alpha,v^\beta)=\hat{e}(u,v)^{\alpha\beta}$；②非退化性，$\hat{e}(g_1,g_1)\neq1$；③可计算性，$\hat{e}(g_1,g_1)$是可以有效计算的，且存在一个同态映射 $\psi:\boldsymbol{G}_2\rightarrow\boldsymbol{G}_1$，使得 $\psi(g_2)=g_1$.

2 一种高效的 ABE 算法

(1)建立. PKG 设定一个阈值 d，使得 $d\leqslant|\boldsymbol{A}_c\cap\boldsymbol{A}^e|$. 其中，$\boldsymbol{A}^e$ 和 $\boldsymbol{A}_c$ 分别为加密者拥有的属性集以及 PKG 管理的属性集. 用控制循环群大小的安全参数 λ 生成两个阶为素数 q 的循环群 $\boldsymbol{G}_1$ 和 $\boldsymbol{G}_2$ 来构造双线性映射 $\hat{e}:\boldsymbol{G}_1\times\boldsymbol{G}_1\rightarrow\boldsymbol{G}_2$. 选取散列函数 $H_1:\{0,1\}^*\rightarrow\boldsymbol{G}_1$ 和 $H_2:\boldsymbol{G}_2\rightarrow\{0,1\}^k$(ABE 的信息空间是一个 k bit 的字符串集合)，并用随机值 $s\in\boldsymbol{Z}_q$ 生成主公钥 g_1^s. 发布如下系统参数 P

$$P=\langle q,\boldsymbol{G}_2,\hat{e},g_1,g_1^s,H_1,H_2\rangle$$

(2)属性变形. 每个用户 u 利用同余式(1)将其属性 $i\in\boldsymbol{A}^u$ 转换为 l

$$l\bmod|\boldsymbol{A}_c^e|=L_i \tag{1}$$

式中：$\boldsymbol{A}_c^e=\boldsymbol{A}^e\cap\boldsymbol{A}_c$；$L_i$ 为 i 在 $\boldsymbol{A}^e$ 上的索引. u 在式(2)中输入 l 生成单元根 $\omega=\exp(2\pi L_i\mathrm{i}/|\boldsymbol{A}_c^e|)$

$$f(x)=\exp(2\pi x\mathrm{i}/|\boldsymbol{A}_c^e|) \tag{2}$$

式中：i 表示虚数单位.

(3)加密. 对于一个 k bit 的消息 M，加密方选择一个随机值 $r\in\boldsymbol{Z}_q$ 来发布如下密文二元组

$$C=\langle E_0=M\oplus Y^r,E_1=g_1^r\rangle \tag{3}$$

式中：$Y^r=H_2(\hat{e}(g_1^s,H_1(u))^r)$.

u 向 PKG 提交其变形属性集 $\boldsymbol{W}^u=\{\omega_n\}_{n\in[1\cdots|\boldsymbol{A}^u|]}$.

(4)利用 DFT 抽取密钥. PKG 接收到 $\boldsymbol{W}^u$ 后，随机地生成 $d-1$ 阶多项式

$$p(x)=s+\sum_{n=1}^{d-1}a_nx^n \tag{4}$$

式中：非常数项系数 $a_n(n=[1,\cdots,d-1])$为随机选取，且常数项系数 $p(0)=s$ 作为秘密值保存. 在式(4)中输入 $\omega\in\boldsymbol{W}^u$ 抽取出分享值(称为子密钥)$D_\omega=H_1(u)^{p(\omega)}$. 这样，子密钥的生成相当于对 d 个不同的 ω_n 作傅里叶变换. PKG 发布 D_ω 给用户.

(5)利用 IDFT 解密. 若 u 的变形属性集 $\boldsymbol{W}^u$ 满足 $|\boldsymbol{W}^u\cap\boldsymbol{W}_c|\geqslant d$，则 u 能够拿到足够多的 D_ω. 因此，根据傅里叶逆变换有

$$s=\frac{1}{d}\sum_{n=1}^{d}p(\omega_n) \tag{5}$$

u 按照如下步骤解密出明文 M

$$E_0\oplus H_2\Big(\prod_{n=1}^{d}\hat{e}(D_{\omega_n},E_1)^{\frac{1}{d}}\Big)=$$
$$E_0\oplus H_2\Big(\prod_{n=1}^{d}\hat{e}(H_1(u)^{p(\omega_n)},g_1^r)^{\frac{1}{d}}\Big)=$$
$$E_0\oplus H_2\Big(\prod_{n=1}^{d}\hat{e}(H_1(u),g_1)^{\frac{rp(\omega_n)}{d}}\Big)=$$
$$E_0\oplus H_2\Big(\hat{e}(H_1(u),g_1)^{\frac{r}{d}\sum_{n=1}^{d}p(\omega_n)}\Big)=$$
$$M\oplus Y^r\oplus H_2(\hat{e}(H_1(u),g_1)^{rs})=$$
$$M\oplus H_2(\hat{e}(g_1^s,H_1(u))^r)\oplus H_2$$
$$(\hat{e}(H_1(u),g_1)^{rs})=M \tag{6}$$

3 安全分析

基于判断双线性 Diffie-Hellman(Bilinear Diffie-Hellman, BDH)问题的困难性，攻击本文方案的困难性等价于在判定性 BDH 攻击游戏中获得成功的低概率，详细的分析证明见文献[3-4]. 我们在密钥密文长度以及网络攻击防护方面与已有的机制进行了比较. 根据表 1 中的理论值，本文方案的密钥和密文长度均小于已有机制的长度，同时利用用户

ID 还可以抵御拒绝服务(DoS)攻击和共谋攻击.

表 1　本文方案与现有机制的安全性比较

参数	Chase[6] ABE 方案	Chase-Chow[7] ABE 方案	本文方案
PKG 密钥长度	$(\lvert\boldsymbol{A}_c^u\rvert+1)B_2$	$(\lvert\boldsymbol{A}_c^u\rvert+N^c)B_2$	$\lvert\boldsymbol{A}_c^u\rvert B_1$
用户密钥长度	$(\lvert\boldsymbol{A}^u\rvert+1)B_2$	$(\lvert\boldsymbol{A}^u\rvert+N^c-1)B_1$	$\lvert\boldsymbol{A}^u\rvert B_1$
密文长度	$B_T+(1+\lvert\boldsymbol{A}^e\rvert)B_2$	$B_T+(1+\lvert\boldsymbol{A}^e\rvert)B_2$	$B_2+\lvert\boldsymbol{A}_c^u\rvert B_1$
DoS 攻击	×	√	√
共谋攻击	×	√	√

注：B_1、B_2 以及 B_T 分别表示 $\boldsymbol{G}_1$、$\boldsymbol{G}_2$ 以及循环群 $\boldsymbol{G}_T$ 中元素的字节长度；N^c 为 PKG 的个数；√表示可抵御攻击；×表示易遭受攻击.

4　实验与性能分析

4.1　实验设置

为了验证本文方案的有效性，我们搭建了一个由 5 台笔记本电脑、3 部手机以及 3 台 PDA 共 10 个节点组成的 ad hoc 网络，如图 1 所示. 每台设备都配备有支持 IEEE 802.11 a/b/g/n 协议的无线网卡，设备之间可以很方便地切换到无线自组织模式下进行通信. 当前的手机和 PDA 在能量、计算能力和存储空间上受限，一般不用作路由，我们把这些设备部署为终端节点. 具有多个属性的用户直接操纵这些设备与网络中的其他节点进行 UDP 通信. 此外，一台与无线自组织网络相连的台式机作为 PKG，负责为用户生成和发布密钥，需要注意的是 PKG 只负责发布密钥给用户，而不转发任何数据包.

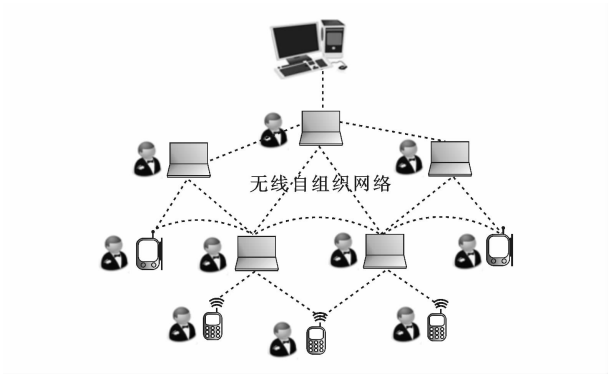

图 1　ABE 在无线自组织网络中的应用

路由协议采用 OLSR 协议，其默认配置见文献[8]. 此外，我们还配置了一些与 ABE 有关的安全参数，其默认值如表 2 所示.

表 2　安全参数默认值

参数	默认值	含义
N^u	10	参与用户数
N^c	1	PKG 个数
$H(m)$	$\lvert m\rvert\leqslant 2^{64}$ B，$\lvert H(m)\rvert=160$ B	安全散列算法以报文 m 作为输入，输出散列值 $H(m)$
λ	97	素阶群的大小

4.2　性能对比

在性能评估测试中，针对本文方案在传送不同容量数据包情况下的能耗以及信息传输延时这两个性能指标，我们将其与运用安全方案之前的性能进行了比较. 对于本文方案还原密钥所产生的计算开销，我们将其与已有机制的性能进行了比较.

(1)通信开销. 图 2 为节点间不采用任何加密措施与采用本文安全方案传输信息时的能量消耗对比. 实验结果表明，本文方案的能耗随数据包携带信息量的增加而增大，但平均能耗与没采用安全方案时的能耗相比差别不大，即使用 ABE 消耗的能量很低. 因此，采用本文方案既能降低节点间通信产生的能耗，又不会影响无线自组织网络传输的信息量.

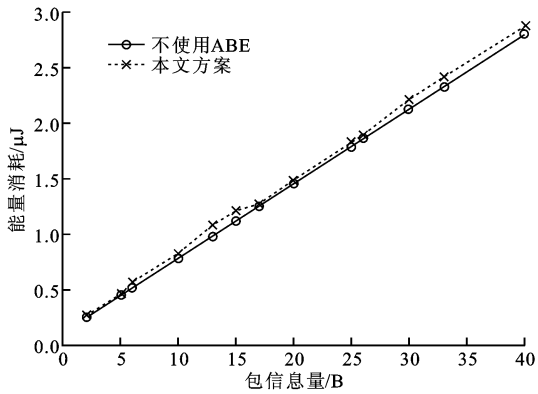

图 2　通信能耗开销

(2)平均延时. 图 3 为节点间进行普通信息传输与采用本文安全方案传输时的传输延时比较. 实验结果表明，虽然数据传输延时随数据包的增加而加大，但本文方案的平均延时要小于 0.2 s，这对数据的发送、传输和接收影响很小. 这是因为本文方案所采用的双线性映射和安全散列函数具有较高的运算效率，其加密敏感信息的速度比常规分组加密算法

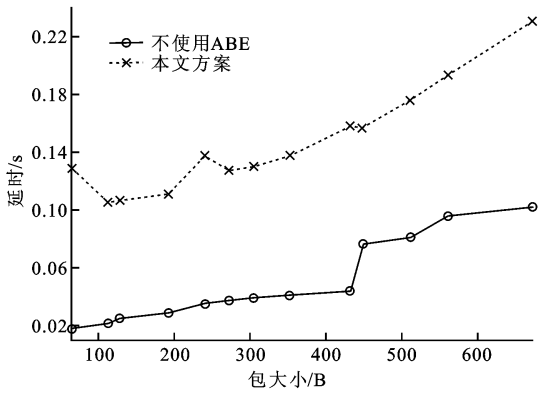

图3 信息传输延时

快很多倍.

(3)计算开销. 如图4所示,$\boldsymbol{A}^u$ 的大小对计算开销也有一定的影响,$|\boldsymbol{A}^u|$ 变大解密需要执行更多的算术加法和乘法. 与 Chase ABE 和 Chase-Chow ABE 机制相比,本文方案需要更少的计算开销. 这是因为本文方案还原密钥所使用的傅里叶逆变换算法的时间复杂度 $O(|\boldsymbol{A}^u|^2)$ 要小于 Chase ABE 和 Chase-Chow ABE 方案所采用的拉格朗日插值算法的复杂度 $O(|\boldsymbol{A}^u|^4)$.

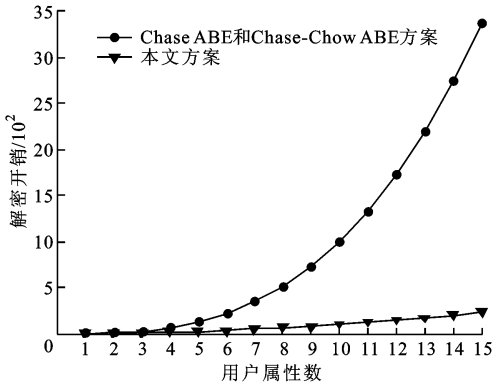

图4 解密的计算开销

5 结 论

本文提出了一种高效的基于属性的加密算法,为 ad hoc 网络中数据的保密传输开辟了一个全新的研究途径,主要贡献如下:①根据加密者属性集与 PKG 属性集的交集,设计了一个阈值访问策略,只要接收方的属性超过此阈值便可解密消息,而加密者无需知道是谁解密,从而实现了群组解密;②利用 DFT 分割密钥,使得密钥的分享值可以通过公开信道发布给用户;③利用 IDFT 还原密钥,使解密过程具有一定的容错性且降低了解密的时间复杂度. 实验结果表明,本文方案具有较低的通信和计算开销,能够降低节点的能耗,同时使用该算法传输消息时延很小,适合在 ad hoc 网络中使用.

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[C]// Proceedings of the 4th Annual International Cryptology Conference on Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985: 47-53.

[2] SAHAI A, WATERS B R. Fuzzy identity-based encryption [C]// Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2005: 457-471.

[3] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, NY, USA: ACM, 2006: 89-98.

[4] 唐强, 姬东耀. 多授权中心可验证的基于属性的加密方案[J]. 武汉大学学报, 2008, 54 (5): 607-610.
TANG Qiang, JI Dongyao. Multi-authority verifiable attribute-based encryption[J]. Journal of Wuhan University, 2008, 54 (5): 607-610.

[5] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE [C]// Proceedings of the 14th ACM Conference on Computer and Communications Security. New York, NY, USA: ACM, 2007: 456-465.

[6] CHASE M. Multi-authority attribute based encryption [C]// Proceedings of the 4th Conference on Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007: 515-534.

[7] CHASE M, CHOW S S M. Improving privacy and security in multi-authority attribute-based encryption [C]// Proceedings of the 16th ACM Conference on Computer and Communications Security. New York, NY, USA: ACM, 2009: 121-130.

[8] MACKER J, LEE R. The NRL OLSR routing protocol implementation [EB/OL]. (2007-01-08) [2012-11-08]. http://cs.itd.nrl.navy.mil/work/olsr/.

(编辑 武红江)