doi:10.3772/j.issn.1002-0470.2013.02.001

移动对等传感器网络的基于属性加密的组密钥管理协议①

张国印②* 付小晶③*** 马春光*

(*哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)

(**网络与数据安全四川省重点实验室 成都 611731)

摘 要 提出了一个具有较小解密代价的密文策略属性基加密(CP-ABE)方案,并在标准模型下证明了其安全性。进而提出一个适用于移动对等传感器网络(MP2PWSN)的基于 CP-ABE 的组密钥管理协议。在该协议下,移动节点和簇头节点首先完成簇间组密钥分发,然后由簇头进行簇内组密钥分发。该协议满足后向安全性,支持节点动态加入,退出以及节点撤销,还能实现细粒度的传感器数据访问控制和隐私保护。仿真结果表明,该协议由于采用低解密代价的 CP-ABE 算法,传感器节点的能耗不随属性数量的增多而显著增加,因此能够较好地满足 MP2PWSN 的匿名组通信安全需求。

关键词 移动对等传感器网络(MP2PWSN),组密钥,属性基加密(ABE),标准模型,匿名通信

0 引 言

近年来,对等(P2P)网络分布式计算模式开始逐渐应用于无线传感器网络[1-3]。2008 年,Rondini 等[3]首次提出移动对等传感器网络(mobile peer-to-peer wireless sensor network,MP2PWSN)概念,即,覆盖于移动传感器网络的对等网络。目前,MP2PWSN 主要采用同构传感器网络结构和集中式存储方式(基站存储)。由于异构传感器网络(heterogeneous sensor network,HSN)[4]包含不同类型的节点,能够更好地满足应用需求,传感器数据的分布式存储比集中式存储具有通信代价较低、单点失效影响较小等优点[5]。因此,MP2PWSN 更适合采用 HSN 结构和分布式数据存储模式。在 MP2PWSN 中,手持终端和机器人等高性能节点可作为移动节点用对等方式通信,实现传感器数据的分布式存储、访问和定位,可更好地实现分布式传感器数据的共享。目前 MP2PWSN 研究主要集中于对等路由、数据搜索定位和带宽控制等领域,密钥管理机制研究较少。传统 HSN 密钥管理机制[6,7]研究主要以集中式存储结构为背景,不能较好地应用于 MP2PWSN。在 MP2PWSN 应用于医疗监控等时,具有共同兴趣爱好或共同任务目标的节点(包括移动终端用户)构成一个通信组,以实现传感器数据的共享,且要求保护用户的隐私。2007 年 Cheung 等[8]采用密文策略属性基加密(ciphertext-policy attribute-based encryption, CP-ABE)[9]设计了一个抗碰撞的组密钥管理协议,组密钥分发无需知道接收者的身份,达到了匿名目的。但属性数量增多时此协议解密代价较高,不适合低性能的传感器节点。2011 年 Yu 等[5]采用密钥策略属性基加密(key-policy ABE, KP-ABE)设计了一个分布式传感器网络数据的细粒度访问控制方案。此方案可使任何满足访问策略的用户解密获得对称密钥,进而解密获得传感器数据,密文中不传递访问结构,不会暴漏接收者的属性信息,从而增强了匿名性,但存在访问结构与私钥绑定并在初始化阶段确定的局限。对此,本文提出了一个解密代价较低的 CP-ABE 方案,进而提出一个适合 MP2PWSN 的高效的组密钥管理协议。

① 国家自然科学基金(61073042,61170241),中央高校基本科研业务费专项资金(HEUCF100606),网络与数据安全四川省重点实验室开放课题资金(201107)和黑龙江省教育厅科学技术研究项目资金(12523049)资助项目。

② 男,1962 年生,博士,教授;研究方向:网络与信息安全,嵌入式系统;E-mail:zhangguoyin@hrbeu.edu.cn

③ 通讯作者,E-mail:fuxiaojing@hrbeu.edu.cn

(收稿日期:2012-04-19)

1 预备知识

1.1 双线性对和困难问题假设

定义 1 双线性对：G_1、G_2 是阶为素数 p 的循环群，g 是 G_1 的生成元。双线性对 $\hat{e}$：$G_1 \times G_1 \rightarrow G_2$ 满足以下条件：

(1) 双线性(bilinearity)：对于任意 $u,v \in G_1$，$a,b \in_R Z_p^*$，$\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$ 都成立；

(2)非退化性(nondegeneracy)：对于任意 $u,v \in G_1$，存在 $\hat{e}(u, v) \neq 1_{G_2}$，$1_{G_2}$ 是 G_2 的单位元；

(3)可计算性(computability)：对于任意 u，$v \in G_1$，存在一种有效的算法计算 $\hat{e}(u, v) \in G_2$。

定义 2 truncated 判定 q-ABDHE 问题：对于 $\alpha \in_R Z_p^*$，已知 $g', g'^{\alpha^{q+2}}, g, g^{\alpha}, \cdots, g^{\alpha^q} \in G_1, Z \in G_2$，判断 $\hat{e}(g^{\alpha^{q+1}}, g') = Z$。

1.2 MP2PWSN 模型

MP2PWSN 可以采用集中式 P2P 和纯 P2P 相结合的混合式 P2P 网络模型[10]，这种模型兼具集中式 P2P 快速查找和纯 P2P 去中心化的优势。网络模型如图 1 所示。网络中包含移动节点(M-Node)、簇头节点(H-Node)和普通传感器节点(S-Node)。M-Node 为高性能节点，具有较强的处理、存储和通信能力，由手持终端或者具有采集能力的机器人充当，具有存储和查找传感器数据的能力。H-Node 为高性能节点，具有感知、存储和查找传感器数据的能力。S-Node 为低性能节点，具有较低的处理、存储、通信和能量等方面性能，具有感知、传输传感器数据的能力。H-Node 与其临近的若干 S-Node 之间构成一个自治的簇，采用基于集中目录式的 P2P 模式，H-Node 与 H-Node 以及 M-Node 之间通过纯 P2P 结构化模式相连。

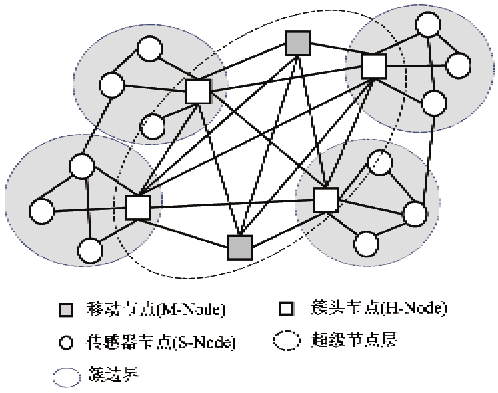

图 1 MP2PWSN 网络模型

2 协议描述

2.1 新的基于属性加密方案

本文在 Gentry IBE 方案[11]基础上，提出一个 CP-ABE 方案。访问策略采用树结构表示，如图 2 所示。非叶子节点为逻辑门节点，叶子节点为属性节点。num_x 表示非叶子结点的孩子节点个数。k_x 表示门限值，$1 \leqslant k_x \leqslant num_x$。当非叶子节点为“与门”(AND)时，$k_x = num_x$，当非叶子节点为“或门”(OR)时，$k_x = 1$。当非叶子节点为“门限门”$(t,n)$ 时，$k_x = t$。令 $parent(x)$ 表示节点 x 的父节点，$att(x)$ 表示属性节点 x 的属性值，$index(x)$ 表示节点 x 的索引值，即节点 x 在兄弟节点中所处序列位置。

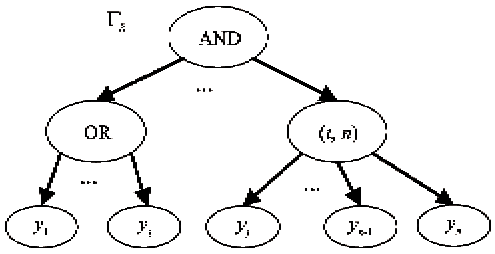

图 2 访问结构树示例

(1)参数建立 $Setup(\ )$

密钥生成中心(private key generator, PKG)选择一个双线性对 $\hat{e}$：$G_1 \times G_1 \rightarrow G_2$，$G_1$、$G_2$ 是阶为素数 p 的循环群。设属性集 $U \subset_R Z_p^*$，拉格朗日插值系数 $\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}, S \subset_R Z_p^*$。随机选取 $g, h \in G_1, \alpha, \beta \in_R Z_p^*$，$\{t_i \in_R Z_p^*\}_{i \in U}$，计算 $g_1 = g^{\alpha}$，$\{T_i\}_{i \in U} = \{g^{-t_i}\}_{i \in U}$，$E = \hat{e}(g, g)$，$H = \hat{e}(g, h)$，保密系统主密钥 $MK = \langle \alpha, \beta, \{t_i\}_{i \in U} \rangle$，公开系统参数 $param = \langle p, G_1, G_2, \hat{e}, g, g_1, h, g^{\beta}, \{T_i\}_{i \in U}, E, H \rangle$。

(2) 私钥生成 $Extrct(MK, \omega_{ID})$

给定用户 ID，其属性集为 $\omega_{ID} \subset U$。PKG 随机选择 $\{r_{ID,i}\}_{i \in \omega_{ID}}$，$r_{ID} \in_R Z_p^*$，计算 $h_{ID,i} = \{h^{r_{ID}} g^{-r_{ID,i}}\}^{1/(\alpha - t_i)}$，用户的私钥为 $sk_{\omega_{ID}} = \langle D_{ID} = h^{(r_{ID}+1)/\beta}, D_{ID,i} = \{r_{ID,i}\}_{i \in \omega_{ID}}, D'_{ID,i} = \{h_{ID,i}\}_{i \in \omega_{ID}} \rangle$。

(3)加密 $Encrypt(\Gamma_R, m)$

采用访问结构 Γ_R，对消息 m 加密。从根节点开始为每个节点 x 构造多项式 q_x，其次数为 $d_x = k_x - 1$。首先，随机选取 $s \in_R Z_p^*$，令 $q_R(0) = s$，再选取

d_R 个点,构造根节点的多项式 q_R。然后为其他节点 x 构造多项式 q_x,并且满足 $q_x(0) = q_{parent(x)}(index(x))$。设叶子节点集合为 Y,则密文为:$CT = (\Gamma_R, \tilde{C} = m \cdot H^{-s}, C = g^{\beta s}, \forall y \in Y, i = att(y), C_y = E^{q_y(0)}, C_y' = (T_i g_1)^{q_y(0)})$。

(4)解密 $Decrypt(\Gamma_R, sk_\omega, CT)$

设密文 $CT = (\Gamma_R, \tilde{C}, C, C_y, C_y')$,接收者属性集为 ω。从根节点开始对每个节点 x 调用解密函数 $DecryptNode(CT, \Gamma, x)$,保存输出为 F_x。如果 x 是叶子节点,并且 $i = att(x), i \in w$,则返回 $\Gamma_x(\omega) = 1$,并计算得到:$F_x = DecryptNode(CT, \Gamma_R, x) = e(C_x', D_{ID,i}') C_x^{D_{ID,i}}$。如果 x 是非叶子节点,设 S_x 是 x 的任意 k_x 个孩子节点 z 组成的集合。$i = index(z)$, $S_x' = \{index(z), z \in S_x\}$,如果 k_x 个孩子节点返回 $\Gamma_z(\omega) = 1$,则返回 $\Gamma_x(\omega) = 1$,计算得到:$F_x = DecryptNode(CT, \Gamma_R, x) = \prod_{z \in S_x} (F_z)^{\Delta_{i,S_x'}(0)}$。如果 $\Gamma_x(\omega) \neq 1$,解密失败。因此,可以计算根节点对应的解密值 $F_R = \hat{e}(g,h)^{r_{ID} q_R(0)} = \hat{e}(g,h)^{r_{ID} s}$。最后解密得到消息明文:$m = \tilde{C} \cdot F_R / \hat{e}(C, D_{ID})$。

正确性证明:

$$
\begin{aligned}
F_x &= e(C_x', D_{ID,i}') C_x^{D_{ID,i}} \\
&= \hat{e}(g^{-q_x(0) \cdot t_i} g_1^{q_x(0)}, \\
&\quad (h^{r_{ID}} g^{-r_{ID,i}})^{1/(\alpha - t_i)}) \hat{e}(g,g)^{q_x(0) \cdot r_{ID,i}} \\
&= e(g,h)^{r_{ID} q_x(0)} \\
F_x &= \prod_{z \in S_x} (F_z)^{\Delta_{i,S_x'}(0)} \\
&= \prod_{z \in S_x} (\hat{e}(g,h)^{r_{ID} q_{parent(z)}(index(z))})^{\Delta_{i,S_x'}(0)} \\
&= \prod_{z \in S_x} (\hat{e}(g,h)^{r_{ID} q_x(i)})^{\Delta_{i,S_x'}(0)} = \hat{e}(g,h)^{r_{ID} q_x(0)} \\
F_R &= \hat{e}(g,h)^{r_{ID} q_R(0)} \\
&= \hat{e}(g,h)^{r_{ID} s} \tilde{C} \cdot F_R / \hat{e}(g^{\beta s}, h^{(r_{ID}+1)/\beta}) \\
&= m \hat{e}(g,h)^{s} \hat{e}(g,h)^{r_{ID} s} / (\hat{e}(g^s, h^{r_{ID}}) \hat{e}(g^s, h)) \\
&= m
\end{aligned}
$$

2.2 组密钥管理协议

(1)网络部署与初始化

设移动节点 M-Node 集合为 $MN = \{m_1, m_2, \cdots, m_{n_M}\}$,簇头节点 H-Node 集合为 $HN = \{h_1, h_2, \cdots, h_{n_H}\}$,网络中包含 n_H 个簇,CL_i 表示第 i 个簇,h_i 为簇 CL_i 的簇头,传感器节点 S-Node 集合为 $SN = \{s_1, s_2, \cdots, s_{n_S}\}$。设属性集为 $U \subset_R Z_p^*$,为所有的节点分配属性,移动节点和簇头节点被分配若干属性,包括一个唯一的标识作为特殊属性,每个传感器节点只被分配一个特殊属性,即唯一的标识。PKG 按照 2.1 节初始化算法和私钥生成算法,生成系统公开参数和主密钥,为所有节点生成私钥(包括唯一标识对应的私钥),并且通过安全方式将私钥发送给 M-Node,其他 H-Node 和 S-Node 传感器节点预先装载私钥。

(2)组密钥分发协议

组密钥分发协议分为两步:簇间组密钥分发和簇内组密钥分发。M-Node 或者 H-Node 可以作为组控制者发起组通信,S-Node 也可以请求簇头节点发起组通信。组控制者在 M-Node 和 H-Node 之间分发组密钥。然后 H-Node 再将组密钥分发给所在簇内的所有 S-Node。

第一步:簇间组密钥分发

设组控制者 $GC \in MN \cup HN$。GC 选择组密钥 $K \in GK$,GK 表示组密钥空间。令消息 $m = K \| time \| sessionID$,$GC$ 调用 2.1 节的加密算法,得到密文 $CT = Encrypt(\Gamma_R, m)$,在组中发送消息:$Message = \langle sessionID, time, \Gamma_R, CT \rangle$。

任何满足访问结构 Γ_R 的组成员 $GM \in MN \cup HN$,收到消息 $Message = \langle sessionID, time, \Gamma_R, CT \rangle$,调用 2.1 节的解密算法,得到明文 $m = Decrypt(\Gamma_R, sk_{\omega_{GM}}, CT)$,得到组密钥 K。

第二步:簇内组密钥分发

簇 CL_i 的簇头节点 h_i 获得组密钥 K 后,设置访问结构 $\Gamma_{R',i} = ID_1 ORID_2 \cdots ORID_{n_i}$,其中,$ID_j$, $1 \leqslant j \leqslant n_i$ 为簇 CL_i 中传感器节点的特殊属性(唯一标识)。令消息 $m = K \| time \| sessionID$,计算 $CT_i = Encrypt(\Gamma_{R',i}, m)$,在簇 CL_i 中发送消息:$Messagei = \langle sessionID, time, \Gamma_{R',i}, CT_i \rangle$。

簇 CL_i 中的传感器节点 s_{ID_j}, $1 \leqslant j \leqslant n_i$ 接到消息 $Messagei = \langle sessionID, time, \Gamma_{R',i}, CT_i \rangle$,计算 $m = Decrypt(\Gamma_{R',i}, sk_{ID_j}, CT_i)$,得到组密钥 K。

(3)节点加入和离开组

当有新节点 $GM \in MN \cup HN \cup SN$ 预加入组时,GC 执行(2)中的组密钥分发过程,使得 GM 获得组密钥 K。节点离开组时,组密钥不需要更新。因为只要满足访问策略的节点无论是在线或者离线都可以获得组密钥,访问传感器数据。而且由于无线网络的抗干扰能力差,导致节点容易"掉线",当节点重新加入组中,即使组密钥更新了,节点只要满足访问结构就可以解密获得组密钥。

(4)节点添加与撤销

如果系统补充新的节点,PKG 执行初始化算法,为新加入系统的节点分配属性和私钥。如果撤

销某些节点,则采用 Yu 方案[5]的用户撤销思想更新系统主密钥和所有未撤销节点的私钥。首先,PKG 生成一个所有剩余节点满足而被撤销节点不满足的访问策略 Γ'_R。随机选择 $\beta' \in_R Z_p^*$,令 $\Delta\beta = \beta/\beta'$,把消息 $\Delta\beta$ 的密文 $CT_{\Delta\beta}$ 签名和密文发送给所有未撤销节点。未撤销节点 ID 接到消息 $CT_{\Delta\beta}$ 解密获得 $\Delta\beta = \beta/\beta'$,计算 $(h^{(r_{ID}+1)/\beta})^{\Delta\beta} = (h^{(r_{ID}+1)/\beta})^{\beta/\beta'} = h^{(r_{ID}+1)/\beta'}$,更新私钥为 $sk'_{\omega_{ID}} = \langle \{r_{ID,i}\}_{i\in\omega_{ID}}, \{h_{ID,i}\}_{i\in\omega_{ID}}, h^{(r_{ID}+1)/\beta'}\rangle$。

3 安全性证明与分析

定理 1 如果 truncated 判定 q-ABDHE 困难问题成立,则所提基于属性加密方案满足 CPA 安全。

证明:本文借鉴 Gentry 方案[11]的证明思想证明该定理。假设攻击者 A 能够在概率多项式时间内以 ε 的优势在下面"模拟-挑战"游戏中获胜,并且 A 最多进行 q_K 次私钥生成询问。构造算法 C,利用 A 解决 truncated 判定 q-ABDHE 问题。即给定输入 $(g', g'^{\alpha^{q+2}}, g, g^{\alpha}, \cdots, g^{\alpha^q}, Z)$,判断 $Z = \hat{e}(g^{\alpha^{q+1}}, g')$ 是否成立。挑战者输出预挑战的访问结构 Γ_R^*。

(1)初始化阶段:模拟器随机选取一个 q 次秘密多项式 $f(x) \in Z_p[x]$,然后根据 $(g, g^{\alpha}, \cdots, g^{\alpha^q})$ 计算 $h = g^{f(\alpha)-f(0)}$。随机选取 $|U|$ 个 q 次秘密多项式 $y_i(x) \in Z_p[x]$,计算 $\{T_i\}_{i\in U} = \{g^{t_i}\}_{i\in U} = \{g^{y_i(0)\alpha}\}_{i\in U}$,系统主密钥为 $\langle \alpha, \beta = f(0)\alpha, \{t_i = y_i(0)\alpha\}_{i\in U}\rangle$(未知)。将系统公开参数 $param = \langle g, g_1, h, g^{\beta}, \{T_i\}_{i\in U}\rangle$ 发送给 A,这样设置的参数与真实系统参数具有相同的分布。C 为攻击者 A 模拟攻击游戏。

(2)询问阶段 1:攻击者 A 对属性集 ω_{ID} 发起产生私钥询问。设 $F_{ID,i}(x) = \dfrac{f(ID)(f(x)-f(0))-f(i)}{x-y_i(0)\alpha}$ 表示 $q-1$ 次多项式,C 产生私钥为 $sk_{\omega_{ID}} = \langle D_{ID} = g^{(f(\alpha)-f(0))(f(ID)+1)/f(0)\alpha}, D_{ID,i} = f(i), D'_{ID,i} = g^{F_{ID,i}(\alpha)}\rangle$。因为 $D_{ID} = g^{(f(\alpha)-f(0))(f(ID)+1)/f(0)\alpha} = h^{(f(ID)+1)/\beta}, D'_{ID,i} = g^{F_{ID,i}(\alpha)} = g^{\frac{f(ID)(f(\alpha)-f(0))-f(i)}{\alpha-y_i(0)\alpha}} = (g^{f(ID)(f(\alpha)-f(0))}g^{-f(i)})^{1/(\alpha-y_i(0)\alpha)} = (h^{f(ID)}g^{-f(i)})^{1/(\alpha-t_i)}$,所以 $sk_{\omega_{ID}}$ 是一个合法的私钥。

(3)挑战:A 输出消息 m_0, m_1 和挑战属性集 $\omega_0, \omega_1, \Gamma_R^*(\omega_0) = 1, \Gamma_R^*(\omega_1) = 1$。$C$ 产生比特 $b \in \{0,1\}, c \in \{0,1\}$。按照(2)过程计算 ω_c 的私钥 $sk_{\omega_{ID_c}} = \langle D_{ID_c}, D_{ID_c,i}, D'_{ID_c,i}\rangle$。设叶子节点集合为 Y。对于任意 $y \in Y, i = att(y)$,设多项式 $f_2(x) = x^{q+2}$,$F_{2,ID_c,i}(x) = \dfrac{f_2(x)-f_2(y_i(0)\alpha)}{x-y_i(0)\alpha}$ 为 $|Y|$ 个 $q+1$ 次多项式。C 根据输入 $(g', g'^{\alpha^{q+2}}, g, g^{\alpha}, \cdots, g^{\alpha^q}, Z)$ 可构造:$\tilde{C}^* = m_b \cdot \hat{e}(C^*, D_c)/F_R, C^* = F'_R, C'^*_y = \{g'^{(f_2(\alpha)-f_2(y_i(0)\alpha))}\}_{y\in Y, i=att(y)}, C_y^* = \{Z \cdot \hat{e}(g', g^{(\frac{1-y_i(0)^{q+2}}{1-y_i(0)})})\}_{y\in Y, i=att(y)}$。

F_R, F'_R 的构造过程:从根节点开始对每个节点 x 调用 $DecryptNode(CT, \Gamma_R, x)$,如果 x 是叶子节点,则计算 $i = att(x), F_x = DecryptNode(CT, \Gamma_R, x) = e(C'^*_x, D'_{ID_c,i})C_x^{*D_{ID_c,i}}, F'_x = g^{f(0)\alpha(\log_g g')F_{2,ID_c,i}(\alpha)} = g'^{f(0)\alpha F_{2,ID_c,i}(\alpha)}$,其中,$\alpha\sum_{i\in\omega'} F_{2,ID_c,i}(\alpha) = \left(\dfrac{1-y_i(0)^{q+2}}{1-y_i(0)}\right)\alpha^{q+2}$ 为 $q+2$ 次多项式。如果 x 是非叶子节点,则设 S_x 是 x 的任意 k_x 个孩子节点 z 组成的集合。$i = index(z), S'_x = \{index(z), z \in S_x\}$,计算 $F_x = DecryptNode(CT, \Gamma_R, x) = \prod_{z\in S_x}(F_z)^{\Delta_{i,S'_x}(0)}$, $F'_x = \prod_{z\in S_x}(F'_z)^{\Delta_{i,S'_x}(0)}$。设 $s_i = (\log_g g')F_{2,ID_c,i}(\alpha) = (\log_g g')\left(\dfrac{1-y_i(0)^{q+2}}{1-y_i(0)}\right)\alpha^{q+1}$,如果 $Z = \hat{e}(g^{\alpha^{q+1}}, g')$,则 $C'^*_x = \{g^{s_i(\alpha-t_i)}\}_{x\in Y, i=att(y)}, C_x^* = \{\hat{e}(g,g)^{s_i}\}_{x\in Y, i=att(y)}, F_x = e(C'^*_x, D'_{ID_c,i})C_x^{*D_{ID_c,i}} = e(g,h)^{f(ID_c)s_i} = e(g,h)^{f(ID_c)s_i}, F'_x = g^{f(0)\alpha(\log_g g')F_{2,ID_c,i}(\alpha)} = g^{\beta s_i}$,所以 $F_R = \prod_{x\in S_R}(F_x)^{\Delta_{i,S'_R}(0)} = e(g,h)^{f(ID_c)q_R(0)}$, $F'_R = \prod_{x\in S_R}(F'_x)^{\Delta_{i,S'_R}(0)} = g^{\beta q_R(0)}$。对攻击者 A 来说 $CT = (\Gamma_R^*, \tilde{C}^*, C^*, C_y^*, C'^*_y)$ 是有效的密文。真实系统参数具有相同的分布。

阶段 2:A 进行密钥产生询问,C 采用阶段 1 相同的方法回答 A。

猜测:A 输出 $b', c' \in \{0,1\}$,如果 $b' = b, c = c'$,则攻击者 A 赢得游戏,则 C 可判断 $Z = \hat{e}(g^{\alpha^{q+1}}, g')$,解决 truncated 判定 q-ABDHE 问题。根据文献[11]的概率分析方法分析 C 解决 truncated 判定 q-ABDHE 问题的优势为:

$$\varepsilon' = |\Pr[B(g', g'^{q+2}, g, g^{\alpha}, \cdots g^{\alpha^q}, \hat{e}(g^{\alpha^{q+1}}, g')) = 0] - \Pr[B(g', g'^{q+2}, g, g^{\alpha}, \cdots g^{\alpha^q}, Z) = 0]| \geqslant \varepsilon - 2/p^{|U|}$$

定理 2 本文密钥管理协议具有抗共谋能力。

证明:本文密钥管理协议采用所提出的基于属性的加密方案实现组密钥的分发,该加密方案的私

钥中含有随机因子 r_{ID}，每个节点的 r_{ID} 是不同的，因此，节点不能联合私钥恢复出 $\hat{e}(g,h)^{r_{ID}s}$，不能解密获得组密钥。因此，本文密钥管理协议具有抗共谋能力，定理 2 成立。

定理 3 本文密钥管理协议具有后向安全性。

证明：节点被撤销后，系统主密钥进行更新，未被撤销的节点不能满足“私钥更新”访问策略，不能解密私钥更新信息，无法更新自己的私钥，不能解密在新的系统参数下建立的组密钥密文，从而保证了被撤销节点不能继续参与组通信和获得传感器数据。因此本文协议具有后向安全性，定理 3 成立。

定理 4 本文密钥管理协议能够实现细粒度访问控制和隐私保护。

证明：移动节点和簇头节点可以设定不同的访问策略进行组密钥分发，满足访问策略的节点组成一个通信组，访问策略可以实现细粒度的访问控制逻辑，控制节点的访问能力，使合法的节点能够根据访问策略访问传感器数据。节点只用属性来标识，组通信不需要知道节点的身份以及满足访问策略的节点有多个，因此无法分辨组中具体包含哪些节点以及节点个数。因此，定理 4 成立。

4 效率分析与仿真实验

表 1 给出了本文协议与其他协议在加密、解密代价和通信代价方面的比较结果。S 表示 G_1 上的幂运算，E 表示 G_2 上的幂运算，P 表示双线性对运算。$|\Gamma_R|$ 表示访问结构树 Γ_R 中所有非叶子结点的门限值总和。$|\omega|$ 表示访问结构树 Γ_R 中所有叶子结点个数(即用于加密的属性个数)。$|\omega'|$ 表示访问结构树 Γ_R 中所有叶子结点的父节点的门限值总和(即用于解密的属性个数)。本文协议分别给出了簇间组密钥分发和簇内组密钥分发代价。对于簇内组密钥分发来说 $|\omega|$ 为簇内节点总数。从表 1 中可以看出，本文协议具有较低的解密代价。由于传感器节点需要解密才能获得组密钥，因此采用本文协议可以节约传感器节点的能耗。在实际应用中，Cheung 方案[8]和 Yu 方案[5]和本文协议在实际应用中还需要采用高效的签名机制实现消息认证，可以采用基于身份签名方案，但组发起者需要暴漏自己的身份，而其他节点无需暴漏身份。

表 1 本文协议与其他协议性能比较

	加密代价	解密代价	通信代价	访问策略
Cheung[8]	$(2\|\omega\|+1)S+E$	$(2\|\omega'\|+1)P+\|\Gamma_R\|E$	$(2\|\omega\|+1)\|G_1\|+\|G_2\|$	密文策略(ciphertext-policy)
Yu[5]	$(2\|\omega\|+1)S+E$	$(2\|\omega'\|+1)P+\|\Gamma_R\|E$	$(2\|\omega\|+1)\|G_1\|+\|G_2\|$	密钥策略(key-policy)
本文协议	$(\|\omega\|+1)P+(\|\Gamma_R\|+1)E$ $(\|\omega\|+1)S+2E$	$(\|\omega'\|+1)P+\|\Gamma_R\|E$ $2P+E$	$(\|\omega\|+1)\|G_1\|+(\|\Gamma_R\|+1)\|G_2\|$ $(\|\omega\|+1)\|G_1\|+2\|G_2\|$	密文策略(ciphertext-policy)

仿真实验中，设 $|p|=160$bit，属性长度为 2byte，*time* 长度为 1byte。M-Node 采用 3.0GHz 嵌入式设备，数据传输率为 100Mb/s，执行一次标量乘(即 S 运算)大约需要 0.72ms[12]，执行一次双线性对运算需要 14ms[5]。H-Node 采用 416MHz Imote2 节点，工作电压 0.95V，工作电流 66mA，数据传输率为 250kb/s，执行一次 S 运算需要 11.25ms[12]，执行一次双线性对运算大约需要 103ms。S-Node 采用低性能节点 Mica2，集成 8 位 8MHz ATmega128L 处理器，工作电压 3V，工作电流 8mA，接收状态下电流 10mA，传输状态下电流 27mA，数据传输率 12.4kbps。执行一次 S 运算需要 0.81s[13]，执行一次双线性对运算大约需要 5.3s[14]。S 运算代价约为 E 运算代价的 3 倍[15]。

图 3 给出了本文协议中 M-Node、H-Node 和 S-Node的计算和通信代价与解密属性 $|\omega'|$ 的关系。*GC* 表示组控制者，*GM* 表示组成员。假设加密属性集 $|\omega|=200$，簇内节点个数 $n_S=100$。从图 3 中可以看出，当 $|\omega'|$ 增加时，M-Node 节点的消耗没有显著增加。当 $|\omega'|\leqslant 50$ 时，H-Node 的时间消耗约为 16s。本文协议由于采用解密代价较低的基于属性加密方案，可以节约 H-Node 的能耗。由于 S-Node只需要利用一个特殊属性私钥，运行 2 个双线性对运算解密获得组密钥，因此计算量较小。

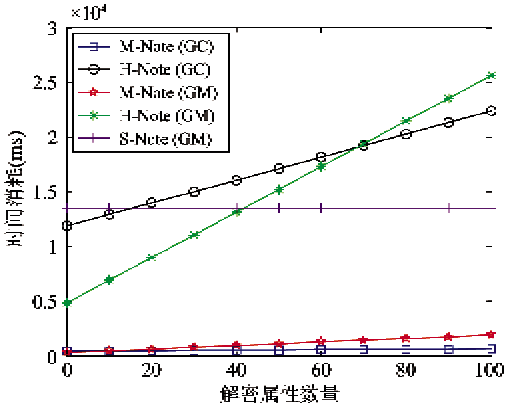

图 3 密钥分发代价与解密属性 $|\omega'|$ 的关系

图 4 给出了本文协议中 M-Node、H-Node 和 S-Node的计算和通信代价与簇内传感器节点数量的关系。假设 $|\omega| = 200$，$|\omega'| = 80$。从图 4 中可以看出，H-Node 的时间消耗会随簇内传感器节点的数量增加而增加，当其数量为 100 时，H-Node 运行时间约为 20s。因为 H-Node 对簇内节点进行组密钥分发时，加密代价与簇内节点成正比，但由于加密过程无需运算代价较高的双线性运算，因此时间消耗增加缓慢。降低簇规模可以有效降低簇头节点的耗时，提高效率。

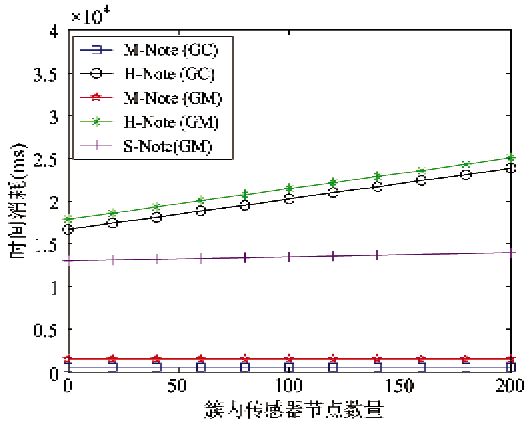

图 4 密钥分发代价与传感器节点数量的关系

图 5 给出了当 $|\omega| = |\omega'| = |\Gamma_R| = 50$，$n_S = 100$ 时，H-Node 和 S-Node 多次运行协议的能耗。从图 5 中可以看出，协议运行 1000 次，H-Node 和 S-Node的能量消耗小于 900J。H-Node 和 S-Node 如果采用 2 节普通 AA 电池供电，那么能够提供电量 6000mWh[16]，即 21600J，因此本文协议代价对 H-Node和 S-Node 来说是完全可以接受的。

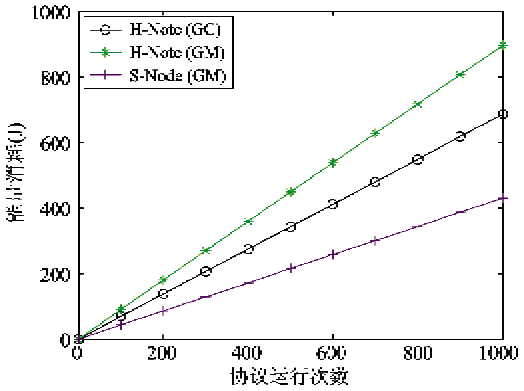

图 5 H-Node 和 S-Node 的能耗

5 结 论

本文提出的 MP2PWSN 组密钥管理协议由于采用了低解密代价的密文策略属性基加密方案，节约了传感器节点的运算代价。该协议提供后向安全性、细粒度访问控制和隐私保护，支持节点动态加入和退出组，并给出了属性私钥更新方法。仿真结果表明，该协议的代价能够被低性能传感器节点接受，能够较好地满足 MP2PWSN 的匿名组通信安全需求。

参考文献

[1] Fang H W, Ko L C, Fang H Y. A design ofservice-based P2P mobile sensor networks. In: Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Taichung, Taiwan, China, 2006. 152-157

[2] Ali M, Langendoen K. A case for peer-to-peer network overlays in sensor networks. In: Proceedings of Workshop on Wireless Sensor Network Architecture, Cambridge, Massachusetts, USA, 2007. 55-60

[3] Rondini E, Hailes S, Li L. Load sharing and bandwidth control in mobile P2P wireless sensor networks. In: Proceedings of the 6th Annual IEEE International Conference on Pervasive Computing and Communications, Hong Kong, China, 2008. 468-473

[4] Zhang Y Y, Gu D W, Li J R. Exploiting unidirectional links for key establishment protocols in heterogeneous sensor networks. *Computer Communications*, 2008, 31(13): 2959-2971

[5] Yu S, Ren K, Lou W. FDAC: toward fine-grained distributed data access control in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 2011, 22(4): 673-686

[6] MizanurRahman S M, El-KhatibK. Private key agreement and secure communication for heterogeneous sensor networks. *Journal of Parallel and Distributed Computing*, 2010,70(8): 858-870

[7] Huang J, Liao I, Tang H. Aforward authentication key management scheme for heterogeneous sensor networks. *EURASIP Journal on Wireless Communications and Networking - Special Issue on Security and Resilience for Smart Devices and Applications*, 2011:1-10

[8] Cheung L, Cooley J A, Khazan R, et al. Collusion-resistant group key management using attribute-based encryption. Cryptology ePrint Archive, Report 2007/161, 2007

[9] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, USA, 2007. 321-334

[10] Sumino H, Ishikawa N, Kato T. Design and implementation of P2P protocol for mobile phones. In: Proceedings of the 4th Annual IEEE International conference on Pervasive Computing and Communications Workshops, Pisa, Italy, 2006. 1-6

[11] Gentry C. Practical identity-based encryption without random oracles. In: Proceedings of Advances in Cryptology-Eurocrypt, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St, Petersburg, Russia, 2006, LNCS 4404: 445-464

[12] AntãoS, Bajard J, Sousa L. RNS-Based elliptic curve point multiplication for massive parallel architectures. *The Computer Journal*, 2011:1-19

[13] Gura N, Patel A, Wander A, et al. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In: Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems, Cambridge, USA, 2004. 119-132

[14] Xiong X, Wong D S, Deng X. TinyPairing: computing tate pairing on sensor nodes with higher speed and less memory. In: Proceedings of the 8th IEEE International Symposium on Network Computing and Applications, Cambridge, USA, 2009. 187-194

[15] Chen L, Cheng Z, Smart N P. Identity-based key agreement protocols from pairings. *International Journal of Information Security*, 2007,6(4): 213-241

[16] Piotrowski K, Langendoerfer P, Peter S. How public key cryptography influences wireless sensor node lifetime. In: Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, USA, 2006. 169-176

A group key management protocol using attribute-based encryption for mobile peer-to-peer wireless sensor networks

Zhang Guoyin*, Fu Xiaojing*,**, Ma Chunguang*,**

(*College of Computer Science and Technology, Harbin Engineering University, Harbin 150001)

(**Network and Data Security Key Laboratory of Sichuan Province,
University of Electronic Science and Technology of China, Chengdu 611731)

Abstract

A new ciphertext-policy attribute-based encryption (CP-ABE) scheme with lower decryption cost was presented, and it was proved secure in a stand model. Then a group key management protocol based on CP-ABE was proposed for mobile peer-to-peer wireless sensor networks (MP2PWSN). Under this protocol, mobile nodes and cluster heads firstly complete the inter-cluster group key distribution, and then a cluster head distributes the group key within its cluster. This protocol satisfies the backward security, permits node dynamically joining, leaving and being revoked, and also implements the control of fine-grained sensor data access and privacy preserving. The simulation results show that sensors' energy consumption does not greatly increase with the number of attributes because the protocol uses a CP-ABE algorithm with lower decryption cost. Therefore, this protocol can meet the security requirements of anonymous group communication for MP2PWSN.

Key words: mobile peer-to-peer wireless sensor network (MP2PWSN), group key, attribute-based encryption (ABE), standard model, anonymous communication