

基于对称平衡不完全区组设计的持续安全管理密钥预分配方案

吴丘林^{1*,2}, 李乔良²

(1. 湖南交通职业技术学院 物流管理学院, 长沙 410004; 2. 湖南大学 信息科学与工程学院, 长沙 410081)

(* 通信作者电子邮箱 wqlhj@163.com)

摘要:针对持续安全管理密钥预分配方案中网络连通度较低的问题,设计实现了一种新的基于对称平衡不完全区组设计(SBIBD)的持续安全管理密钥预分配方案。该方案每一个网络节点的密钥环对应于SBIBD中的一个区组,保证了在同一个部署阶段任意两个节点存在共享密钥,不同部署阶段的节点通过桥节点进行连接。仿真结果表明,该方案能提高网络的全局连通率和局部连通率,节省了节点之间建立安全通信的开销。

关键词:无线传感器网络;密钥管理;安全;对称均衡不完全区组设计;密钥预分配

中图分类号: TP309; TP393 **文献标志码:** A

Secure management of continuity key pre-distribution scheme based on SBIBD

WU Qiu-lin^{1*,2}, LI Qiao-liang²

(1. College of Logistics Management, Hunan Communication Polytechnic, Changsha Hunan 410004, China;

2. School of Information Science and Engineering, Hunan University, Changsha Hunan 410081, China)

Abstract: In order to solve the problem of low connectivity in continuous security key management scheme, the authors implemented a new scheme based on Symmetric Balanced Incomplete Block Design (SBIBD). In the new scheme, the key ring of each node corresponded to a block of the SBIBD, which ensured that any two nodes shared a common key in the deployment stage, and the nodes in different stage could be connected by bridge nodes. The simulation demonstrates that the new scheme can improve the global and local connectivity of the network, and save the overhead in establishing communication between nodes.

Key words: Wireless Sensor Network (WSN); key management; security; Symmetric Balanced Incomplete Block Design (SBIBD); key pre-distribution

无线传感器网络由于其体积小、能量小、计算能力与存储空间均有限等因素限制,使其在安全方案的设计上带来了许多挑战^[1]。Eschenauer等^[2]首先提出了基本的随机密钥预分配模型,在保证节点之间建立安全通信的前提下,尽量减少模型对节点资源的要求。Chan等^[3-4]在文献[2]的基础上提出了 q -composite,把公共密钥的个数要求提高到了 q 个,提高了系统的抗毁性,但节点的连通率难以保证,且节点多次部署使用同一个密钥池,导致密钥在预分配之前就存在安全隐患。Duresi等^[5]提出了持续安全管理的密钥预分配方案(Secure management of continuity in sensor networks, SCON),该方案在节点的每一个部署阶段都使用独立的密钥池,安全性能有明显提高,但由于每一次部署阶段的密钥是基于随机分布的,随着部署阶段的增加,全局连通度和局部连通度会越来越低,节点之间建立通信的开销也会越来越大。

1 持续安全管理密钥预分配方案

无线传感器网络节点由于自身能量等特点的限制,一般来说,整个网络的生命周期要大于单个节点的生命周期。为了保持网络的持续工作,需要适时地向网络中添加新的节点。SCON方案是一种持续安全管理的密钥预分配方案,通过不断地向网络中添加新的节点,保证网络的持续正常运行^[6]。

该方案的最大特点在于将密钥池分成多个部分,在不同的密钥分发阶段,将会用到不同的密钥池,不同阶段分发的节

点通过一种叫“桥节点”的特殊节点进行通信。桥节点的密钥长度是普通节点的2倍,它一半是来自前一个密钥预分配阶段的密钥池,另外一半是下一个密钥预分配阶段的密钥池(如图1)。

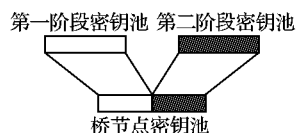


图1 桥节点密钥结构

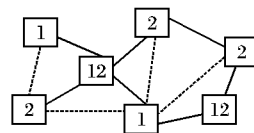


图2 节点布局和桥节点结构

不同阶段的节点如果都能直接跟桥节点有共同密钥,可以通过“路径密钥”的方式建立安全连接,如图2所示。

图2中“1”表示第一阶段部署的节点,“2”表示第二部署阶段的节点,“12”

表示桥节点,实线表示直接共享密钥,虚线表示共享路径密钥。

2 对称均衡不完全区组设计

区组设计在密钥安全管理方面得到广泛应用。本章从区组设计的基本理论出发,根据对称均衡不完全区组设计的定义,提出一种特殊的对称均衡不完全区组设计(Symmetric Balanced Incomplete Block Design, SBIBD)。

收稿日期:2011-09-28;修回日期:2011-12-21。

基金项目:国家自然科学基金资助项目(11071272);国家火炬计划项目(2011GH521681)。

作者简介:吴丘林(1983-),男,湖南岳阳人,讲师,硕士研究生,主要研究方向:无线传感器网络密钥安全、图像识别;李乔良(1966-),男,湖南湘潭人,教授,博士生导师,主要研究方向:无线传感器网络密钥安全、数字指纹。

2.1 区组设计相关理论

定义1 设 $X = \{x_1, x_2, \dots, x_v\}$, B_1, B_2, \dots, B_b 是 X 的 b 个 k -子集, 如果满足:

- 1) X 中每个元素的重复数都是 r ;
- 2) X 中每两个不同的元素 x, y 的相遇数都是 $\lambda_D(x, y) = \lambda$;
- 3) $k < v$;

则称 $B = \{B_1, B_2, \dots, B_b\}$ 是有参数 $\{b, v, r, k, \lambda\}$ 的均衡不完全区组设计, 简称 $BIBD\{b, v, r, k, \lambda\}$ 。

定义2 在上述 $BIBD\{b, v, r, k, \lambda\}$ 定义的基础上, 如果进一步 $b = v$, 则是对称的均衡不完全区组设计, 记为 $SBIBD$ 。显然, 当 $b = v$ 时 $k = r$ 。因此, 对称的均衡不完全区组设计可以简记为 $SBIBD\{v, k, \lambda\}$ 。

定义3 拉丁方。

A 为 $n \times n$ 矩阵, 若 A 的每行、每列都恰好是 $(1, 2, \dots, n)$ 的一个置换, 则称 A 是 n 阶拉丁方。若 $A = (a\{i, j\})$, $B = (b\{i, j\})$ 都是 n 阶拉丁方, 且满足: $(a\{i, j\}, b\{i, j\}; i = 1 \dots n, j = 1 \dots n) = N \times N$, 则称 A, B 是正交拉丁方。

定义4 正交拉丁方组。

$\{A_1, A_2, \dots, A_n\}$ 是个 n 阶拉丁方, 若它们两两正交, 则称它们是一个正交拉丁方组。如果两个阶拉丁方在同一位置上的数依次配置成对时, 这两个有序数对恰好各不相同 (一般处理方法为把当中某些行或列对调) 则构成正交拉丁方组。式(1)是两个互为正交的4阶拉丁方。

$$\begin{bmatrix} 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 3 & 4 & 2 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix} \quad (1)$$

2.2 对称的均衡不完全区组设计的构造

定理1 若 q 为素数幂, 则存在 q 阶正交拉丁方完备组。

根据定理1, 任意给定一个素数幂, 可以构造一个阶正交拉丁方组^[7-8]。正交拉丁方组的拉丁方分别记为 $A_k (k = 1, 2, \dots, q; i = 0, 1, \dots, q-1; j = 0, 1, \dots, q-1)$ 。以 $q = 4$ 为例, 根据下列方法可以构造出 $SBIBD\{21, 5, 1\}$ 。首先, 由公式 $A_{k,i,j} = (k \times i + j) \bmod q + 1$, 构造 $q-1$ 个拉丁方 A_1, A_2, A_3 , 如式(2)~(4)所示。

$$A_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} \quad (2)$$

$$A_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix} \quad (3)$$

$$A_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix} \quad (4)$$

接着再构造一个标准矩阵 U , 其中标准矩阵 U 中的第 i 行 j 列的元素由公式 $U_{i,j} = (i-1) \times q + j$ 确定, 其中 $i, j \in \{1, 2, \dots, q\}$, 如式(5)所示:

$$U = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix} \quad (5)$$

然后将正交拉丁方组的三个矩阵 A_1, A_2, A_3 分别与上述

的标准矩阵 U 进行重合, 得到这些拉丁方矩阵 A_1 与标准矩阵 U 的交差矩阵。式(6)是 A_1 与标准矩阵 U 重合的交差矩阵:

$$\begin{bmatrix} 1/1 & 2/2 & 3/3 & 4/4 \\ 2/5 & 1/6 & 4/7 & 3/8 \\ 3/9 & 4/10 & 1/11 & 2/12 \\ 4/13 & 3/14 & 2/15 & 1/16 \end{bmatrix} \quad (6)$$

其中斜杠左边是 A_1 矩阵中的元素, 右边是 U 矩阵中的元素。

在式(6)中, 元素为“1”所对应 U 矩阵的元素4个, 分别为“1”、“6”、“11”、“16”, 记为数 $\{1, 6, 11, 16\}$, 同样可得出元素为“2”, “3”, “4”对应 U 矩阵的元素分别为 $\{2, 5, 12, 15\}$, $\{3, 8, 9, 14\}$, $\{4, 7, 10, 13\}$ 。依此类推, A_2, A_3 分别与 U 矩阵的交差矩阵, 同样可以得出 $\{1, 7, 12, 14\}$, $\{2, 8, 11, 13\}$, $\{3, 5, 10, 16\}$, $\{4, 6, 9, 15\}$, $\{1, 8, 10, 15\}$, $\{2, 7, 9, 16\}$, $\{3, 6, 12, 13\}$, $\{4, 5, 11, 14\}$ 等8组数据。标准矩阵 U 的每一行作为一个数组, 共有四个数组 $\{1, 2, 3, 4\}$, $\{5, 6, 7, 8\}$, $\{9, 10, 11, 12\}$, $\{13, 14, 15, 16\}$; 每一列作为一个数组, 同样得到另外四个数组 $\{1, 5, 9, 13\}$, $\{2, 6, 10, 14\}$, $\{3, 7, 11, 15\}$, $\{4, 8, 12, 16\}$, 加上正交拉丁方与标准矩阵 U 交差产生前面最开始的12个数组, 一共得到了20组数据, 每一组数据有4个元素。正交拉丁方矩阵 A_1, A_2, A_3 产生的数据分别加入一个大于数组中所有元素的 $\infty_1, \infty_2, \infty_3$, 再将标准矩阵 U 的每一行、每一列产生的数组分别加入 ∞_4, ∞_5 , 共得到了长度为5的数据20组, 再加上 $\{\infty_1, \infty_2, \infty_3, \infty_4, \infty_5\}$, 一共得到21组数据。

为了方便计算和表示, $\{\infty_1, \infty_2, \infty_3, \infty_4, \infty_5\}$ 可用大于区组中所有元素的数字 $\{17, 18, 19, 20, 21\}$ 来表示, 不影响区组设计效果。这样, $q = 4$ 时的 $SBIBD$ 所有区组为 $\{1, 6, 11, 16, 17\}$, $\{2, 5, 12, 15, 17\}$, $\{3, 8, 9, 14, 17\}$, $\{4, 7, 10, 13, 17\}$, $\{1, 7, 12, 14, 18\}$, $\{2, 8, 11, 13, 18\}$, $\{3, 5, 10, 16, 18\}$, $\{4, 6, 9, 15, 18\}$, $\{1, 8, 10, 15, 19\}$, $\{2, 7, 9, 6, 19\}$, $\{3, 6, 12, 13, 19\}$, $\{4, 5, 11, 14, 19\}$, $\{1, 2, 3, 4, 20\}$, $\{5, 6, 7, 8, 20\}$, $\{9, 10, 11, 12, 20\}$, $\{13, 14, 15, 16, 20\}$, $\{1, 5, 9, 13, 21\}$, $\{2, 6, 10, 14, 21\}$, $\{3, 7, 11, 15, 21\}$, $\{4, 8, 12, 16, 21\}$ 。可以看出, $SBIBD$ 任意两个区组之间有且只有一个公共元素。

3 基于 SBIBD 的 SCON 方案

SCON 方案是一种持续安全管理的密钥预分配方案, 它的优点是不同的节点部署阶段, 将用到不同的密钥池, 它的不足就是不同阶段的节点要通过桥节点建立连接, 随着部署阶段的增加, 局部连通率会越来越低。因此, 尝试用 $SBIBD$ 的区组来构造密钥预分配方案的密钥, 图3是基于 $SBIBD$ 的 SCON 方案的算法和具体步骤。

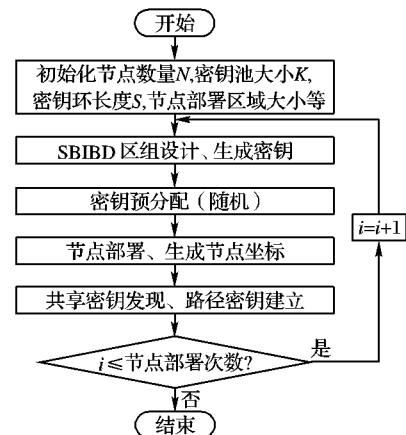


图3 基于 $SBIBD$ 的 SCON 方案算法

第1步 初始化。

与一般的 SCON 方案一样,在方案实施前,无线传感器网络也要进行一些初始化的工作,如密钥池大小、密钥环长度、节点广播的通信范围、网络节点总数、部署区域的大小、部署的总次数等^[9-10]。SBIBD 是一种特殊的 BIBD,表1是各参数说明以及参数之间的关系。

表1 参数说明表

参数	值	表示说明
q	素数幂	构造 SBIBD 的参数必须为素数幂
K	$q^2 + q + 1$	密钥池大小,所有节点的密钥从 K 中进行选取
S	$q + 1$	每个节点能够存储的密钥的个数,即密钥长度
K_i	K	第 i 部署阶段的密钥池,每一个阶段的大小都等于 K
p		节点之间存在公共密钥的概率

第2步 SBIBD 构造。

给定参数 q ,根据上一节的设计构造方法,可以构造对象的均衡不完全区组 SBIBD($q^2 + q + 1, q + 1, 1$)。其中节点的密钥长度 S 、密钥池大小 K 与参数 q 存在一定函数关系,即 $K = q^2 + q + 1, S = q + 1$ 。根据公式 $A_{k,i,j} = (k \times i + j) \bmod q + 1$,建立 $q - 1$ 个拉丁方矩阵 A_1, A_2, \dots, A_{q-1} 。然后根据表达式 $U_{i,j} = (i - 1) \times q + j$ 生成标准矩阵 U 。这个标准矩阵大小 U 也是根据密钥池大小 S 而确定的,与拉丁方矩阵的大小一样为 $q \times q$ 。将得到的 $q - 1$ 个拉丁方矩阵分别与标准矩阵 U 进行覆盖、重叠,生成交差矩阵。在交差矩阵中,记录拉丁方矩阵中“1”对应的标准矩阵 U 中的数值,共有 q 个数字,这 q 个数字构成一个区组。一个拉丁方矩阵可以产生 q 个区组,一共有 $q - 1$ 个拉丁方,即可以构成 $q \times (q - 1)$ 个区组。标准矩阵 U 每一行分别构成 q 个区组,每一列也分别构成 q 个区组,总共构成了 $q \times (q - 1) + 2q = q^2 + q$ 个区组。最后以 $\{q^2 + 1, q^2 + 2, \dots, q^2 + q + 1\}$ 作为最后一个区组;前面 $q^2 + q$ 个区组中,拉丁方组 A_1, A_2, \dots, A_{q-1} 产生的区组分别加上 $q^2 + 1, q^2 + 2, \dots, q^2 + q + 1$ 。这样 SBIBD 中所有的区组已经生成。总共有 $q^2 + q + 1$ 个区组,每个区组中公含有 $q + 1$ 个元素。

第3步 密钥生成,密钥预分配。

密钥池大小为 $K = q^2 + q + 1$,所以生成编号从 1 到 $q^2 + q + 1$ 的密钥 ID,将这些密钥 ID 放入密钥池 K_1 (表示第一部署阶段密钥池) 中。密钥预分配是在节点部署之前进行的,从密钥池 K_i 中随机选择一个区组的元素存储在一个节点中,恰好 $q^2 + q + 1$ 个密钥 ID 放入 $q^2 + q + 1$ 个节点中,节点对应的区组两两不相同。第二次部署的密钥池 K_2 即在第一次部署密钥 ID 基础上加上 $q^2 + q + 1$,依此类推,第 $i + 1$ 次部署阶段的密钥池 K_{i+1} 中的密钥 ID 不需要重新构造 SBIBD,只需在密钥池 K_i 中所有的密钥加上 $q^2 + q + 1$ 。桥节点在 SCON 方案中是一种特殊的节点,第 i 阶段桥节点的密钥 ID 分别来自于第 $i - 1$ 次部署的密钥池 K_{i-1} 和第 i 次部署的密钥池 K_i ,它的密钥长度是普通节点的两倍,其中一半是在 K_{i-1} 中随机抽取一个区组的密钥,另一半是从 K_i 随机抽取。

第4步 传感器节点部署。

在无线传感器网络中,传感器节点通常是被随机部署在一个目标区域内,每个节点的位置是未知的,任何两个节点之间是否存在直接连接也是未知的,因此网络的安全协议的设计不能依赖节点部署后的任何位置信息^[11]。这里,为了模拟分析的需要,假设传感器节点是按照随机分布原则,将传感器节点随机分布在部署区域里。

第5步 共享密钥的发现阶段。

这个过程是在网络节点部署之后进行的,每一个节点可以在自己的通信范围内广播自身密钥环中所有密钥,其他节点在收到广播信息后,就开始遍历自身所有的密钥,如果发现自身的密钥跟广播的密钥有相同时,就将这个密钥 ID 对应的所有公共密钥异或后建立一个全新的通信密钥,这个通信密钥是用来加密节点与节点之间的通信^[12]。在第一次部署阶段,所有节点的密钥来自与同一个密钥池,且两两存在公共密钥,所以任意两个节点只要在通信范围内,就可以建立一个安全通信链路。从第二次部署阶段开始,网络中的一些节点可能来自于不同的密钥池,不能直接建立安全通信,需要找到桥节点,为下阶段的路径密钥建立作为准备,如不作特殊说明,桥节点将随机抽取的普通节点作为桥节点。

第6步 路径密钥建立阶段。

这个阶段是在建立共享密钥阶段之后进行的,如果邻居节点之间没有存在公共密钥,那么可以通过其他节点进行协商,建立安全链路。如节点 N_1 与 N_2 之间没有存在公共密钥,但节点 N_1 与节点 N_3 、节点 N_2 与节点 N_3 都存在公共密钥,那么可以通过节点 N_3 协商安全密钥,一旦协商成功,那么节点 N_1 与节点 N_2 可以利用这对路径密钥直接进行通信,不需要通过其他节点的中间转发。在第 i 次节点部署阶段的桥节点因为同时具有 K_{i-1} 和 K_i 中的密钥,所以它能够与这两个阶段部署的节点进行直接通信,因此两个不同阶段部署的节点需要通过桥节点建立路径密钥进行通信。

第7步 节点捕获阶段。

无线传感器网络一般被部署在应用者无法监控的区域内,甚至是敌方的领域,这种情况下传感器节点很容易被一些攻击者捕获。在这个阶段中,假设入侵者在网络中捕获了部分节点,捕获的节点是随机的,那么这些节点中对应的密钥 ID 就会被发现并破解,其他以这些密钥 ID 建立连接的节点也可能被截获。本文假设捕获的节点所有的密钥都被破解,且通过该密钥建立通信的所有节点也被捕获。

第8步 转第3步。

由于一些节点的密钥被捕获或能量耗尽,原来建立的安全链路不再安全,导致整个传感器网络的整体功能受损,必须在下一个部署阶段中重新部署新的节点以保证整个网络的连通性和功能的完整性。

4 模拟分析

在本章中,分别对原有 SCON 方案和基于 SBIBD 的 SCON 方案进行仿真模拟实验,在全局连通概率、局部连通概率、通信开销(节点建立安全通信的平均跳数)三个方面进行了分析对比。

模拟的节点部署区域为 $560 \text{ m} \times 560 \text{ m}$ 的矩形区域,每个节点通信距离为 40 m ,假定所有的链接是对称的,即如果节点 N_1 在节点 N_2 内的通信范围内,那么节点 N_2 也能与节点 N_1 进行通信。本文还设定,如果一个节点被捕获,那么节点密钥环中的密钥将会全部破解,以该节点中的密钥建立安全通信的链接全部被捕获。在构造 SBIBD 时,参数 $q = 139$,根据 SBIBD 区组设计性质,密钥池大小为 $K = q^2 + q + 1 = 19461$,密钥环长度 $S = q + 1 = 140$,桥节点的密钥环长度是普通节点的两倍即 280。

4.1 全局连通度

这里对原有的 SCON 方案和基于 SBIBD 的 SCON 方案进

行了全局连通率的比较,如图4所示。不难看出,在每一个节点部署阶段,基于SBIBD的SCON方案都体现了较高的全局连通率。在节点的第一次部署阶段,每个节点的密钥对应于SBIBD中的一个区组,任意区组之间存在公共元素,所以任意两个通信范围内节点存在公共密钥。只要保持网络中的节点一定的密度就可以保证网络的全局连通度达到1。但在传感器节点的第二、第三次部署节点过程中,由于不同部署节点的密钥池不同,局部连通率降低,从而影响全局连通率。基于SBIBD的SCON方案有效地解决了这个问题,它的全局连通率远高于原有的SCON方案。

4.2 局部连通度

本文分别对原有的SCON方案和基于SBIBD的SCON方案进行了局部连通率的比较,如图5所示。仿真结果表明,在每一个节点部署阶段,基于SBIBD的SCON方案都体现了良好的局部连通度。在传感器节点的第一次部署阶段,因为SBIBD方案保证任意两个节点之间存在公共密钥,所以基于

SBIBD的SCON方案的局部连通度是100%,远高于基于EG方案的无线传感器网络的局部连通度。在传感器节点的第二、第三部署节点,由于不同部署节点的密钥池不同,不同部署阶段的无线传感器节点之间不能直接建立通信,局部连通率降低。但基于SBIBD的SCON方案由于在同一个密钥池中的密钥两两共享公共密钥,局部连通度远高于原有的SCON方案。

4.3 路径密钥长度、通信开销分析

由于无线传感器节点体积小、能量小等特点,网络之间如何保持低功耗也是研究的主题。节点之间进行通信的开销是节点消耗能量的主要方式,而建立通信的开销取决于节点之间建立路径密钥的平均跳数(路径长度)。从图6可以看出,在第一次部署阶段,基于SBIBD的SCON方案的平均跳数为1,在通信范围内任意节点存在公共密钥,可以直接通信;随着部署次数的增加,节点之间的平均跳数也会相应增加,新的方案在各个部署阶段都大大减少了节点连通的平均跳数。

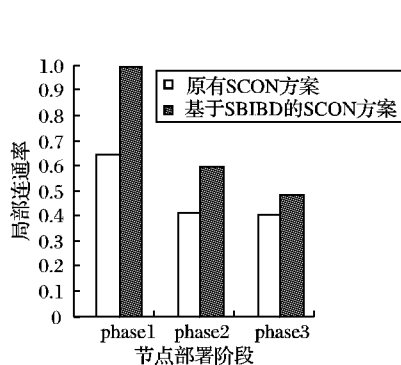


图4 全局连通率比较

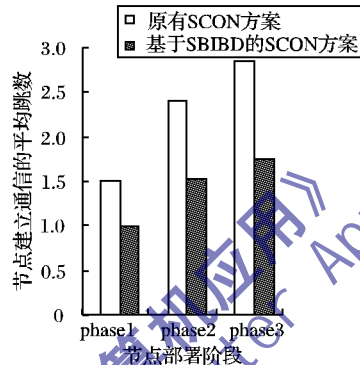


图5 局部连通率比较

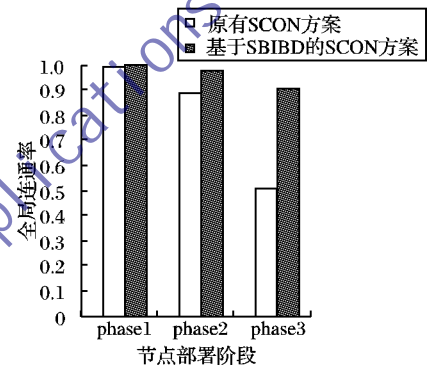


图6 节点连通的平均路径长度

5 结语

密钥预分配是无线传感器网络主要的密钥管理方式。随着节点的能量耗尽,或节点的被捕获,需要对无线传感器网络进行持续的安全管理。现有的持续安全管理方案在原来的基础上将密钥池独立出来,使得网络的抗毁性得到提高,但随着部署次数的增加,网络连通度难以得到保证。本文基于对称平衡的不完全区组设计的持续安全管理密钥预分配方案,设计实现了一种特殊的SBIBD区组构造,将该区组对应于传感器网络中的密钥环,改进了原有SCON方案网络连通度低的问题,比现有密钥预共享方案有更高的共享密钥概率,以及节点之间更小的平均跳数,减少了节点通信的能耗,提高了网络的使用寿命。

参考文献:

- [1] 雷凤宇,崔国华.无线传感器网络密钥管理研究[D].武汉:华中科技大学,2010.
- [2] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[C]// CCS'02: Proceedings of the 9th ACM Conference on Computer and Communications Security. New York: ACM, 2002: 18-22.
- [3] CHAN H, PERRIG A, SONG D. Random key-predistribution schemes for sensor networks[C]// SP'03: Proceedings of the 2003 IEEE Symposium on Security and Privacy. Washington, DC: IEEE Computer Society, 2003: 197-213.
- [4] PRZYDATEK B, SONG D, PERRIG A. SIA: Secure information aggregation in sensor networks[C]// SenSys'03: Proceedings of the 1st International Conference on Embedded Networked Sensor Sys-

- tems. New York: ACM, 2003: 255-265.
- [5] DURRESI A, BULUSU V, PARUCHURS V. SCON: Secure management of continuity in sensor networks[J]. Computer Communications, 2006, 29(13/14): 2458-2468.
- [6] ÇAMTEPE S A, YENER B. Combinatorial design of key distribution mechanisms for wireless sensor networks[J]. IEEE/ACM Transactions on Networking, 2007, 15(2): 346-358.
- [7] LEE J Y, STINSON D R. On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs[J]. ACM Transactions on Information and System Security, 2008, 11(2): 1-35.
- [8] SUSHMITA L, BIMAL R. Key predistribution using combinatorial designs for grid-group deployment scheme in wireless sensor networks[J]. ACM Transactions on Sensor Networks, 2009, 6(1): 4.
- [9] ERDÖS P, RÉNYI A. On the evolution of random graphs[EB/OL]. [2011-06-01]. http://www.renyi.hu/~p_erdos/1961-15.pdf.
- [10] PERRIG A, SZEWCZYK R, WEN V, et al. SPINS: Security protocols for sensor networks[J]. Wireless Networks, 2001, 8(5): 521-534.
- [11] BLACKBURN S R, ETZION T, MARTIN K M, et al. Efficient key predistribution for grid-based wireless sensor networks[C]// ICITS'08: Proceedings of the 3rd International Conference on Information Theoretic Security. Berlin: Springer-Verlag, 2008: 54-69.
- [12] WU JIANG, STINSON D R. Minimum node degree and kappa-connectivity for key predistribution schemes and distributed sensor networks[C]// Proceedings of the First ACM Conference on Wireless Network Security. [S.l.]: IEEE, 2008: 119-124.