WSN中基于非双线性对的无证书群组密钥协商协议

钱琦锋 程春玲
(南京邮电大学计算机学院 南京 210003)

摘 要 针对无线传感网(Wireless Sensor Network,WSN)群组密钥协商协议计算开销较大的问题,提出一种基于非双线性对的无证书群组密钥协商协议。在系统初始化阶段,协议通过无证书加密体制的密钥生成中心生成节点部分私钥,各个节点依据秘密值与对应的部分密钥相乘产生私钥;在节点认证阶段,协议基于椭圆曲线上的点乘运算提出节点认证机制,利用节点的部分私钥与具有身份信息的临时公钥进行点乘运算来确定节点的身份信息;在生成会话密钥阶段,通过点乘运算生成会话密钥,以降低节点的计算开销。最后,分析了协议的计算开销和通信开销。结果表明,所提出的群组密钥协商协议能保证群组节点通信的安全性,并有效降低群组节点通信的计算开销。

关键词 无线传感网,群组密钥协商,非双线性对,无证书
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.7.041

Pairing-free Certificateless Group Key Agreement Protocol for Wireless Sensor Network

QIAN Qi-feng CHENG Chun-ling
(College of Computer,Nanjing University of Posts and Telecommunications,Nanjing 210003,China)

Abstract Due to the high computational overhead of group key agreement protocol in wireless sensor network(WSN), this paper presented a pairing-free certificateless group key agreement protocol. During system initialization phase, the partial private key is generated by key generation center of the certificateless public key cryptography. Each node generates private key via multiplying secret value by corresponding partial private key. During node authentication phase, this protocol introduces node authentication mechanism based on scalar multiplication of elliptic curves, determining the nodes identity information by calculating scalar multiplication of partial private key and temporary public key with authentication information. During session key generation phase, session key is generated by utilizing scalar multiplication to reduce the computational overhead. Finally, we analyzed computational overhead and communication cost. The results show that this protocol can not only ensure security of node communication, but also reduce computational overhead.

Keywords Wireless sensor network, Group key agreement, Pairing-free, Certificateless

1 引言

随着无线传感网应用的不断增加,出现的问题越来越多,尤其是在安全方面。无线传感器网络的安全问题主要来源于:无线通信的特性、传感器节点的资源严格受限、传感器网络分布区域广及密集、缺少固定的网络基础设施、配置前无法获知网络的拓扑结构、部署区域的开放性等。目前,在无线传感网中,节点间的机密信息大多通过广播明文消息传输。既使对明文消息进行加密传输,由于节点间未进行协商操作,攻击者也能够单向截取并进行破解。因此,信道上传输的信息安全性低,发送双方的身份信息易伪造,数据的完整性、机密性、有效性得不到保证[1]。而密钥协商机制能够让通信系统中的两个或者多个参与主体在一个公开、不安全的信道上通信协商,来联合建立会话所需的临时会话密钥,保证了数据的安全性,因此在WSN中需要引入密钥协商机制[2]。另外,无线传感网中节点数量众多且通信次数频繁,众多节点常常分为一个个群组来进行广播通信,其通信方式为群组通信。群组密钥协商机制通过各个节点成员进行密钥协商,共同生成并认证有效的群组会话密钥,生成的会话密钥被各个节点所共享。

目前,在无线传感网中,群组密钥协商协议需要解决如下问题[3]:

(1)已知会话密钥安全。协议中原先的某个会话密钥泄漏或被攻击者主动获取时,攻击者无法获得其他会话密钥。

(2)隐式密钥身份认证。协议中每一方都确信共享会话密钥只有协议的参与者知道,攻击者无法得知。

(3)抗未知密钥共享。协议参与者之间,在未确定对方身份信息之前,不会共享会话密钥。

(4)抗密钥泄露伪装。实体协商协议时,假如其中一方的长期私钥泄露后,获得该泄露密钥的攻击者能向其它实体冒充该实体,反之则不行。

(5)前向安全。若协议参与者间的长期私钥被泄露,获得

到稿日期:2014-06-24 返修日期:2014-10-22
钱琦锋(1989-),男,硕士生,主要研究方向为无线传感器网络安全,E-mail:qianqifeng1223@qq.com;程春玲(1972-),女,教授,硕士生导师,主要研究方向为大数据管理、分布式环境下的资源管理和性能优化、计算机在通信中的应用。

该泄露密钥的攻击者不能求出在此之前协商得到的其他会话密钥。

(6)已知会话临时信息安全。协议协商生成会话时,用户的临时私钥被泄露,不影响最终会话密钥的安全。

在无线传感器网络密钥协商协议中,无证书密码体制[4]既避免了数字证书管理的复杂性,也避免了基于身份加密体制的长期私钥托管的弊端。无证书群组密钥协商协议是无线传感器网络密钥协商协议的发展趋势。

Cao 等人[5]提出了第一个无证书群组密钥协商协议,该协议适用于无线传感网。其节点身份认证机制基于双线性对运算,会话密钥通过拉格朗日内插值法求导得到,但该协议不满足前向安全性,也不满足隐式密钥身份认证需求,协议通信效率低,需进行 $2n$ 次双线性对运算(n 为节点个数),计算开销较大。Heo 等人[6]提出了第一个基于二叉树结构的无证书群组密钥协商协议,该协议适用于动态群组,例如无线传感网等。其提供较为有效的通信效率,但没有节点身份认证操作,不满足抗未知密钥共享的安全性;其会话密钥基于双线性对生成,计算开销较大,双线性对运算次数为$3n-2$,协议不满足(完美)前向安全性的安全需求,也不满足隐式密钥身份认证需求。基于文献[6],Lee 等人[7]通过二叉树最右子节点随机产生的临时值,使得群组密钥不断更新,保证了协议前向安全性,但是该协议无节点身份认证机制,不满足抗未知密钥共享且易遭受已知临时会话密钥攻击,协议需 $2n-2$ 次双线性对运算,计算开销仍较大。Geng 等人[8]的无证书群组密钥协商协议运用无证书数字签名技术,有效保障了节点身份信息。其会话密钥基于双线性对运算得到,协议安全性较好,但该协议的计算开销大,需 $4n$ 次双线性对运算,文献[9]指出该协议的安全分析方法不严谨,建立的安全模型不规范。Teng 等人[9]提出了一个无证书群组密钥协商协议,基于随机预言模型证明出协议能有效防御主动攻击,且最多能够容忍 $n-2$ 个被俘的节点而不受影响。协议协商轮数为常数,协议安全性好,但其双线性对运算次数多,达到 $2n^2-2$ 次,计算开销很大。

根据上述文献分析可知,目前的无证书群组密钥协商协议主要基于双线性对运算,协议安全性较高,但计算开销大,且无有效身份信息认证的情况。因此,本文提出一个适用于无线传感网的非双线性对无证书群组密钥协商协议。本文所提协议可应用于通信安全性要求高、节点抗毁性能力强的无线传感网应用场景,例如军事指挥系统、目标跟踪。协议加入基于椭圆曲线上点乘运算的节点身份认证机制;在会话密钥生成阶段,采用点乘运算来生成会话密钥,代替计算复杂度高的双线性对运算。协议运用点乘运算代替双线性对生成会话密钥,既降低了计算开销,又保证了运算的安全性[10]。协议安全性基于椭圆曲线上的离散对数问题和计算 *D-H* 问题。最后,对方案的计算开销、通信开销、安全性进行了分析。

2 预备知识

椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem,ECDLP):$E(F)$ 表示定义在有限域 F_q 上的椭圆曲线 E 在扩域 F 上的有理子群,设 $P,Q\in E(F)$,求解满足 $mP=Q$ 的解 m。对于基点 P 而言,计算点的倍乘 mP(即 m 个 P 相加)相对容易;但已知 P 和 mP,计算 m 是很困难的。

计算 *D-H* 问题(Computational Diffie-Hellman Problem,CD-HP):设 G 是阶为 q 的一个加法循环群,P 为生成元,给定 $aP,bP\in G$,对任意未知 $a,b\in Z_q^*$(其中 Z_q^* 为单位元乘法群,a,b 为整数),计算 abP 是困难的。

3 基于非双线性对的无证书群组密钥协商协议

本协议在 Lee[7]协议的基础上,基于椭圆曲线的点乘操作来降低密钥协商的计算复杂度。协议引入节点认证机制,采用节点的部分私钥与具有身份信息的临时公钥进行点乘运算,保证节点的身份真实性;在生成会话密钥阶段,采用节点的私钥、临时秘密值与协商另一方的临时公钥、公钥进行点乘运算,生成会话密钥。

本协商协议基于文献[11]的满二叉树模型,建立群组节点的逻辑结构且基于二叉树假设。假设:每个节点都了解群组的二叉树结构、各个节点的 ID 号以及对应二叉树上的逻辑位置,根节点确定且唯一;群组中的节点可以决定各自的中心节点(父节点)、监测节点(右子节点);群组中的节点进行相同的协商运算操作。其中,此满二叉树高度为 $h(h>2)$,节点运用 $N_{\langle l,r\rangle}$ 表示,$\langle l,r\rangle$ 含义为第 l 层第 r 个节点。整个协议分为系统初始化和会话密钥协商两个阶段,此两个阶段只针对参与通信协商的节点。

3.1 系统初始化阶段

系统初始化阶段主要分为系统建立,密钥生成中心(Key Generation Center,KGC)产生节点部分私钥,节点生成秘密值、私钥、公钥。

(1)系统建立:密钥生成中心随机选择 $s\in Z_q^*$,s 作为系统主密钥秘密存储。双线性映射 $e:G_1\times G_1\rightarrow G_2$;$q$ 为一个大素数;G_1 是阶为 q 的循环加法群;G_2 是阶为 q 的循环乘法群;P 为 G_1 的一个生成元;P_{pub} 是 KGC 的公开钥,$P_{pub}=sP$;H_1 是哈希函数:$\{0,1\}^*\rightarrow G_1$,H_2 是哈希函数 $G_1\times G_1\rightarrow Z_q^*$,系统公开参数$\{G_1,G_2,q,P,P_{pub},H_1,H_2\}$。

(2)生成节点部分私钥:KGC 随机选择临时值 $r_i\in Z_q^*$,计算临时公钥 $R_i=r_iP$ 并公开。KGC 给定节点身份 ID_i,生成部分私钥 $D_i=(H_1(ID_i\parallel R_i)+s+r_i)^{-1}$,把 D_i 作为节点的部分私钥通过安全通道传送给节点 i。

(3)生成节点秘密值:节点随机选取 $x_i\in G_1$ 作为节点秘密值。

(4)生成节点私钥:节点计算 $S_i=x_iD_i\in G_1$ 作为节点自身的私钥。

(5)生成节点公钥:节点计算 $P_i=x_iP$ 作为节点自身的公钥。

3.2 会话密钥协商阶段

会话密钥协商阶段主要分为 4 个步骤:叶子节点认证、子树会话密钥生成、中间节点(父节点)认证、群组会话密钥生成。其中叶子节点 M_i 主要包含临时值 r_i、临时公钥 R_i、秘密值 x_i、节点认证信息 Q_i、具有认证信息的临时公钥 T_i($T_i=r_i(H_1(ID_j\parallel R_j)P+P_{pub}+R_j)$)、部分私钥 D_i、私钥 S_i、认证信息($Q_i=(H_1(ID_j\parallel R_j)P+P_{pub}+R_j)$)。

由于原先无证书群组密钥协商协议无有效节点认证机制,节点身份信息安全性低,易造成节点身份信息被破解并泄漏,因此本协议引入基于椭圆曲线上点乘运算的节点认证机

制来保证节点身份信息的安全性。

叶子节点认证：M_i 发送消息$\{T_i, P_i\}$给 M_j，相应地，M_j 发送消息$\{T_j, P_j\}$给 M_i。接收到消息之后，M_i 和 M_j 首先查看对方公钥信息，接着 M_i 计算临时公钥 $R_j' = T_j D_i$，M_j 计算 $R_i' = T_i D_j$，若 $R_j = R_j'$ 以及 $R_i = R_i'$，则叶子节点 M_i 和 M_j 完成了身份认证。若认证不正确，则重新认证。

子树会话密钥生成：M_i 根据私钥 S_i、临时值 r_i 以及消息$\{T_j, P_j\}$，计算 $k_{i,j} = (T_j S_i)(P_j r_i)$。相应地，$M_j$ 计算 $k_{j,i} = (T_i S_j)(P_i r_j)$。因此 $K_{\langle i,j\rangle} = k_{i,j} = k_{j,i} = (r_i x_j P)(x_i r_j P)$，$M_i$ 和 M_j 共享的会话密钥 $SK = H_2(K_{\langle i,j\rangle})$。右子树叶子节点 M_g 和 M_h 共享的会话密钥协商过程相同，计算得到 $K_{\langle i,j+1\rangle} = k_{g,h} = k_{h,g} = (r_g x_h P)(x_g r_h P)$。$M_g$ 和 M_h 共享的会话密钥 $SK = H_2(K_{\langle i,j+1\rangle})$。

叶子节点协商结束后，由每个子群组节点中最右子节点向子群组根节点（父节点）广播消息$\{K_{\langle l,r\rangle}, P_{2n}\}$，并且互相向邻居组群中的最右子节点广播临时公钥 $B_{\langle l,r\rangle}$，进行临时公钥 $B_{\langle l,r\rangle}$ 的交换并认证。其中 $B_{\langle l,r\rangle} = K_{\langle l,r\rangle} Q_i$，$Q_i = (H_1(ID_j \| R_j)P + P_{pub} + R_j)$。

中间节点（父节点）认证：叶子节点 M_i、M_j 对应中间节点 $N_{\langle i,j\rangle}$，M_g、M_h 对应中间节点 $N_{\langle i,j+1\rangle}$。中间节点 $N_{\langle i,j\rangle}$ 向中间节点 $N_{\langle i,j+1\rangle}$ 发送消息$\{B_{\langle i,j\rangle}, Q_{j+1}\}$，中间节点 $N_{\langle i,j+1\rangle}$ 向中间节点 $N_{\langle i,j\rangle}$ 发送消息$\{B_{\langle i,j+1\rangle}, Q_{2j+2}\}$。由于 $K_{\langle i,j\rangle}$ 与 $K_{\langle i,j+1\rangle}$ 为子树生成的会话密钥，会话密钥 $K_{\langle i,j\rangle}$、$K_{\langle i,j+1\rangle}$ 已知，因此，只需验证身份信息 Q_{j+1} 和 Q_{2j+2}，中间节点 $N_{\langle i,j\rangle}$ 和 $N_{\langle i,j+1\rangle}$ 分别进行等式 $D_i Q_{j+1}$ 和 $D_{j+1} Q_{2j+2}$ 的计算，验证等式结果是否等于 P。若认证不正确，则重新认证。

群组会话密钥生成：中间节点 $N_{\langle i,j\rangle}$ 得知消息$\{B_{\langle i,j+1\rangle}, Q_{2j+2}\}$，中间节点 $N_{\langle i,j+1\rangle}$ 得知消息$\{B_{\langle i,j\rangle}, Q_{j+1}\}$，因此可产生群组密钥。以 $N_{\langle i,j+1\rangle}$ 为例，来进行群组密钥 $K_{\langle i-1,j\rangle}$ 计算：

$$\begin{aligned} K_{\langle i-1,j\rangle} &= (B_{\langle i,j\rangle} S_{2j+2})(P_{j+1} K_{\langle i,j+1\rangle}) \\ &= (K_{\langle i,j\rangle} x_{2j+2} P)(K_{\langle i,j+1\rangle} x_{j+1} P) \\ &= (K_{\langle i,j+1\rangle} P_{j+1})\ (K_{\langle i,j\rangle} P_{2j+2}) \end{aligned} \tag{1}$$

群组会话密钥 SK 生成之后，根节点分别向左、右子树的节点成员广播会话密钥 SK，此时协议运行结束。

下面以有通信需求的 7 个节点为例，来说明本协议过程。首先，节点预先布置在通信场景中，接着协议在系统初始化阶段采用文献[11]的方法生成一高度为 3 的满二叉树，实际的物理节点一一对应满二叉树中的逻辑位置。此处节点间的链接为逻辑链接，表示对应的逻辑关系。节点的位置为逻辑位置且自行分配决定[12]，如图 1 所示。

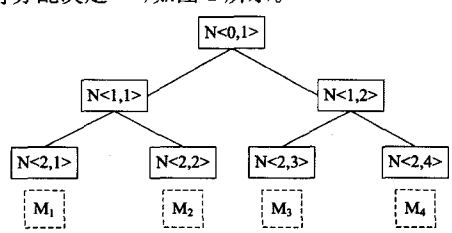

图 1　满二叉树逻辑结构图

叶子节点认证：以左子树叶子节点 M_1 和 M_2 认证为例，M_1 发送消息$\{T_1, P_1\}$给 M_2，其中 $T_1 = r_1(H_1(ID_2 \| R_2)P + P_{pub} + R_2)$，$P_1 = x_1 P$。相应地，$M_2$ 发送消息$\{T_2, P_2\}$给 M_1，接收到消息之后，M_1 和 M_2 首先查看对方的公钥，接着 M_1 计算临时公钥 $R_2' = T_2 D_1$，M_2 计算 $R_1' = T_1 D_2$。若 $R_2 = R_2'$ 以及 $R_1 = R_1'$，则叶子节点 M_1 和 M_2 完成了身份认证。若认证不正确，则重新认证。

叶子节点认证计算式如下所示：

$$M_1: R_2' = T_2 D_1 \tag{2}$$

$$M_2: R_1' = T_1 D_2 \tag{3}$$

图 2 所示为叶子节点认证流程图。通过检验临时公钥和公钥的过程后，节点的身份认证阶段结束。

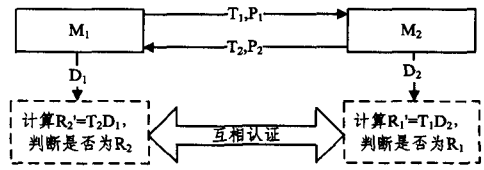

图 2　叶子节点认证

子树会话密钥生成：以左子树为例，叶子节点 M_1 根据私钥 S_1、临时值 r_1 以及消息$\{T_2, P_2\}$来计算密钥 $k_{1,2} = (T_2 S_1)(P_2 r_1)$。相应地，$M_2$ 计算 $k_{2,1} = (T_1 S_2)(P_1 r_2)$。因此左子树密钥 $K_{\langle 1,1\rangle} = k_{1,2} = k_{2,1} = (r_1 x_2 P)(x_1 r_2 P)$，$M_1$ 和 M_2 共享的会话密钥 $SK = H_2(K_{\langle 1,1\rangle})$。相应地，右子树密钥 $K_{\langle 1,2\rangle} = k_{3,4} = k_{4,3} = (r_3 x_4 P)(x_3 r_4 P)$，$M_3$ 和 M_4 共享的会话密钥 $SK = H_2(K_{\langle 1,2\rangle})$。

子树会话密钥计算式如下所示：

$$M_1: k_{1,2} = (T_2 S_1)(P_2 r_1) = (r_1 x_2 P)(x_1 r_2 P) \tag{4}$$

$$M_2: k_{2,1} = (T_1 S_2)(P_1 r_2) = (r_1 x_2 P)(x_1 r_2 P) \tag{5}$$

图 3 所示为叶子节点 M_1 和 M_2 密钥协商过程。

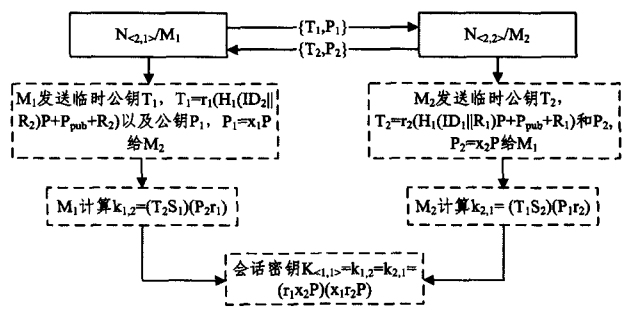

图 3　叶子节点密钥协商

中间节点（父节点）认证：高度为 3 的满二叉树，中间节点为 $N_{\langle 1,1\rangle}$ 和 $N_{\langle 1,2\rangle}$。中间节点 $N_{\langle 1,1\rangle}$ 向中间节点 $N_{\langle 1,2\rangle}$ 发送消息$\{B_{\langle 1,1\rangle}, Q_2\}$，其中 $B_{\langle 1,1\rangle} = K_{\langle 1,1\rangle} Q_2$，身份信息 $Q_2 = (H_1(ID_1 \| R_1)P + P_{pub} + R_1)$。中间节点 $N_{\langle 1,2\rangle}$ 向中间节点 $N_{\langle 1,1\rangle}$ 发送消息$\{B_{\langle 1,2\rangle}, Q_4\}$，其中 $B_{\langle 1,2\rangle} = K_{\langle 1,2\rangle} Q_4$，$Q_4 = (H_1(ID_2 \| R_2)P + P_{pub} + R_2)$。由于 $K_{\langle 1,1\rangle}$ 与 $K_{\langle 1,2\rangle}$ 为子树生成的会话密钥，会话密钥 $K_{\langle 1,1\rangle}$、$K_{\langle 1,2\rangle}$ 已知，因此只需验证身份信息 Q_2 和 Q_4，中间节点 $N_{\langle 1,1\rangle}$ 和 $N_{\langle 1,2\rangle}$ 分别进行等式 $D_1 Q_2$ 和 $D_2 Q_4$ 的计算，验证等式结果是否等于 P。若认证不正确，则重新认证。

群组会话密钥生成：高度为 3 的满二叉树，$N_{\langle 1,2\rangle}$、$N_{\langle 1,1\rangle}$ 为中间节点。由于在中间节点认证阶段，中间节点 $N_{\langle 1,1\rangle}$ 得知消息$\{B_{\langle 1,2\rangle}, Q_4\}$，中间节点 $N_{\langle 1,2\rangle}$ 得知消息$\{B_{\langle 1,1\rangle}, Q_2\}$。以 $N_{\langle 1,2\rangle}$ 为例，进行群组密钥 $K_{\langle 0,1\rangle}$ 计算：$K_{\langle 0,1\rangle} = (B_{\langle 1,1\rangle} S_4)(P_2 K_{\langle 1,2\rangle}) = (K_{\langle 1,1\rangle} x_4 P)(K_{\langle 1,2\rangle} x_2 P) = (K_{\langle 1,2\rangle} P_2)(K_{\langle 1,1\rangle} P_4)$。因此群组会话密钥 $SK = H_2(K_{\langle 0,1\rangle})$。对于中间节点 $N_{\langle 1,1\rangle}$ 而言，相应地，群组密钥 $K_{\langle 0,1\rangle}' = (B_{\langle 1,2\rangle} S_2)(P_4 K_{\langle 1,1\rangle}) = (K_{\langle 1,2\rangle} P_2)(K_{\langle 1,1\rangle} P_4)$，群组会话密钥 $SK = H_2(K'_{\langle 0,1\rangle})$。群组会话密钥 SK 生成之后，根节点分别向左、右子树的节点成员广播会话密钥 SK，此时协议运行结束。

群组会话密钥计算式如下所示：

$$\begin{aligned} K_{\langle 0,1\rangle}' &= (B_{\langle 1,2\rangle} S_2)(P_4 K_{\langle 1,1\rangle}) \\ &= (K_{\langle 1,2\rangle} x_2 P)(K_{\langle 1,1\rangle} x_4 P) \\ &= (K_{\langle 1,2\rangle} P_2)(K_{\langle 1,1\rangle} P_4) \\ &= K_{\langle 0,1\rangle} \end{aligned} \tag{6}$$

4 安全分析

本协议考虑了攻击者 A，分为 $A1$ 和 $A2$。$A1$ 是指不能获得主密钥但是能够替换参与者的公钥；$A2$ 是指攻击者能够获得主密钥，但是不能替换实体的公钥。

(1)已知会话密钥安全：协议生成会话密钥时，使用随机生成的临时值。即使会话密钥泄漏或被破解，也不影响原先或者以后的会话。

(2)隐式密钥身份认证：对于 $A1$ 来说，即使置换公钥，也无法获得节点的临时值，更无法获得对应的子树会话密钥，因此无法获得群组会话密钥；对于 $A2$ 来说，虽然拥有主密钥，但即使获得部分私钥，也得不到相应的私钥。

(3)抗未知密钥共享：节点协商之前，节点的身份得以认证。对于 $A1$ 来说，虽然能够获得协商者们的部分公钥，但是无法获得对应的临时值。对于 $A2$ 来说，其不能获得临时值或者秘密值，即使有主密钥也无法获得临时公钥。

(4)抗密钥泄露伪装攻击：若攻击者 A 获得节点私钥 S_i，且也截取到了对应协商者的临时密钥、公钥，但 A 仍计算不出群组会话密钥。因为计算会话密钥需获取协商者们的私钥和临时值，而攻击者 A 窃取不到这些值。

(5)前向安全性：协议协商生成会话密钥时，即使协议参与者的长期私钥被泄露，攻击者 A 也需获得节点的临时值 r_i，以及相应协商者们的临时值，即使是 KGC 也恢复不出会话密钥。

(6)已知会话临时信息安全：若攻击者 A 获得节点临时值 r_i，但是 A 无法获得对应秘密值 x_i，由于 $P_i = x_i P$，A 若想破解则面临着计算 $D\text{-}H$ 问题，因此群组会话密钥的安全性得到了保证。

5 性能分析和仿真

5.1 协议开销分析

本节比较 Cao 方案[5]、Heo 方案[6]、Lee 方案[7]、Geng 方案[8]、Teng 方案[9]和本文方案的计算开销和通信开销。计算开销由协议中的双线性对、点乘、模乘与幂乘开销相加产生。通信开销由协议中通信轮数和传输信息大小构成。其中的参数包括：p：双线性对；M：加法群 G_1 上的点乘；E：乘法群 G_2 上模乘与幂乘；$|P|$：加法群 G_1 上基点的长度；$|q|$：单位元乘群 Z_q^* 上元素的长度；n：群组的参与用户数。各方案开销如表 1 所列。

表 1 算法开销比较

协议	轮数	传输信息大小	计算开销
Cao	2	$O(n^2)\|q\|+O(n)\|P\|$	$O(n)p+O(n^2)M+O(1)E$
Heo	lgn	$O(n)\|P\|$	$O(n)p+O(n)M+O(nlgn)E$
Lee	lgn	$O(n)\|P\|$	$O(n)p+O(n)M+O(nlgn)E$
Geng	2	$O(n^2)\|P\|$	$O(n)p+O(n^2)M+O(nlgn)E$
Teng	2	$O(n^2)\|P\|$	$O(n^2)p+O(n)M+O(nlgn)E$
Ours	lgn	$O(n)\|P\|$	$O(n)M+O(nlgn)E$

如表 1 所列，本文所提协议不使用双线性对，而上述对比协议的双线性对运算至少达到 $O(n)$ 数量级，Teng 方案[9]达到 $O(n^2)$ 数量级，因此本协议的计算开销得到降低。由于二叉树结构在节点通信、密钥产生、更新时效率较高，从表中数据可知本协议通信开销较低。虽然 Cao 方案[5]、Geng 方案[8]、Teng 方案[9]的运行次数是两轮，但是其传输的信息量都达到 $O(n^2)$ 数量级，通信开销和计算开销都大于本方案；与 Heo、Lee 等人的协议相比，虽然本文所提协议的通信开销属于同一数量级，但是未使用双线性对，而运用点乘运算，虽增加 $2n$ 次点乘运算，但降低了计算开销，也保证了协议的安全性。

5.2 仿真及结果分析

仿真主要从节点能量消耗、方案运行时间两个方面对本文所提方案与 Heo 方案[6]、Lee 方案[7]进行对比分析。由于 Cao[5]方案、Geng 方案[8]、Teng 方案[9]的通信开销与计算开销都高于本文方案，因此未做仿真对比。仿真时假设 400 个节点均匀地部署在一块 $360\times360m^2$ 的仿真区域，每个节点的传输半径设为 50m，节点能量消耗采用简单线性能量消耗模型[13]，节点接收一个字节消耗 400uJ，发送一个字节消耗 720uJ，每个节点初始能量设置为 9.8J。其中，仿真工具是 OMNet++，运用 C++以及 Ned 实现仿真实验。实验设备是一台运行 Windows 7 SP1、具有 Intel Core i5-2410 2.30 GHz 双核处理器、8.00GB DDR3 内存的 PC。

仿真对比实验中，通信节点发送一个由 AES 算法使用群组会话密钥加密的 *message* 信息包，消息格式如式(7)所示。

$$E_K(message \parallel (ID_i \parallel r_i)) \tag{7}$$

其中，*message* 是信息类型(2000bit 的 HELLO 包)，ID_i 是节点身份标识，K 是群组节点建立的会话密钥，r_i 为随机数。若接收节点接收到对应信息，其对应解密算法利用 K 对接收的信息包进行解密，格式如下：

$$D_K(E_K(message \parallel (ID_i \parallel r_i))) \tag{8}$$

节点能量消耗：仿真对比本文方案、Heo 方案[6]、Lee 方案[7]。实验中，选择高度为 3 的满二叉树节点群组，监测能耗最高的最右子节点，运行各协商方案 20 次，取节点前 1000s 能量消耗情况值。结果如图 4 所示。

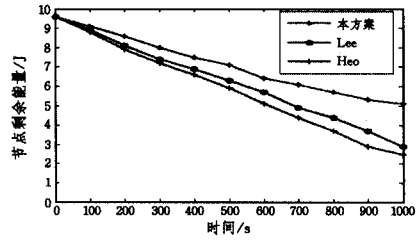

图 4 节点能量消耗速率

如图 4 所示，3 种方案的消耗速率情况接近线性递减，本文方案的递减速率最慢。例如，在 400s～500s 时间段内，本方案的节点消耗速率为 4mJ/s，而 Lee 方案[7]约为 6mJ/s，Heo 方案[6]约为 7mJ/s。本方案节点平均消耗速率约为 4mJ/s，Lee 方案[7]约为 8mJ/s，Heo 方案[6]约为 9mJ/s。因此本文所提方案对节点能量的消耗速率最小，Lee 方案[7]其次，Heo 方案[6]最大。

方案运行时间：仿真对比本文方案、Heo 方案[6]、Lee 方案[7]的运行时间。实验中，选择同为高度为 3 的满二叉树的节点群组，重复运行各方案 20 次所花费时间的曲线如图 5 所

示。其中，方案运行时间包括协议系统初始化时间（系统参数初始化时间、参数交换）、节点认证、会话密钥生成和消息加、解密时间。

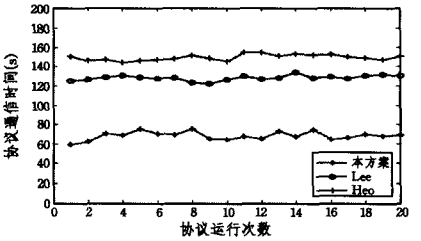

图 5　协议运行时间曲线

如图 5 所示，Lee 方案[7]、Heo 方案[6]的运行时间曲线较平稳，而本方案的运行曲线有波折，尤其是在协议运行第 8 次、第 15 次时。曲线不平稳的原因是本方案加入了基于点乘的节点认证机制，节点计算认证信息的时间波动较大，尤其是计算具有身份信息的临时密钥，从而影响了整个协议的运行时间。本方案的平均运行时间约为 68s，Lee 方案[7]约为 128s，Heo 方案[6]约为 147s。可以看出，运行本方案所花时间最少，Lee 方案[7]其次，Heo 方案[6]最多。

结束语　本文提出一种 WSN 中基于非双线性对的无证书群组密钥协商协议，协议引入基于点乘的节点认证机制，生成会话密钥时运用点乘替换双线性对运算。本协议既有效认证了节点身份信息，又降低了计算开销，并简易分析了协议的安全性。将来的研究重点是随机预言模型下证明协议安全性。本协议适用于军事对战，例如节点先初始化，接着节点被炮弹发射到敌友双方零界区域；节点部署之后，节点各自组成群组，各个群组中的节点进入会话密钥协商阶段，生成会话密钥；接着，节点若监测到敌军具体位置、动向及敌军设备等机密信息，则通过会话密钥加密信息传递给汇聚节点，最终传递给友方数据中心；友方通过数据分析，准确定位敌方目标位置，从而提供精准的火力控制进行打击。

参 考 文 献

[1] Islam K, Shen W, Wang X. Wireless sensor network reliability and security in factory automation: A survey[J]. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 2012, 42(6): 1243-1256

[2] Wei G, Yang X, Shao J. Efficient certificateless authenticated asymmetric group key agreement protocol[J]. KSII Transactions on Internet and Information Systems, 2012, 6(12): 3352-3365

[3] Lu C F, Wu T C, Hsu C L. Certificateless authenticated group key agreement scheme with privacy-preservation for resource-limited mobile devices[J]. International Journal of Innovative Computing Information and Control, 2012, 8(1B): 599-615

[4] Al-Riyami S, Paterson K. Certificateless public key cryptography [C]// Proc of 9th International Conference on the Theory and Application of Cryptology and Information Security. Taipei, Taiwan, 2003: 205-217

[5] Cao C, Ma J, Moon S. Provable efficient certificateless group key exchange protocol[J]. Wuhan University Journal of Natural Sciences, 2007, 12(1): 41-45

[6] Heo S, Kim Z, Kim K. Certificateless authenticated group key agreement protocol for dynamic groups[C]// Proc of Global Telecommunications Conference (GLOBECOM'07). Washington, USA, 2007: 464-468

[7] Lee E J, Lee S E, Yoo K Y. A certificateless authenticated group key agreement protocol providing forward secrecy[C]// Proc of International Symposium on Ubiquitous Multimedia Computing (UMC'08). Hobart, Australia, 2008: 124-129

[8] Geng M, Zhang F, Gao M. A secure certificateless authenticated group key agreement protocol[C]// Proc of International Conference on Multimedia Information Networking and Security (MINES'09). Wuhan, China, 2009: 342-346

[9] Teng J, Wu C. A provable authenticated certificateless group key agreement with constant rounds[J]. Journal of Communications and Networks, 2012, 14(1): 104-110

[10] Yang G, Tan C H. Certificateless public key encryption: A new generic construction and two pairing-free schemes[J]. Theoretical Computer Science, 2011, 412(8): 662-674

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

[12] Kalpakis K. Everywhere sparse approximately optimal minimum energy data gathering and aggregation in sensor networks[J]. ACM Transactions on Sensor Networks (TOSN), 2010, 7(1): 12-37

（上接第 173 页）

[6] Stolfo S J, Salem M B, Keromytis A D. Fog computing: Mitigating insider data theft attacks in the cloud[C]// 2012 IEEE Symposium on Security and Privacy Workshops (SPW). IEEE, 2012: 125-128

[7] Hong K, Lillethun D, Ramachandran U, et al. Mobile fog: A programming model for large-scale applications on the internet of things[C]// Proceedings of the second ACM SIGCOMM Workshop on Mobile Cloud Computing. ACM, 2013: 15-20

[8] Gkantsidis C, Rodriguez P R. Network coding for large scale content distribution[C]// INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, 2005, 4: 2235-2245

[9] Ahlgren B, Dannewitz C, Imbrenda C, et al. A survey of information-centric networking[J]. IEEE Communications Magazine, 2012, 50(7): 26-36

[10] 刘云浩. 物联网导论[M]. 北京：科学出版社，2011
Liu Yun-hao. Introduction to Internet of Things[M]. Beijing: Science Press, 2011

[11] 孙利民，李建中，陈渝，等. 无线传感器网络[M]. 北京：清华大学出版社，2005
Sun Li-min, Li Jian-zhong, Chen Yu, et al. Wireless Sensor Networks[M]. Beijing: Tsinghua University Press, 2005

[12] Li Q, Han Q, Cheng X, et al. QueueSense: Collaborative recognition of queuing on mobile phones[C]// 2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). IEEE, 2014: 230-238