第 38 卷 第 3 期
Vol.38 No.3

计 算 机 工 程
Computer Engineering

2012 年 2 月
February 2012

• 安全技术 •

文章编号：1000—3428(2012)03—0116—03 文献标识码：A 中图分类号：TP393

分簇式传感器网络多项式密钥预分配改进方案

江琼希，周南润

(南昌大学电子信息工程系，南昌 330031)

摘 要：针对分簇式传感器网络，提出一种改进的多项式密钥预分配方案。利用二元四次多项式密钥预分配方案，建立簇头节点之间的通信密钥，以解决阈值安全问题，降低节点开销，采用认证机制保证密钥建立过程的安全性，并支持节点加入与撤销。分析结果证明，该方案可以保证网络的连通性和安全性，节点的存储、通信及计算开销均较小。

关键词：密钥预分配；多项式；阈值安全；认证；分簇式传感器网络

Improved Polynomial Key Predistribution Scheme for Clustered Sensor Network

JIANG Qiong-xi, ZHOU Nan-run

(Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China)

【Abstract】An improved polynomial key predistribution scheme is proposed for clustered sensor networks. The communication keys among cluster head nodes are obtained according to the symmetric property of two-parameter 4th-order polynomial, which solves the threshold security problem and makes the node overheads lower. The communication keys between the cluster head node and its common nodes are built with little communication after all the nodes are deployed, the authentication mechanism guarantees the security during communication keys establishment. It indicates that the scheme appears to be connective and secure, simultaneously makes the overheads of nodes low. It is shown that addition and revocation of the nodes are feasible in the scheme.

【Key words】key predistribution; polynomial; threshold security; authentication; clustered sensor network

DOI: 10.3969/j.issn.1000-3428.2012.03.039

1 概述

通信密钥的建立是无线传感器网络安全性的关键。受能量和存储空间的限制，建立传感器网络通信密钥常采用密钥预分配方案[1]。文献[2]基于对称矩阵的性质提出了确定性的密钥预分配方案，任意节点之间可以通过计算一个对称矩阵得到通信密钥，但其扩展性较差。文献[3]的方案中每个节点预分配一定数量的密钥，节点之间通过预分配的相同密钥建立安全通信。为降低该方案中任意 2 对节点通信密钥相同的概率，文献[4]提出 q-composite 随机密钥预分配方案，其中任意 2 个节点至少拥有 q 个相同密钥。文献[5]结合文献[2-3]的方案，提出多密钥空间随机密钥预分配方案，节点预分配一定数量的矩阵，节点之间通过预分配的相同矩阵计算它们的通信密钥，兼顾了网络连通性和扩展性。文献[6]提出基于多项式的组密钥分配方案，只要俘获的组内成员不超过设定的阈值，方案就能保证绝对安全。文献[7]在此基础上提出了基于多项式的无线传感器网络密钥预分配方案，节点被预分配一个多项式，在多项式上赋值得到通信密钥。当被俘节点数大于或等于阈值时，敌方解方程组可以得出多项式系数，计算出通信密钥，这样网络的安全性迅速遭到破坏，即该方案是阈值安全的。

由于分簇式传感器网络能够减少发往基站的冗余数据，因此能够提高网络性能和网络的存活时间[8]，易实现网络的优化和管理。文献[9]在多项式密钥预分配方案的基础上提出了改进方案 IKDM，将其应用于分簇式网络，该方案通过设置多项式次数大于簇头节点个数解决阈值安全问题，但由此会增加节点开销，不利于扩大网络规模，而且该方案在密钥建立过程中易遭受篡改、伪造等主动攻击。传感器节点经常应用在战场用于监视敌情，或部署在医院来实时监视患者位置和状态，这些环境极其恶劣或者性命攸关，对传感器网络的连通性、安全性及节点开销要求很高，以上密钥预分配方案不能适用。

为解决多项式方案普遍存在的阈值安全问题，提高传感器网络安全性，且保证较小的节点开销和整个网络的连通性，本文针对分簇式传感器网络，提出了一种改进的密钥预分配方案。

2 多项式密钥预分配方案安全性分析

文献[7]和文献[9]均使用有限素数域 F_q 上的二元 t 次对称多项式：

$$g(x,y)=g(y,x)=\sum_{i,j=0}^{t}a_{ij}x^iy^j \tag{1}$$

其中，$a_{ij}=a_{ji}$，a_{ij} 不对外公开。文献[7-9]认为基于多项式的密钥预分配方案是阈值安全的。然而，只要将二元对称多项式进行保密，网络即可避免遭受恶意节点的合谋攻击和敌方采取的阈值攻击，理由如下：

(1)在初始化阶段，基站使用节点的 ID 对 $g(x,y)$ 的 x 进

基金项目：国家自然科学基金资助项目(10647133)；江西省自然科学基金资助项目(2009GQS0080)；江西省教育厅科技基金资助项目(GJJ11339)

作者简介：江琼希(1988－)，男，硕士研究生，主研方向：无线传感器网络安全，密码学理论；周南润，教授、博士

收稿日期：2011-07-11 **E-mail：**znr21@163.com

行赋值，因此，预分配到的节点其实是一个一元 t 次多项式 $g(\mathrm{ID},y)$。节点在密钥建立过程中只要使用 $g(\mathrm{ID},y)$，不需要使用 $g(x,y)$。因此，对二元对称多项式进行保密不会妨碍节点密钥的建立。

(2)敌方俘获节点后可得到 t 的值，将 t 和节点 ID 代入 $g(x,y)$，得到 $g'(\mathrm{ID},y)$，令：

$$g(\mathrm{ID},y)=g'(\mathrm{ID},y) \tag{2}$$

敌手俘获 t 个节点后，解 t 个方程得到 a_{ij}，从而得到所有密钥。由以上分析可知，如果敌手没得到二元对称多项式，或者基站改变 $g(x,y)$，便无法根据方程组解出多项式。

3　分簇式传感器网络多项式密钥预分配改进方案

3.1　密钥预分配

假设簇头节点之间可以互相通信，而普通节点仅与它们的簇头节点进行通信，网络中有 n 个节点和 c 个簇头节点，基站的 ID 为 $n+1$。基站为每个传感器节点分配一个唯一的 ID，对所有节点和其自身 ID 在 $f(x,y)$ 的变量 x 上赋值，$f(x,y)$ 为定义在有限素数域 F_q 上的二元四次多项式：

$$f(x,y)=\sum_{k=1}^{3}\left[(2k+1)\left(x^k+y^k\right)+(2k+7)(xy)^k\right] \tag{3}$$

显然，$f(x,y)$ 为对称多项式。基站为每一个簇头节点 c_i 预分配一个多项式 $f(c_i,y)$，为每个普通节点 i 分配一个密钥 k_i。c_i 是该簇头节点的 ID，k_i 计算如下：基站随机选择 3 个簇头节点的节点标识符 c_a、c_b、c_c，利用多项式 $f(i,y)$ 对 y 赋值，则：

$$k_i=f(i,c_a)\oplus f(i,c_b)\oplus f(i,c_c) \tag{4}$$

基站将 $\{c_a,c_b,c_c,k_i\}$ 存储在普通节点 i 上。

3.2　簇头节点间通信密钥的建立

簇头节点间使用二元四次多项式 $f(x,y)$ 建立通信密钥，具有以下优点：(1)簇头节点之间距离较远，存在安全威胁，采用多项式使簇头节点间密钥的建立只需对多项式赋值，无需进行相互通信，有效防止敌方攻击。(2)密钥建立过程中无通信开销。传感器网络节点能量消耗主要是通信开销，小部分为计算开销，能量消耗较小。(3)密钥建立所需的计算和存储开销较小。如果多项式次数太少，易遭受字典攻击。

首先由基站生成 $f(x,y)$。假设簇头节点 c_i 要与 c_j 建立通信密钥，c_i 对存储的多项式 $f(c_i,y)$ 在 y 上赋值，计算 $f(c_i,c_j)$。簇头节点 c_j 只需对 $f(c_j,y)$ 在 y 上赋值，计算 $f(c_j,c_i)$。根据 $f(c_j,c_i)=f(c_i,c_j)$，2 个簇头节点可建立通信密钥。

3.3　簇头节点与普通节点通信密钥的建立

簇头节点和普通节点的通信密钥建立过程如下：

(1)普通节点 i 将标识符 i 及存储的 c_a、c_b、c_c 发送给簇头节点 c_i。

(2) c_i 接收到数据后，发送信息到簇头节点 c_a、c_b、c_c。簇头节点 c_i 分别用多项式 $f(c_i,c_a)$、$f(c_i,c_b)$、$f(c_i,c_c)$ 对标识符 i 加密，并发送 m_{c_a}、m_{c_b}、m_{c_c} 到 c_a、c_b、c_c，其中：

$$m_{c_\lambda}=i\|c_i\|E_{f(c_i,c_\lambda)}(i),\ \lambda=a,b,c \tag{5}$$

(3)收到来自 c_i 的信息后，c_λ 用 $f(c_\lambda,c_i)$ 加密 i，假如 $E_{f(c_a,c_i)}(i)\neq E_{f(c_i,c_\lambda)}(i)$，表明簇头节点之间的信息被敌方篡改或伪造，则 c_λ 对接收到的信息不做处理。反之，c_λ 利用 $f(c_\lambda,y)$ 计算 $f(c_\lambda,i)$，发送信息 m'_{c2} 回 c_i。

$$m'_{c2}=c_\lambda\|E_{f(c_\lambda,c_i)}\left(c_\lambda\|f(c_\lambda,i)\right) \tag{6}$$

(4)簇头节点 c_i 接收到信息后，解密信息 $E_{f(c_\lambda,c_i)}\left(c_\lambda\|f(c_\lambda,i)\right)$。如果发现解密出的 c_λ 与 m'_{c2} 中前一部分的 c_λ 不相等，则丢弃该信息，否则，c_i 利用 $f(c_\lambda,i)$ 计算：

$$f(c_a,i)\oplus f(c_b,i)\oplus f(c_c,i)=k_i \tag{7}$$

普通节点 i 由此建立与簇头节点 c_i 的通信密钥。

3.4　节点的加入与撤销

传感器网络部署在开放的环境下，节点易遭受自然环境的影响导致节点失效。分簇式传感器网络中的普通节点具有较小的能量，随着时间的推移，会因能量耗尽而失效。因此，节点的加入与撤销机制至关重要。

假设 i' 为待加入节点，基站为其预分配节点标识符 i'和 3 个簇头节点的节点标识符 c_a、c_b、c_c。当 i'部署到网络后，确定其簇头节点 c'_i，发送 i'、c_a、c_b、c_c 到 c'_i，c'_i 根据在通信密钥建立阶段的步骤建立与 i'的通信密钥。当节点失效需撤销时，基站发送撤销节点命令到失效节点的簇头节点，簇头节点删除与失效节点建立的通信密钥。

4　方案特性分析

4.1　安全性分析

分簇式传感器网络多项式密钥预分配改进方案是一个确定性的密钥预分配方案，该方案保证任意两节点能建立通信密钥，使整个传感器网络完全连通。在簇头节点和普通节点密钥建立阶段，簇头节点之间距离相对较大，易遭受敌方的篡改和伪造，在簇头节点间的信息交换过程中引入认证机制，能有效防止敌方的攻击。

当敌方俘获普通节点 i 时，获得 c_λ、k_i，由于多项式 $f(x,y)$ 未知，已知 c_λ 没有意义，而由 k_i 不能推导出 $f(i,c_\lambda)$，只影响该节点与其簇头节点之间的通信，不影响其他节点间的通信。当簇头节点被俘时，因簇头节点间的通信密钥建立在二元四次多项式的密钥预分配的基础上，由第 2 节的分析可知，该簇头节点的被俘不会泄露其他簇头节点对的密钥。

4.2　计算与通信开销分析

节点计算开销为计算通信密钥消耗的能量，通信开销为通信密钥建立过程中数据发送和接收消耗的能量。

(1)普通节点要建立与簇头节点的通信密钥，仅需发送存储的 3 个簇头节点 ID 及自身 ID，计算开销为 0。对于分簇式传感器网络，普通节点与其簇头节点之间的距离较小，普通节点发送的数据包只包括 4 个节点的 ID，数据包的长度很短，所需的通信开销较小。

(2)簇头节点要与 $n/c-1$ 个普通节点建立通信密钥，需接收 $n/c-1$ 个普通节点的数据，对其节点标识符加密，发送这些普通节点 ID 及其加密值及自身 ID 到另外 $3(n/c-1)$ 个簇头节点，并接收这些簇头节点发送的信息，解密得出由其计算的多项式，再进行 $n/c-1$ 次异或运算。节点 ID 长度很短，加密计算开销很小。该簇头节点需计算存储其 ID 的其他簇普通节点的多项式，还需与其他 $c-1$ 个簇头建立通信密钥，如果某一簇头节点要与另一簇头节点建立密钥，则只需对其存储的多项式进行赋值，不产生通信开销。

4.3　存储开销分析

节点存储开销即通信密钥建立需要的存储空间。每个簇头节点 c_i 需存储一个一元三次多项式 $f(c_i,y)$，所需的存储空间是 $O(4\log q)$。普通节点 i 需存储密钥 k_i 以及 3 个簇头节点

的 ID，即 c_a、c_b、c_c。由于节点在存储空间上受限，因此在通信密钥建立阶段结束后，普通节点删除其存储的 3 个簇头节点的 ID。

4.4 方案比较

用 PKPS 表示本文方案。连通性为节点之间建立密钥的概率，抗毁性用节点被俘获时网络中其他节点的受损概率表示，受损概率越小，抗毁性越强。文献[2]方案、IKDMS 和 PKPS[9]的连通性为 1，其受损概率分别为 $0\ (x\leqslant\lambda)$，$1\ (x>\lambda)$；$0\ (x\leqslant t)$，$1\ (x>t)$ 和 0，而文献[3]方案和 q-composite 方案[4]的连通性分别为 $p=1-\sum_{i=0}^{q-1}p(i)$ 和 $1-(|S|-m)!/((|S|-2m)!|S|!)$，受损概率分别为 $1-(1-m/|S|)^x$ 和 $\sum_{i=q}^{m}\left(1-(1-m/|S|)^x\right)^i p(i)/p$。

$|S|$ 为密钥池中密钥的数量，m 为预分配到节点的密钥数量，x 为被俘节点数，λ 为文献[3]方案的阈值，t 为 IKDMS 多项式次数，$p(i)=C_{|S|}^{i}C_{|S|-i}^{2(m-i)}C_{2(m-i)}^{m-i}\Big/\left(C_{|S|}^{m}\right)^2$。显然，PKPS 在网络连通性和抗毁性方面都具有明显的优势。

表 1 为各方案节点开销比较，符号 O 表示计算复杂度。PKPS 和 IKDMS 中普通节点开销很小，而簇头节点的电池能量比普通节点高很多，允许通信开销较大。在计算开销方面，簇头节点为建立与普通节点的通信密钥，需发送数据到 $3(n/c-1)$ 个其他簇头节点，由于不同的普通节点存储的簇头节点 ID 中会重合，因此簇头节点最多只需将数据发送到其他 $c-1$ 个簇头节点。由表 1 可知，相比 IKDMS，PKPS 簇头节点计算、存储开销较小。

表 1 方案开销比较

方案	存储开销	通信开销	计算开销
文献[2]方案	$O(2(\lambda+1))$	$O(2)$	$O(\lambda+1)$
文献[3-4]方案	$O(m)$	$O(2)$	$O(m)$
IKDMS/PKPS 普通节点	$O(4)$	$O(1)$	0
IKDMS 簇头节点	$O((t+1)\log q)$	$O(4)$	$\leqslant(c-1)$次 t 次多项式赋值、解密，$n/c-1$ 次异或运算
PKPS 簇头节点	$O(4\log q)$	$O(4)$	$\leqslant(c-1)$次 4 次多项式赋值、解密，$n/c-1$ 次异或运算

5 结束语

结合多项式密钥预分配方案和分簇式传感器网络，本文提出了一个密钥预分配改进方案，利用二元四次多项式建立簇头节点之间的密钥，利用预分配到普通节点的 3 个其他簇头节点 ID 建立普通节点和其簇头节点之间的密钥。针对多项式密钥预分配方案普遍存在的阈值安全和节点开销问题，通过对二元四次对称多项式进行保密，使方案能够抵抗合谋攻击和阈值攻击，同时节点开销很小。而在簇头节点和普通节点密钥建立过程中，认证机制保证簇头节点间信息交换的安全性，能抵抗篡改和伪造等主动攻击。该方案能较好地支持节点的加入与撤销，与其他典型传感器网络密钥预分配方案相比，该方案在连通性和抗毁性方面都具有较大的优势。

参考文献

[1] Mohatar O D, Sabater A F, Sierra J M. A Light-weight Authentication Scheme for Wireless Sensor Networks[J]. Ad Hoc Networks, 2010, 9(5): 727-735.

[2] Blom R. An Optimal Class of Symmetric Key Generation Systems[C]//Proceedings of EUROCRYPT'84. Berlin, Germany: Springer-Verlag, 1984: 335-338.

[3] Eschenauer L, Gligor V D. A Key-management Scheme for Distributed Sensor Networks[C]//Proceedings of the 9th ACM Conference on Computer and Communication Security. New York, USA: ACM Press, 2002: 41-47.

[4] Chan H, Perrig A, Song D. Random Key Predistribution Schemes for Sensor Networks[C]//Proceedings of 2003 IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Computer Society, 2003: 197-213.

[5] Du Wenliang, Deng Jing, Yunghsiang S H, et al. A Pairwise Key Predistribution Scheme for Wireless Sensor Networks[J]. ACM Transactions on Information and System Security, 2005, 8(2): 228-258.

[6] Blundo C, Santis A D, Herzberg A. Perfectly-secure Key Distribution for Dynamic Conferences[C]//Proceedings of the 12th Annual International Conference on Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1993: 471-486.

[7] Liu Donggang, Ning Peng, Li Rongfang. Establishing Pairwise Keys in Distributed Sensor Networks[J]. ACM Transactions on Information and System Security, 2005, 8(1): 41-77.

[8] 岳海兵，葛洪伟. 基于能量分布的异构传感器网络分簇算法[J]. 计算机工程, 2010, 36(1): 118-120.

[9] Cheng Yi, Agrawal D P. An Improved Key Distribution Mechanism for Large-scale Hierarchical Wireless Sensor Networks[J]. Ad Hoc Networks, 2007, 6(1): 35-48.

编辑 张正兴

(上接第 106 页)

算法在网络负载均衡和网络吞吐量方面都优于 GAFH 算法，并且当 i=2 时的性能还优于 i=1 的情况，GAFHH 算法的性能得到优化，其原因是负载均匀性得到提高。但 i 的取值也不能过大，必须在保证连通性的情况下，根据节点密度适当选取 i 的大小。当节点密度比较稀疏的情况下，如果 i 的取值太大，则可能会出现有些小蜂窝栅格内节点太少，甚至没有节点，在这种情况下，GAFHH 算法的设计相对 GAFH 算法就失去了意义。下一步将研究 i 的取值，以优化无线传感器网络的性能。

参考文献

[1] Akyildiz I F, Su Weilian, Sankarasubramaniam Y, et al. A Survey on Sensor Network[J]. IEEE Communications Magazine, 2002, 40(8): 102-114.

[2] 明光照，李 鸥，张延军. 基于无线传感器网络的智能家居系统设计[J]. 通信技术, 2009, 42(2): 233-237.

[3] Xu Ya, Heidemann J, Estrin D. Geogrph-informed Energy Conservation for Ad Hoc Routing[C]//Proc. of the 7th Annual International Conference on Mobile Computing and Networking. [S. l.]: ACM Press, 2001: 70-84.

[4] 黄 星，张会生，李立欣. 基于蜂窝结构模型的 GAF 算法研究[J]. 信息安全与通信保密, 2010, (1): 73-75.

[5] 刘 曙，刘林峰，陶 军. 一种基于蜂窝结构的改进 GAF 算法[J]. 计算机技术与发展, 2009, 19(1): 39-42.

[6] 赵远东，曹 平，倪兴荣. 一种可绕过障碍物的网格路由算法[J]. 通信技术, 2009, 42(12): 125-127.

编辑 陆燕菲