基于动态多簇密钥管理模型的安全数据聚合方案

雷凤宇[1,2] 秦玉化[2] 陈文鑫[2] 陈 晶[3]
(华中科技大学计算机学院信息安全系 武汉 430074)[1]
(广州军区75741部队 广州 510510)[2] (武汉大学计算机学院 武汉 430079)[3]

摘 要 军事领域需要强有力的安全措施,但由于环境恶劣,缺乏物理保护,难以展开固定的通信设施。设计了一种基于身份的动态多簇密钥管理模型。该模型以簇为单位进行密钥管理,每个成员节点只需存储本簇的公钥因子矩阵,极大地节省了密钥存储空间,且可抵抗同谋攻击;密钥分发过程安全高效,节点加入和退出时密钥更新开销小;不依赖可信第三方便可实现身份认证,且不需要固定基础设施的支持。基于该模型提出了一种安全数据聚合方案。列举了部分可以抵御的攻击;讨论了该方案握手过程需要消耗的能量。结果显示,在新模型下将公钥密码体制用于无线传感器网络是可行的。

关键词 无线传感器网络,数据聚合,基于身份的公钥密码体制,密码系统
中图法分类号 TP309 **文献标识码** A

Data Aggregation Security Solution Based on Key Management Scheme of Dynamic Multi-cluster

LEI Feng-yu[1,2] QIN Yu-hua[2] CHEN Wen-xin[2] CHEN Jing[3]
(College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan 430074, China)[1]
(PLA 75741 Troops Guangzhou, Guangzhou 510510, China)[2]
(Computer School, Wuhan University, Wuhan 430079, China)[3]

Abstract A dynamic multiple cluster key management model based on identity was designed in wireless sensor network. The key management in the model is cluster-based. Every node in the network is just required to store its private key and the public key factor matrix of the cluster that it belongs to, which consumes little storage space and can resist the collusion attack. The key distribution is secure and effective. It costs little during the node joining and leaving. And it realizes the identity authentication independent of the third party and has no use for infrastructure to sustain the key distribution center. A secure data aggregation solution based on the model was proposed. Security of the proposed solution was analyzed and some attacks that can be resisted were listed. The energy consumption during the handshaking process was discussed, which indicates that it is feasible to use the identity-based cryptography in the wireless sensor networks.

Keywords Wireless sensor networks, Data aggregation, IBE, Cryptography

1 引言

无线传感器网络是具有密集性以及随机分布等特点的特殊网络,因而十分适合于恶劣的战场环境,包括侦察敌情、监控兵力、装备和物资;判断生物化学攻击等多个方面。那么如何保证无线传感器网络的安全性是其业务功能得以施展的重要基础和保障,是一个重要论题。与其他网络一样,无线传感器网络的安全性主要包括以下几个部分:数据机密性、真实性、完整性、鲁棒性和残存性。由于传感器网络的固有特性,要实现这些安全目标,挑战和机遇并存。

无线链路的应用使得无线传感器网络首先易于受到主动攻击(例如:伪装攻击、重放攻击、信息的篡改和破坏等)和被动攻击(例如:监听、通信量分析)。其次,在恶劣的环境中,如战场环境下,无线传感器几乎没有任何物理保护,无线传感器的安全问题不仅需要考虑来自网络外部的恶意攻击,也应该考虑内部恶意节点发动的攻击。无线传感器网络中,中心实体容易存在漏洞,因此一旦中心节点妥协了,整个网络就可能瘫痪,所以为了获得高安全性,无线传感器网络需要使用无中心实体的分布式体系结构。最后,无线传感器网络通常由大量密集的传感器节点部署而成。由于传感器节点能量有限,一旦能量耗尽,传感器节点就会死亡,因此传感器网络在拓扑结构和其成员构成方面都是动态变化的,所以无线传感器网络的安全方案必须适合于大型网络且适合节点更新。

目前通常使用基于密码的协议来保证无线传感器的安全

到稿日期:2010-10-19 返修日期:2011-02-01 本文受国家自然科学基金(60903175,60903196和60703048)资助。
雷凤宇(1980—),女,博士生,主要研究方向为公钥密码、可证明安全性、密码学理论和实践等,E-mail:4485179@qq.com,秦玉化(1979—),男,主要研究方向为信息安全等;陈文鑫(1980—),男,工程师,主要研究方向为信息安全等;陈 晶(1981—),男,研究生,主要研究方向为信息安全、密码学、无线传感器网络。

性。由于基于密码的协议包括计算开销、存储开销和通信开销，而传感器节点资源有限且受能量制约，因此无线传感器网络对密码体制的选择有更严格的要求。基于对称密钥密码体制的协议消耗能量较少，但是难以安全地进行密钥分发；基于公钥密码体制的协议在密钥建立和分发方面具有较好地优势，但是需要较多的计算、存储和通信开销。近年来，一些基于密码的协议应用于不同的传感器网络。文献[1,2]针对分布式传感器网络提出了几个密钥建立方案，然而其计算开销比较大，且中间节点必须解密其收到的信息，再应用相应的聚合函数，加入其个人的聚合数据，加密之后再将加密结果进行转发。文献[3,4]提出了同态加密密码，该协议在转发过程中无需解密，然而该方案无法提供邻居节点间的安全保证。目前无线传感器网络的安全研究主要集中在对称密码算法上，但是在一个大型传感器网络中，由于资源制约，节点无法存储所有的密钥对。为了解决这个问题，基于密钥池的随机预分配方案提出了简单的密钥分配方法[5]。随机预分配方案分配方法简便，但是其具有几个缺点：一是节点间不能保证安全连通，连通概率与节点密钥存储量、抗俘获能力成正比；二是每个节点中存放了大量无用的密钥，浪费节点内存，而且冗余的信息使敌人在攻破少数的节点后就可获得较大份额的密钥，被俘虏的节点抗毁性差；三是不同的节点对之间可能建立相同的会话密钥，导致密钥冲突，而有一些节点对却不存在共同密钥，从而无法建立会话密钥。

1984 年，Shamir 提出了基于身份的加密方案(Identity-Based Encryption，IBE)[6]，其初始动机是简化 E-mail 系统中的认证管理。IBE 方案允许任何通信双方安全通信，且不需要询问公钥就可以实现签名的验证。此外，该方案不需要保存密钥目录，不依赖可信的第三方提供认证服务。2001 年，Dan Boneh 等人提出了第一个基于身份的实用系统[7]。文献[8]于 2003 年提出了一种基于 IBE 的密钥管理方法。文献[9]提出了一种非双线性映射下的安全 IBE 方案。文献[10]提出了一种分等级的 IBE 系统。IBE 系统不需要固定基础设施的支持，却可以实现类似于 PKI 的安全服务。但是 IBE 系统在抵制同谋攻击方面没有高效的解决方法，目前的研究都是通过双线性映射抵制同谋攻击，而其计算开销非常大，无法直接用于传感器网络。

文献[11]提出了两种安全数据聚合方法：CPDA 和 SMART。然而这两种方案都无法获得良好的鲁棒性。CPDA 对于簇的大小有严格的要求，该方案只有在簇成员为 3～5 个时，才能获得较好的安全性和较高的通信效率。一旦簇成员增加，其多项式的计算开销就急剧上升，无法适应于大型的分布式传感器网络。SMART 将聚合数据分成数据片，再将数据片经不同路由进行传输，从而获得其安全传输，然而该方案只有在数据分片为 2～4 片时方可获得较好地性能，随着数据分片的增加，通信开销急剧增加。文献[12]提出了一种密钥管理协议——基于身份的对称密钥协议，该协议较好地适应于某一类网络，然而无法应用于大型的传感器网络。总之，对于恶劣战争环境下的大型传感器网络，目前仍然没有合适的、既能提供安全服务又不需要基础设施作为密钥分发中心的安全数据聚合方法。

本文设计了基于身份的动态多簇密钥管理模型，并基于该机制提出了一种新型的安全数据聚合方案，该方案适合于大型的分布式无线传感器网络。与已有的安全数据聚合方案相比，新方案具有以下优点：(1)提出基于身份的动态簇密钥管理模型，各簇头充当密钥代管中心，具有较好的灵活性和自主性，能有效抵制合谋攻击。(2)该方案能较大地节约密钥存储空间。即便在大规模的传感器网络中，每个成员节点只需少量的存储空间存储公钥因子矩阵，且可获得任何节点的公开密钥。(3)该方案便于传感器节点的加入和退出，当一个节点加入或退出时，密钥更新开销很小。(4)该方案使用对称密钥作为会话密钥，而使用基于身份的密码体制建立会话密钥，完成握手过程。(5)该方案不依赖可信任第三方便可提供身份认证，不需要固定基础设施的支持。

2 提出的动态多簇密钥管理模型

目前，基于身份的加密系统中，合谋攻击问题难以得到有效解决。本文采用组合公钥的思想，提出了基于身份的动态多簇密钥管理模型，该模型按照一定的属性规则，将大型网络划分为多个簇，各簇头充当密钥代管中心，实行自主管理。动态多簇密钥管理模型有几个优点：一是各节点只需存储各自的私钥和本簇的公钥因子矩阵，极大地节约了密钥存储空间；二是公/私钥因子矩阵更新方便，即便某个私钥因子矩阵泄露，只需要更换该簇的公/私钥因子矩阵，而不会影响整个传感器网络的稳定性；三是即便传感器网络中所有节点共谋，私钥因子矩阵仍然不会泄漏；四是通过各簇独立管理，增强了自主性、灵活性和实用性。

安全中心主要由密钥生成中心、身份认证中心、密钥分发中心和密钥撤销中心组成 。密钥的生成和管理都是集中的。密钥生成中心产生公/私钥因子矩阵。身份认证中心受理身份认证。

2.1 密钥生成

在本模型中，为了节约存储空间，提高计算效率，使用基于椭圆曲线的因子矩阵生成公/私钥对。私钥由传感器节点各自保存，公钥因子矩阵公开。为了保证其安全性，密钥生成中心离线产生和保存私钥因子矩阵。

以下阐述公/私钥的生成。

令 $T=\{g,G,q\}$，g 为大素数 q 阶椭圆曲线加法群 G 的生成元。密钥生成中心生成公/私钥因子矩阵，其私钥因子矩阵保密，而公钥因子矩阵公开。假设公/私钥因子矩阵为 $m\times n$ 矩阵，则私钥因子矩阵 SSK 和公钥因子矩阵 PSK 如下：

$$SSK=\begin{pmatrix} k_{1,1} & \cdots & k_{1,n} \\ \vdots & \ddots & \vdots \\ k_{m,1} & \cdots & k_{m,n} \end{pmatrix}$$

$$PSK=\begin{pmatrix} k_{1,1}\cdot g & \cdots & k_{1,n}\cdot g \\ \vdots & \ddots & \vdots \\ k_{m,1}\cdot g & \cdots & k_{m,n}\cdot g \end{pmatrix}$$

用户的公钥由唯一标识符决定。根据公/私钥因子矩阵，可以采用映射算法计算公/私钥如下。假设 ID_A 是成员节点 A 的唯一标识符，$\{H_1,H_2,\cdots H_n\}$ 为 n 个不同的哈希算法。

根据哈希算法和唯一标识符，A 对 $\forall i\in\{1,\cdots,n\}$ 计算

$map_i = H_i(ID_A)$，并根据私钥因子矩阵 SSK 可以得到私钥：$SK_A = (k_{map_1,1} + k_{map_2,2} + \cdots + k_{map_n,n}) \bmod q$。由于公钥因子矩阵是公开的，任何人都可以计算 A 的公钥。

就其安全性而言，显然，给定 $k \cdot g$，其中 $k \in \mathbb{Z}_q$ 随机选取，当群 G 的规模足够大时，计算 k 是不可行的。故给定公钥因子矩阵，敌手无法计算出私钥因子矩阵。本方案的安全性主要取决于私钥因子矩阵，故保证私钥因子矩阵的安全性非常重要。为了抵抗合谋攻击，基于因子矩阵的 IBE 系统中用户数必须小于公钥因子矩阵的元素个数，即在 $m \times n$ 阶矩阵中，用户数 $< mn$。以 ECC-160 为例，当系统用户数达到 100 万个时，各用户需存储约 20MB 的公钥因子矩阵。显然在大型传感器网络中，将由于公钥因子矩阵过大而无法直接应用该加密系统。

2.2 动态多簇基本模型

在基于因子矩阵的 IBE 系统中，对于 $m \times n$ 阶矩阵，用户数必须 $< mn$，才能有效抵制合谋攻击。为了节约存储空间，且能抵抗合谋攻击，作者根据无线传感器网络的特点，设计了动态多簇密钥管理模型，将大型网络以簇为单位进行密钥分发和管理。以 100 万成员节点为例，在传感器网络中，由于每个节点能量有限、传输半径小，在实际通信中，每个普通节点通信的用户通常只是所有节点中一个很小的子集。假设任意节点都存储 100 万个用户的公钥因子矩阵，则势必造成大量存储数据的冗余。故可将传感器网络按照某种属性（如地理位置或通信关联性）划分成多个簇，各簇有自己的公/私钥因子矩阵，簇头充当密钥代管中心，负责管理本簇内的事务，而每个传感器节点只需存储其所在簇的公钥因子矩阵，既减少了每个成员节点需要存储的公钥因子矩阵，又可以获得整个网络的安全性。基于公钥因子矩阵的多簇基本模型具体方案如下。

1）符号说明。所有用户按照簇结构进行划分，设传感器网络划分成 r 个簇 $F(C_1, C_2, \cdots, C_r)$，C_j，$(j \in 1, \cdots, r)$ 表示簇头），$F(C_j)$，$(j \in 1, \cdots, r)$ 表示一个簇。簇头 C_j 充当本簇的密钥代管中心。令簇 $F(C_j)$ 的公/私钥因子矩阵为 SSK_j / PSK_j，公开参数为：$PubP_j = \{g, G, q, PSK_j\}$。设簇 $F(C_j)$，$(j \in 1, \cdots, r)$ 共有 v 个成员节点。令 $\forall i \in 1, \cdots, v$，簇内所有成员唯一标识符的集合为：$T(ID_{A_i}) = \{ID_{A_1}, \cdots, ID_{A_v}\}$。通过 ID 号计算各自的私钥因子为：$T(SK_{A_i}) = \{SK_{A_1}, SK_{A_2}, \cdots, SK_{A_v}\}$，令簇中节点 A_i 与安全中心之间的会话密钥为 $k_{A_i,S}$，使用各自与安全中心的会话密钥加密各用户的私钥得：$T(Enc_{SK_{A_i}}) = \{\{SK_{A_1}\}k_{A_1,S}, \{SK_{A_2}\}k_{A_2,S}, \cdots, \{SK_{A_v}\}k_{A_v,S}\}$。令 r 个簇头的公钥信息为：$T(PK_j) = \{PK_1, \cdots, PK_r\}$。

2）身份认证。假设一个节点 A_i 要加入该网络，它可以使用其唯一标识符 ID_{A_i} 提交申请，身份认证中心收到申请后，验证其身份信息，如果该节点合法，则密钥分发中心离线分发一个对称密钥 $k_{A_i,S}$ 给该节点，作为该节点今后与安全中心通信的会话密钥。

3）簇的构建。每个传感器节点以概率 p 推荐自己做簇头[13]，并且发送广播信息。广播信息转发到距离簇头 k 跳内的所有节点。当传感器收到信息，如果自己不是簇头，则加入该簇；如果自己是簇头，且本簇只有一个成员，则也加入该簇。在这个网络中，簇中的任意成员距离簇头最远 k 跳。显然，簇头可以以 t 为间隔时间向处理中心转发聚合信息（其中，t 是数据转发 k 跳所需要的时间，也就是通信周期）。

4）密钥分发。密钥分发共分为 4 步。①密钥代管中心 C_j 加密本簇所有成员的唯一标识符得 $\{T(ID)\}k_{C_j,S}$，并发送到安全中心请求本簇成员密钥分配。②安全中心经过身份验证后，按照 2.1 节给出的密钥生成算法产生公/私钥因子矩阵 SSK_j / PSK_j，并计算 $T(Enc_{SK_{A_i}})$，公/私钥因子矩阵的阶 $m \times n > v$ 且必须有部分密钥因子冗余以便于新成员加入。③公/私钥因子矩阵生成后，安全中心加密该簇的密钥相关信息得 $\{T(PK_j), PubP_j, T(Enc_{SK_{A_i}})\}k_{C_j,S}$，并将其传输到密钥代管中心 C_j。④C_j 公布本簇公开参数 $PubP_j$，并将本簇成员的私钥信息 $\{SK_{A_i}\}k_{A_i,S}$ 分发给各普通用户，各用户使用 $k_{A_i,S}$ 解密获得私钥，如图 1 所示。

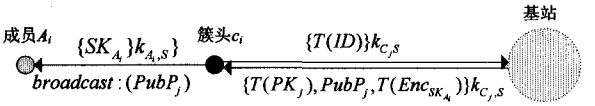

图 1 密钥分发流程图

每个簇头需要保存本簇的公钥因子矩阵和各簇头的公钥，每个普通节点仅需要存储其私钥和所在簇的公钥因子矩阵。

5）用户间通信：实现簇内用户和跨簇间用户通信。当簇内通信时，用户根据公钥因子矩阵和公开参数直接进行通信；当跨簇通信时，用户 A 提交接收方 B 的身份信息 ID_B 给本簇的密钥代管中心 C_j，C_j 通过 B 所在的簇密钥代管中心获得 B 的公钥信息，A 利用 B 的公钥实现跨簇通信。

2.3 握手

由于公钥密码体制消耗能量较多，故本文中在方案设计方面在保证安全性的同时，尽量减少公钥密码的使用，本文在会话密钥建立过程中，仅在第一步使用公钥密码体制。假设节点 A 和节点 B 需要建立会话密钥，则其握手过程如下。

1）A 生成随机对称加密密钥 k_{ab}，使用 B 的公钥加密 k_{ab}，再使用自己的私钥对密文签名，最后发送结果给节点 B，其中 B 的公钥可通过 B 的唯一标识符和公钥因子矩阵计算获得。

2）B 验证签名后，解密获得 k_{ab}。B 向 A 发送确认信息，该信息使用会话密钥 k_{ab} 进行加密。

最后，A 和 B 使用 k_{ab} 作为会话密钥。显然，因为加密方案是基于唯一标识符的，密钥协商过程能有效地建立会话密钥，且能抵制各种攻击（如中间人攻击等）。

3 提出的基于动态多簇密钥管理模型的数据聚合方案

会话密钥建立后，两个节点可以通过已建立的会话密钥进行通信，从而实现数据聚合。在本节中，数据聚合协议由三个部分构成：簇内保密数据聚合、簇间数据聚合以及节点的加入和退出。

3.1 簇内的保密数据聚合

令节点 B 是簇头，节点 A 是簇内的成员。当 A 向簇头 B 发送保密数据时，A 和 B 之间的路径可能有两种情况：单跳

路由或多跳路由。同一簇内任何节点的公钥均可使用该节点的唯一标识符，通过本簇的公钥因子矩阵计算获得。

3.2 簇数据聚合

当簇头收集到各簇敏感数据后，需要将数据聚合后发送到信息处理中心。在密集型无线传感器网络中，相邻节点可能重复采集到同一信息，为了节省有限的资源，减少转发的数据量，簇头有必要将簇内信息进行融合和压缩。本文中簇头可以解密获得簇成员收集的数据，运用数据融合技术将采集的信息进行归类压缩，采用路由树建立路由，路由转发过程中，若通信双方在同一个簇，则可以直接计算获得对方的公钥信息；若通信双方不在同一个簇内，则按照 2.2 节给出的用户间通信算法获得对方节点的公钥并进行簇间通信。

3.3 节点加入和退出

无线传感器能量机器有限，维持通信时间较短，有些情况下，部分节点能量已经耗尽而指定的任务尚未完成，此时，需要部署新的节点代替已死亡节点。本方案便于节点的加入和退出。

1)节点加入。当一个节点 A_i 加入时，安全中心验证其身份，并分配会话密钥 $k_{A_i,S}$，当其加入到某个簇后，其所在簇 $F(C_j)(j\in 1,\cdots,r)$ 的簇头 C_j 向安全中心发送密钥请求信息，安全中心根据该簇的私钥因子矩阵、该成员的唯一标识符 ID_{A_i} 和哈希算法 $\{H_1,H_2,\cdots,H_n\}$ 计算用户的 n 个哈希值 $map_1=H_1(ID_{A_i}),\cdots,map_n=H_n(ID_{A_i})$，然后通过簇 $F(C_j)$ 的私钥因子矩阵 SSK_j 计算私钥 $SK_{A_i}=(k_{map_1,1}+k_{map_2,2}+\cdots+k_{map_m,n}) \bmod q$，并将 $\{SK_{A_i}\}k_{A_i,S}$ 传送给 A_i。其相应的公钥可以通过其所在簇的公钥因子矩阵计算得出，公钥因子矩阵无需改变。

2)节点退出。假设一个节点死亡或作废，密钥撤销中心宣布私钥取消并保存节点标识，用于处理以后可能发生、需要仲裁的事件，最后广播撤销消息：

$S\rightarrow broadcast:\{revoke,cert_r\}K_S^{-1}$

若死亡或作废节点为簇密钥代管中心，则按照 2.2 节的规则重新选举新的簇密钥代管中心，负责本簇密钥管理。因为簇成员私钥各自保存，故即便簇密钥代管中心节点叛变，也无需重新生成公/私钥因子矩阵。

4 安全性分析

无线传感器节点通常部署在恶劣危险的环境中，缺乏物理保护。其安全性异常重要。

在战场环境下，节点所收集和传输的信息都是高度机密信息。为了保护机密信息的安全性，标准方法是使用传输双方共知的密钥进行加密。下面基于安全目标讨论本方案的安全性。

数据机密性：本文中，应用公钥密码体制建立会话密钥，保证密钥交换过程的安全性，然后使用建立的对称密钥加密敏感数据。“被动信息收集”是无线传感器网络中的一种典型攻击。敌手通过分析信息拦截数据流，根据分析数据内容，定位节点位置，毁坏节点，获取信息 ID、时间戳等信息。本文中通过强加密技术能将“被动信息收集”攻击的威胁降到最小。

数据真实性：由于传感器网络通常都部署在开放式环境中，敌手可以轻易地将恶意节点部署到网络中。这些节点消耗大量的能量资源，且可向无线传感器网络注入恶意代码。本文使用基于身份认证的安全方案，任何未认证的实体或非法节点都不可能注入恶意信息。故本文方案能有效抵制这一类攻击，如“睡眠剥夺”攻击[14]。

数据完整性：数据完整性保证数据在传输过程中不被敌手篡改，而数据真实性的验证过程即可确保数据的完整性。

数据新鲜性：数据新鲜性确保数据不会被敌手重放。本文使用时间戳抵制“重放攻击”和“虫洞攻击”[15]。

鲁棒性和残存性：军事用途的传感器网络需要有好的鲁棒性以应对各种安全攻击。鲁棒性好的方案，敌手一次攻击的得手或单个节点的妥协都不会破坏整个网络的安全性。本方案中，由于对任何簇 $F(C_j)$，其密钥因子矩阵阶数均大于该簇的成员节点数($mn>v$)，故即便所有节点共谋，仍然不会导致密钥因子矩阵泄漏，由此可推出某一个节点被俘，整个网络的安全性仍然可以保证。因此本方案可以有效抵制“单节点颠覆”攻击。

“女巫攻击”[16](单个节点对外冒充多个身份)：是严重威胁无线传感器网络安全的攻击。由于身份认证和加密技术可以阻止外部的“女巫攻击”，公钥密码体制可以阻止来自内部的“女巫攻击”，因此本文中节点间通过采用基于身份的公钥密码体制协商密钥和使用会话密钥加密的信息聚合，可以完美地阻止“女巫攻击”。

5 能量分析

本章主要做了仿真：一是针对目前对于公钥密码体制无法应用于无线传感器网络的偏见，在 8-bit 微控制器平台下仿真了新方案中公钥密码体制的能量消耗，结果显示，在本文提出的动态多簇密钥管理模型下，新数据聚合方案中使用的公钥密码体制在计算、存储和通信方面是完全可行的。

无线传感器网络计算能力、存储能力和能量等均非常有限。资源的严格限制制约了公钥密码体制在无线传感器网络中的应用。基于无线传感器网络设备无法承受公钥密码体制开销的假定，目前，几乎没有公钥密码体制用于提供无线传感器网络的安全保证[17]。然而，基于对称密钥的密码系统无法提供与公钥密码系统媲美的安全服务。前面已提到，本文所提的新方案只需少量的公钥存储空间。故本方案只需就计算开销和能量开销进行详细的讨论和验证。近年来的研究显示，在 8-bit 微控制器中，运行公钥密码体制在计算开销上是可行的[18]。文献[19]讨论了基于公钥密码体制的密钥交换和认证过程所需的能量开销。本文在 8-bit 微控制器平台下进行仿真。由于新方案是基于身份的，每个节点都有唯一标识符，且通过其唯一标识符生成公/私钥对，故本文中，认证过程在密钥交换过程即可获得，且公钥密码体制仅用于密钥交换过程中的一步。本文采用椭圆曲线密码体制，因此在整个握手过程中，总能量主要包含：公钥计算、握手信息的传输和接收、哈希计算以及随机数生成，其中公钥的计算为主要开销，其次是通信开销。

将电池容量的一定比例用于握手过程，在不同电池容量下得到能完成的握手过程次数，并通过结果可以分析在能量

有限的传感器网络中应用公钥密码系统的可能性。电池容量的5%或10%用于握手时完成的握手次数如图2所示。

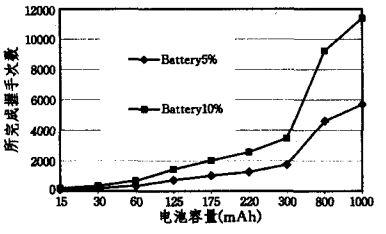

图2 电池容量的5%或10%用于握手时完成的握手次数

握手过程和随后传输数据所需的能量开销对比如图3所示。由图可看出:随着传输的总数据量的增加,握手过程的能量消耗所占比重都逐渐下降。当总传输量达到64kB时,握手过程的能量消耗几乎可以忽略不计。方案通过合理的设计,既保证了方案安全性,又在能量开销方面有明显优势,更适用于无线传感器网络应用。

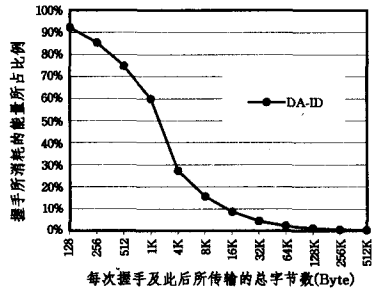

图3 握手过程和其随后数据聚合所需的能量开销对比

结束语 本文提出了基于身份的动态多簇密钥管理模型。该模型以簇为密钥管理的基本单位,将簇头作为密钥代管中心,负责管理本簇内的公钥信息,并提供跨域认证。而簇成员的私钥由各成员各自掌握,簇头无需掌握簇成员的私钥信息;多簇动态密钥管理模型巧妙地运用对称密码体制进行节点私钥分发,并使用公钥密码体制建立通信时过程使用的会话密钥,可实现安全密钥分发和认证服务;每个普通成员节点只需存储节点与安全中心的会话密钥、自己的私钥和本簇的公钥因子矩阵,簇头(密钥代管中心)还需存储所有簇头的公钥信息。该模型使用分簇的公/私钥因子矩阵,极大地节约了密钥存储空间;可以实现与PKI等同的安全认证且无需部署固定的基础设施。

基于动态多簇密钥管理模型提出了一种安全数据聚合方案。从数据机密性、真实性、完整性、鲁棒性和残存性等方面分析了新方案的安全性,且列举了部分可以抵制的攻击。分析了新方案的能量开销,证明公钥密码系统在无线传感器网络中的应用是可行的,而本方案采用密钥长度短的ECC作为密码体制,使用基于身份的因子公钥进行密钥管理,使该方案更适应于无线传感器网络。

参考文献

[1] Eschenauer L, Gligor V D. A key-management scheme for distributed sensor networks[C]// Proceedings of the 9th ACM Conference on Computer and Communications Security. November 2002:41-47

[2] Liu D, Ning P. Establishing pairwise keys in distributed sensor networks[C]// Proceedings of 10th ACM Conference on Computer and Communications Security(CCS03). October 2003:52-61

[3] Girao J, Westhoff D, Schneider M. CDA:Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks[C]// 40th International Conference on Communications. IEEE ICC, May 2005

[4] Castelluccia C, Mykletun E, Tsudik G. Efficient Aggregation of Encrypted Data in Wireless Sensor Networks[Z]. Mobiquitous, 2005

[5] Ren M. Random Key Predistribution for Wireless Sensor Networks Using[C]// 8th Central European Conference on Cryptography. 2008

[6] Shamir A. Identity based cryptosystems and signature schemes [C]// Advances in Cryptology-proceedings of Crypto'84

[7] Boneh D, Franklin M. Identity based encryption from the Weil pairing[C]// Advances in Cryptology 2001, Lecture Notes in Computer Science. Vol. 2139, Springer-Verlag, Aug. 2001:231-229

[8] 南湘浩. CPK标识认证[M]. 北京:国防工业出版社,2006

[9] 徐鹏,崔国华,雷凤宇. 非双线性映射下一种实用的和可证明安全的IBE方案[J]. 计算机研究与发展,2008:1687-1695

[10] Waters B. Dual System Encryption:Realizing Fully Secure IBE and HIBE underSimple Assumptions[C]// CRYPTO 2009. 2009:619-636

[11] He Wen-bo, Liu Xue, Nguyen H, et al. PDA:Privacy-preserving Data Aggregation in Wireless Sensor, Networks[C]// IEEE INFOCOM. 2007

[12] Carmen D, Kruus P, Matt B. Constraints and approaches for distributed sensor network security[R]. 00-010. NAI Labs, 2000

[13] Bandyopadhyay S, Coyle E J. An Energy-Efficient. Hierarchical Clustering Algorithm for Wireless. Sensor Networks[C]// IEEE INFOCOM'03

[14] Stajano F, Anderson R. The Resurrecting Duckling:Security Issues for Ad-hoc Wireless Networks[C]// 3rd AT&T Software Symposium. Middletown, NJ, October 1999

[15] Hu Y C, Perrig A, Johnson D B. Wormhole detection in wireless ad hoc networks[R]. TR01-384. Department of Computer-Science, Rice University, June 2002

[16] Douceur J R. The Sybil Attack[C]// 1st International workshop on Peer-to-Peer Systems(IPTPS '02). March 2002

[17] Perrig A, Stankovic J, Wagner D. Security in Wireless Sensor Networks[J]. Communications of the ACM, 2004, 47(6)

[18] Gura N, Patel A, Wander A, et al. Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs[J]. CHES, August 2004

[19] Wander A S, Gura N, Eberle H, et al. Energy analysis of public-key cryptography for wireless sensor networks[C]// Third IEEE International Conference on In Pervasive Computing and Communications. 2005