文章编号:1671-4598(2023)03-0208-07 DOI:10.16526/j.cnki.11—4762/tp.2023.03.030 中图分类号:TP309;TN918 文献标识码:A

基于六边形网格组部署的对称密钥预分配模型

庞浩杰[1],常 凯[2],金 琰[1],朱 亮[3]
(1.河南省洛阳正骨医院(河南省骨科医院),郑州 450016;2.湖北中医药大学 信息工程学院,武汉 430065;
3.郑州轻工业大学 计算机与通讯工程学院,郑州 450002)

摘要:针对无线传感器网络的加密体制进行了研究;首先,提出了一种基于六边形网格组的传感器网络节点的部署策略,以获得传感器节点的最佳分布;其次,将密钥空间定义为采用Blundo模型生成的一个t次二元多项式$f(x,y)$的全部密钥的集合;然后通过密钥预分配阶段将密钥材料分配给每个节点,通过直接密钥建立阶段使得每个传感器节点找到与其相邻节点的共享密钥空间;如果两个相邻节点之间没有共享密钥空间,则通过间接密钥建立阶段使得一个或多个中间节点建立起一个路径密钥,从而完成共享密钥空间的建立;仿真实验结果表明,提出的对称密钥预分配模型不仅具有良好的加密性能,而且相比于其他模型的密钥方案有更好的内存开销、运行时间和节点受损攻击时的网络恢复能力。

关键词:无线传感器网络;节点部署;共享密钥空间;预分配;连通性

Symmetric Key Pre-distribution Model Based on Hexagonal Grid Group Deployment

PANG Haojie[1], CHANG Kai[2], JIN Yan[1], ZHU Liang[3]
(1. Henan Luoyang Orthopedic Hospital (Henan Orthopedic Hospital), Zhengzhou 450016, China;
2. Information Engineering College, Hubei University of Traditional Chinese Medicine, Wuhan 430065, China;
3. School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China)

Abstract: The encryption system of wireless sensor networks is studied. Firstly, a deployment strategy of sensor network nodes based on hexagonal grid group is proposed to obtain the optimal distribution of sensor nodes. Secondly, the key space is defined as the set of all keys of a t-degree binary polynomial f (x, y) generated by the Blundo model. Then, the key materials are allocated to each node through the key pre-distribution stage, and each sensor node finds the shared key space with its neighboring nodes through the direct key establishment stage. If there is no shared key space between two adjacent nodes, one or more intermediate nodes are required to establish a path key through the indirect key establishment stage, so the establishment of shared key space is completed. The simulation results show that the proposed symmetric key pre-distribution model not only has good encryption performance, compared with other key schemes, but also has the better features of memory overhead, running time and network recovery capability in case of node damage.

Keywords: wireless sensor networks; node deployment; shared key space; pre-distribution; connectivity

0 引言

传感器网络有许多应用,如家庭安全监控、军事侦察、环境监测和目标跟踪等等[1-4]。典型的传感器网络通常由大量的微小感知设备构成,这些设备又称为传感器节点,它们的电池电量和数据处理能力有限,并且通常通过短距离无线电信号彼此通信;在许多应用中,传感器节点通常随机分布在特定区域,以感知和收集有用的信息。

传感器网络最基本的安全要求之一是保证传感器节点间发送信息的保密性和完整性。尤其是传感器网络部署在“敌对”环境中时,密钥的建立在认证和加密中起着很重要的作用。攻击者可以通过对传感器节点发起物理攻击,或者对不同的通信协议采用逻辑攻击来窃听消息或使网络失效[5-6]。因此,传感器网络需要加密和认证服务。由于资源的限制,实现有效的密钥建立机制并不是一项简单的任务。除了目前流行的椭圆曲线密码体制外[7],对称密钥算法[8]也是解决这一问题的可行途径。

文献[9]提出的随机密钥预分配模型离线生成一个大的密钥池,每个传感器从密钥池中随机选取一个密钥子集。通信范围内的任意两个节点只有共享一个公用密钥才能相互通信。根据密钥池的大小和网络中传感器节点的数量,这种体制可以实现不同的连通性和恢复能力;文献[10]提出将部署知识应用到基本的随机成对密钥中;文献[11]通过应用部署知识提出了一种密钥预分配模型。在这种模型中,把整个网络分成组,每个组执行基本的随机密钥预分配。一个组的密钥池与水平组密钥池共享(个密钥,与对角组密钥池共享(个密钥;从Blom解决方案[12]发展而来的密钥矩阵方案还有文献[13]的多空间密钥预分配模型。

文献[14]提出了采用多项式的随机密钥生成思想。

收稿日期:2022-10-26; **修回日期**:2022-12-05。
基金项目:河南省科技攻关项目(212102210095)。
作者简介:庞浩杰(1981-),男,河南洛阳人,大学本科,工程师,主要从事计算机网络技术、人工智能技术、医院信息化技术方向的研究。
引用格式:庞浩杰,常 凯,金 琰,等.基于六边形网格组部署的对称密钥预分配模型[J].计算机测量与控制,2023,31(3):208-214.

它采用对称多项式计算来获得成对密钥。这种方案对捕获的节点具有 t－串谋抵抗能力，即小于 $t+1$ 个节点的攻击不会泄露任何关于其他节点密钥的信息；文献［15］基于该思想和基本随机密钥预分配[9]，提出了随机子集分配密钥预分配模型。与生成大型密钥池和创建密钥环不同，该方案创建一个大型多项式池，并从池中为每个节点分配一个多项式子集。这样，两个节点只有共享至少一个公用多项式才能相互通信。结果表明，与文献［9］模型相比，这种模型提高了恢复能力；文献［16］提出了利用预部署知识的私有多项式预分配方案，文献［17］提出了基于 8－方形网格的多项式预分配方案；文献［18］针对 Sheetal Kalra 方案容易在数据库泄露和用户智能卡丢失的情况下受到用户的假冒攻击、并且不能达成正确的共享密钥的分析，基于口令的无线传感器网络认证方案，提出了一种改进的带有智能卡的认证方案，解决了 Sheetal Kalra 方案中的安全性问题，提供了用户、传感器、网关节点之间的相互认证并达成正确的共享密钥。此外，还给出了提出方案的安全性分析，以此证明提出的方案可以满足无线传感器网络中的安全需求；文献［19］针对移动异构无线传感器网络模型，提出了在一种安全高效的密钥管理方法。方法采用椭圆曲线密码学加密算法实现移动节点位置信息到基站的安全上传，以及基于密钥哈希的消息认证码来实现消息源的身份认证。基站则对收集的移动节点位置信息进行统计分析来协助完成固定节点与移动节点间的身份认证及会话密钥建立。实验结果表明，所提出的方法在密钥建立过程中节省了网络资源，同时可有效防御攻击者发起重放攻击，节点复制攻击和女巫攻击等，增强了网络的安全性；文献［20］基于具有节点移动性的动态传感器网络安全通信，分析了一种证书无效密钥管理（CL-EKM，certificate less-effective key management）协议，保护数据和通信需要适当的加密密钥协议。针对具有节点移动性的动态传感器网络的安全通信，提出了一种证书无效密钥管理（CL-EKM）协议。CL-EKM 协议支持在节点离开或加入集群时进行高效的密钥更新，并保证了向前和向后的密钥保密。该协议还支持对被破坏的节点有效的密钥撤销，并将节点被破坏对其他通信链路安全的影响降到最低。对方案的安全性分析表明，该方案能够有效地防御各种攻击。

上述这些解决方案在采用预部署知识来提高性能和安全性方面仍有一些局限性。对此，本文提出了一种基于六边形网格组部署的无线传感器网络对称密钥预分配模型。模型将多项式信息分配到一个六边形网格组中的特定区域内有限数量的传感器节点上，从而使得每个传感器节点找到与其相邻节点的共享密钥空间；仿真实验结果表明，提出的对称密钥预分配模型不仅具有良好的加密性能，而且相比于其他模型的密钥方案有更好的内存开销、运行时间和节点受损攻击时的网络恢复能力。

1　相关模型

1.1　基于 Blom 思想的密钥预分配模型

基于 Blom 思想提出的密钥预分配模型[9]能够确保组中的任何一对成员都可以计算公用共享密钥。用 $\boldsymbol{N}$ 表示网络中传感器节点数目，$\boldsymbol{G}$ 为有限域上大小为 $(t+1)\times N$ 的生成矩阵，$\boldsymbol{D}$ 为大小为 $(t+1)\times(t+1)$ 的秘密随机矩阵，其中 t 为攻击者攻击的节点个数。从矩阵 $\boldsymbol{G}$ 和 $\boldsymbol{D}$，构造一个 $N\times N$ 的对称矩阵 $\boldsymbol{K}$，它的元素是节点之间的成对密钥，则矩阵 $\boldsymbol{K}$ 为：

$$\boldsymbol{K}=(\boldsymbol{D}\cdot\boldsymbol{G})^{T}\cdot\boldsymbol{G} \tag{1}$$

每个节点 i 存储私有矩阵 $\boldsymbol{A}=(\boldsymbol{D}\cdot\boldsymbol{G})^{T}$ 对应的第 i 行。如果节点 i 想要与节点 j 通信，则它计算其存储的行向量与 $\boldsymbol{G}$ 的第 j 列的内积，得到公用密钥 $K_{i,j}$。文献［13］的多空间密钥预分配模型将 Blom 思想与文献［9］的基本随机密钥预分配模型相结合应用于传感器网络。在这种方法中，他们将每个元组（D，G）生成的密钥空间表示为密钥集合。网络中的每个节点随机存储来自于 ω 个预生成空间的 τ 个空间。基于概率，任意两个节点可以共享一个公用空间，该空间可以计算出一个公用秘密密钥。所有密钥矩阵解决方案都具有阈值 t－安全特性，即当攻击者攻击的节点不超过 t 个时，未被攻击的节点之间的通信仍然是安全的。

1.2　基于 Blundo 思想的密钥预分配模型

基于 Blundo 思想提出的多项式密钥预分配模型[15]采用对称多项式计算来获得成对密钥，方案使用 n 个变量的 t 次多项式来建立 t-安全 n-联盟的密钥分配。应用于两个对象之间的成对密钥，密钥预分配服务器在一个有限域 F_q 上随机生成一个二元 t 次多项式：

$$f(x,y)=\sum_{i,j=0}^{t}a_{ij}x^{i}y^{j} \tag{2}$$

其中：q 是一个足够大的素数，可以容纳一个密码密钥，函数 $f(x,y)$ 是对称的即 $f(x,y)=f(y,x)$。每个节点有唯一的整数 ID i，加载来自于多项式 $f(x,y)$ 的信息 $f(i,y)$。这样，任意两个节点 i 和 j 可以计算节点 i 的密钥 $K_{i,j}=f(i,j)$ 和节点 j 的密钥 $K_{j,i}=f(j,i)$。由于对称特性，有：

$$K_{i,j}=K_{j,i} \tag{3}$$

故两个节点有一个共用的成对密钥。

每个节点必须存储 $t+1$ 个系数，每个系数有 $\log_2 q$ 比特（bits）。因此，该模型中每个节点的内存存储需求为 $(t+1)\log_2 q$ 比特。由于存储密钥的内存开销很大，这种方案不能直接应用于传感器网络，因为内存的大小按指数规律依赖于网络的规模，因此对于资源受限的传感器节点等设备来说是不可行的；对此，本文将通过采用预部署知识来解决这个问题，并表明相比其他基于多项式的、应用预期位置知识的方案更具优势；此外，我们在计算成对密钥中还加入了一些随机数，这样，对手就很难对未捕获节点的额外安全连接造成破坏。

2　基于六边形网格组部署的对称密钥预分配模型

在提出本文方案之前，我们将密钥空间定义为采用 Blundo 模型生成的一个 t 次二元多项式 $f(x,y)$ 的全部密钥的集合，密钥空间中的密钥数量表示密钥空间大小。

假设如果一个节点携带 $f(x, y)$ 生成的信息，则它将选择一个密钥空间。任意两个选择公用密钥空间的节点总是计算它们的成对密钥。

节点 n_A 选择密钥空间 $f_{u,v}(x, y)$，如果它携带 $f_{u,v}(n_A \oplus Rv_A, y)$ 的系数，其中 Rv_A 是节点 n_A 的随机值，将在密钥预分配阶段进行描述。当两个节点在相同的密钥空间时，它们可以计算成对密钥来建立安全通道。

本文方案允许传感器节点在部署后找到与其相邻的每个节点的公用密钥空间。方案共分为 3 个阶段：密钥预分配阶段、直接密钥建立阶段和间接密钥建立阶段。在部署前执行密钥预分配阶段，将凭证信息预加载到每个传感器节点。之后，如果两个传感器节点至少共享一个共用密钥空间，则可在它们之间建立一个直接密钥，否则，它们可以在间接密钥建立阶段的基础上商定一个间接密钥。

首先，要解决传感器网络的部署模型。

2.1 基于六边形网格组的传感器节点部署

在本文模型中，把目标区域划分为六边形网格。六边形网格提供了对圆的最佳近似，比在连续区域中可以重复使用的其他 2 种几何图形（三角形和矩形）所覆盖的面积更大。与矩形的 8 个或三角形的 12 个相邻单元格相比，六边形有最少的相邻单元格（6 个）。传感器节点在单元格上进行划分并分组。这种模型适合于实际场景，当每组的传感器节点一起部署时，预期的相邻组更有可能彼此接近。

一般情况下，传感器节点的排列依赖于某个概率分布函数（PDF，probability distribution function）。假设目标部署区域是二维的，其大小为 $X \times Y$，节点 n_i（$i=1, \cdots, N$）位置的 PDF 在二维区域上为 $f_i(x, y)$，其中 x（$[0, X]$，y（$[0, Y]$。N 个传感器节点被分成 G 个大小相等的组。PDF 可以是均匀分布的，或者是更符合实际的高斯分布，故假设每个组服从二维高斯分布。当组 G_i 的部署点在（x_i^o，y_i^o）处时，属于组 G_i 的节点 n_i 的 PDF 计算如下：

$$f(n_i(x_i, y_i) \mid n_i \in G_i) = \frac{1}{2\pi\sigma^2}\exp\{-[(x_i - x_i^o)^2 + (y_i - y_i^o)^2]/2\sigma^2\} = f(x_i - x_i^o, y_i - y_i^o) \quad (4)$$

式中，(x_i, y_i) 为组 G_i 中的节点 n_i 的坐标，σ 为分布的标准偏差。基于六边形网格组的部署模型如图 1 所示。

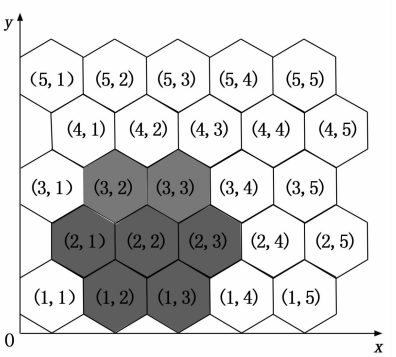

图 1 基于六边形网格组的部署模型

在描述本文方案的原理之前，定义集群为 3 个相邻组的集合，一个组有 3 种类型的集群：1－集群、2－集群和 3－集群。对于任何一个组（i，j），1－集群包含这个组（i，j）和组（$i+1$，j）以及（$i+1$，$j+1$），2－集群包含这个组（i，j）和组（i，$j-1$）以及（$i-1$，j），3－集群包含这个组（i，j）和组（$i-1$，$j+1$）以及（i，$j+1$）。

例如在图 1 中，对于组（2，2）来说，组（3，2）和组（3，3）属于 1－集群（2，2），组（2，1）和组（1，2）属于 2－集群（2，2），组（2，3）和组（1，3）属于 3－集群（2，2）。

在一个单元格上，分布函数可能是不均匀的，但可以在部署点之间选择合适的距离，使得总体分布接近均匀。

2.2 密钥预分配阶段

此阶段的目标是将密钥材料分配给每个节点。基于这些密钥材料，相邻节点在部署后可以对密钥进行配对设置。

这个任务是通过离线服务器完成的。首先，服务器为每个集群生成一个多项式池 F，它包含足够多的 t 次对称二元多项式。然后将每个多项式分配给每个集群中的所有传感器节点。由于每个单元格属于 3 个集群，所以每个节点要存储 3 个 t 次二元多项式的知识。换句话说，每个节点要选择 3 个密钥空间。算法 1 所示为多项式预分配实现的伪代码。

这一阶段完成后，每个传感器节点存储一个节点 ID、3 个空间 ID、一个随机值和 3 个对应于 3 个密钥空间的系数向量的值。这些密钥材料将用于下一阶段的成对钥匙建立。

算法 1：多项式预分配算法

Input：网络中的节点集合 N，集群集合 Ψ，多项式池 F

Output：加载密钥材料给网络中的每个传感器节点

```
1. For 每个组 G_{i,j}
2.    For 1－集群(G_{i,j})中的每个组 G_{u,v}
3.       If 不在 polynomial_sharing(G_{u,v}, G_{i,j})中
4.          生成一个 f(x,y)
5.          把 f(x,y)分配给 1－集群(G_{i,j})
6.       Endif
7.  Endfor
8.    For 2－集群(G_{i,j})中的每个组 G_{u,v}
9.       If 不在 polynomial_sharing(G_{u,v}, G_{i,j})中
10.         生成一个 f(x,y)
11.         把 f(x,y)分配给 2－集群(G_{i,j})
12.  Endif
13. Endfor
14. For 3－集群(G_{i,j})中的每个组 G_{u,v}
15.   If 不在 polynomial_sharing(G_{u,v}, G_{i,j})中
16.         生成一个 f(x,y)
17.         把 f(x,y)分配给 3－集群(G_{i,j})
18.      Endif
19.   Endfor
20. Endfor
```

2.3 直接密钥建立阶段

在传感器节点部署到目标区域后，每个传感器节点必须找到与其相邻节点的共享密钥空间。假设节点 n_A 具有 3

个空间 ID f_i，f_j，f_k，需要与其邻居发现共享密钥空间。它广播一个 1－跳发现消息—密钥空间发现消息（KSDM，key-space discovery message）如下：

$$(n_A, Rv_A, H(f_i \oplus Rv_A), H(f_j \oplus Rv_A), H(f_k \oplus Rv_A)) \tag{5}$$

式中，H 为哈希函数，$\oplus$为异或运算。

当 A 的一个邻居（设为 B）接收到这个消息时，它会发现它可以与 A 共享 3 个、1 个或不共享公用密钥空间。类似地，节点 A 也接收到 B 的 KSDM 消息并发现公用密钥空间。如果共享至少 1 个公用密钥空间，则 B 和 A 之间的成对密钥在 B 点计算如下：

$$K_{B,A} = f(n_B \oplus (Rv_B, n_A \oplus Rv_A)) \tag{6}$$

在获得 $K_{B,A}$之后，节点 B 从它的内存中删除 Rv_A 值。计算 A 点的成对密钥的过程与此类似。由于二元多项式的对称性，所以：

$$K_{A,B} = K_{B,A} \tag{7}$$

完成这一阶段后，除了前一阶段的密钥空间信息和一个随机值外，每个节点还存储一个与其相邻节点的成对密钥列表。

2.4　间接密钥建立阶段

如果两个相邻节点之间没有公用密钥空间，则需要通过一个或多个中间节点建立一个路径密钥，实现过程如下。

在直接密钥建立阶段之后，每个节点 A 知道其安全邻接节点的集合 S_A。源节点 A 希望与其邻居 B 建立一个成对密钥，但是 B 和 A 不共享任何密钥空间。在这种情况下，A 生成一个会话密钥 K_S，并找到在 S_A 中与节点 B 有相同的组 ID 或包含节点 B 的组的相邻组 ID 的节点 C，然后节点 A 向节点 C 发送一条包含通过密钥 $K_{A,C}$加密的 K_S 消息。然后，节点 C 通过密钥 $K_{C,B}$保护的安全通道向 B 发送会话密钥，则密钥 K_S 作为节点 A 和节点 B 之间的成对密钥。

在以上 3 个阶段完成之后，每个节点都存储一个包含邻居的 IDs 和对等的密钥表。密钥材料的存在使得传感器网络能够增加新的节点供后面替换。

2.5　传感器节点的添加和删除

为了增加一个新的传感器节点，密钥建立服务器只需要将相关的多项式共享预先分配给新节点，类似于预分配阶段。由于密钥空间的大小是有限的，添加的传感器越多，该单元中的安全性就越低；删除方法很简单。每个传感器节点只需要存储一个与自身共享至少一个二元变量多项式的被破坏传感器的黑名单 IDs。如果有超过 t 个被破坏节点共享同一个多项式，则拥有该多项式的非被破坏节点将删除该多项式和所有相关的被破坏节点。

算法 2 为密钥建立和分配实现的伪代码。

算法 2：密钥建立和分配算法

1. For N 中每个传感器节点 n_A **Do**
2.　对 n_A 的预加载数据生成并插入一个随机值 Rv_A；
3. **Endfor**
4. **For**（中每个集群 C_i **Do**
5. 从 F 中获取一个二元多项式 $f_{i(}x,y)$；
6. **For** C_i 中每个节点 n_A **Do**
7.　计算 $f_i(n_A \oplus Rv_A, y) = \sum_{j=0}^{t} b_j y_j$；
8.　插入 n_A 的预加载数据 $\{b_j \mid j = 0,\ldots,t\}$；
9.　将多项式的 ID(也称为了空间－ID) f_i 插入到 n_A；
10. **Endfor**
11. 从 F 中删除 $f_i(x,y)$；
12. **Endfor**

3　算法仿真实验结果及分析

仿真中采用的度量指标如下。

1）网络连通性：包括局部连通性和全局连通性。局部连通性是指一个节点可以在其传输范围内与相邻节点连接的概率。全局连通性是最终密钥图 G 中形成最大独立连通部分的传感器节点数目与整个网络的大小之比。

2）内存开销和运行时间：内存开销为模型中在节点上存储密钥材料的内存需求，运行时间为密钥空间形成和分配，直至最终两个节点获得成对密钥所消耗的时间。

3）对捕获节点攻击的恢复能力：对手通常发起节点捕获攻击，以窃听网络中的安全通道，或者利用捕获节点泄露的密钥材料进行节点复制攻击。在此分析中，我们评价节点破坏攻击对剩余网络通信的影响，即对手能够发现一个二元多项式的概率，这意味着它们可以泄露所有由这个多项式得到的加密安全连接。

3.1　系统配置

采用表 1 中的设置进行仿真和数值分析。在这种场景下，假设节点部署遵循二维高斯分布，其 PDF 函数如式（1）所示。

表 1　仿真设置

符号	值	描述
N	10 000	网络中传感器节点数
S	1 000×1 000(m^2)	网络部署区域
R	40(m)	传感器节点的通信范围
M	200(密钥)	存储密钥材料的内存
σ	50(m)	高斯分布的标准偏差

3.2　网络连通性

假设 A（n_i，n_j）和 B（n_i，n_j）为事件，节点 n_i 为节点 n_j 的邻居，它们共享至少 1 个共用密钥空间。局部连通性可以计算为：

$$P_{local} = P(B(n_i,n_j) \mid A(n_i,n_j)) = \frac{P(B(n_i,n_j) \cap A(n_i,n_j))}{P(A(n_i,n_j))} \tag{8}$$

节点 $n_i \in G_i$ 为节点 n_j（x_j，y_j）的邻居的概率是在节点 n_j 周围半径为 R 的圆上的 PDF f（n_i）的积分：

$$P(n_j(x_j,y_j)) = \iint_{G_i \cdot \| (x,y),(x_j,y_j) \| \leqslant R} f(n_i(x,y))\mathrm{d}x\mathrm{d}y \tag{9}$$

由于 n_j 按式（1）分布在组 G_j 中，所以 $n_i \in G_i$ 为 $n_j \in G_j$ 的邻居的概率为：

$$P(A(n_i,n_j)\mid G_i,G_j)=\iint_{G_j}P(n_j(x_j,y_j))f(n_j(x,y))\mathrm{d}x\mathrm{d}y \tag{10}$$

因此：

$$P(A(n_i,n_j))=\sum_{G_i\in\Psi}\sum_{G_j\in\Psi}P(n_i\in G_i)P(n_j\in G_j)\cdot P(A(n_i,n_j)\|G_i,G_j) \tag{11}$$

用 $S(G_i)$ 表示 G_i 相邻组的集合，则有：

$$P(B(n_i,n_j)\cap A(n_i,n_j))=\sum_{G_i\in\Psi}\sum_{G_j\in S(G_i)}P(n_i\in G_i)\cdot P(n_j\in G_j)\cdot P(A(n_i,n_j)\|G_i,G_j) \tag{12}$$

由于传感器节点是在给定的组中以相等的概率被选择的，因此局部连通性可以计算为：

$$P_{\text{local}}=\frac{\sum_{G_i\in\Psi}\sum_{G_j\in S(G_i)}P(A(n_i,n_j)\|G_i,G_j)}{\sum_{G_i\in\Psi}\sum_{G_j\in\Psi}P(A(n_i,n_j)\|G_i,G_j)} \tag{13}$$

用 $d=k\times\sigma$ 表示两个相邻单元格的两个部署点之间的距离（k 为比例系数），这个值会影响网络的局部连通性和全局连通性。当 k 值较大时，则一个组中几乎每个节点都位于自己的单元格区域内，而且相邻节点都来自自己的组。在这种情况下，局部连通性非常高，但网络完全被分割成单独的部分，这意味着全局连通性非常低；当 d 值较小时，可能局部连通性较低，但全局连通性较高。因此，选择合适的 d 值会影响网络的连通性。由于无线传感器网络中密钥建立的最终目标是形成尽可能高的全局连通性网络，因此必须适当选择相邻部署点的距离 d 的值。

表 2 所示为通过改变 k 来得到不同的 d 值获得的局部连通性和全局连通性。可以看到，当两个相邻单元格的两个部署点之间的距离过小（k =0.4，0.6，0.8 或 1.0）时，在任意节点 A，其周围分布着许多非相邻单元格的节点，这些节点不与节点 A 共享任何密钥空间，因此降低了局部连通性和全局连通性；而当选择合适的部署点距离值时，模型能够获得较高的局部和全局连通性，如当 k=1.5 时，全局连通性为 0.999 0，即网络中只有 0.01% 的节点是浪费的。

表 2 仿真结果

k	局部连通性	全局连同性
0.4	0.078 7	0.654 6
0.6	0.157 7	0.929 0
0.8	0.252 4	0.970 4
1.0	0.364 3	0.992 1
1.5	0.603 6	0.999 0
2.0	0.772 0	0.999 4
2.5	0.861 7	0.999 8
3.0	0.922 6	0.999 9
3.5	0.955 5	0.999 9
4.0	0.965 7	1.000 0

3.3 内存开销和运行时间

在无线传感器网络协议设计中，长寿命是关键目标。在本文模型中，我们最小化相邻节点之间发现公用密钥空间的广播数据需求，1－跳广播消息长度为：

节点 ID 的大小 + Rv 的大小 + 3 × H 的大小(bits) (14)

用于存储从多项式得到的密钥材料的内存大小为：

$$M=3\times(t+1)\log_2 q+\text{节点 ID 的大小}+\text{Rv 的大小(bits)} \tag{15}$$

这个值连同共享一个多项式的节点数量影响成对密钥建立之前节点受攻击的恢复能力。这将在 3.4 中详细讨论。

将本文模型与文献［13］～［15］的模型在不同网络规模下的内存开销即所需要的内存大小进行比较，结果如表 3 所示。从表 3 可见，不同模型随着网络规模的增大，内存开销也增大，这是因为要完成更多节点间的密钥空间计算、交换和配对，但是本文模型的内存开销始终是最小的。这是由于本文模型在密钥建立阶段将全部节点进行集群分组，而且尽可能使传感器节点均匀分布，减少了密钥分配和建立阶段计算空间的存储开销和信息交换。

表 3 不同模型的内存开销比较

内存开销(Mbits)				
网络规模	本文模型	文献[13]模型	文献[14]模型	文献[15]模型
N=2 000	33.61	39.57	37.61	35.55
N=4 000	49.52	58.21	56.59	54.61
N=6 000	62.28	76.15	74.42	70.43
N=8 000	77.09	92.13	90.01	86.67
N=10 000	94.02	112.12	110.00	108.08

将本文方案与文献［13］～［15］的模型在不同网络规模下的的运行时间进行比较，结果如表 4 所示。从表 4 可以看到，不同模型随着网络规模的增大，运行时间也是增加的，这是由于随着节点数目的增大，不仅增加了节点部署和多项式分配的时间开销，更重要的要花更多时间完成密钥空间的计算和配对；但是本文模型在密钥建立阶段采用了密钥材料的预加载和 1－跳密钥空间发现消息来实现相邻节点的共享密钥空间分配，所以仍然有最小的运行时间。

表 4 不同模型的运行时间比较

运行时间/ms				
网络规模	本文模型	文献[13]模型	文献[14]模型	文献[15]模型
N=2 000	1 295	2 079	1 664	1 648
N=4 000	2 045	2 823	2 456	2 418
N=6 000	2 879	3 676	3 246	3 217
N=8 000	3 759	4 686	4 245	4 203
N=10 000	4 768	5 766	5 379	5 318

3.4 对捕获节点攻击的恢复能力

由于传感器网络工作环境通常比较恶劣，传感器节点很容易被捕获并泄露信息。捕获的传感器节点数量依赖于多项式的次数，也就是存储密钥材料的内存。对捕获节点攻击的恢复能力定义为当 x 个节点被攻破时，泄漏一个多项式的概率，这相当于在未受损的传感器节点之间泄漏直

接密钥。

文献［14］表明，基于多项式的方案具有 $t-$安全性：即除非公开了一个二元多项式的超过 t 个多项式共享，否则对手不会知道使用该多项式建立的非受损节点的成对密钥。因此，本文模型的安全性依赖于共享同一多项式的传感器节点的平均数量，即期望位于 3 个相邻六边形单元格中的传感器节点的数量。

把期望位于一个单元格内的传感器节点的平均数量表示为 N_c，则共享一个多项式的传感器节点的平均数量可计算为：

$$N_G = 3N_c = 3\bar{\omega}S_c = \frac{3\sqrt{3}a^2\sigma^2\bar{\omega}}{2} \tag{16}$$

式中，$\bar{\omega}$ 为传感器节点密度。

如前所述，存储密钥材料的内存需求为 M（bits），因此二元多项式的次数为：

$$t = [M/3] - 1 \tag{17}$$

只要 $N_G \leqslant t$，本文模型就能很好地抵抗节点捕获。换句话说，受损的传感器节点不会导致非受损传感器节点之间共享的直接密钥受损。

由于攻击是随机的，假设网络中有一小部分传感器节点 p_c 被攻击者破坏。在具有多项式共享的 N_G 个传感器节点中，正好有 i 个传感器节点被攻击的概率可以计算为：

$$p_c(i) = \binom{N_G}{i} p_c^i (1-p_c)^{N_s - i} \tag{18}$$

因此，二元多项式被破坏的概率可计算为：

$$p_c = 1 - \sum_{i=0}^{t} p_c(i) \tag{19}$$

图 2 所示为本文模型在不同部署点距离 d 节点受损攻击时仿真得到的网络恢复能力。可以看到，部署点距离越长即单元格越大，对节点受损攻击的网络恢复能力越脆弱。这是因为当单元格较大时，在一个单元格中有更多的传感器节点共享一个密钥空间，从而导致安全性降低。

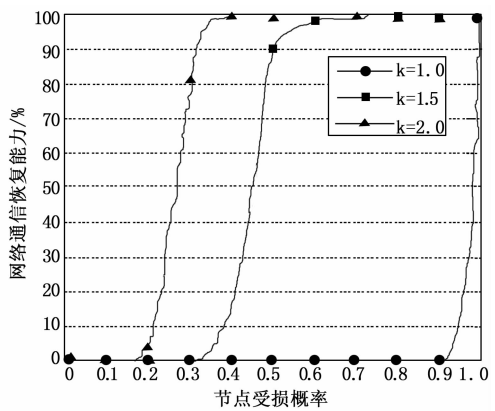

图 2　不同部署点距离下节点受损攻击时网络的恢复能力

图 3 所示为本文模型在不同内存大小 M（bits）情形下节点受损攻击时仿真得到的网络恢复能力。可以看到，随着内存的增大，网络的恢复能力增强，这是因为多项式的次数更高，就越不容易被攻击破坏。

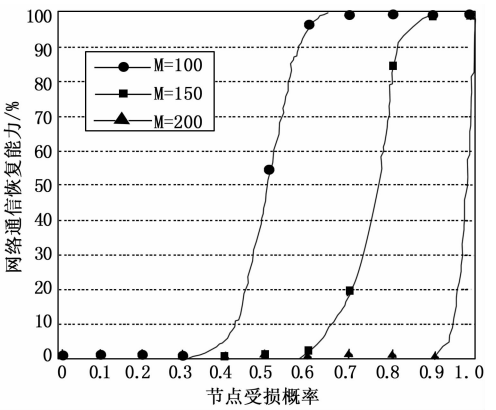

图 3　不同内存大小情形下节点受损攻击时网络的恢复能力

图 4 所示为不同模型的传感器节点被攻击时的网络恢复能力比较。可见，与文献［13］、［14］和［15］模型相比，本文模型在节点受损时的具有更好的安全性。这是由于本文模型存在密钥预分配阶段，而且离线服务器为每个集群生成一个包含足够多的 t 次对称二元多项式多池，然后将每个多项式分配给每个集群中的所有传感器节点，以确保每个节点都要存储 3 个 t 次二元多项式的共享知识，对手更难获得融合多个节点的密钥材料，从而提高了安全性。

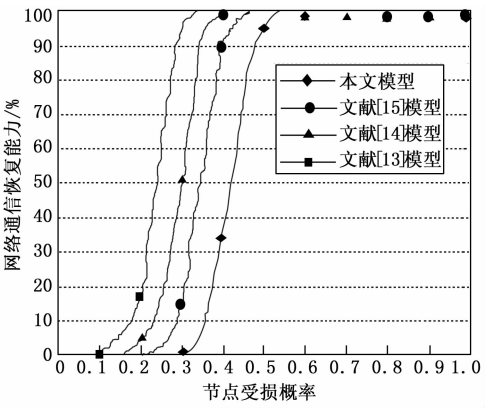

图 4　传感器节点被攻击时不同模型的网络恢复能力比较

4　结束语

本文提出了一种可实现的基于多项式的密钥预分配模型，它利用了高斯分布的预部署知识。同时还表明了模型在网络连通性、通信开销和内存需求等方面具有的优势。它还可以抵御非捕获节点间受损附加密钥的攻击；未来的研究将集中在部署误差率对网络连通性的影响和分析多跳间接密钥建立的可能性。

参考文献：

［1］毛一超．基于无线传感器网络的智能家居监控系统设计与实现［D］．武汉：武汉理工大学，2016.

[2] 牟建伟，滕　伟. 无线传感器网络的军事应用及发展趋势 [J]. 科技展望，2016，26 (7)：269－269，312.
[3] 周东蕴. 基于 ZigBee 无线传感器网络的环境监测系统实现 [D]. 哈尔滨：哈尔滨工业大学，2018.
[4] 胡　波，王祺尧，冯　辉，等. 一种无线传感器网络中目标跟踪的自适应节点调度算法 [J]. 电子与信息学报，2018，40 (9)：2033－2041.
[5] OSANAIYE O，ALFA A S，HANCKE G P. Denial of Service (DoS) Defence for Resource Availability in Wireless Sensor Networks [J]. IEEE Access，2018，6：6975－7004.
[6] SANTHI G，SOWMIYA R. A Survey on Various Attacks and Countermeasures in Wireless Sensor Networks [J]. International Journal of Computer Applications，2017，159 (7)：7－11.
[7] 刘恒壮. 基于椭圆曲线密码体制和 AES 的混合加密技术研究 [D]. 哈尔滨：哈尔滨工程大学，2019.
[8] 王文婷，石鑫磊，刘　新，等. 基于对称密钥算法的智能电网安全技术研究 [J]. 能源与环保，2017，39 (12)：279－281，285
[9] LIU Y H，WU Y M. A Novel Sub-regional Key Management Scheme for Distributed Wireless Sensor Network [C] // Proceedings of 2018 3rd International Conference on Communications，Information Management and Network Security (CIMNS2018)，Wuhan，China，2018：18－22.
[10] 王金全. 基于代密钥环分裂的无线传感器网络密钥管理方案研究 [D]. 沈阳：东北大学，2019.
[11] ZHU L，ZHANG Z，LI J，et al. An Improved Random Key Predistribution Scheme for Wireless Sensor Networks Using Deployment Knowledge [J]. International Journal of Security & Its Applications，2016，10 (5)：225－234.
[12] FROLOV A. On Some Computational and Security Aspects of the Blom Scheme [C] //Proceedings of 2019 International Conference on Engineering in Dependability of Computer Systems and Networks，Brunow，Poland，2019，987：205－214.
[13] 钟靖龙，吕丽平. 实现传感器网络安全的多空间密钥分配算法 [J]. 电子测量与仪器学报，2019，33 (4)：125－132
[14] ZHANG J M，LI H，LI J. Key Establishment Scheme for Wireless Sensor Networks Based on Polynomial and Random Key Predistribution Scheme [J]. Ad Hoc Networks，2017，71：68－77.
[15] YANG C N，LI J M，CHOU Y S. On the Analysis of k-Secure t-Conference Key Distribution Scheme [C] // Proceedings of the 2017 the 7th International Conference on Communication and Network Security，Tokyo Japan，2017：91－95.
[16] KLONOWSKI M，SYGA P. Enhancing privacy for ad hoc systems with predeployment key distribution [J]. Ad Hoc Networks，2017，59：35－47.
[17] ABDALLAH W，BOUDRIGA N. A location-aware authentication and key management scheme for wireless sensor networks [C] //Proceedings of 2016 22nd Asia-Pacific Conference on Communications (APCC)，Yogyakarta，Indonesia，2016：488－495.
[18] 王　牧，亢保元，景东亚. 无线传感器网络中身份认证与密钥共识方案 [J]. 计算机技术与发展，2017，27 (12)：98－102.
[19] 李　峰，李亚平，张志军，等. 移动场景下异构无线传感器网络密钥管理方法 [J]. 数据采集与处理，2021，36 (5)：1020－1029.
[20] ROKHADE S，HANUMATHAPPA S N. Peer-To-Peer Key Exchange Mechanism in Dynamic Wireless Sensor Networks [J]. International Journal of Advanced Research in Electrical，Electronics and Instrumentation Engineering，2016，5 (7)：6508－6514.

(上接第 179 页)

[17] RUBIO J D J. Robust feedback linearization for nonlinear processes control [J]. ISA Transactions，2018，74：155－164.
[18] 邢丽娟，杨世忠. 时变非线性不确定系统的鲁棒模型预测控制 [J]. 计算机仿真，2020，37 (11)：245－249.
[19] KAVITHA K R，VIJAYALAKSHMI S，SENTHILVADIVU M，et al. Resilient Model Predictive Control (RMPC) Technique Based Induction Motor Monitoring and Control using Labview [J]. International Journal of Recent Technology and Engineering，2020，8 (6)：191－197.
[20] WAN Z Y，KOTHARE M V. Robust output feedback model predictive control using off-line linear matrix inequalities [J]. Journal of Process Control，2002，12 (7)：763－774.
[21] MA Y，YANG P，ZHANG C Q，Robust H-infinity control for uncertain singular discrete T-S fuzzy time-delay systems with actuator saturation [J]. Journal of the Franklin institute，2016，353 (13)：3290－3311.
[22] 管　萍，吴希岩，戈新生，等. 大型挠性航天器的鲁棒模型预测姿态控制 [J]. 宇航学报，2022，43 (4)：476－485.
[23] 王乘熙，李　泽，崔国增，等. 多区域暖通空调温湿度鲁棒模型预测控制策略 [J]. 科学技术与工程，2022，22 (14)：5681－5692.
[24] LIU Z，XUE L，SUN W，et al. Robust output feedback tracking control for a class of high-order time-delay nonlinear systems with input dead-zone and disturbances [J]. Nonlinear Dynamics，2019，97 (3)：921－935.
[25] WANG J Y，DUAN Z S，WEN G H，et al. Distributed robust control of uncertain linear multi-agent systems [J]. International Journal of Robust and Nonlinear Control，2015，13 (25)：2162－2179.
[26] 周　琪，陈　兵，李鸿一. 马尔可夫跳跃时滞系统的时滞相关鲁棒 H∞性能分析 [J]. 渤海大学学报 (自然科学版)，2007，28 (4)：330－334.
[27] 王耀锋. 基于 T-S 模糊模型的鲁棒预测控制器在啤酒发酵温度控制中的应用研究 [D]. 青岛：青岛科技大学，2008.
[28] YU K，LIEN C，Stability criteria for uncertain neutral systems with interval time-varying delays [J]. Chaos，Solitons and Fractals，2008，38 (3)：650－657.
[29] BOYD S，GHAOUI L，FERON E，et al. Linear matrix inequalities in system and control theory [M]. Philadelphia：Society for industrial and applied mathematics，1994.