基于分层网格的无线传感器网络密钥预分配方案*)

崔国华[1] 章丽平[1,2] 喻志刚[3] 徐 鹏[1] 陈 晶[1]
(华中科技大学计算机学院 武汉 430074)[1] (中国地质大学计算机学院 武汉 430074)[2]
(武汉邮电科学研究院虹信技术有限责任公司 新一代光纤通信技术和网络国家重点实验室 武汉 430074)[3]

摘 要 无线传感器网络自身的特征,如网络规模庞大、动态的拓扑结构、有限的计算、通信和存储能力等,使得传统的密钥分配和管理机制无法进行直接应用。基于分层网格提出了一种新的适用于无线传感器网络的密钥预分配方案。该方案采用多项式方法在传感器节点间建立共享密钥,并引入分层网格结构实施密钥的预分配。这种设计方法有效地降低了部分节点被俘获后对网络安全造成的影响,增强了网络的健壮性,而且其计算和存储开销也不大,具有一定的实用性。

关键词 分层网格,网络安全,密钥预分配,无线传感器网络

Key Predistribution Scheme for Wireless Sensor Networks Based on Hierarchical Grid

CUI Guo-hua[1] ZHANG Li-ping[1,2] YU Zhi-gang[3] XU Peng[1] CHEN Jing[1]
(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)[1]
(College of Computer Science and Technology, China University of Geosciences, Wuhan 430074, China)[2]
(State Key Laboratory for New Optical Communication Technologies and Networks, Wuhan Research Institute of Posts&Telecommunication, Wuhan 430074, China)[3]

Abstract Providing a suitable key establishment scheme in wireless sensor networks is challenging due to all the characteristics of these networks, such as dynamically changing topology and limitations of power, computation capability and storage resources. Presented a key predistribution scheme based on hierarchical grid which is suitable for wireless sensor networks. Our scheme uses symmetric bivariate polynomial to generate a secure key for two sensor nodes. The distribution of the keying material was performed on a hierarchical grid. In our scheme different polynomials for different sections of the network to take the merit that compromising of $(t+1)$ nodes will only affect the related polynomial zone, and thus, using different polynomials with different t degrees will lead to higher survivability against attacks. The proposed key predistribution scheme enhances the security of the wireless sensor network and only spends moderate computation cost, so it is quite practical.

Keywords Hierarchical grid, Network security, Key predistribution, Wireless sensor network

1 引言

无线传感器网络由大量功能相同或不同的无线传感器节点组成,其目的是协作地感知、采集和处理其覆盖区域中被感知对象的信息,发送给使用者[1]。与传统的无线计算机网络相比,无线传感器网络具有其自身的特点:网络规模庞大、节点由电池供电、计算和通信能力有限。无线传感器网络自身的特点使其安全性面临严峻挑战。为了保证无线传感器网络的安全运行,应对传感器节点间的通信进行加密,并对重要的网络传输数据进行认证。而要达到此目的,则必须提供安全有效的密钥分配方案,在相互通信的传感器节点间建立安全的共享密钥。由于传感器节点由电池供电,其能量、计算能力和通信带宽都非常有限,因此不宜采用公钥密码[2],而应该采用对称加密算法、低能耗的认证机制以及 Hash 函数来构建安全的密钥分配方案。此外,无线传感器网络中所有节点都是对等的,没有认证中心,因此传统网络中使用的基于可信第三方的密钥分配方案不适用于无线传感器网络。目前普遍认为可行的方法是采用密钥预分配方案,把需要的密钥预先装入传感器节点中。

密钥预分配方案最简单的实现方法是让所有的节点都事先存储一个相同的对称密钥,通信双方都用这个密钥进行通信。该方法实现简单,所需存储空间小,但安全性很差。一旦某个传感器节点被攻破,全网就被攻破。另一种方法是预置所有节点密钥对,让每个节点存储 $N-1$ 个(N 为网络节点数目)密钥,使节点能和网络中其它 $N-1$ 个节点进行安全通信。该方案增强了网络的健壮性,但需要较大的存储空间,而传感器节点的存储能力往往是有限的,因此该方案不可行。Eschenauer 和 Gligor 提出了一种随机密钥预分配方案(以下简称 E-G 方案[3])。其基本思想是对预置所有节点密钥对方案的改进,它将预存网络中的所有节点密钥对改为预存部分节点密钥对,降低了节点存储量需求。但该方案是基于概率的,因此不能提供确定的安全性,且节点密钥对中可能存在相同的共享密钥,单点失效会引起网络中其余部分的不安全。

Chen 等人在 E-G 方案的基础上提出了 q-composite 随机

*)国家自然科学基金资助项目(60403027),中国地质大学(武汉)优秀青年教师资助计划资助项目(CUGQNL0836)。崔国华 教授,博士生导师,主要研究方向为密码学和信息安全;章丽平 博士研究生,讲师,研究方向为密码学和网络安全。

密钥预分配方案[4]。该方案主要对 E-G 方案中的共享密钥发现进行了改进。q-composite 随机密钥预分配方案要求传感器节点之间必须至少共享 q 个密钥时才能建立安全链路。如果不少于 q，则用传感器节点间所有的密钥来建立共享密钥。由于每对通信节点共有 q 个密钥，从而降低了网络中使用相同会话密钥的概率，提高了抵抗小范围内节点俘获失效的能力。但是随着被俘获节点的增多，网络中剩余部分受影响的范围将迅速增加。

Cheng 等人对 E-G 方案进行了改进，提出了一种新的随机密钥预分配方案[5]。与 E-G 方案不同之处在于，该方案使用一个长的比特字符串作为密钥集合，每个传感器节点从该集合中随机选取一段作为该传感器节点的密钥子集，并用传感器节点间的共享比特字符串来代替会话密钥。其优点在于占用内存较少，对于不同应用程序的不同安全需求，调节灵活；缺点在于，由于共享字符串的长度可能不相等，使得传感器节点间所使用的密钥长度不等，从而导致硬件实现困难以及全网中的安全性能不均匀。

以上文献[3-5]所提出的随机密钥预分配方案都不能有效降低部分节点被俘获后对网络安全造成的影响，网络的健壮性较差。本文提出了一种基于分层网格的密钥预分配方案(HG-SBP)，该方案在分层网格结构上基于 Blundo 所提出的对称二元多项式构建传感器节点间的共享密钥。在 Blundo 方案[6]中，传感器网络采用一个 t 次对称二元多项式来构建所有传感器节点对之间的共享密钥。为了抵抗部分传感器节点被俘获后对网络安全造成的影响，需要 t 充分大，但是 t 值越大，传感器节点需要用于计算该多项式的能量就越多。为了解决该问题，HG-SBP 方案中引入了分层网格的概念，利用分层结构使位于不同层的网格对应不同的多项式，传感器节点通过选择不同的多项式来构建共享密钥。这种设计方法使得 HG-SBP 方案在控制节点计算量的同时能有效降低部分节点被俘获后对网络安全造成的影响，增强了网络的健壮性。本文第 2 节简要介绍了 Blundo 提出的基于多项式的密钥预分配方案[6]。第 3 节提出了一种新的基于分层网格的密钥预分配方案(HG-SBP)。在第 4 节和第 5 节对 HG-SBP 方案的性能以及安全性进行了分析。最后总结全文。

2 预备知识

Blundo 提出的基于对称二元多项式的密钥预分配方案的基本思想是：首先由一个可信的密钥服务中心按如下方式生成一个对称二元多项式：

$$f(x,y)=\sum_{i,j=0,\cdots,t} a_{ij}x^i y^j \pmod q \tag{1}$$

其中，q 为大素数，$1\leqslant a_{ij}\leqslant q-1$，$t$ 表示多项式的次方。初始化阶段密钥服务中心为每个节点 u 设置一个惟一的秘密多项式：

$$f_u(y)=f(Id_u,y)=\sum_{i,j=0,\cdots,t} a_{ij}(Id_u)^i y^j \pmod q \tag{2}$$

其中，Id_u 是节点 u 在网络中的惟一标志符。网络中任意两个节点 u,v 可以通过如下计算建立它们之间的共享密钥：

$$K_{u,v}=f(Id_u,Id_v)=f(Id_v,Id_u)=K_{v,u} \tag{3}$$

当网络中被俘获的节点数少于 $t+1$ 时，该网络是安全的[6]。t 值越大，更能有效降低部分节点被俘获后对网络安全造成的影响，网络的安全性越高。

3 基于分层网格结构的密钥预分配方案

3.1 符号

基于分层网格结构的密钥预分配方案(HG-SBP)中使用到的符号说明如表 1。

表 1 符号说明表

符号	符号说明
N	无线传感器网络中传感器节点总数
n	分层网格结构中的总层数
m	单位网格中传感器节点总数
k	无线传感器网络中传感器节点的均匀分布单元
L_i	分层网格结构中的第 i 层，其中 $i\in[1,\cdots,n]$
u,v	传感器节点
G_n	分层网格结构中单位网格的总数
ID	单位网格标志符
Id_{G_u}	传感器节点 u 所在的单位网格的标志符
Id_{L_u}	单位网格中传感器节点 u 的本地标志符，$Id_{L_u}\in[0\cdots m-1]$
$f_{(i,j)}(x,y)$	L_i 层中第 j 个网格对应的对称二元多项式，$j\in[1\cdots 2^{i-1}]$
$t_{f_{(i,j)}}$	对称二元多项式 $f_{(i,j)}(x,y)$ 的次方
$f_{(i,j)u}(y)$	节点 u 的秘密多项式
$K_{u,v}=K_{v,u}$	节点 u,v 之间的共享密钥
$MAC_K(M)$	采用共享密钥 K 对信息 M 进行 MAC 计算

3.2 分层网格

在移动 ad hoc 网络中，分层网格结构[7]已被成功应用于构建健壮的路由。为了在无线传感器网络中实现安全的密钥分配，在 HG-SBP 方案中引入了分层网格的概念，并在分层网格结构上提出了一种新的设置单位网格标志符的方法，使得该结构更适合于密钥的分配。HG-SBP 方案中采用的分层网格结构如图 1 所示。

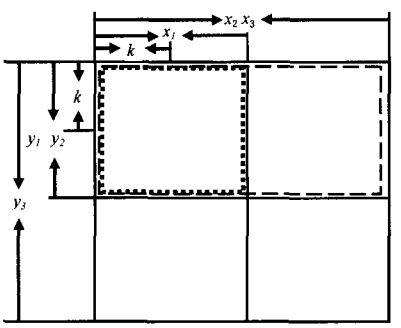

图 1 三层网格结构图

如图 1，无线传感器网络覆盖范围被划分成若干层，每一层包含若干个网格。设 L_1 层为最高层，其下一层为 L_2 层，以此类推，L_n 层为最底层。且 L_i 层中包含 2^{i-1} 个网格，则最底层 L_n 层中包含 $G_n=2^{n-1}$ 个大小为 $[2k,2k]$ 的单位网格，其中 k 是无线传感器网络中传感器节点的均匀分布单元。设单位网格中的传感器节点总数 $m=(2k)^2$，则整个网络包含的传感器节点总数为 $N=m\times G_n=(2k)^2\times 2^{n-1}$ 个。

举例：图 1 中，无线传感器网络被划分为三层，L_3 层中包含 $2^{3-1}=4$ 个单位网格，$[x_1,y_1]$ 所示区域为其中一个单位网格。L_2 层中包含 $2^{2-1}=2$ 个网格，$[x_2,y_2]$ 所示区域为其中一个网格，即 L_3 层中横向相邻的两个单位网格构成了 L_2 层中的一个网格。L_1 层中则包含 $2^{1-1}=1$ 个大小为 $[x_3,y_3]$ 的网格。该网络中传感器节点总数为 $N=m\times G_3=(2k)^2\times 2^{3-1}=(2k)^2\times 4=16k^2$ 个。

HG-SBP 方案在分层网格结构中为每个单位网格中的每一个传感器节点分配一个该区域内惟一的本地标志符 Id_{L_u}，则 $|Id_{L_u}|=\log_2 m$，并为 L_n 层中的每一个单位网格设定一个惟一的单位网格标志符 ID。ID 的设置方法如图 2 所示。

设无线传感器网络被划分为 n 层，单位网格标志符的位长由网格总层数 n 来决定，即 $|ID|=n-1$。ID 的设置从 L_n 层最左上角的单位网格开始，设定该单位网格的 $ID=\underbrace{0\ldots0}_{n-2}0$。然后，在田字形区域内按顺时针方向顺序设置标志符，标志符 ID 值每次增 1，则最左上角的单位网格右侧相邻单位网格的 $ID=\underbrace{0\ldots0}_{n-2}1$，以此类推。该田字形区域中所有单位网格的标志符设置完成后，在高一级田字形区域中按顺时针方向找到未设置标志符的下一级田字形区域，并按照同样的方法从未设置标志符的田字形区域中最左上角的单位网格开始继续设置标志符。不断重复以上过程，直到 L_n 层中最左下角的单位网格的标志符设置完成为止，整个标志符设置过程结束。

举例：图 2 中无线传感器网络被划分为 5 层，则单位网格标志符的位长 $|ID|=5-1=4$。单位网格标志符的设置从 L_5 层的最左上角的单位网格开始，设定该单位网格的 $ID=0000$。然后，在田字形区域内按顺时针方向顺序设置标志符，为 $ID=0000$ 单位网格右侧相邻的单位网格分配标志符 $ID=0001$，以此类推。该田字形区域中所有单位网格的标志符设置完成后，在高一级田字形区域中按顺时针方向找到未设置标志符的下一级田字形区域，并给该区域中最左上角的单位网格分配标志符 $ID=0100$，并按上述方法继续设置标志符。不断重复以上过程，直到为 L_5 层中最左下角的单位网格设置标志符 $ID=1111$ 为止，整个标志符设置过程结束。

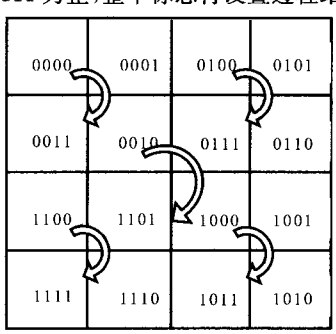

图 2　单位网格标志符设置图，其中 $n=5$，$G_5=16$

为每一个单位网格设置一个惟一标志符的目的在于，可以通过该标志符快速判断网络中任意两个传感器节点 u，v 共同存在于哪些高层的同一网格中。其判断方法是比较节点 u，v 所在单位网格的标志符。将两个单位网格的标志符字串从左到右按位比较，当对应位上的值不相同或对应位上所有值都相同时比较结束。设找到的值不相同的对应位为第 k 位（对应位上所有值都相同时 $k=n$），则节点 u，v 在 L_k，L_{k-1}，…，L_1 这些高层的同一网格中共同存在。其中，L_k 层是节点 u，v 共同存在于同一网格中的层数最低的高层网格，即节点 u，v 不会共同存在于 L_{k+1} 层以及更低层的同一网格中。

3.3　密钥预分配方案

HG-SBP 方案中，假设传感器节点是静止的，即传感器节点是固定的或者不需要传感器节点的移动来完成任务。此外，该方案是基于 3.2 小节所描述的分层网格结构的。HG-SBP 方案的基本思想是：初始化阶段，由无线传感器网络中的基站生成一组对称二元多项式，分别对应于 L_i 层中的每个网格。共享密钥建立阶段，当任意两个传感器节点需要建立共享密钥时，首先通过相互通信获取对方节点所在单位网格的标志符以及对方节点的本地标志符，然后利用获取的单位网格标志符来选择进行共享密钥计算的秘密多项式，最后双方节点采用该秘密多项式计算它们之间的共享密钥。HG-SBP 方案的具体过程如下：

(1)初始化阶段。该过程由基站完成，其具体步骤如下：

步骤一　对称二元多项式的生成。基站随机地生成 2^n-1 个对称二元多项式（参见式(1)）$f_{(n,1)}(x,y)$，…，$f_{(n,2^{n-1})}(x,y)$，$f_{(n-1,1)}(x,y)$，…，$f_{(n-1,2^{n-2})}(x,y)$，…，$f_{(1,1)}(x,y)$。这 2^n-1 个多项式次方的关系如下：$\underbrace{t_{f_{(n,1)}}=t_{f_{(n,2)}}=\cdots=t_{f_{(n,2^{n-1})}}}_{2^{n-1}}<\underbrace{t_{f_{(n-1,1)}}=\cdots=t_{f_{(n-1,2^{n-2})}}}_{2^{n-2}}<\underbrace{t_{f_{(n-2,1)}}=\cdots}_{2^{n-3}}<\cdots<\underbrace{t_{f_{(1,1)}}}_{1}$。

设对称二元多项式 $f_{(n,1)}(x,y)$，…，$f_{(n,2^{n-1})}(x,y)$ 分别对应于 L_n 层中的 G_n 个单位网格。对称二元多项式 $f_{(n-1,1)}(x,y)$，…，$f_{(n-1,2^{n-2})}(x,y)$ 与 L_{n-1} 层中的网格相对应。以此类推，$f_{(1,1)}(x,y)$ 与 L_1 层中的网格相对应。即为每一层 L_i 分配 2^{i-1} 个同次方的对称二元多项式，每一个对称二元多项式与该层中的一个网格相对应。网格所在层越高，对应的对称二元多项式的次方越高。

步骤二　为每一个传感器节点 u 设置一组秘密多项式。设 L_i 层中传感器节点 u 所在网格对应的多项式为 $f_{(i,j)}(x,y)(i\in[1\cdots n],j\in[1\cdots 2^{i-1}])$，则基站为传感器节点 u 计算如下 n 个秘密多项式，并将这 n 个秘密多项式存储到传感器节点 u 中。

$$f_{(1,1)u}(y)=f_{(1,1)u}(Id_{G_u}\parallel Id_{L_u},y)$$

$$f_{(2,j)u}(y)=f_{(2,j)u}(Id_{G_u}\parallel Id_{L_u},y)\quad(j\in[1,2])$$

……

$$f_{(n-1,j)u}(y)=f_{(n-1,j)u}(Id_{G_u}\parallel Id_{L_u},y)\quad(j\in[1\cdots 2^{n-2}])$$

$$f_{(n,j)u}(y)=f_{(n,j)u}(Id_{G_u}\parallel Id_{L_u},y)\quad(j\in[1\cdots 2^{n-1}])$$

(参见式(2))

网络中任意两个传感器节点 u，v 所拥有的秘密多项式是不一样的，因为任意两个传感器节点 u，v 要么属于同一个单位网格，要么属于不同的单位网格。如果节点 u，v 属于同一个单位网格，则 $Id_{G_u}=Id_{G_v}$，但 $Id_{G_u}\neq Id_{L_v}$，所以 $Id_{G_u}\parallel Id_{G_u}\neq Id_{G_v}\parallel Id_{L_v}$，保证了节点 u，v 拥有不同的秘密多项式。如果节点 u，v 属于不同的单位网格，则 $Id_{G_u}=Id_{L_v}$ 有可能成立，但是由于它们来自不同的单位网格，必然有 $Id_{G_u}\neq Id_{G_v}$，因此 $Id_{G_u}\parallel Id_{G_u}\neq Id_{G_v}\parallel Id_{L_v}$。同理，在节点 u，v 属于不同单位网格的情况下，它们各自拥有的秘密多项式也不相同。由以上分析，网络中任意两个传感器节点所存储的秘密多项式都不相同。

(2)共享密钥建立阶段。网络中任意两个传感器节点 u，v 之间的共享密钥建立过程如图 3 所示，其具体步骤如下：

步骤一　节点 u 发送 $Hello$ 信息$\{Hello,Id_{G_u},Id_{G_u},N_u\}$给节点 v，其中 N_u 用于保证信息的新鲜性。

步骤二　节点 v 接收到节点 u 发送的信息后，进行如下操作：

① 秘密多项式的选取。首先节点 v 将自身的 Id_{G_v} 与节点 u 的 Id_{G_u} 从左到右按位进行比较，找出第一个值不相同的对应位，设为 k（若 $Id_{G_v}=Id_{G_u}$，则 $k=n$）。然后节点 v 从其所拥有的一组秘密多项式中选取 $f_{(k,j)v}(y)=f_{(k,j)v}(Id_{G_v}\parallel Id_{L_v},y)$ 作为将要进行共享密钥计算的秘密多项式。

②共享密钥的计算。利用选取出来的秘密多项式和接收

到的信息 Id_{G_u}，Id_{G_u}，计算共享密钥 $K_{v,u}=f_{(k,j)v}(y)=f_{(k,j)v}(Id_{G_u}\|Id_{L_u})$。

③ 发送信息$\{Id_{G_v},Id_{L_v},N_v,MAC_{K_{v,u}}(Id_{G_v},Id_{L_v},N_v,N_u)\}$给节点 u。

步骤三　节点 u 接收到节点 v 发送的信息后，进行如下操作：

① 按照步骤二中①的方法选取秘密多项式 $f_{(k,j)u}(y)=f_{(k,j)u}(Id_{G_u}\|Id_{G_u},y)$作为将要进行共享密钥计算的多项式。

② 计算共享密钥 $K_{u,v}=f_{(k,j)u}(y)=f_{(k,j)u}(Id_{G_v}\|Id_{L_v})$。

③ 使用共享密钥 $K_{u,v}$ 计算 $MAC_{K_{u,v}}(Id_{G_v},Id_{L_v},N_v,N_u)$，并将计算得到的 MAC 值与接收到的 MAC 值进行匹配。若匹配成功，则将 $K_{u,v}$ 作为它与节点 v 之间的共享密钥进行保存，并向节点 v 发送确认信息$\{ok,MAC_{K_{u,v}}(ok,N_v)\}$。否则，删除 $K_{u,v}$。

步骤四　节点 v 接收到节点 u 发送的信息后，使用共享密钥 $K_{v,u}$ 计算 $MAC_{K_{v,u}}(ok,N_v)$，进行信息认证。若通过认证，则将 $K_{v,u}$ 作为与节点 u 之间的共享密钥进行存储，否则删除 $K_{v,u}$。

上述过程结束后，节点 v,u 之间的共享密钥为

$$\begin{aligned}K_{v,u}&=f_{(k,j)v}(y)=f_{(k,j)v}(Id_{G_v}\|Id_{L_v},Id_{G_u}\|Id_{G_u})\\&=f_{(k,j)u}(Id_{G_u}\|Id_{G_u},Id_{G_v}\|Id_{L_v})\\&=f_{(k,j)u}(y)=K_{u,v}\end{aligned}$$

1. $u\xrightarrow{\{hello,ID_{G_u},ID_{L_u},N_u\}}v$

2. $u\xleftarrow{\{ID_{G_v},ID_{L_v},N_v,MAC_{K_{v,u}}(ID_{G_v},ID_{L_v},N_v,N_u)\}}v$

计算 $K_{v,u}=f_{(k,j)v}(Id_{G_u}\|Id_{L_u})$

3. $u\xrightarrow{\{ok,MAC_{K_{v,u}}(ok,N_v)\}}v$

计算 $K_{v,u}=f_{(k,j)v}(Id_{G_u}\|Id_{L_u})$

进行信息验证，验证通过则保存 $K_{u,v}$，并发送信息给节点 v，否则删除 $K_{u,v}$

4. u　　v

对接收到的信息进行验证，验证通过则保存 $K_{v,u}$，否则删除 $K_{v,u}$

图 3　节点 u,v 共享密钥建立过程图

当有新节点要求加入网络时，需要通过离线的认证机构对请求加入的节点进行身份认证。通过认证后，基站将根据新节点将要加入的单位网格，为其分配本地标志符，并根据新节点将要加入的单位网格的标志符以及分配的本地标志符，为其计算一组秘密多项式，并存储在该节点中。该过程完成后，新节点加入网络，并可与网络中任意一个节点建立它们之间的共享密钥。

基于分层网格的密钥预分配方案，在共享密钥建立过程中利用单位网格标志符来决定任意两个传感器节点应该采用哪个秘密多项式进行共享密钥的计算。该方案利用不同的对称二元多项式完成了不同节点间共享密钥的构建。方案最大的优点在于，即使某个单位网格内的所有节点都被敌手俘获了，也不会暴露其它网格内节点之间的共享密钥信息，有效地降低了部分节点被俘获后对网络安全造成的影响。

4　性能分析

从存储开销和计算开销两方面分析 HG-SBP 方案的性能。

(1) 存储开销。HG-SBP 方案中每个传感器节点所需要存储的信息有：

① 用于标识传感器节点的标志符。该标志符由传感器节点 u 所在的单位网格标志符 Id_{G_u} 串接节点 u 的本地标志符 Id_{G_u} 构成，则用于存储该标志符的存储开销 MC_1 为：

$$MC_1=|Id_{G_u}|+|Id_{L_u}|=n-1+log_2 m=n-1+\lceil\log_2\frac{N}{2^{n-1}}\rceil \quad (4)$$

② n 个秘密多项式。HG-SBP 方案中，每一个传感器节点都需要存储 n 个秘密多项式。设 $L_i(i\in[1\cdots n])$层的网格对应 $2^{n-i}\times t_1$ 次方秘密多项式，并设 $t_1=0.6\times m$[8]。由于任意一个系数在 $GF(q)$ 中的 t_1 次方对称二元多项式可以用$(t_1+1)\times\log(q)$位来表示[9]，则每个传感器节点存储 n 个秘密多项式的存储开销 MC_2 为：

$$MC_2=P_{t_1}\sum_{i=1}^{n}(2^{n-i})t_1=(\frac{0.6\times N}{2^{n-1}})(2^n-1)(\frac{0.6\times N}{2^{n-1}}+1)\log_2(q) \quad (5)$$

其中 P_{t_1} 表示存储 t_1 次方多项式 $f(Id_{G_u}\|Id_{L_u},y)$所需的开销。综合以上，HG-SBP 方案中每个传感器节点的存储开销 MC 为：

$$MC=MC_1+MC_2=n-1+\lceil\log_2\frac{N}{2^{n-1}}\rceil+(\frac{0.6\times N}{2^{n-1}})(2^n-1)(\frac{0.6\times N}{2^{n-1}}+1)\log_2(q) \quad (6)$$

(2) 计算开销。HG-SBP 方案中的计算开销主要是传感器节点进行共享密钥建立过程中所需要的计算开销，主要包括如下 3 个部分：

① 秘密多项式选取的开销，即匹配两个单位网格标志符的计算开销。设两个二进制字符串比较的计算开销为常量 c，则传感器节点用于选取秘密多项式的计算开销 CC_1 为：

$$CC_1=c \quad (7)$$

② 秘密多项式计算的平均开销。设 P_i 为两个传感器节点在 $L_i(i\in[1\cdots n])$层同一网格中的概率，并设与 L_i 层中的网格相对应的秘密多项式的计算开销为 SBP_i，则秘密多项式计算的平均开销 CC_2 为：

$$CC_2=\sum_{i=1}^{n}(P_iSBP_i) \quad (8)$$

③ 信息认证开销。两次 MAC 计算，一次 MAC 值的匹配。设一次 MAC 计算开销为 d，MAC 值的匹配的计算量为 e，则用于信息认证的计算开销 CC_3 为：

$$CC_3=2d+e \quad (9)$$

综合以上，HG-SBP 方案中每个传感器节点的计算开销 CC 为：

$$CC=CC_1+CC_2+CC_3=\sum_{i=1}^{n}(P_iSBP_i)+c+2d+e \quad (10)$$

HG-SBP 方案中，不同层中的网格对应的对称二元多项式的次方不同，网格所在层越高，对应的对称二元多项式的次方越大。假设 HG-SBP 方案中 L_1 层中的网格对应的对称二元多项式的次方与 Blundo 方案中的对称二元多项式次方相同，则由式(8)知 HG-SBP 方案中秘密多项式的平均计算量要小于 Blundo 方案中秘密多项式的计算量。显然与 Blundo 方案相比，HG-SBP 方案有效地降低了传感器节点的能量消耗。

随机密钥预分配方案中，每个传感器节点的存储开销由其所需要存储的密钥数来衡量。而这类方案中，每对相邻节点共享密钥数与密钥子空间维数和节点存储的密钥数相关。例如，对维数 1000 的密钥子空间，每个节点存储 50 个密钥，

存在共享密钥的概率为 0.9[10]。随机密钥预分配方案中的计算开销包括密钥发现阶段需要进行的哈希函数运算、异或运算以及节点间的通信运算。此外，当有新节点加入网络时，随机密钥预分配方案必须重新执行密钥发现过程。因此，HG-SBP 方案与随机密钥预分配方案，例如 E-G[3]，q-Composite[4] 方案相比，存储和计算开销处在同一层次。

5 安全性分析

HG-SBP 方案在分层网格结构上基于 Blundo 所提出的对称二元多项式构建传感器节点间的共享密钥。在 Blundo 方案中，当网络中被敌手俘获的节点总数小于 $t+1$ 时(其中 t 为对称二元多项式的次方)，该网络是安全的[6]。t 值越大，网络的安全性越高。在 HG-SBP 方案中不同网格对应不同的多项式，传感器节点在构建共享密钥时，首先选择相应的多项式，然后由该多项式进行共享密钥的计算。这种设计方法能有效降低部分节点被俘获后对网络安全造成的影响，增强了网络的健壮性。详细分析如下：

(1)敌手 A 俘获了 $W(W<t_1+1$，其中 t_1 为单位网格对应的对称二元多项式的次方)个传感器节点。假设敌手 A 俘获了 W 个传感器节点，由 Blundo 方案的安全性知，即使这 W 个传感器节点都属于同一个单位网格，敌手 A 也无法从这 W 个传感器节点所存储的信息中破解任何一个对称二元多项式，保证了 W 个传感器节点信息的泄漏不会暴露其它传感器节点的秘密信息，此时的网络仍然是安全的。

(2)针对单位网格的攻击。假设敌手 A 俘获了 S 个传感器节点，其中 $t_1+1\leqslant S\leqslant m$，且至少有 t_1+1 个传感器节点属于同一个单位网格，则敌手 A 可以破解该单位网格所对应的对称二元多项式，但是无线传感器网络中一共有 2^{n-1} 个单位网格，t_1+1 个传感器节点属于同一个单位网格的概率 P_S 为：

$$P_S=\sum_{i=t_1+1}^{S}\binom{S}{i}\left(\frac{1}{2^{n-1}}\right)^i\left(1-\frac{1}{2^{n-1}}\right)^{S-i} \tag{11}$$

显然，敌手 A 所俘获的 S 个传感器节点中存在 t_1+1 个节点属于同一个单位网格的概率较小。针对其它单个网格的攻击分析同上。此外，由于每一个网格对应的对称二元多项式都不相同，因此即使敌手 A 破解了某个网格所对应的对称二元多项式，他也无法从得到的信息中破解其它网格所对应的对称二元多项式，保证了其它网格中未俘获传感器节点间信息传输的安全性，增强了网络的健壮性。

(3)针对整个网络的攻击。针对整个网络攻击的一般形式是逐个破解所有对称二元多项式。敌手 A 想要破解 $2^{n-i}\times t_1$ 次方对称二元多项式，就需要俘获该多项式对应网格中的 $2^{n-i}\times t_1+1$ 个传感器节点。而 L_i 层中有 2^{i-1} 个网格，它们对应的对称二元多项式的次方为 $2^{n-i}\times t_1$，因此敌手 A 想要破解 L_i 层中的所有对称二元多项式，就至少需要俘获 $2^{i-1}\times(2^{n-i}t_1+1)$ 个传感器节点。而敌手 A 想要针对整个网络进行攻击，就至少需要俘获 $2^{n-1}\times(t_1+1)$ 个传感器节点来破解所有的对称二元多项式，显然敌手 A 需要俘获的传感器节点总数较大(例如超过网络中传感器节点总数的 3/5)。

在随机密钥预分配方案中，网络的健壮性用概率来描述。如 q-composite 方案中，某个节点被俘获后，其它节点不被俘获的概率是 $(1-m/S)^x$，其中 x 是被俘获的节点数，m 是节点中存储的密钥总数，S 是密钥子空间的维数。要想保证网络的健壮性，就需要 S 充分大，m 充分小。但是 S 过大或者 m 过小都可能导致相邻节点找不到共有的密钥，造成无法通信的严重后果[11]。HG-SBP 方案中，不同的网格所对应的对称二元多项式都是不同的，而且网格所在层越高，对应的对称二元多项式的次方越大。由前面的安全性分析知，分层网格的设计能够有效降低部分节点被俘获后对网络安全造成的影响，增强了网络的健壮性，与目前的随机密钥预分配方案相比更具有优越性。

此外，随机密钥预分配方案中，所有节点的密钥都是从一个密钥子空间中选取的，这就无法避免多对节点拥有相同的共享密钥。节点数目越大，节点对之间共享密钥的重复性就越大，从而给网络安全带来隐患。HG-SBP 方案中，每对传感器节点间所构建的共享密钥都是惟一的。因此，与目前的随机密钥预分配方案相比，HG-SBP 方案在安全性方面更具有优越性。

结束语 无线传感器网络自身的特点使其安全机制面临严峻挑战。密钥管理机制则是构建安全的无线传感器网络的核心技术。本文提出了一种基于分层网格结构的无线传感器网络密钥预分配方案 HG-SBP。在该方案中给出了一种新的单位网格标志符设置方法，并利用该标志符选取不同的秘密多项式来构建节点间的共享密钥。这种设计方法在控制传感器节点计算量的同时能有效地降低部分节点被俘获后对网络安全造成的影响，增强了网络的健壮性。与随机密钥预分配方案相比，HG-SBP 方案在计算和存储开销方面与其处在同一层次，在健壮性和安全性方面则具有一定的优势。在今后的工作中，我们将进一步研究如何降低节点的计算和存储开销。

参 考 文 献

[1] Akyildiz L F, Weilian S, Sankarasubramaniam Y, et al. A survey on sensor networks [J]. IEEE Communications Magazine, 2002, 40(8):102-114

[2] Carman D W, Kruus P S, Matt B J. Constraints and approaches for distributed sensor security [R]. Technical Report, 002010. NAI Labs, 2000

[3] Eschenauer L, Gligor V D. A key-management scheme for distributed sensor networks // Proceeding of the 9th ACM Conference on Computer and Communications Security[C]. Washington DC, USA: ACM Press, 2002:41-47

[4] Chan H, et al. Random key predistribution schemes for sensor networks[C] // IEEE Symposium on Research in Security and Privacy. New York: IEEE Publishing, 2003:197-213

[5] Cheng B, Sungha D. Reduce radio energy consumption of key management protocol for wireless sensor networks [C] // ISLPED'04. 2004:351-356

[6] Blundo R, Suntis A D, Herzbeg A, et al. Perfectly secure key distribution for dynamic conferences[C] // Advances in Cryptology-CRYPTO'92. LNCS 740. 1993:471-486

[7] Li J, Janotti J, DeCouto D S J, et al. A Scalable Location Service for Geographic Ad Hoc Routing[C] // The Sixth Annual International Conf. on Mobile Computing and Networking. 2000: 120-130

[8] Huang D, Mehta M, Mehdi D, et al. Location-aware Key Management Scheme for Wireless Sensor Networks [C] // Proc. of 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04). 2004:29-42

[9] Mohaisen A, Nyang D-H. Hierarchical Grid-Based Pairwise Key Predistribution Scheme for Wireless Sensor Networks [C] // EWSN 2006. LNCS3868. 2006:83-98

[10] Du W, et al. A pairwise key predistribution scheme for wireless sensor network [J]. ACM Transactions on Information and System Security, 2005, 8(1):41-47

[11] 杨庚，王江涛，程宏兵，等. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报，2007，35(1)：180-184