DOI:10.7544/issn1000-1239.2018.20170651
55(12):2651-2663,2018

簇间非对称群组密钥协商协议

张启坤[1] 甘 勇[1] 王锐芳[1] 郑家民[2] 谭毓安[2]
[1](郑州轻工业学院计算机与通信工程学院 郑州 450002)
[2](北京理工大学计算机学院 北京 100081)
(zhangqikun04@163.com)

Inter-Cluster Asymmetric Group Key Agreement

Zhang Qikun[1], Gan Yong[1], Wang Ruifang[1], Zheng Jiamin[2], and Tan Yu'an[2]
[1](*Institute of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou* 450002)
[2](*School of Computer Science and Technology, Beijing Institute of Technology, Beijing* 100081)

Abstract Wireless sensor networks have some obvious characteristics, such as communication range is limited, energy-constraint, network is vulnerable et al. Group key agreement in this environment requires a cross-cluster, and computation and communication overhead are lightweight and highly safe group key agreement protocol. Aiming at these demands, the paper proposes a cross-domain lightweight asymmetric group key agreement, in order to establish a safe and efficient group communication channel among sensor nodes. Firstly, the protocol establishes the secret information among the cluster heads, and the cluster head as the bridge node to realize the sensor nodes in different cluster have the same group key information, thus realizing the cross cluster asymmetric group key agreement. The whole network node can share the secret information with the internal nodes of the group, which realizes the group security communication mechanism of the message sender unconstraint; proposed an asymmetric calculation to achieve computation and communication migration technologies to ensure that the sensor nodes are lightweight computing and communication consumption. For our asymmetric GKA protocol, the key confirmation is simple and requires no additional rounds if the protocol has been correctly executed. Proven and analysis show that the proposed protocol has the advantages in security and energy consumption.

Key words wireless sensor networks; asymmetric group key agreement; authenticated; key self-confirmation; asymmetric calculation

摘 要 无线传感器网络中传感器节点资源受限,传感器节点的通信能力及范围限制了其协同操作的规模,该环境下的群组密钥协商往往以簇为单元,群组之间的安全信息交换也限制于簇内通信.针对传感器通信能力及计算能力的限制,提出一种簇间轻量级非对称群组密钥协商协议(inter-cluster lightweight asymmetric group key agreement, CL-AGKG),为簇间传感器节点间建立一条安全高效的

收稿日期:2017-09-06;**修回日期**:2018-04-08
基金项目:国家自然科学基金项目(U1636213,61772477,61572445,61501406);河南省自然科学基金项目(162300410322);河南省科技攻关项目(172102210059);北京市自然科学基金项目(4172053)
This work was supported by the National Natural Science Foundation of China (U1636213, 61772477, 61572445, 61501406), the Natural Science Foundation of Henan Province of China (162300410322), the Science and Technology Project of He'nan Province (172102210059), and the Beijing Natural Science Foundation (4172053).
通信作者:王锐芳(wangruifang29@163.com)

群组通信信道.该协议首先建立簇头间的联盟共享密钥,以簇头为桥接节点,实现不同簇的传感器节点具有相同的群组密钥因子信息,进而实现跨簇非对群组密钥协商.全网节点都可以与群组内部节点共享其秘密信息,实现消息发送者不受群组约束的群组安全通信机制.通过非对称计算将更多传感器节点的计算与通信量迁移到能量较大的簇头节点,确保传感器节点的计算及通信开销轻量级性.并实现密钥自证实性,不需要额外的通信轮数,传感器节点可自证实其计算群组密钥的正确性.经分析并证明:该协议在安全及性能方面具有较高的优势.

关键词 无线传感网;非对称群组密钥协商;可认证;密钥自证实性;非对称计算

中图法分类号 TP309

传感器网络中节点共同收集信息、协同处理数据是传感器网络群组通信的应用体现,如何保障传感器网络群组通信的安全是当前研究的一个重要问题.群组密钥协商是为群组成员之间建立一条安全的通信信道.多年来无线传感器网络密钥协商机制一直是传感网络安全研究的重点技术,典型的研究有潘耘等人[1]融合了基于 CA 的公钥认证框架和基于身份的公钥认证框架二者的优点,提出了适合于无线传感器网络环境的轻量级的、高效的密钥预分配方案;夏戈明等人[2]提出基于对称平衡不完全区组设计的密钥预分配方案,安全强度有所提高,并在能量消耗方面进行了优化;黄海平等人[3]提出基于逻辑网格的密钥预分配方案,传感器节点间通过求解网格矩阵系数,计算共同的密钥参数,进而实现共享对称加密密钥;Walid 等人[4]提出一个高度可扩展性密钥预分配方案,有效地提高了共享密钥节点的连通性,提高节点存储共享密钥的性能;Monjul 等人[5]通过扩展图论的方法设计一个密钥预分配方案,密钥预分配方案有其固有的缺陷.

传感器节点之间通过在线计算生成它们之间的共享密钥,是传感网密钥协商的另一种可行技术.近年来典型的方案有 Tseng 等人[6]提出一种非平衡环境下群组密钥协商协议,但其不具有可认证性和动态性;张启坤等人[7]对 Tseng 等人[6]的群组密钥协商协议进行了改进,提出一种新的动态可认证群组密钥协商协议,具有可认证性和动态性;Cheng 等人[8]采用双线映射技术对 Tseng 等人[6]的协议进行改进,使之能够抵抗密钥临时泄露攻击;张启坤等人[9-10]采用组合密钥技术实现密钥协商,但其容易遭受密钥信息共谋攻击;Teng 等人[11]提出无线网络环境下可认证的群组密钥协商协议,协议具有动态灵活性,能抵御积极攻击;Thomas 等人[12]提出无线传感网络中一种节约资源的群组密钥协商,其主要是针对特定的无线网络环境下在计算量尽可能少、信息传播轮数尽可能少的节能性群组密钥协商;Walid 等人[13]提出无线传感网络中一种可扩展的密钥管理机制,该方案针对传感器存储资源受限及传感网节点易变性提出的密钥管理机制,适用于传感网特定的应用环境.

非对称群组密钥协商的主要特点是群组成员协商一对公/私密钥对,分别用于群组交换信息的加密与解密.伍前红等人[14]在 2009 年 EUROCRYPT 会议上提出非对称群组密钥协商(asymmetric group key agreement, AGKA)协议,由于群组加密密钥和解密密钥不相同,加密密钥可以对外公开,这使得消息发送者不局限于群组内部人员,该方案具有较高的安全性,但在效率方面没有优势,该方案只适用于静态群组;2011 年伍前红等人[15]对其 EUROCRYPT 会议提出的 AGKA 进行了扩展与改进,使其具有动态性,增强了方案的灵活性和实用性;张磊等人[16-17]提出可认证的非对称群组密钥协商,提高了非对称群组密钥协商的安全性;Zhao 等人[18]提出一种应用于 ad hoc 网络的动态 ASGKA,该方案的群组间认证采用多方签名技术来实现,增加了较大的计算量.在移动设备资源受限的环境下,该方案有待于进一步简化计算量与通信量;徐畅等人[19]提出具有隐藏特性的可认证非对称群组密钥协商协议,对参与群组密钥协商的成员隐私信息具有一定的保护能力;Lü 等人[20]提出基于无证书密码系统的可认证非对称群组密钥协商方案,避免了基于身份密码系统中密钥托管问题,在 Diffie-Hellman 困难假设下可证明安全的;2014 年张启坤等人[21]利用短签名技术实现动态可认证非对称群组密钥协商,进一步提高了群组密钥协商的安全性及效率,但群组密钥协商的计算量及通信消耗比较大,不适用于移动网络环境中.

综上分析,无线传感网中基于预置的密钥分配方案,由于传感器节点存储能力的限制,使其在大规

模的无线网络中的应用受到限制;基于在线计算的对称群组密钥协商,其安全度不高,且灵活性较差,不适用于网络易受攻击及节点易被捕获的传感网络;当前非对称群组密钥协商,其计算量及通信量较大,有待进一步优化以适用节点资源受限的无线传感网.

本文提出可认证非对称群组密钥协商具有3项优势:

1) 可跨簇性.参与群组密钥协商的传感器节点可分布在不同的簇,在传感器节点通信能力受限的情况下通过桥接技术实现跨簇非对称群组密钥协商,完成传感器节点远距离信息安全交换与信息安全传输;

2) 轻量级计算.由于非对称群组密钥涉及的通信与计算较对称群组密钥协商要大,通过不对等计算技术,将传感器节点的计算与通信负载迁移簇头节点来完成,弥补传感器节点资源受限的限制问题,达到非对称群组密钥协商的性能,具有对称群组密钥协商的轻量级计算和非对称群组密钥协商的安全性及灵活性;

3) 群组密钥自证实性.群组成员计算完群组密钥后,不需要经过额外的通信广播轮数,只需通过简单函数映射关系,自己能够验证其所计算的群组密钥的正确性.

1 基础知识

1.1 双线性映射

首先给出双线性映射的定义[15-16],假设 G_1 为加法群,G_2 为乘法循环群,其具有共同的大素数阶 q,$q\geqslant 2^k+1$,k 是安全参数,且 G_1 和 G_2 上的离散对数是困难的.群 G_1 和 G_2 是一对双线性群,设 $G_1=\langle g_1\rangle$,e 是可高效计算的双线性映射,$e:G_1\times G_1\rightarrow G_2$,有关双线性映射性质如下[17,19-20]:

性质1. 双线性.对所有的 $g_1,g_2\in G_1$,及 $a,b\in\mathbb{Z}_q^*$,有 $e(ag_1,bg_2)=e(g_1,g_2)^{ab}$.

性质2. 非退化性.即 $e(g_1,g_2)\neq 1$.

性质3. 可高效计算性.存在有效的算法,对于 $g_1,g_2\in G_1$ 可高效计算 $e(g_1,g_2)$.

1.2 计算复杂性问题

假设1. 离散对数问题[17,19-20].设 $g_1,g_1'\in G_1$,寻找一个整数 a 使得 $g_1'=ag_1$ 在计算上是困难的.

假设2. DCDH(divisible computational Diffie-Hellman)问题[17,19-20].假设一个三元组 $(g_1,ag_1,bg_1)\in G_1$,对于未知数 $a,b\in\mathbb{Z}_q^*$,计算 $(a/b)g_1$ 是困难的.

1.2.1 安全模型与安全假设

本节参考了文献[18,21],在其基础上给出了非对称群组密钥协商协议参与者安全模型属性,然后给出安全模型的形式化定义及要实现的安全目标.

1) 安全模型属性及相关符号

假设 U 是参与密钥协商协议的传感器节点组成的集合,该集合的大小为多项式有界,U 中每个传感器节点都有自己的身份信息及对应的公/私密钥对,U 的任意子集 $U_{\text{sub}}=\{u_1,u_2,\cdots,u_n\}$ 中的节点可以随时执行密钥协商协议 Π,用 $\Pi_{u_i}^{\pi}$ 表示节点 u_i 与其伙伴节点 $\{u_1,u_2,\cdots,u_{i-1},u_{i+1},\cdots,u_n\}$ 执行非对称密钥协商的第 π 个实例,$\pi\in\mathbb{Z}_q^*$,每个参与节点实例 $\Pi_{u_i}^{\pi}$ 拥有多个属性,定义如下:

$sid_{u_i}^{\pi}$——实例 $\Pi_{u_i}^{\pi}$ 的会话密钥身份标识,参与本次会话密钥协商的所有伙伴具有相同的会话密钥身份.

$pid_{u_i}^{\pi}$——实例 $\Pi_{u_i}^{\pi}$ 的伙伴身份标识,是所有与实例 $\Pi_{u_i}^{\pi}$ 建立一个会话密钥的参与者身份的集合,包括实例 $\Pi_{u_i}^{\pi}$ 自己.

$ek_{u_i}^{\pi}$——实例 $\Pi_{u_i}^{\pi}$ 执行密钥协商协议 Π 后,参与者计算出的群组会话加密密钥.

$dk_{u_i}^{\pi}$—— 实例 $\Pi_{u_i}^{\pi}$ 执行密钥协商协议 Π 后,计算出的群组会话解密密钥.

$ms_{u_i}^{\pi}$—— 实例 $\Pi_{u_i}^{\pi}$ 在执行密钥协商过程中接收和发送所有消息的链接.

$state_{u_i}^{\pi}$—— 实例 $\Pi_{u_i}^{\pi}$ 的当前状态,如果执行协议结束,实例 $\Pi_{u_i}^{\pi}$ 执行完所有接收和发送的消息,并且它已经成功计算出参数($ek_{u_i}^{\pi}\neq$null),($dk_{u_i}^{\pi}\neq$null),$sid_{u_i}^{\pi}$ 和 $pid_{u_i}^{\pi}$,则该协议成功终止,实例 $\Pi_{u_i}^{\pi}$ 进入接受状态,否则进入终止状态.

定义1. 伙伴关系(partnering).实例 $\Pi_{u_i}^{\pi}$ 的伙伴定义为与实例 $\Pi_{u_i}^{\pi}$ 一起参与本次会话密钥的所有实例,实例 $\Pi_{u_i}^{\pi}$ 与其伙伴 $\Pi_{u_j}^{\pi'}$ 满足4个条件:

1) 实例 $\Pi_{u_i}^{\pi}$ 与其伙伴不能为同一实体,即 $u_i\neq u_j$;

2) 他们成功的完成群组会话密钥协商;

3) $sid_{u_i}^{\pi}=sid_{u_j}^{\pi'}$;

4) $pid_{u_i}^{\pi}=pid_{u_j}^{\pi'}$.

1.2.2 敌手模型

本文所设计的跨簇非对称密钥协商协议方案中,参与群组密钥协商的传感器节点所计算的公开

群组密钥是群组加密密钥,而群组解密密钥是由各不相同的传感器节点自身的密钥参数计算的.本文把保密性定义为任意概率多项式时间的敌手区分用群组加密密钥加密的2个等长消息的优势是可忽略的.通过一个挑战者 $\mathcal{C}$ 与一个敌手 $\mathcal{A}$ 之间的游戏规则来定义该群组密钥协商协议的安全性,安全模型中包括一个主动攻击者和一个协议参与者集合,每个参与者被模拟成一个随机预言机,该游戏分为3个步骤:

1) 初始化阶段.该阶段挑战者 $\mathcal{C}$ 运行系统函数 $Setup(\ell)$(ℓ 是一个安全参数),输出相关的系统参数及主密钥.然后将系统参数发给敌手 $\mathcal{A}$,并保留主密钥.

2) 训练阶段.敌手 $\mathcal{A}$ 通过以下询问与挑战者 $\mathcal{C}$ 进行交互:

$Send(\Pi_{u_i}^{\pi},m)$—— 敌手 $\mathcal{A}$ 伪装成 $pid_{u_i}^{\pi}$ 向预言机 $\Pi_{u_i}^{\pi}$ 发送消息 m,如果消息 $m=$null(null 表示空串),则预言机 $\Pi_{u_i}^{\pi}$ 作为会话的主动发起者发起一次会话.否则它作为一个响应者,按照协议规则对敌手相应的询问做出回应,并做出接受或拒绝该会话的决定,并将每次接收和发送的消息记录下来.

$Ek.Reveal(\Pi_{u_i}^{\pi})$—— 预言机 $\Pi_{u_i}^{\pi}$ 收到此查询后,返回群组密钥协商执行计算出的群组加密密钥 $ek_{u_i}^{\pi}$,如果预言机状态不接受,则返回一个终止符号 $\perp$.

$Dk.Reveal(\Pi_{u_i}^{\pi})$—— 预言机 $\Pi_{u_i}^{\pi}$ 收到此查询后,返回群组密钥协商执行计算出的群组解密密钥,如果预言机状态不接受,则返回一个终止符号 $\perp$.用它来模拟已知密钥安全性.

$Corrupt(u_i)$—— 该查询要求被询问的参与者返回它的长期私钥 SK_{u_i},敌手一旦拥有参与者 u_i 的长期私钥,便可以通过 $Send$ 伪装成参与者 u_i.响应过 $Corrupt$ 询问的实体状态被称为"已腐化".用它来模拟密钥的向前安全性.

$Test(\Pi_{u_i}^{\pi})$—— 在游戏的某个时刻,$\mathcal{A}$ 发送2个消息 $(m_0,m_1)(|m_0|=|m_1|)$,向一个新鲜的(新鲜定义,见定义2)预言机 $\Pi_{u_i}^{\pi}$ 发出 $Test$ 询问,只允许敌手 $\mathcal{A}$ 进行一次 $Test$ 查询.预言机 $\Pi_{u_i}^{\pi}$ 随机选择一个比特 $b\in\{0,1\}$,然后将 m_b 用群组加密密钥加密后返回给敌手 $\mathcal{A}$.

3) 输出.游戏结束后,敌手 $\mathcal{A}$ 输出一个对比特 b 的猜测值(记为 b').若 $b'=b$,则称敌手 $\mathcal{A}$ 赢得了此游戏.定义敌手 $\mathcal{A}$ 成功赢得游戏的概率为 $Adv^{A}(\ell)=|2Pr[b'=b]-1|$($\ell$ 为安全参数).

定义2. 新鲜性(freshness).一个随机预言机 $\Pi_{u_i}^{\pi}$ 在游戏结束时满足以下条件,则称该预言机 $\Pi_{u_i}^{\pi}$(满足 $pid_{u_i}^{\pi}=P_j$)是新鲜的:

1) $\Pi_{u_i}^{\pi}$ 处于接受状态;

2) $\mathcal{A}$ 没有对预言机 $\Pi_{u_i}^{\pi}$ 及搭档预言机 $\Pi_{u_j}^{\pi'}$ 做过 $Dk.Reveal(\Pi_{u_i}^{\pi})$ 或者 $Dk.Reveal(\Pi_{u_j}^{\pi'})$ 查询;

3) 未对参与实体集合 P_j 做过 $Corrupt$ 查询.

定义3. 安全性.称该非对称群组密钥协商协议具有 适应性选择挑战ID和选择明文攻击下的语义不可区分性(indistinguishability against identity-based chosen plaintext attack, IND-ID-CPA),如果没有概率多项式时间(probabilistic polynomial time, PPT)内敌手 $\mathcal{A}$ 以不可忽略的优势赢得以上游戏,或者任意概率多项式时间 IND-ID-CPA 敌手 $\mathcal{A}$ 赢得该游戏的优势 $Adv^{A}(\ell)=|2Pr[b'=b]-1|$ 可以忽略.

2 簇间非对称群组密钥协商过程

在无线传感网中簇间非对称群组密钥协商协议分为2个部分:1)簇头之间的联盟密钥建立;2)簇间传感器节点非对称群组密钥协商协议.

2.1 初始化

假设 G_1 和 G_2 分别是具有相同大素数阶 q 的加法群和乘法群,$q\geqslant 2^{\ell}+1$,ℓ 是安全参数,且 G_1 和 G_2 上的离散对数是困难的,设 $G_1=\langle g_1\rangle$.e 是可高效计算的双线性映射,$e:G_1\times G_1\rightarrow G_2$,$H_1$,$H_2:G_2\rightarrow\mathbb{Z}_q^*$ 为2个散列函数.系统的参数为 $params=(q,G_1,G_2,g_1,e,H_1,H_2)$.

2.2 簇头间联盟密钥的计算

设 N 个簇的簇头集合为 $\phi=\{U_1,U_2,\cdots,U_N\}$,任意簇头 $U_i(1\leqslant i\leqslant N)$ 随机选择 $SK_i\in\mathbb{Z}_q^*$,并计算 $PK_i=SK_ig_1$,则 $U_i(1\leqslant i\leqslant N)$ 的公/私密钥对为 (PK_i,SK_i),SK_i 由簇头秘密保存,PK_i 广播出去并对外公开.

将 N 个簇的簇头 $U_i(1\leqslant i\leqslant N)$ 作为三叉树的叶子节点,构建一个完全三叉树,如图1所示.其中 $T_{h,l}$ 表示非叶子节点,h 为分枝节点 $T_{h,l}$ 在树中的高度(层数),l 为该分枝节点 $T_{h,l}$ 在 h 层中的第 l 个节点,且

$$1\leqslant h\leqslant\lfloor\log_3 N\rfloor+1,0\leqslant l\leqslant\lfloor N/3\rfloor.$$

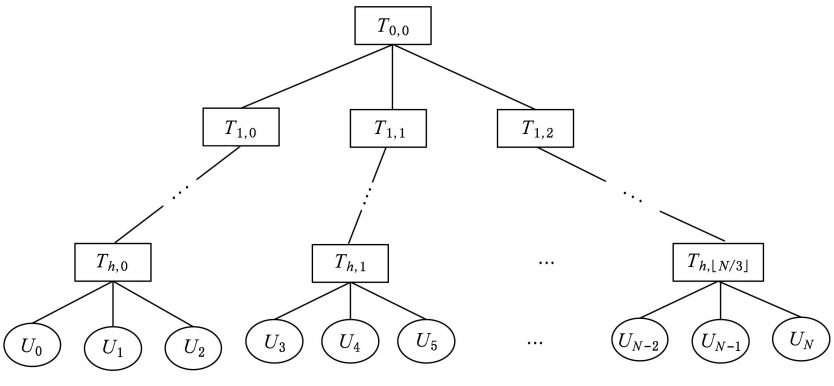

Fig. 1 The logical structure of key agreement for cluster heads

图 1 簇头联盟密钥建立的逻辑结构

每个左孩子叶子节点 $U_i(1\leqslant i\leqslant N)$,用自己的私钥及其兄弟节点的公钥可计算出其父节点 $T_{h,\lfloor i/3 \rfloor}(0\leqslant i\leqslant N)$的私钥,即其父节点私钥表示为 $TX_{h,\lfloor i/3 \rfloor}=H_1(e(PK_{i+1},PK_{i+2})^{SK_i})=H_1(e(PK_i,PK_{i+2})^{SK_{i+1}})=H_1(e(Y_i,Y_{i+1})^{SK_{i+2}})=H_1(e(g_1,g_1)^{SK_iSK_{i+1}SK_{i+2}})$,$TX_{h,\lfloor i/3 \rfloor}$秘密保存,其父节点对应的公钥 $TY_{h,\lfloor i/3 \rfloor}=TX_{h,\lfloor i/3 \rfloor}g_1$ 对外广播. 每个叶子节点逐层向上计算,直到根节点 $T_{0,0}$. 当某个叶子节点 $U_i(1\leqslant i\leqslant N)$没有兄弟节点,可计算其父节点的私钥 $TX_{h,\lfloor i/3 \rfloor}=H_1(e(g_1,g_1)^{SK_i})$,其父节点对应的公钥 $TY_{h,\lfloor i/3 \rfloor}=TX_{h,\lfloor i/3 \rfloor}g_1$. 当某个叶子节点 $U_i(1\leqslant i\leqslant N)$缺少一个兄弟节点时,其可计算其父节点的私钥 $TX_{h,\lfloor i/3 \rfloor}=H_1(e(PK_{i+1},g_1)^{SK_i})=H_1(e(PK_i,g_1)^{SK_{i+1}})=H_1(e(g_1,g_1)^{SK_iSK_{i+1}})$,其父节点对应的公钥 $TY_{h,\lfloor j/3 \rfloor}=TX_{h,\lfloor j/3 \rfloor}g_1$. 根据双线性映射的性质可知,所有簇头节点(叶子节点)都能计算出一个共同的树根节点 $T_{0,0}$ 私钥,把该私钥作为簇头节点之间共享的联盟密钥.

为简述方便,以 9 个簇头的传感网为例,由 9 个簇头组建的三叉树分 3 层,假设簇头分别为 $U_0,U_1,U_2,U_3,U_4,U_5,U_6,U_7,U_8$ 其对应的公/私密钥对分别为 $(SK_0,PK_0),(SK_1,PK_1),(SK_2,PK_2),(SK_3,PK_3),(SK_4,PK_4),(SK_5,PK_5),(SK_6,PK_6),(SK_7,PK_7),(SK_8,PK_8)$,则簇头间联盟密钥生成过程如下:

1) U_0,U_1,U_2 通过各自自己的私钥和其兄弟节点的公钥可计算出其父节点 $T_{1,0}$ 的私钥 $TX_{1,0}$. 如 U_0 计算 $TX_{1,0}=H_1(e(PK_1,PK_2)^{SK_0})=H_1(e(g_1,g_1)^{SK_0SK_1SK_2})$ 及对应公钥 $TY_{1,0}=H_1(e(g_1,g_1)^{SK_0SK_1SK_2})g_1$,并广播 $TY_{1,0}$. U_1 计算 $TX_{1,0}=H_1(e(PK_0,PK_2)^{SK_1})=H_1(e(g_1,g_1)^{SK_1SK_0SK_2})$;$U_2$ 计算 $TX_{1,0}=H_1(e(PK_0,PK_1)^{SK_2})=H_1(e(g_1,g_1)^{SK_2SK_0SK_1})$.

2) 同理,U_3,U_4,U_5 各自计算出其父节点私钥 $TX_{1,1}=H_1(e(PK_4,PK_5)^{SK_3})=H_1(e(PK_3,PK_5)^{SK_4})=H_1(e(PK_3,PK_4)^{SK_5})=H_1(e(g_1,g_1)^{SK_3SK_4SK_5})$,$U_3$ 计算对应的公钥 $TY_{1,1}=TX_{1,1}g_1$,并广播出去.

3) 同理,U_6,U_7,U_8,U_5 各自计算出其父节点私钥 $TX_{1,2}=H_1(e(PK_7,PK_8)^{SK_6})=H_1(e(PK_6,PK_8)^{SK_7})=H_1(e(PK_6,PK_7)^{SK_8})=H_1(e(g_1,g_1)^{SK_6SK_7SK_8})$,$U_6$ 计算对应的公钥 $TY_{1,2}=TX_{1,2}g_1$,并广播出去.

4) 所有叶子节点收到 U_0,U_3 和 U_6 的广播后,可计算出根节点 $T_{0,0}$ 的私钥

$$TX_{0,0}=H_1(e(TY_{1,1},TY_{1,2})^{H_1(e(g_1,g_1)^{SK_2SK_0SK_1})})=H_1(e(TY_{1,0},TY_{1,2})^{H_1(e(g_1,g_1)^{SK_3SK_4SK_5})})=H_1(e(TY_{1,0},TY_{1,1})^{H_1(e(g_1,g_1)^{SK_6SK_7SK_8})}),$$

则传感器网络中每个簇头可协商出一个共同的联盟密钥 $TX_{0,0}$.

2.3 跨簇传感器节点间非对称群组密钥协商

本节提出一种轻量级的关于无线传感器节点之间的跨簇可认证的非对称群组密钥协商协议,以一个簇的传感器节点的群组密钥协商为例,有 2 种假设需要考虑:

1) 每个簇有一个簇头和 n 个传感器节点组成. 簇头 U_i 内的低能量节点集合表示为 $u=\{u_{i,1},u_{i,2},\cdots,u_{i,n}\}$,其对应的身份集合表示为 $I=\{id_{u_{i,1}},id_{u_{i,2}},\cdots,id_{u_{i,n}}\}$,任意节点 $u_{i,j}(1\leqslant j<n)$的公私密钥对 $(sk_{i,j},pk_{i,j})$,其中 $sk_{i,j}\in\mathbb{Z}_q^*$,$pk_{i,j}=sk_{i,j}g_1$. U_i 为本簇能量较大的簇头,其对应的身份表示为 id_{U_i}. U_i 的公私密钥对(SK_i,PK_i),其中 $SK_i\in\mathbb{Z}_q^*$,$PK_i=SK_ig_1$.

2) 每个节点在执行协议之前都能知道其他成员的身份信息.

定义 4. 非对称群组密钥协商(asymmetric group key agreement, AGKA)[21]. 一个群组密钥协商 Σ 是非对称的,如果该协议成功终止,有等式 $ek_{u_{i,t}}=ek_{u_{i,k}}$, $ek_{u_{i,t}}\neq dk_{u_{i,t}}$ 或 $ek_{u_{i,t}}=ek_{u_{j,k}}$, $ek_{u_{j,k}}\neq dk_{u_{j,k}}$,其中 $ek_{u_{i,t}}/dk_{u_{i,t}}$, $ek_{u_{j,k}}/dk_{u_{j,k}}$ 分别是 $u_{i,t}$ 和 $u_{i,k}$ 及 $u_{i,t}$ 和 $u_{j,k}$ 分别是同簇和不同簇的 2 个不同的节点,其计算出的群组加密/解密密钥($t,k,i,j\in\mathbb{N}_+$, $1\leqslant t\leqslant n$, $1\leqslant k\leqslant n$, $t\neq n$, $1\leqslant i\leqslant N$, $1\leqslant j\leqslant N$, $i\neq j$).

2.3.1 跨簇传感器节点间群组密钥计算

如果参与群组密钥协商的传感器节点分布在不同的簇,则跨簇群组密钥协商过程如下:

1) 每个传感器节点 $u_{i,t}$($1\leqslant i\leqslant N$, $1\leqslant t\leqslant n$)随机选择 2 个数 $m_{i,t},q_{i,t}\in\mathbb{Z}_q^*$. 然后计算 $Q_{i,t}=q_{i,t}g_1$, $T_{i,t}=((m_{i,t}+sk_{i,t})/q_{i,t})g_1$, $M_{i,t}=m_{i,t}PK_i$. 并将 $(id_{u_{i,t}},Q_{i,t},T_{i,t},M_{i,t})$ 发送给簇头 U_i(注:$(id_{u_{i,t}},Q_{i,t},T_{i,t},M_{i,t})$提前存储在对应传感器内存卡上,以减少在线计算量,延长传感器使用寿命).

2) 收到 $(id_{u_{i,t}},Q_{i,t},T_{i,t},M_{i,t})$($1\leqslant i\leqslant N$, $1\leqslant t\leqslant n$)后,簇头节 U_i($1\leqslant i\leqslant N$)验证等式 $e(Q_{i,t},T_{i,t})=?e(g_1,SK_i^{-1}M_{i,t})e(g_1,pk_{i,t})$ 是否成立,如果成立,则 U_i 可以确保消息 $(id_{u_{i,t}},Q_{i,t},T_{i,t},M_{i,t})$ 是由 $u_{i,t}$ 发送的,然后令 $m_{U_i}=TX_{0,0}$,计算 $f_{i,t}=SK_i^{-1}m_{U_i}M_{i,t}$,($1\leqslant i\leqslant N$, $1\leqslant t\leqslant n$).

3) 各簇头 U_i($1\leqslant i\leqslant N$)之间,将各簇内参与群组密钥协商的传感器节点信息 $f_{i,t}$ 相互传递共享. 为描述方便,假设有 2 个簇的传感器节点参与群组密钥协商,分别是以簇头 U_i 和簇头 U_j 为首的跨簇群组密钥协商. 则 U_i 将其内部参与密钥协商的节点信息 $(f_{i,t},Q_{i,t},T_{i,t},pk_{i,t})$($1\leqslant t\leqslant n$)发送给 U_j, U_j 将其内部参与密钥协商的节点信息 $(f_{j,t},Q_{j,t},T_{j,t},pk_{j,t})$($1\leqslant t\leqslant n$)发送给 U_i.

① U_i 选择一个随机数 $q_{U_i}\in\mathbb{Z}_q^*$, U_i 计算 $Q_{U_i}=q_{U_i}g_1$, $T_{U_i}=((m_{U_i}+SK_i)/q_{U_i})g_1$, $PK=\sum_{t=1}^{n}pk_{i,t}+\sum_{t=1}^{n}pk_{j,t}$, $QT=\prod_{t=1}^{n}e(Q_{i,t},T_{i,t})\times\prod_{t=1}^{n}e(Q_{j,t},T_{j,t})$, $P=m_{U_i}PK$, $R=QT^{m_{U_i}^2}$, $\phi_{U_i}=m_{U_i}g_1$. U_i 可以计算出群组加密密钥 $ek_{U_i}=(R,P)$ 和群组解密密钥 $dk_{U_i}=e(\phi_{U_i},\sum_{t=1}^{n}f_{i,t}+\sum_{t=1}^{n}f_{j,t})$. 然后,$U_i$ 将 $(id_{U_i},f_{i,1},f_{i,2},\cdots,f_{i,n},f_{j,1},f_{j,2},\cdots,f_{j,n},Q_{U_i},T_{U_i},R,P)$ 广播给簇内传感器节点.

② 同理,U_j 选择一个随机数 $q_{U_i}\in\mathbb{Z}_q^*$, U_j 计算 $Q_{U_j}=q_{U_j}g_1$, $T_{U_j}=((m_{U_j}+SK_j)/q_{U_j})g_1$, $PK=\sum_{t=1}^{n}pk_{j,t}+\sum_{t=1}^{n}pk_{i,t}$, $QT=\prod_{t=1}^{n}e(Q_{j,t},T_{j,t})\times\prod_{t=1}^{n}e(Q_{i,t},T_{i,t})$, $P=m_{U_j}PK$, $R=QT^{m_{U_j}^2}$, $\phi_{U_j}=m_{U_j}g_1$. U_j 可以计算出群组加密密钥 $ek_{U_j}=(R,P)$ 和群组解密密钥 $dk_{U_j}=e(\phi_{U_j},\sum_{t=1}^{n}f_{i,t}+\sum_{t=1}^{n}f_{j,t})$. 然后,$U_j$ 将 $(id_{U_j},f_{j,1},f_{j,2},\cdots,f_{j,n},f_{i,1},f_{i,2},\cdots,f_{i,n},Q_{U_j},T_{U_j},R,P)$ 广播给簇内传感器节点.

4) 群组密钥计算. 各簇内每个节点 $u_{i,t}$($1\leqslant i\leqslant N$, $1\leqslant t\leqslant n$)在接收到各自簇头 U_i($1\leqslant i\leqslant N$)广播之后,验证等式 $e(Q_{U_i},T_{U_i})\stackrel{?}{=}e(g_1,m_{i,t}^{-1}f_{i,t})e(g_1,PK_i)$ 是否立,如果成立,则每个 $u_{i,t}$($1\leqslant i\leqslant N$, $1\leqslant t\leqslant n$)可以确保 $(id_{U_i},f_{i,1},f_{i,2},\cdots,f_{i,n},f_{j,1},f_{j,2},\cdots,f_{j,n},Q_{U_i},T_{U_i},R,P)$ 是由簇头 U_i 发送过来的. 然后各个 $u_{i,t}$($1\leqslant i\leqslant N$, $1\leqslant t\leqslant n$)可获得群组加密密钥 $ek_{u_{i,t}}=(R,P)$,并通过自己的密钥参数 $m_{i,t}$ 计算 $\phi_{i,t}=f_{i,t}m_{i,t}^{-1}$ 及群组解密密钥 $dk_{u_{i,t}}=e(\phi_{i,t},\sum_{i=1,t=1}^{i=n,t=n}f_{i,t})=e(m_{U_i}g,\sum_{i=1,t=1}^{i=n,t=n}f_{i,t})$.

5) $u_{i,t}$($1\leqslant i\leqslant N$, $1\leqslant t\leqslant n$)通过验证等式 $e(P,\phi_{i,t})dk_{u_{i,t}}\stackrel{?}{=}R$ 是否成立,来验证 $ek_{u_{i,t}}$ 和 $dk_{u_{i,t}}$ 计算的正确性. 此方案的示意图如图 2 所示.

2.4 无线传感器节点间群组安全通信

对任意明文信息 $m\in\mathcal{M}^*$($\mathcal{M}^*$:明文空间),任意成员 $u_{i,t}$ 拥有群组加密密钥 $ek_{u_{i,t}}$ 和群组解密密钥 $dk_{u_{i,t}}$ 作如下操作.

加密:消息发送者 $u_{i,t}$ 随机选择整数 $\gamma_{i,t}\in\mathbb{Z}_q^*$ 并计算 $\delta_{i,t}=\gamma_{i,t}g_1$, $\eta_{i,t}=m\oplus H_2(e(g_1,(H_2(Re(P,\phi_{i,t})^{-1})g_1)^{\gamma_{i,t}})$. 然后广播密文 $c=\langle\delta_{i,t},\eta_{i,t}\rangle$,簇间传感器节点的通信,可由簇头进行转发广播.

解密:当收到消息发送者广播的密文 $c=\langle\delta_{i,t},\eta_{i,t}\rangle$,群组内任意成员 $u_{j,t}$ 可用计算的群组私钥 $dk_{u_{j,t}}$ 计算出明文 $m=\eta_{i,t}\oplus H_2(e(\delta_{i,t},H_2(dk_{u_{j,t}})g_1))$.

3 安全性及性能分析

本节首先给出相关等式的正确性证明,其次对提出的协议进行安全性分析,最后给出协议的性能比较与分析.

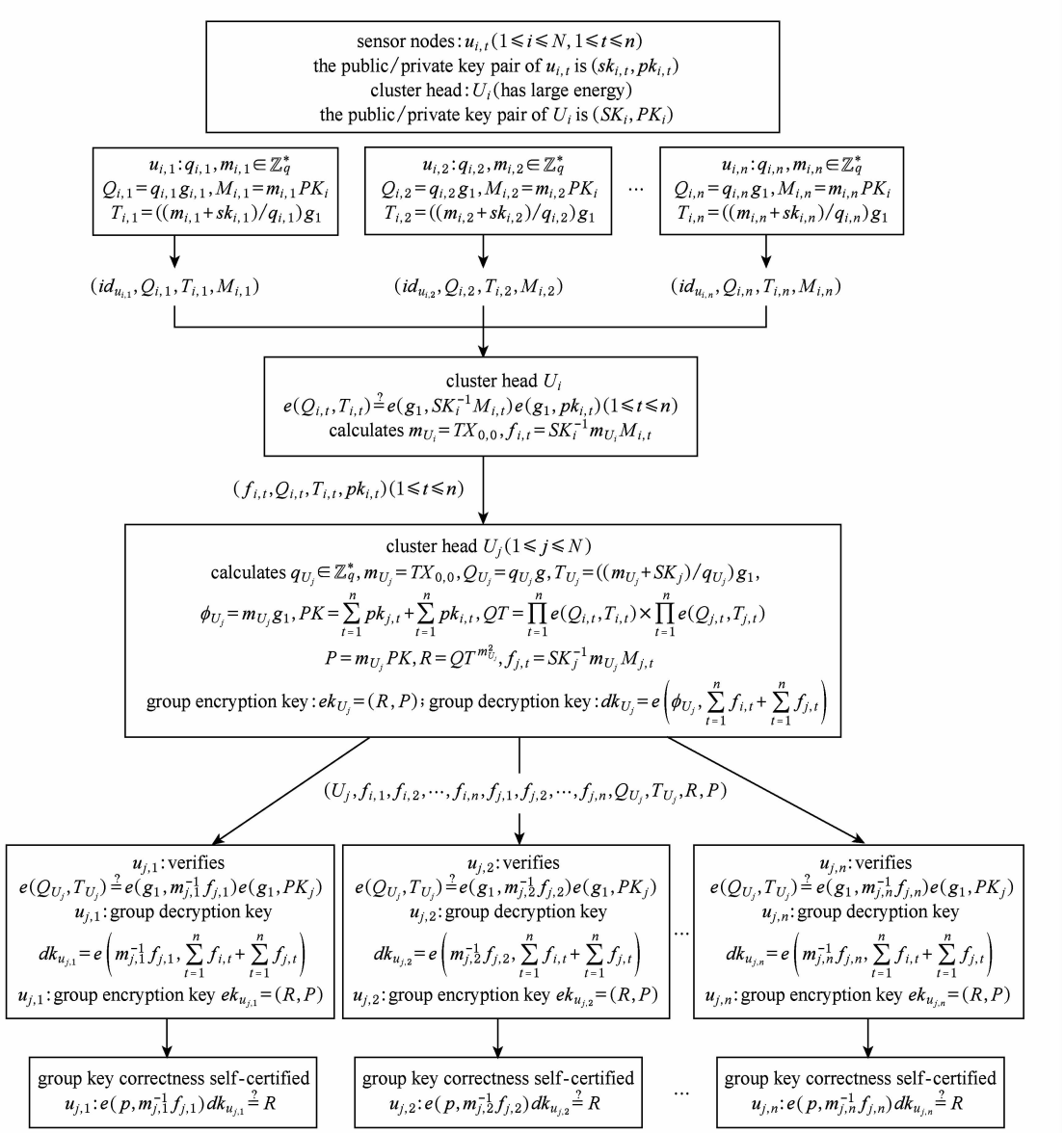

Fig. 2 Cross-cluster sensor node group key agreement

图 2 簇间传感器节点群组密钥协商

3.1 关键技术的正确性证明

定理 1. 正确性. 群组密钥协商阶段,如果参与群组密钥协商的任意传感器节点 $u_{i,t}$ 计算无误,则都可计算出一致的群组解密密钥 $dk_{u_{i,t}}$,即:

$$dk_{u_{i,t}}=e(\phi_{i,t},\sum_{r=1}^{n}f_{i,r})=e(\phi_{i,k},\sum_{r=1}^{n}f_{i,r})=dk_{u_{i,k}},$$
$$1\leqslant t\leqslant n,1\leqslant k\leqslant n,t\neq n.$$

证明.

由于 $f_{i,t}=SK_i^{-1}m_{U_i}M_{i,t}$,$M_{i,t}=m_{i,t}PK_i$,$\phi_{i,t}=f_{i,t}m_{i,t}^{-1}$,$\phi_{j,t}=f_{j,t}m_{j,t}^{-1}$ 和双线性配对的特性,有:

$$dk_{u_{i,t}}=e(\phi_{i,t},\sum_{t=1}^{n}f_{i,t})=e(f_{i,t}m_{i,t}^{-1},\sum_{t=1}^{n}f_{i,t})=$$

$$e(SK_i^{-1}m_{U_i}M_{i,t}m_{i,t}^{-1},\sum_{t=1}^{n}f_{i,t})=$$

$$e(SK_i^{-1}m_{U_i}m_{i,t}PK_im_{i,t}^{-1},\sum_{t=1}^{n}f_{i,t})=$$

$$e(SK_i^{-1}m_{U_i}PK_i,\sum_{i=1}^{n}f_{i,t})=$$

$$e(SK_i^{-1}m_{U_i}SK_ig_1,\sum_{t=1}^{n}f_{i,t})=$$

$$e(m_{U_i}g_1,\sum_{t=1}^{n}f_{i,t})=e(m_{U_i}g_1,\sum_{t=1}^{n}SK_i^{-1}m_{U_i}M_{i,t})=$$

$$e(m_{U_i}g_1,\sum_{t=1}^{n}m_{U_i}m_{i,t}g_1)=$$

$$e(m_{U_i}g_1,m_{U_i}(m_{i,1}+m_{i,2}+\cdots+m_{i,n})g_1)=$$

$$e(g_1,g_1)^{m_{U_i}^2(m_{i,1}+m_{i,2}+\cdots+m_{i,n})}.$$

观察上述公式,群组解密密钥 $dk_{u_{i,t}}$ 是一个固定量,与具体成员自身的固定参数有关. 只要每个成员

计算无误,则群组解密密钥 $dk_{u_{i,t}}$ 是一个定值. 证毕.

定理 2. 贡献性. 该群组密钥协商是贡献性群组密钥协商.

证明. 根据定理 1 的证明,如果参与群组密钥协商的成员在密钥协商过程中计算无误的情况下都可计算出一致的群组解密密钥,即 $dk_{u_{i,t}}=e(g_1,g_1)^{m_{U_i}^2(m_{i,1}+m_{i,2}+\cdots+m_{i,n})}$,最终的群组密钥包含每个参与者 $u_{i,t}(1\leqslant t\leqslant n)$ 的贡献参数 $m_{i,t}(1\leqslant t\leqslant n)$. 即只有所有群组成员全部参与协商才能最终获得群组密钥,任何群组成员事先不知群组密钥或也不能控制群组密钥. 证毕.

定理 3. 一致性自证实. 如果等式 $e(P,\phi_{i,t})dk_{u_{i,t}}=R(1\leqslant t\leqslant n)$ 成立,因为参数 P 和 R 是公开的,$\phi_{i,t}$ 是通过公开参数 $f_{i,t}$ 和成员自身的保留参数简单计算的. 因此,如果 $\phi_{i,t}$ 计算无误,则只要等式成立,簇内每个群组成员 $u_{i,t}$ 就可以验证群组解密密钥 $dk_{u_{i,t}}$ 计算的正确性.

证明. 由 $P=m_{U_j}PK$, $\phi_{i,t}=f_{i,t}m_{i,t}^{-1}$, $f_{i,t}=SK_i^{-1}m_{U_i}M_{i,t}$, $M_{i,t}=m_{i,t}PK_i$, $PK=\sum_{t=1}^{n}pk_{i,t}$, $R=QT^{m_{U_i}^2}$ 和双线性映射的特性,有:

$$e(P,\phi_{i,t})dk_{u_{i,t}}=e(m_{U_j}PK,f_{i,t}m_{i,t}^{-1})dk_{u_{i,t}}=$$

$$e(m_{U_j}\sum_{t=1}^{n}pk_{i,t},m_{U_j}g_1)dk_{u_{i,t}}=$$

$$e(m_{U_j}\sum_{t=1}^{n}pk_{i,t},m_{U_j}g_1)e(g_1,g_1)^{m_{U_i}^2(m_{i,1}+m_{i,2}+\cdots+m_{i,n})}=$$

$$e(g_1,g_1)^{m_{U_i}^2\sum_{t=1}^{n}(m_{i,t}+sk_{i,t})}.$$

$$R=QT^{m_{U_i}^2}=(\prod_{t=1}^{n}e(Q_{i,t},T_{i,t}))^{m_{U_i}^2}=$$

$$(\prod_{t=1}^{n}e(q_{i,t}g_1,((m_{i,t}+sk_{i,t})/q_{i,t})g_1))^{m_{U_i}^2}=$$

$$(\prod_{t=1}^{n}e(g_1,g_1)^{(m_{i,t}+sk_{i,t})})^{m_{U_i}^2}=$$

$$(e(g_1,g_1)^{\sum_{t=1}^{n}(m_{i,t}+sk_{i,t})})^{m_{U_i}^2}=e(g_1,g_1)^{m_{U_i}^2\sum_{i=1}^{n}(m_{i,t}+sk_{i,t})},$$

所以,等式 $e(P,\phi_{i,t})dk_{u_{i,t}}=R$. 证毕.

定理 4. 如果公式 $e(Q_{U_i},T_{U_i})=?e(g_1,m_{i,t}^{-1}f_{i,t})e(g_1,PK_i)$ 成立,$u_{i,t}(1\leqslant t\leqslant n)$ 可以确保信息 $(id_{U_i},f_{i,1},f_{i,2},\cdots,f_{i,n},Q_{U_i},T_{U_i},R,P)$ 是 U_i 发送的,因为消息经过 U_i 的签名认证.

证明. 由 $Q_{U_i}=q_{U_i}g_1$, $T_{U_i}=((m_{U_i}+SK_i)/q_{U_i})g_1$, $f_{i,t}=SK_i^{-1}m_{U_i}M_{i,t}$, $M_{i,t}=m_{i,t}PK_i$,和双线性配对的特性,则有:

$$e(Q_{U_i},T_{U_i})=e(q_{U_i}g_1,((m_{U_i}+SK_i)/q_{U_i})g_1)=$$

$$e(g_1,g_1)^{(m_{U_i}+SK_i)}.$$

$$e(g_1,m_{i,t}^{-1}f_{i,t})e(g_1,PK_i)=$$

$$e(g_1,m_{i,t}^{-1}SK_i^{-1}m_{U_i}M_{i,t})e(g_1,PK_i)=$$

$$e(g_1,m_{i,t}^{-1}SK_i^{-1}m_{U_i}m_{i,t}PK_i)e(g_1,PK_i)=$$

$$e(g_1,m_{U_i}g_1)e(g_1,PK_i)=$$

$$e(g_1,g_1)^{m_{U_i}}e(g_1,g_1)^{SK_i}=e(g,g)^{(m_{U_i}+SK_i)},$$

所以,等式 $e(Q_{U_i},T_{U_i})=e(g_1,m_{i,t}^{-1}f_{i,t})e(g_1,PK_i)$ 成立. $u_{i,t}(1\leqslant t\leqslant n)$ 可以确保信息 $(id_{U_i},f_{i,1},f_{i,2},\cdots,f_{i,n},Q_{U_i},T_{U_i},R,P)$ 是 U_i 签名的. 证毕.

3.2 安全性分析

定理 5. 对于一个 DCDH 问题实例 $(G_1,G_2,q,g_1,ag_1,bg_1,e,h,H_1,H_2)$,我们构造一个多项式时间模拟器 $\mathcal{C}$,利用攻击者 $\mathcal{A}$ 来解决 DCDH 问题. 假如存在能成功攻击协议 CL-AGKG,我们可以证明 $\mathcal{C}$ 可以不可忽略的优势解决 DCDH 问题,首先,我们假设敌手 $\mathcal{A}$ 在攻击实验中请求为 q_0 个用户私钥,对 *Dk*. *Reveal* 进行 q_1 次询问. 对 *Corrupt* 进行 q_2 次询问,$\mathcal{A}$ 最多建立 q_3 协议运行. 敌手 $\mathcal{A}$ 以优势 $Adv(A)=\varepsilon$ 赢得这场游戏,则存在一个算法以优势 $\varepsilon'=\varepsilon\frac{q_0-1}{q_3q_0^2q_1q_2}$ 解决 DCDH 问题.

证明. 设挑战者 $\mathcal{C}$ 是一个挑战者,$\mathcal{A}$ 是一个能破译该协议的敌手. 给定 $\mathcal{C}$ 一个实例 $(G_1,G_2,q,g_1,ag_1,bg_1,e,h,H_1,H_2)$,未知数 $a,b\in\mathbb{Z}_q^*$,h 是公开的散列函数,H_1 和 H_2 是 $\mathcal{C}$ 所控制的 2 个随机预言机. $\mathcal{C}$ 利用 $\mathcal{A}$ 来求解 DCDH 问题. 定义一个新的会话,他将有一个唯一的会话 ID. 挑战者 $\mathcal{C}$ 随机选择一个会话,该会话的 ID 用符号 sid_t 表示. 对应的模拟会话的 ID 用 $\mathcal{C}_{sid_t}$ 表示,则该会话被选中的概率设为 $Pr[\mathcal{C}_{sid_t}=0]=\sigma$,对应的 $Pr[\mathcal{C}_{sid_t}=1]=1-\sigma$. 同时该挑战者 $\mathcal{C}$ 记下二元组 $(sid_t,\mathcal{C}_{sid_t})$.

1) 初始化阶段. 游戏开始,$\mathcal{C}$ 选择系统参数 $params=(G_1,G_2,q,g_1,ag_1,bg_1,e,h,H_1,H_2)$,$\mathcal{C}$ 将参数发送给敌手 $\mathcal{A}$.

2) 训练阶段. 挑战者 $\mathcal{C}$ 与敌手 $\mathcal{A}$ 交互如下:

$KG(u_i)$ 模拟用户私钥生成—— $\mathcal{A}$ 询问预言机 H_1. $\mathcal{C}$ 维护一个列表 $\mathcal{C}_{L1}=(d_{u_i},s_{u_i},p_{u_i},\mathcal{C}_{H_1^i})$,其中,$d_{u_i}$ 是用户 u_i 的身份标识,s_{u_i} 是对应用户私钥,p_{u_i} 是对应用户公钥,$\mathcal{C}_{H_1^i}\in\{0,1\}$ 为用户类型标识(其中,$\mathcal{C}_{H_1^i}=1$ 表示用户 $\mathcal{C}$ 不能计算该用户密钥,$\mathcal{C}_{H_1^i}=0$ 表示用户 $\mathcal{C}$ 可以计算该用户密钥). 对于用户 u 的密钥请求,$\mathcal{C}$ 查找列表 $\mathcal{C}_{L1}$,如果存在匹配的列表 d_{u_i},则返回对应的 s_{u_i} 和 p_{u_i};否则,作如下处理:

① $\mathcal{C}$ 随机选择 $s_{u_i}\in\mathbb{Z}_q^*$,计算 $p_{u_i}=s_{u_i}g_1$,并把

$(d_{u_i}, s_{u_i}, p_{u_i}, 0)$插入列表 $\mathcal{C}_{L1}$.

② $\mathcal{C}$无法为该用户产生密钥,$\mathcal{C}$设置该用的列表为$(d_{u_i}, \perp, \perp, 1)$.

③ $\mathcal{C}$检查用户列表 $\mathcal{C}_{L1}$,如果列表存在多个 $\mathcal{C}_{H_1^i}=1$ 或者列表长度等于 q_g 但不存在 $\mathcal{C}_{H_1^i}=1$ 的列表项,$\mathcal{C}$则终止模拟(*Event* 1).

Send($\Pi_{u_i}^{\pi}$,m)——$\mathcal{C}$保留一个初始化为空的列表 $\mathcal{C}_{L2}$.假设 $pid_{u_i}^{\pi}=\{d_{u_1}, d_{u_2}, \cdots, d_{u_n}\}$,$\mathcal{C}$初始化定义一个与 $sid_{u_i}^{\pi}$ 相对应的会话身份 $\mathcal{C}_{sid_{u_i}^{\pi}}$.然后将 d_{u_i} 提交给随机预言机 H_2,如果该成员以前没有询问过.则如同询问预言机 H_1 一样,做相应处理后将$(d_{u_i}, s_{u_i}, p_{u_i}, \mathcal{C}_{H_1^i})$加入 $\mathcal{C}_{L1}$.$\mathcal{C}$开始模拟如下预言:

1) 如果 $\mathcal{C}_{H_1^i}=0$ 且 $\mathcal{C}_{sid_{u_i}^{\pi}}=0$

① $\mathcal{C}$选择系统参数 $p_C=bg_1$ 作为公钥返回给 $\mathcal{A}$,并保留参数 b;

② $\mathcal{A}$随机选择 $a_i, r_i \in \mathbb{Z}_q^*$,并根据查询列表 $\mathcal{C}_{L1}$ 获得的私钥 s_{u_i},计算 $Q_i'=r_ig_1$, $T_i'=((a_i+s_{u_i})/r_i)g_1$, $M_i'=a_ip_C$,并将$(d_{u_i}, Q_i', T_i', M_i')$发送给 $\mathcal{C}$;

③ $\mathcal{C}$收到$(d_{u_i}, Q_i', T_i', M_i')$,$\mathcal{C}$随机选择 $c \in \mathbb{Z}_q^*$,计算 $f_i'=cb^{-1}M_i'=cb^{-1}a_ip_C=ca_ig_1$,并将$(d_{u_i}, Q_i', T_i', M_i', f_i')$加入列表 $\mathcal{C}_{L2}$.

2) 如果 $\mathcal{C}_{H_1^i}=0$ 且 $\mathcal{C}_{sid_{u_i}^{\pi}}=1$

① $\mathcal{C}$选择系统参数 $p_C'=b'g_1$ 作为公钥返回给 $\mathcal{A}$,并保留参数 b';

② $\mathcal{A}$随机选择 $a_i, r_i \in \mathbb{Z}_q^*$,并根据查询列表 $\mathcal{C}_{L1}$ 获得的私钥 s_{u_i},计算 $Q_i''=r_ig_1$, $T_i''=((a_i+s_{u_i})/r_i)g_1$, $M_i''=a_ip_C'$,并将$(d_{u_i}, Q_i'', T_i'', M_i'')$发送给 $\mathcal{C}$;

③ $\mathcal{C}$收到$(d_{u_i}, Q_i'', T_i'', M_i'')$,$\mathcal{C}$随机选择 $c \in \mathbb{Z}_q^*$,计算 $f_i''=cb^{-1}M_i''=cb^{-1}a_ip_C'=ca_ig_1$,并将$(d_{u_i}, Q_i'', T_i'', M_i'', f_i'')$加入列表 $\mathcal{C}_{L2}$.

Ek.Reveal($\Pi_{u_i}^{\pi}$)——如果 $state_{u_i}^{\pi}$ 为成功结束,则 $\mathcal{C}$计算根据列表 $\mathcal{C}_{L2}$ 和 c 计算出 R',P',并返回 $ek'=(R', P')$,否则返回 null.

Dk.Reveal($\Pi_{u_i}^{\pi}$)——如果 $state_{u_i}^{\pi}$ 没有成功结束,则返回 null.如果 $\mathcal{C}_{sid_{u_i}^{\pi}}=0$,$\mathcal{C}$计算 $t_c=cg_1$,并查找 $\mathcal{C}_{L2}$ 列表,计算 $X=\sum_{i=1}^{n} f_i'$,输出 $dk'=e(t_c, X)$;否则如果 $\mathcal{C}_{sid_{ui}^{\pi}}=1$,则输出符号 $\perp$(*Event* 2).

Corrupt(u_j)—— $\mathcal{C}$收到 *Corrupt* 询问后,首先在 $\mathcal{C}_{L1}$中查找 u_j 对应的身份 d_{u_j}.如果列表中没有,则表示该询问是第 1 次询问.然后向询问预言机 H_1 一样,做相应处理后将$(d_{u_j}, s_{u_j}, p_{u_j}, \mathcal{C}_{H_1^i})$加入 $\mathcal{C}_{L1}$.如果 $\mathcal{C}_{H_1^i}=1$,则输出符号 $\perp$($\perp$表示是终止)(*Event* 3);否则返回 s_{u_j}.

Test($\Pi_{u_i}^{\pi}$)——敌手 $\mathcal{A}$ 相关的询问结束后,他向 $\mathcal{C}$发起挑战,$\mathcal{A}$选择一个新鲜的预言机 $\Pi_{u_i}^{\pi *}$ 和 2 个消息 m_0, m_1,且有$|m_0|=|m_1|$.假设 $pid_{u_i}^{\pi *}=\{d_{u_1}^*, d_{u_2}^*, \cdots, d_{u_n}^*\}$,$\mathcal{C}$作如下应答:

1) $\mathcal{C}$在 $\mathcal{C}_{L1}$列表中查询相关的信息$(id_{u_i}^*, s_{u_i}^*, p_i^*, \mathcal{C}_{H_1^i}^*)$.

2) 如果 $\mathcal{C}_{sid_{u_i}^{\pi}}=1$,则在 $\mathcal{C}_{L2}$ 列表中提取信息$(d_{u_i}^*, Q_i^*, T_i^*, M_i^*, f_i^*)$,计算 $L=\sum_{i=1}^{n} f_i^*$,否则输出符号 $\perp$(*Event*4).

3) $\mathcal{C}$选择一个随机数 $b \in \{0,1\}$,$\gamma_i^* \in \mathbb{Z}_q^*$ 计算 $\delta_i^*=\gamma_i^* g_1$,然后加密 m_b,$\eta_i^*=m_b \oplus h((R^* \cdot e(P^*, cg_1^*))^{-1})^{\gamma^*})$.

4) 返回 $c^*=\langle \delta^*, \eta^* \rangle$给 $\mathcal{A}$.

Response——$\mathcal{A}$完成所有的询问后,返回一个 $b' \in \{0,1\}$作为对 b 的猜测.如果 $\mathcal{A}$能获得一定的优势正确猜测 $b'=b$,$\mathcal{A}$必须询问 H_2 获取列表 $\mathcal{C}_{L2}$ 中的信息$(d_{u_i}^*, Q_i^*, T_i^*, M_i^*, f_i^*)$,计算 $L=\sum_{i=1}^{n} f_i^*$ 以及 $dk^*=e(L, cg_1)$,从而获取 $m_b=\eta^* \oplus h(e(\delta^*, dk^*))$的猜测优势.则 $\mathcal{C}$可以根据 $\mathcal{A}$ 的方法计算 DCDH 问题,因为 $M_i^*=abg_1$, $f_i^*=acg_1$,根据系统参数(g_1, ag_1, bg_1),$\mathcal{C}$可高效计算 $cg_1=(ac/a)g_1$ 的值. 证毕.

引理 1. 如果 $\mathcal{C}$没有终止上述模拟游戏,则敌手 $\mathcal{A}$ 无法区分模拟世界和真实世界环境.

证明.

在上述的模拟游戏中的所有输出都符合协议 CL-AGKG 的规则要求,同时实体输出的消息符合消息空间上的均匀分布.因此,敌手 $\mathcal{A}$ 无法觉察到模拟世界和真实世界的不一致性. 证毕.

$\mathcal{C}$成果的概率为

$$Pr[C \text{ wins }]=Pr[\overline{Event1} \wedge \overline{Event2} \wedge \overline{Event3} \wedge \overline{Event4} \wedge \mathcal{A} \text{ wins }]=$$
$$Pr[A \text{ wins } | \overline{Event1} \wedge \overline{Event2} \wedge \overline{Event3} \wedge \overline{Event4}]$$
$$Pr[\overline{Event4} | \overline{Event1} \wedge \overline{Event2} \wedge \overline{Event3}]$$
$$Pr[\overline{Event3} | \overline{Event1} \wedge \overline{Event2}]Pr[\overline{Event2} | \overline{Event1}]Pr[\overline{Event1}]=$$
$$\varepsilon \frac{1}{q_3}\left(\left(1-\frac{1}{q_0}\right)\frac{1}{q_1}\right)\frac{1}{q_2}\frac{1}{q_0}=\varepsilon \frac{q_0-1}{q_3 q_0^2 q_1 q_2}.$$

3.3 性能分析

由于传感器节点资源受限,协议设计过程中除安全性外,协议的计算量、通信量及能量消耗是衡量协议性能的重要指标. 本文就近年来可以进行量化计算的文献进行对比分析. 这些协议都适用于无线传感器网络,具有可比性及代表性. 依据这些协议所提供的数据,分别从计算与通信复杂度及协议消耗的总能量进行对比分析. 表 1 列举了本文协议与这些具有可比性和代表性的 4 个群组密钥协商协议在计算复杂度及通信量方面进行比较分析.

Table 1 Complexity Analysis of Authenticated Protocols

表 1 可认证协议的复杂度分析

Protocol	Modular Exponentiation	Tate Pairing	Scalar Multiplication	Length of Message Sent	Length of Message Received
Ref [22]	3	0	n	$2\|G_1\|$	$n\|G_1\|$
Ref [23]	2	3	3	$3\|G_1\|$	$(n+1)\|G_1\|$
Ref [24]	n	4	$4n+1$	$(2n+3)\|G_1\|$	$(2n+3)\|G_1\|$
Ref [25]	$n+5$	4	$5n+2$	$(n+4)\|G_1\|$	$(n+4)\|G_1\|$
Ours		5	2	$4\|G_1\|$	$(n+4)\|G_1\|$

从表 1 可以看出计算复杂度较小的是 Tsai[23] 及本文方案,其计算复杂度不随节点的数量变化而变化. Chen 等人[24] 及张磊等人[25] 计算复杂度最高,通信复杂度 Chen 等人[24] 最高.

从协议执行时间上看,我们通过文献[26]提供的数据进行分析,该文献通过 PBC 实验室提供的实验程序 pbc-0.5.12 版本,在硬件 Intel® Core™2 Duo E8400 CPU(3.00 GHz),操作系统 ubuntu-10.04 上运行相关算法,结果显示在 G_1 上的乘法平均运行时间为 0.016 ms,在 G_1 和 G_2 上的指数平均运算时间分别是 3.886 ms 和 0.489 ms,双线对的平均运行时间为 4.354 ms. 总结如表 2 所示:

Table 2 Cost Time of Some Algorithms

表 2 运算消耗时间

Algorithm	Cost Time/ms
Scalar Multiplication Over G_1	0.016
Modular Exponentiation Over G_1	3.886
Modular Exponentiation Over G_2	0.489
Tate Pairing	4.354

无线传感器网络中根据以上计算复杂度和相关算法运行的时间分析,我们的方案和前期 4 种研究成果的时间消耗对比分析如图 3 所示.

从图 3 可以看出协议运行时间最长为张磊等人[25] 提出的方案. 其次是 Chen 等人[24] 方案这 2 种方案的运行时间远远比其他 3 种方案消耗时间长. 运行时间最短的是 Lee 等人[22] 和本文提出的协议,这 2 种协议运行时间相当.

从协议的能量消耗上分析,本文把群组密钥协商所消耗的总能量简单地量化成群组成员在协商过程中的计算量消耗和通信量消耗的总和. 不失一般性,根据文献[21]提供的资料,一个 133 MHz "Strong ARM"微处理器执行一个模幂运算需要消耗 9.1 mJ 能量,执行一个纯标量乘法运算需要消耗 8.8 mJ 能量,执行一个 Tate 对运算需要消耗 47 mJ 能量. 一个 IEEE 802.11 频谱 24 WLAN 卡发送 1 b 信息需要消耗 0.66 μm 能量,其接收 1 b 信息需要消耗 0.31 μm 能量,如表 3 所示:

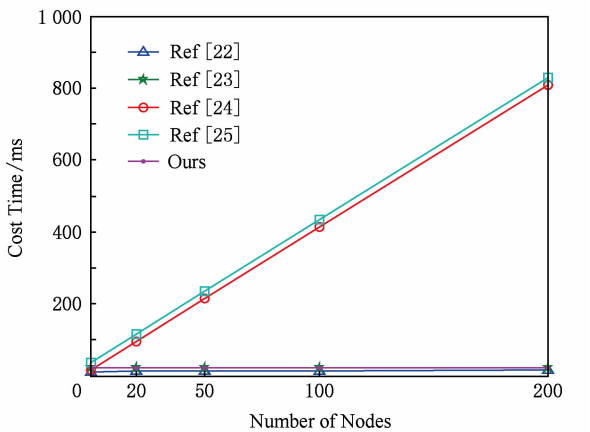

Fig. 3 The time cost of the five protocols

图 3 5 种协议运行时间对比

Table 3 Energy Costs for Computation and Communication

表 3 计算与通信能量消耗

Type of Communication	Energy Costs/mJ
Computation Cost of Modular Exponentiation	9.1
Computation Cost of Scalar Multiplication	8.8
Computation Cost of Tate Pairing	47.0
Communication Cost for Transmitting 1 bit	0.66×10^{-3}
Communication Cost for Receiving 1 bit	0.31×10^{-3}

假设群组密钥协商协议在有限域 F_p 上交换一个单位信息的信息长度为 1 024 b. 由于传统加密方法用 1 024 b 长度的密钥加密信息的安全度等同于椭圆曲线加密方法采用 160 b 长度的密钥加密的安全性. 假设基于椭圆曲线加密方案的群组密钥协商协议的单个信息量为 160 b. 由于这 5 个有效的协议均为 160 b 的加密密钥. 设每个信息量的大小为 160 b,则这 5 个协议的计算消耗如图 4 所示:

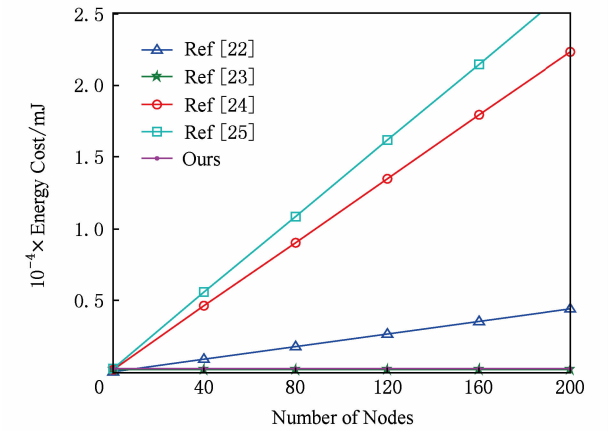

Fig. 4 Computation cost of the unauthenticated protocols

图 4 协议计算所消耗能量

由图 4 可以看出,计算消耗能量最大的为张磊等人[25]提出的协议,计算消耗能量最低的为 Tsai 等人[23]及本文提出的协议,两者的计算能量消耗线几乎重叠. Chen 等人[24]和张磊等人[25]计算量消耗的原因是因为其计算量随着参与群组密钥协商的成员数量的增加而增加,且幂指数计算消耗能量较大.

通信能量消耗如图 5 所示,Lee 等人[22],Tsai[23]与本文这 3 种方案的通信能量消耗相当,通信消耗曲线几乎重合,通信消耗较少,具有明显的优势. Chen 等人[24]方案通信消耗较大.

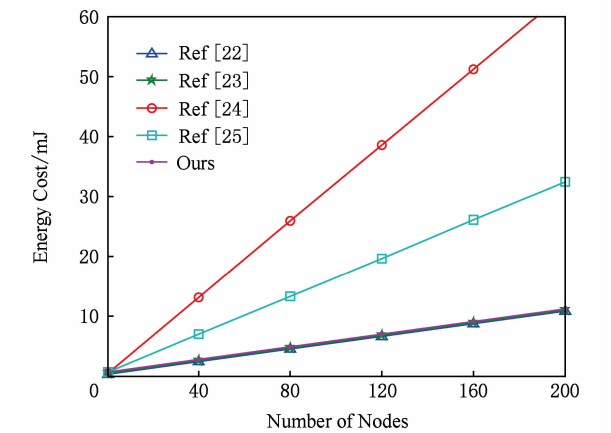

Fig. 5 Communication cost of the unauthenticated protocols

图 5 协议通信所消耗能量

总能量消耗分析如图 6 所示,Chen 等人[24]及张磊等人[25]这 2 种方案的总能耗随着群组成员的规模增大上升较快,因此不适用于大规模的群组密钥协商协议. Tsai[23]及本文协议总能量消耗处于明显优势,该方案适用于大规模的大规模群组密钥协商协议,如网格计算及云计算等大型分布式协同计算. 但本文方案与 Tsai[23]具有较大性能的优势体现在,本文方案是可认证的非对称群组密钥协商,与对称群组密钥协商相比具有加大的灵活性和较高的安全性.

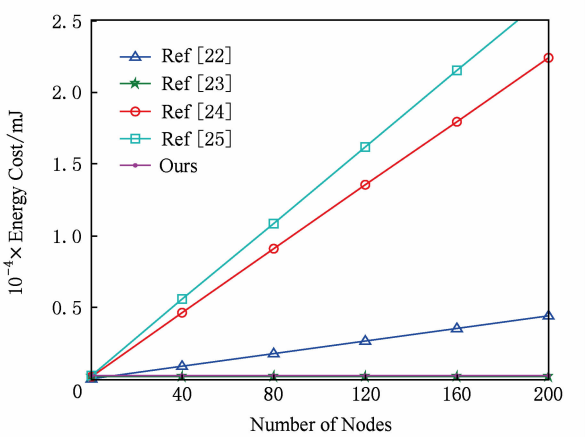

Fig. 6 Total energy cost of the authenticated protocols

图 6 总能量消耗

4 总 结

分析了现有的群组密钥协商协议的方案,为适用新型网络应用需求,如移动云计算网络、无线传感器网络等,其网络终端易受攻击、网络节点资源受限、计算能力和通信范围有限等特性,提出跨簇非对称群组密钥协商协议,即传感器节点的信息交换采用非对称密码体制,具有更高的安全性和灵活性;跨簇群组密钥协商使得通信范围有限的资源节点更容易扩展簇间协同计算的范围;采用了非对称计算,使得传感器节点承担轻量级的计算及通信量. 经证明和分析验证了协议的安全性及能耗性能具有较好的优势.

参 考 文 献

[1] Pan Yun, Wang Licheng, Cao Zhenfu, et al. Lite-CA based key pre-distribution scheme in wireless sensor network [J]. Journal on Communications, 2009, 30(3): 130-134 (in Chinese)

(潘耘, 王励成, 曹珍富, 等. 基于轻量级 CA 的无线传感器网络密钥预分配方案[J]. 通信学报, 2009, 30(3): 130-134)

[2] Xia Geming, Huang Zunguo, Wang Zhiying. A key pre-distribution scheme for wireless sensor networks based on the symmetric balanced incomplete block design [J]. Journal of Computer Research and Development, 2008, 45(1): 154-164 (in Chinese)
(夏戈明, 黄遵国, 王志英. 基于对称平衡不完全区组设计的无线传感器网络密钥预分配方案[J]. 计算机研究与发展, 2008, 45(1): 154-164)

[3] Huang Haiping, Wang Ruchuan, Sun Lijuan, et al. Key distribution scheme of wireless sensor networks based on logic grid [J]. Journal on Communications, 2009, 30(8): 131-140 (in Chinese)
(黄海平, 王汝传, 孙力娟, 等. 基于逻辑网格的无线传感器网络密钥分配方案[J]. 通信学报, 2009, 30(8): 131-140)

[4] Bechkit W, Challal Y, Bouabdallah A, et al. A highly scalable key pre-distribution scheme for wireless sensor networks [J]. IEEE Transactions on Wirelss Communications, 2013, 12(2): 948-959

[5] Monjul S, Irani A, Hussain M A. A review on desirable measures for good key pre-distribution scheme in wireless sensor network [C] //Proc of Int Conf on Green Computing and Internet of Things. Piscataway, NJ: IEEE, 2016: 129-134

[6] Tseng Y M. A resource-constrained group key agreement protocol for imbalanced wireless networks [J]. Computer Security, 2007, 26(4): 331-333

[7] Zhang Qikun, Zhang Quanxin, Ma Zhongmei, et al. An authenticated asymmetric group key agreement for imbalanced mobile networks [J]. Chinese Journal of Electronics, 2014, 23(4): 827-835

[8] Cheng Qingfeng, Ma Changui, Wei Fushan. Analysis and improvement of a new authenticated group key agreement in a mobile environment [J]. Annals of Telecommunications, 2011, 64(11/12): 331-337

[9] Zhang Qikun, Yuan Junling, Guo Ge, et al. An authentication key establish protocol for WSNs based on combined key [J]. Wireless Personal Communication, 2018, 99(1): 95-110

[10] Zhang Qikun, Tan Yu'an, Zhang Li, et al. A combined key management scheme in wireless sensor networks [J]. Sensor Letters, 2011, 9(4): 1501-1506

[11] Teng Jikai, Wu Chuankun. Efficient group key agreement for wireless mobile networks [C] //Proc of the IET Int Conf on Wireless Sensor Network. Herts, UK: IET, 2010: 323-330

[12] Thomas R H, Thomas A C, Keith M C, et al. Energy-efficient group key agreement for wireless networks [J]. IEEE Transactions on wireless Communication, 2015, 14(10): 5552-5564

[13] Walid A, Noureddine B. An efficient and scalable key management mechanism for wireless sensor networks [J]. ICACT Transactions on Advanced Communications Technology, 2014, 3(4): 480-493

[14] Wu Qianhong, Mu Yi, Susilo W, et al. Asymmetric group key agreement [C] //Proc of the 28th EUROCRYPT 2009. Berlin: Springer, 2009: 153-170

[15] Wu Qihong, Zhang Xinyu, Tang Ming, et al. Extended asymmetric group key agreement for dynamic groups and its applications [J]. China Communications, 2011, 8(4): 32-40

[16] Zhang Lei, Wu Qianhong, Qin Bo, et al. Identity-based authenticated asymmetric group key agreement protocol [G] //LNCS 6196: Proc of Int Computing and Combinatorics. Berlin: Springer, 2010: 510-519

[17] Zhang Qikun, Li Yuanzhang, Song Danjie, et al. Alliance authentication protocol in clouds computing environment [J]. China Communications, 2012, 9(7): 42-54

[18] Zhao Xingwen, Zhang Fangguo, Tian Haibo. Dynamic asymmetric group key agreement for ad hoc networks [J]. Ad Hoc Networks, 2011, 9(5): 928-939

[19] Xu Chang, Li Zhoujun, Mu Yi, et al. Affiliation-hiding authenticated asymmetric group key agreement based on short signature [J]. Computer Journal, 2014, 57(10): 1580-1590

[20] Lü Xixiang, Li Hui, Wang Baocang. Authenticated asymmetric group key agreement based on certificateless cryptosystem [J]. International Journal of Computer Mathematics, 2014, 91(3): 447-460

[21] Zhang Qikun, Wang Ruifang, Tan Yu'an. Identity-based authenticated asymmetric group key agreement [J]. Journal of Computer Research and Development, 2014, 51(8): 1727-1738 (in Chinese)
(张启坤, 王锐芳, 谭毓安. 基于身份的可认证非对称群组密钥协商协议[J]. 计算机研究与发展, 2014, 51(8): 1727-1738)

[22] Lee C C, Lim T H, Tsai C S. A new authenticated group key agreement in a mobile environment [J]. Annals of Telecommunications, 2011, 64(11/12): 735-744

[23] Tsai J L. A novel authenticated group key agreement protocol for mobile environment [J]. Annals of Telecommunications, 2011, 64(11/12): 663-669

[24] Chen Yong, He Mingxing, Zeng Shengke, et al. Universally composable asymmetric group key agreement protocol [C] //Proc of the 10th Int Conf on Information, Communications and Signal Processing (ICICS). Piscataway, NJ: IEEE, 2015: 1-6

[25] Zhang Lei, Wu Qianhong, Josep D F. Round-efficient and sender-unrestricted dynamic group key agreement protocol for secure group communications [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(11): 2352-2364

[26] Wei Guiyi, Yang Xianbo, Jun Shao. Efficient certificateless authenticated asymmetric group key agreement protocol [J]. KSII Transactions on Internet and Information System, 2012, 6(12): 3352-3365

Zhang Qikun, born in 1980. PhD. His main research interests include information security and cryptography.

Gan Yong, born in 1965. PhD, professor, senior member of CCF. His main research interests include multimedia communications, image processing, coding and network engineering.

Wang Ruifang, born in 1982. Master, Her main research interests include information security and cryptography.

Zheng Jiamin, born in 1975. PhD. His main research interests include information security and cloud computing.

Tan Yuan, born in 1972. PhD, professor. His main research interests include information security and network storage.