计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
45(1):154~164, 2008

基于对称平衡不完全区组设计的无线传感器网络密钥预分配方案

夏戈明　黄遵国　王志英
(国防科学技术大学计算机学院　长沙　410073)
(victor_xgm@163.com)

A Key Pre-Distribution Scheme for Wireless Sensor Networks Based on the Symmetric Balanced Incomplete Block Design

Xia Geming, Huang Zunguo, and Wang Zhiying
(*School of Computer Science, National University of Defense Technology, Changsha* 410073)

Abstract　This paper focuses on key pre-distribution, a foundational problem of security in wireless sensor networks. A novel key pre-distribution scheme named $sBIBD_{Hadamard}$ KPS was devised by authors based on combinatorial designs technique. The essence of $sBIBD_{Hadamard}$ KPS is constructing symmetric balanced incomplete block design with Hadamard matrix and mapping it to a key pre-distribution scheme. The derivation and data illuminated that $sBIBD_{Hadamard}$ KPS and its extended versions improvement themselves than the most scheme in existence, mainly on three facets. First, $sBIBD_{Hadamard}$ KPS make the pair sensor nodes to share common keys at a higher sharing probability with the same key chain size, and achieved a smaller average key path length, especially to do all of that without asking for a node neighbor degree more than 2. Second, $sBIBD_{Hadamard}$ KPS make the pair sensor nodes to share more than one keys, and by carrying out a particular method to compositing the common key in time, it enhanced the security by enlarged the key space in the face of attacks using key analyzing. Finally, $sBIBD_{Hadamard}$ KPS upgrade itself to support many more nodes by two means named complementary set design and key slicing, and optimize the energy expenditure at the same time.

Key words　wireless sensor networks; security; key pre-distribution; block design; Hadamard matrix

摘　要　针对无线传感器网络的密钥预分配问题,利用哈达玛矩阵,设计实现了新的基于组合设计方法的密钥预分配方案——基于对称平衡不完全区组设计的密钥预分配方案 $sBIBD_{Hadamard}$ KPS 系列方案. 首先,$sBIBD_{Hadamard}$ KPS 改进了现有多数方案只能共享单个密钥的问题,并实现了同等节点密钥组长度和共享密钥强度下,比现有支持多密钥共享的随机预分配方案更高的共享概率和更小的密钥路径长度,并且只要求大于 2 的节点邻居度数;其次,$sBIBD_{Hadamard}$ KPS 提出了一种实时合成共享密钥的方法,在节点密钥组物理长度不变的前提下,大大扩大了共享密钥选择空间,提高了安全强度;最后,$sBIBD_{Hadamard}$ KPS 使用补集设计和密钥分片两种方法进行扩展设计,实现了对较大网络规模的支持,并且在一定程度上优化了能量消耗.

关键词　无线传感器网络;安全;密钥预分配;区组设计;哈达玛矩阵

中图法分类号　TP309;TP393

收稿日期:2007-05-31;**修回日期**:2007-07-17
基金项目:国家"八六三"高技术研究发展计划基金项目(2006AA01Z401)

目前,无线传感器网络[1-3]被广泛应用在国防军事、环境监测、交通管理等领域. 随着应用的普及,传感器网络的安全[4-5]日益显得重要,尤其是其中最基础和最关键的密钥管理[6-7]问题. 在节点能量以及计算和通信能力非常有限的无线传感器网络中,一般采用密钥预分配机制实现安全引导,在部署之初为节点预分配若干密钥,使得部署后不同节点之间通过共享密钥建立安全基础,然后进行进一步的密钥协商.

目前已有很多无线传感器网络的密钥预分配的研究[8-13],包括基本随机预分配模型和扩展的随机预分配模型,以及之后出现的许多具有确定性特点的方案,围绕共享概率、密钥路径长度指标、支持的网络规模、密钥安全强度等指标进行了大量工作. 由于传感器网络要求具备规模、开放暴露环境和节点能力严格受限等特殊性,使得许多指标难以达到较好水平,密钥预分配的研究仍然充满问题和挑战.

本文提出一种新的无线传感器网络密钥预分配方案,研究致力于提高共享概率,减小密钥路径长度,扩大网络规模和增强密钥强度等指标,并降低密钥共享的复杂性和提高部署的实际可行性.

1 无线传感器网络密钥预分配相关研究

按密钥的选取方式,目前的无线传感器网络密钥预分配方案可以分成概率性方案和确定方案两种.

概率性预分配方案是一种得出概率结果的密钥预分布模型,从密钥池中随机抽取包含多个密钥的密钥组,使得任意两个节点存在共享密钥的概率高于一定值,进而使得整个系统的密钥共享图构成连通图. 主要的随机密钥预分布模型有以下 2 种:

1) 基本的随机密钥预分布模型(basic random key scheme)

基本的随机密钥预分布模型[8]由 Eschenauer 和 Gligor 提出. Basic Random 方案的密钥预分布和协商过程分为以下 3 个主要阶段:

① 密钥预分发. 从密钥区间内选取一个密钥池 S,为每个密钥分配 ID,每个节点从密钥池中随机地选取 k 个密钥构成自己的密钥组. k 的大小选择要保证每两个节点存在相同密钥的概率大于要求的概率值 p.

② 密钥发现. 节点之间通信时,通过交换各自的 ID 来发现共享密钥.

③在②不成功时,通过中间节点寻求一条安全到达对方的密钥路径,然后协商密钥;所谓密钥路径是指相邻节点存在共享密钥的路径.

在基本的随机密钥预分布模型方案中,两个节点之间共享密钥的概率 p 与密钥池 S 的大小 W 和密钥组的长度 k 存在以下数学关系:

$$p = 1 - \frac{\left(1 - \frac{k}{W}\right)^{2\left(W-k+\frac{1}{2}\right)}}{\left(1 - \frac{2k}{W}\right)^{\left(W-2k+\frac{1}{2}\right)}}.$$

2) 扩展的随机密钥预分布模型(q-composite random key scheme).

Basic Random 方案中要求两个节点的密钥组中至少有一个共享密钥. Chan 等人提出的 q-composite 方案[9]将共享密钥个数的要求提高到 q. 此时 p 和 w 及 k 的数学关系表示为

$$p = 1 - \sum_{0}^{q-1} \frac{C\binom{i}{W} C\binom{2(k-i)}{W-i} C\binom{k-i}{2(k-i)}}{\left(C\binom{k}{W}\right)^2}.$$

q-composite 方案协商共享密钥的方法和 Basic Random 方案也不同. 后者简单选取一个公共密钥直接作为共享密钥. 前者用所有的共享密钥 $k_1, k_2, \cdots, k_q, \cdots, k_{q'}$ 生成新的共享密钥:$K = \mathrm{Hash}(k_1, k_2, \cdots, k_q, \cdots, k_{q'})$,其中 Hash 函数的密钥自变量的顺序可以预先议定.

概率性预分配方案还有 Chan 等人提出的随机密钥对模型[9],不再全局共享密钥,而是每个节点存储与其他节点的独立密钥对,在节点数为 n 的系统中,为保证节点之间以概率 p 共享密钥,每个节点存储 $k = np$ 个对密钥. 这种方案安全性得到加强,但是扩展性较差. Liu 等人[10]也提出了基于有限域上对称二元多项式的随机密钥预分配方案,通过预分配的对称多项式来计算出共享密钥,但是却带来了较大的计算开销.

概率性预分配方案优点是算法简单,便于实施. 但只能用概率值衡量节点间能否共享密钥和计算密钥路径的长度,网络的安全连通程度也是概率结果. 在网络规模较大时共享概率下降很快,并且方案都基于随机图理论,对节点的邻居度数有一定的要求.

确定性模型是指在预分发时不是随机选取密钥,而是按照特定模型去构造节点密钥组. 第 1 个确定性密钥预分布模型是由 Camtepe 等人提出的基于组合数学方法的密钥预分布模型 Symmetric Design[11],该方案利用区组设计和有限广义四边形构造密钥预

分配模型,可以构造出节点数为 n^2+n+1,密钥组长度为 $n+1$,每对节点正好共享 1 个密钥的模型.

还有一些研究提出了确定性的密钥预分配方法,Lee 和 Stinson 提出了利用正则图构造的密钥预分配方案[12],Du 等人提出了基于多密钥空间的增强的 Blom 模型[13]等等,但是这些方案都存在算法复杂、计算开销大的问题,有的还需要节点共享较多的先验信息,如生成矩阵或公用大素数等等.

确定性模型在可扩展性上一般不如随机概率模型,例如 Camtepe 的方案就采用与随机预分布模型互补的混合模型来解决扩展性问题. Camtepe 方案的一些相关细节将在第 2 节给出.

2 基于区组设计的密钥预分布方案

2.1 区组设计简介

区组设计是组合数学中的一个研究问题. 以下给出与本文研究相关的一些关于区组设计的定义和定理,来源于组合数学中的相关理论[14-16].

定义 1. 设有基集 $S=\{x_1,x_2,x_3,\cdots,x_v\}$,$B_1$,$B_2$,…,$B_b$ 是 S 的 b 个子集,则子集族 $B=\{B_1,B_2,\cdots,B_b\}$ 叫做 S 上的一个区组设计,$B_1,B_2,\cdots,B_b$ 称做 b 个区组. 若 B 是 S 满足特定条件的全排列,则 B 为 S 的一个完全区组设计,否则叫不完全区组设计.

定义 2. 设 $B=\{B_1,B_2,\cdots,B_b\}$ 是 $S=\{x_1,x_2,x_3,\cdots,x_v\}$ 的一个区组设计,如果 B 满足条件:

1) $|B_1|=|B_2|=\cdots=|B_b|=k$;

2) 任意元素 x_j 在 $B_1,B_2,\cdots,B_b$ 中恰好出现 r 次;

3) 任何一对元素 (x_i,x_j) 在 $B_1,B_2,\cdots,B_b$ 中恰好同时出现 λ 次,

则 B 是 S 的一个平衡不完全区组设计,记做 BIBD (balanced incomplete block design). 若进一步有 $b=v$,则称该区组设计为对称的 BIBD(symmetric BIBD),简记为 sBIBD(v,k,λ).

定理 1. 在对称的 BIBD 中,任意两个区组都正好有 λ 个公共元素.

定理 2. 假定集合 X 存在对称平衡不完全区组设计 $D=$sBIBD(v,k,λ),则 $D'=\{B_1',B_2',\cdots,B_v'\}$,($B_i'=X-B_i$)也构成 X 的对称平衡不完全区组设计,而且 $D'=$sBIBD($v,v-k,b-2k+\lambda$). 称 D' 为 D 的补集设计(complementary set design).

例 1. 对集合 $S=\{1,2,3,4,5,6,7\}$,存在一个 sBIBD(7,3,1)及其补集设计 sBIBD(7,4,2):

sBIBD(7,3,1)	sBIBD(7,4,2)
$B_1=\{2,4,6\}$	$B_1'=\{1,3,5,7\}$
$B_2=\{1,4,5\}$	$B_2'=\{2,3,6,7\}$
$B_3=\{3,4,7\}$	$B_3'=\{1,2,5,6\}$
$B_4=\{1,2,3\}$	$B_4'=\{4,5,6,7\}$
$B_5=\{2,5,7\}$	$B_5'=\{1,3,4,6\}$
$B_6=\{1,6,7\}$	$B_6'=\{2,3,4,5\}$
$B_7=\{3,5,6\}$	$B_7'=\{1,2,4,7\}$
B_i,B_j 有 1 个公共元素	B_i',B_j' 有 2 个公共元素

定义 3. sBIBD 的区组矩阵为 $Q=(a_{ij})_{v\times v}$,$i=1,2,\cdots,v$,$j=1,2,\cdots,v$,

其中,
$$a_{ij}=\begin{cases}1, & x_j\in B_i;\\ 0, & x_j\notin B_i.\end{cases}$$

区组矩阵描述了区组设计的结构,是利用区组设计进行具体组合构造(例如构造密钥预分配方案)的工具,例 1 中 sBIBD(7,3,1)的区组矩阵如下:

$$Q=\begin{array}{c} \\ B_1\\B_2\\B_3\\B_4\\B_5\\B_6\\B_7\end{array}\begin{array}{c}\begin{array}{ccccccc}x_1&x_2&x_3&x_4&x_5&x_6&x_7\end{array}\\ \begin{pmatrix}0&1&0&1&0&1&0\\1&0&0&1&1&0&0\\0&1&0&1&0&0&1\\1&1&1&0&0&0&0\\0&1&0&0&1&0&0\\1&0&0&0&0&1&1\\0&0&1&0&1&1&0\end{pmatrix}\end{array}.$$

2.2 sBIBD 与密钥预分布方案的映射

基于 sBIBD 的良好结构特性,我们可以将一个 sBIBD 映射到一个密钥预分配方案.

定义一个密钥预分配方案(key predistribution scheme)为 KPS(N,m,β,p,x,y),其中:

$L=$密钥池中密钥组的总数;

$N=$方案可以容纳的节点个数;

$m=$节点密钥组长度,即密钥组包含的密钥个数;

$p=$任意两个节点的密钥组存在共享密钥的概率;

$\beta=$任意两个节点的密钥组共享密钥的个数;

$x=$平均密钥路径长度;

$y=$最大密钥路径长度.

密钥路径长度是指两节点建立密钥路径需要的跳数,当存在共享密钥时,$x=1$.

当 $\beta>1$ 时,为更好地描述 β 的作用,我们引入一个定义:共同密钥选择空间.

定义 4. 共同密钥选择空间是节点共同拥有的密钥集合,节点可以在这个集合中选取任意的密钥

或密钥组合作为公共密钥.我们将共同密钥选择空间的大小称为 KPS 的共享密钥强度.

在对称加密算法中,加大密钥长度可以抵御穷举猜测攻击,但是基于明文样本的统计性分析会大大降低密钥分析的难度,而扩大共同密钥选择空间,提高了密钥动态变换的程度,有效提高了基于统计性分析的密钥分析攻击的能力.而且大的共同密钥选择空间使得节点对可以不用基于已有密钥进行密钥传输或密钥协商来实现密钥更新,提高了密钥更新的安全性.

一个 sBIBD(v,k,λ)可以和一个 KPS(L,N,m,β,p,x,y)建立如表 1 所述的映射关系:

Table 1 Mapping of a sBIBD to a Key Pre-Distribution
表 1 sBIBD 与密钥预分配方案的映射关系

sBIBD(v,k,λ)		KPS(L,N,m,p,β,x,y)
Element	Comment	
S	base set	key pool
B	block$_i$	key chain of node
Q_i	raw of block matrix	index vector of a key chain
$\|S\|$	size of base set	L = number of key chains
v	number of blocks	N = number of nodes
k	size of block	m = size of key chain
λ	size of a intersection of twoblock	β = number of shared keys in two key chains
		$p=1$,$x=1$,$y=1$

在表 1 的映射下,构造密钥预分配方案等价于构造不同参数的 sBIBD.

在文献[11]中,Camtepe 等人提出了 Symmetric Design 方案,设计出节点数为 n^2+n+1,密钥组长度为 $n+1$,每对节点正好共享 1 个密钥的方案,即一个 KPS(n^2+n+1,n^2+n+1,$n+1$,$n+1$,1,1).

Symmetric Design 的方法基于组合数学中的区组设计和有限几何设计的有关定理:n 阶正交拉丁方的一个完备组对应一个 n 阶仿射平面;n 阶仿射平面对应一个 n 阶射影平面;n 阶射影平面等价对应到 sBIBD(n^2+n+1,$n+1$,1).

Symmetric Design 给出了构造密钥预分配方案的可行性,但对具体的构造方法没有阐述,尤其没有给出可以具体进行密钥预分配操作的区组矩阵.Symmetric Design 是一种密钥强度为 1 的设计.

2.3 基于哈达玛矩阵构造的 sBIBD 密钥预分配方案

本文使用哈达玛矩阵进行 sBIBD 的构造,进而导出基于 sBIBD 的密钥预分布方案,本文的方法可以得出确定的区组矩阵,从而确定每个节点的密钥组组成.并且构造复杂性只决定于哈达玛矩阵的构造,不需要多种数据结构的多次映射.

2.3.1 哈达玛矩阵与 sBIBD

哈达玛矩阵(Hadamard 矩阵)是组合数学中的一个重要矩阵,现给出本文将要使用的哈达玛矩阵的有关定义、定理和性质,具体推导可以参见组合数学的有关理论书籍[10-12].

定义 5. 设 $\boldsymbol{H}_n$ 是 n 阶方阵,其元素都是 1 或 -1,并且 $\boldsymbol{H}_n\boldsymbol{H}_n^{\mathrm{T}}=n\boldsymbol{I}_n$,$\boldsymbol{I}_n$ 为 n 阶单位矩阵,则称 $\boldsymbol{H}_n$ 是一个 n 阶哈达玛矩阵.如果 $\boldsymbol{H}_n$ 的第 1 行和第 1 列的元素都为 1,则 $\boldsymbol{H}_n$ 是一个规范的哈达玛矩阵.

定理 3. 对一个哈达玛矩阵进行初等变换,还将得到一个哈达玛矩阵.

由定理 3 我们不难得到将哈达玛矩阵规范化的一个简单方法,即将第 1 列为 -1 的行乘以 -1,再将第 1 行为 -1 的列乘以 -1.

定理 4. 一个 n 阶($n\geqslant 8$)规范哈达玛矩阵 $\boldsymbol{H}_n$ 对应一个 sBIBD($n-1$,$n/2-1$,$n/4-1$).并且,将 $\boldsymbol{H}_n$ 去掉第 1 行和第 1 列,将剩余元素中为 -1 的元素置为 0,得到对应 sBIBD($n-1$,$n/2-1$,$n/4-1$)的区组矩阵 $\boldsymbol{Q}_{n-1}$.

2.3.2 sBIBD$_{\text{Hadamard}}$密钥预分配方案

本文设计由哈达玛矩阵构造 sBIBD 的密钥预分配方案 sBIBD$_{\text{Hadamard}}$ KPS(key predistribution scheme based on sBIBD constructed by Hadamard matrix).

用 sBIBD$_{\text{Hadamard}}$设计密钥预分配方案 KPS(L,N,m,β,p,x,y)可以认为是为确定参数 L,N,m,计算出指标 p,β,x,y 和得出每个节点密钥组的过程.

一般的,一个传感器网络密钥预分配方案的设计模式是给定传感器节点密钥组长度 m,设计密钥强度 β 和支持的最大节点数 N.我们按此给出 sBIBD$_{\text{Hadamard}}$的设计流程如下:

1) 求最大的 b,满足:

① $b\leqslant m$;

② 存在 $n=2b+2$ 阶哈达玛矩阵 $\boldsymbol{H}_n$.

2) 构造 $\boldsymbol{H}_n$.

3) 将 $\boldsymbol{H}_n$ 规范化后,去掉首行和首列,得到 $\boldsymbol{M}_{n-1}$.

4)生成 sBIBD($n-1$,$n/2-1$,$n/4-1$)的区组矩阵:

$$\boldsymbol{Q}_{n-1}=1/2\times(\boldsymbol{M}_{n-1}+(1)_{n\times n}).$$

5) 为节点 i 分配密钥组 $B_i=\{x_j\}$,$q_{ij}=1$.

6) 结束.

构造的 KPS 有:

$L=N=n-1=2b+1\approx 2m$,

$\beta=n/4-1\approx m/2$,

$p=1$,$x=1$,$y=1$.

我们将以上所述构造的密钥预分配方案称之为 $\text{sBIBD}_{\text{Hadamard}}$ KPS. 可以认为,在 $\text{sBIBD}_{\text{Hadamard}}$ 中,N,m 和 β 存在近似的线性关系,即

$$N\approx 2m\approx 4\beta. \tag{1}$$

$\text{sBIBD}_{\text{Hadamard}}$ KPS 具有以下优点:

① 能确保共享成功,共享概率为 1;

② 共享密钥强度大,节点之间可以拥有多个共享密钥进行选择;

③ 密钥组利用率高,预分配存储在节点的密钥组有一半可以作为共享密钥使用;

④ 在随机预分配方案中需要一定的节点邻居度支持,即对每个节点的邻居数存在期望值,而 $\text{sBIBD}_{\text{Hadamard}}$ KPS 对节点邻居度没有依赖性.

$\text{sBIBD}_{\text{Hadamard}}$ KPS 是一种构造出多个共享密钥($\beta>1$)的方案,同样可以实现多个共享密钥的方案是 q-composite Random,我们通过计算,在表 2 中将基本的 $\text{sBIBD}_{\text{Hadamard}}$ KPS 和 q-composite Random Key Scheme 实现的共享概率进行了对比,随着节点数的增大,q-composite 方案共享概率呈下降趋势,在节点规模大于 1000 以后基本只能收敛在 0.5 左右.

Table 2 Contrast on the Shareing Probabilities of $\text{sBIBD}_{\text{Hadamard}}$ with q-composite

表 2 $\text{sBIBD}_{\text{Hadamard}}$ 与 q-composite 共享概率的对比

Number of Nodes	Key Chain Length	Key Intensity	Key Sharing Probabilities	
			q-composite	$\text{sBIBD}_{\text{Hadamard}}$
7	3	1	0.8377	1
31	15	7	0.6701	1
103	51	25	0.6165	1
211	105	52	0.5819	1
419	209	104	0.5583	1
511	255	127	0.5528	1
1007	503	251	≈0.5	1
2003	1001	500	≈0.5	1
4095	2048	1023	≈0.5	1

在本文之后的论述中,除了特别提出以外,所有 Basic Random 和 q-composite 的数据计算在满足其节点平均度数要求前提下计算得出,即取都是其最优结果.

2.4 扩展的 $\text{sBIBD}_{\text{Hadamard}}$ 密钥预分配方案

相比随机预分配 KPS 和 Symmetric Design KPS 而言,$\text{sBIBD}_{\text{Hadamard}}$ KPS 能支持的节点数目较小.

我们利用补集设计扩展和密钥分片的方法对 $\text{sBIBD}_{\text{Hadamard}}$ KPS 进行改进,可以支持较大的节点数,并且共享概率几乎不受损失. 尤其密钥分片的方法还带来了共享密钥强度的大大增强.

2.4.1 基于补集设计的扩展 $\text{sBIBD}_{\text{Hadamard}}$ 方案

按定理 2 我们为 $\text{sBIBD}_{\text{Hadamard}}(n-1,n/2-1,n/4-1)$ 构造一个补集设计 $\text{sBIBD}_{\text{Hadamard}}(n-1,n/2,n/4)$. 记 $\text{sBIBD}_{\text{Hadamard}}(v,k,\lambda)$ 的区组设计为 $D=\{B_1,B_2,\cdots,B_{n/2-1}\}$,其补集设计为 $D'=\{X-B_1,X-B_2,\cdots,X-B_{n/2}\}$.

我们可以用 D' 为基于 D 构造的 $\text{sBIBD}_{\text{Hadamard}}$ KPS 进行补充,在同一个密钥池上扩展出新的 KPS. 我们称该 KPS 为 $\text{sBIBD}_{\text{Hadamard}}$ KPS 的补集设计扩展 Cextended_$\text{sBIBD}_{\text{Hadamard}}$ KPS(the extended KPS by the Complementary set Design of a $\text{sBIBD}_{\text{Hadamard}}$).

下面给出在构造 $\text{sBIBD}_{\text{Hadamard}}$ 的过程中同时扩展出 Cextended_$\text{sBIBD}_{\text{Hadamard}}$ 的步骤:

1) 求最大的 b,满足:

① $b\leqslant m$;

② 存在 $n=2b+2$ 阶哈达玛矩阵 $\boldsymbol{H}_n$.

2) 构造 $\boldsymbol{H}_n$.

3) 将 $\boldsymbol{H}_n$ 规范化后去掉首行和首列,得到 M_{n-1}.

4) 生成 $\text{sBIBD}(n-1,n/2-1,n/4-1)$ 的区组矩阵:

$\boldsymbol{Q}_{n-1}=1/2\times(\boldsymbol{M}_{n-1}+(1)_{n\times n})$.

5) For $1\leqslant i\leqslant n-1$,为节点 i 分配密钥组 B_i:

$B_i=\{x_j\}$, $q_{ij}=1$, $|B_i|=n/2-1$.

6) For $n\leqslant i\leqslant 2(n-1)$,令 $j=i-n+1$,为节点 i 分配密钥组 B_j':

$B_j'=X-B_j$, $|B_j'|=n/2$.

7) 结束.

构造的 KPS 有:

$L=N=2(n-1)=4b+2\approx 4m$,

$\beta=\min\{n/4-1,n/4\}=(2b-2)/4\approx m/2$,

$p=1-\dfrac{1}{N}$,

$x=1$,$y=2$,

其中参数 p,x,y 的推导计算如下:

从 Cextended_$\text{sBIBD}_{\text{Hadamard}}$ KPS 中任取节点 a 和 b,密钥组为 B_a,B_b,a,b 的分布存在 4 种情况:

① $a,b\in D$,则 B_a,B_b 共享 $n/4-1$ 个密钥;

② $a,b\in D'$,则 a,b 共享 $n/4$ 个密钥;

③ $a\in D,b\in D'$ 且 $B_b\neq B'_a$,

则 B_b 与 B'_a 恰好共享 $n/4$ 个密钥,$\Rightarrow B_b$ 的剩余的$(n/2-n/\frac{1}{N}4)=n/4$ 个密钥$\in B_a\Rightarrow a,b$ 共享 $n/4$ 个密钥;

④ $a\in D,b\in D'$ 且 $B_b=B'_a$,则 a,b 不共享密钥. 综合①~④,有:

1) $p=1-P(B_b\cap B_a=\{\})=$

$1-P(a\in D$ 且 $b\in D'$ 且 $B_b=B'_a)=$

$$1-\frac{n-1}{C(\frac{2}{2}(n-1))}=1-\frac{1}{N}.$$

2) 任取 $B_a,B_b,B_c\in D\cup D'$,B_a,B_b,B_c 两两不同,则 $B_a\cap B_c=\{\}$ 与 $B_a\cap B_c=\{\}$ 不能同时成立. 否则:$B_a\cap B_b=\{\}\Rightarrow B_b=B'_a$,

$B_a\cap B_c=\{\}\Rightarrow B_c=B'_a$,

即 $B_b=B_c$,与前提矛盾,

所以 B_a,B_b,B_c 必有一对存在共享密钥,即 $y=2$.

3) $x=1\times p+2\times(1-p)=1+\frac{1}{N}$.

Cextended_sBIBD$_{\text{Hadamard}}$ KPS 具有如下特性:

① 在同等密钥组长度下,将最大支持的节点数较 sBIBD$_{\text{Hadamard}}$ KPS 扩大了一倍.

② 密钥共享概率损失小,尤其在 N 较大时;

③ 不小于原有 sBIBD$_{\text{Hadamard}}$ KPS 的共享密钥强度;

④ 平均密钥路径短,最大密钥路径长度 $=2$;

⑤ 对节点邻居度数依赖性低,任意两个节点最多需要一个共同邻居即可建立密钥路径;即对节点邻居度的要求为不小于 2.

表 3 给出了 Cextended_sBIBD$_{\text{Hadamard}}$ 主要性能参数:

Table 3 The Shareing Probabilities and Average Key Path Length of Cextended_sBIBD$_{\text{Hadamard}}$

表 3 Cextended_sBIBD$_{\text{Hadamard}}$ 的共享概率与平均密钥路径长度

Number of Nodes	Key Chain Length	Key Intensity	Cextended_sBIBD$_{\text{Hadamard}}$		q-composite
			Key Path Length	Key Sharing Probabilities	Key Sharing Probabilities
14	4	1	1.076923	0.923077	0.7895
22	6	2	1.047619	0.952381	0.6487
118	30	14	1.008547	0.991453	0.0029
502	126	62	1.001996	0.998004	≈0
2014	504	251	1.000497	0.999503	≈0
5006	1252	625	1.000200	0.999800	≈0

相对式(1),在 Cextended_sBIBD$_{\text{Hadamard}}$ 中,N,m 和 β 存在的近似线性关系变为

$$N\approx 4m\approx 8\beta. \tag{2}$$

2.4.2 基于密钥分片的扩展 sBIBD$_{\text{Hadamard}}$ 方案

在 sBIBD$_{\text{Hadamard}}$ 方案中,节点可以共享多个密钥,基于这一点,我们通过将密钥分片,进一步扩大 sBIBD$_{\text{Hadamard}}$ 能支持的网络尺寸.

视节点密钥组为一个集合,在 Basic Random 和 Symmetric Design 中,节点密钥组共享一个元素,只能以基本密钥为单位进行密钥分配. 在 sBIBD$_{\text{Hadamard}}$ 中,节点密钥组共享多个元素,可以用比基本密钥小的单位进行分配,我们称这个单位为密钥分片 key slice. 在预分配时,以密钥分片为单位构造密钥组,密钥组变为密钥分片的集合,节点对用共享的多个密钥分片实时合成共享密钥. 定义这个方案为基于密钥分片的 sBIBD$_{\text{Hadamard}}$ 方案,KS_sBIBD$_{\text{Hadamard}}$ KPS (a sBIBD$_{\text{Hadamard}}$ KPS with Key Slicing).

设有 sBIBD$_{\text{Hadamard}}$ KPS,对应的区组设计为 sBIBD$(n-1,n/2-1,n/4-1)$. 基本密钥长度为 w,密钥分片度数为 d,对密钥池 $X=\{x_1,x_2,\cdots,x_L\}$ 中的基本密钥进行分片,密钥分片大小为 w/d,生成大小为 $L\times d$ 的密钥分片池 $X'=\{x'_1,x'_2,\cdots,x'_{Ld}\}$,KS_sBIBD$_{\text{Hadamard}}$ KPS$(L',N',m',\beta',p',x',y')$设计流程如下:

1) 求最大的 m',满足:

① $m'\leqslant md$;

② 存在 $n=2m'+2$ 阶哈达玛矩阵 $\boldsymbol{H}_n$.

2) 构造 $\boldsymbol{H}_n$.

3) 将 $\boldsymbol{H}_n$ 规范化后,去掉首行和首列,得到 $\boldsymbol{M}_{n-1}$.

4) 生成 sBIBD$(n-1,n/2-1,n/4-1)$的区组矩阵:

$\boldsymbol{Q}_{n-1}=1/2\times(\boldsymbol{M}_{n-1}+(1)_{n\times n})$.

5) 为节点 i 分配密钥组 B_i:

$B_i=\{x'_j\}$, $q_{ij}=1$, $|B_i|=n/2-1$.

6) 结束.

构造的 KPS 有:

$L'=N'=2m'+1\approx 2md+1\approx dN$,

$\beta'=n/4-1\approx md/2$(个密钥分片),

$p'=1,x'=1,y'=1$.

KS_sBIBD$_{\text{Hadamard}}$ KPS 通过将密钥分片,节点之间不再共享完整的密钥,而是由共享的多个密钥分片

实时合成共享密钥.下面给出一个 KS_sBIBD$_{\text{Hadamard}}$ KPS 的例子进行说明:

例 2. KS_sBIBD$_{\text{Hadamard}}$ KPS 示例.

设有 sBIBD$_{\text{Hadamard}}$ KPS,密钥池 $X=\{x_1,x_2,\cdots,x_7\}$,节点密钥组存储能力为 3 个基本密钥单位,可以支持 7 个节点 $B_1,\cdots,B_7$,其密钥组如下:

$B_1=\{2,4,6\}$,$B_2=\{1,4,5\}$,$B_3=\{3,4,7\}$,

$B_4=\{1,2,3\}$,$B_5=\{2,5,7\}$,$B_6=\{1,6,7\}$,

$B_7=\{3,5,6\}$.

每对节点共享一个基本密钥,如 B_1 与 B_7 共享密钥 x_6.

通过将每个基本密钥分片,分片度数 $d=2$,将密钥分片按照任意乱序排列得到密钥分片池:

$$X'=\{x_1',x_2',\cdots,x_7',\cdots,x_{14}'\}.$$

则 KS_sBIBD$_{\text{Hadamard}}$ KPS 可以支持 11 个节点 $B_1,\cdots,B_{11}$,其密钥组如下:

$$B_1=\{x_2',x_4',x_5',x_6',x_{10}'\},$$
$$B_2=\{x_3',x_5',x_6',x_7',x_{11}'\},$$
$$B_3=\{x_1',x4',x_6',x_7',x_8'\},$$
$$B_4=\{x_2',x_5',x_7',x_8',x_9'\},$$
$$B_5=\{x_3',x_6',x_8',x_9',x_{10}'\},$$
$$B_6=\{x_4',x_7',x_9',x_{10}',x_{11}'\},$$
$$B_7=\{x_1',x_5',x_8',x_{10}',x_{11}'\},$$
$$B_8=\{x_1',x_2',x_6',x_9',x_{11}'\},$$
$$B_9=\{x_1',x_2',x_3',x_7',x_{10}'\},$$
$$B_{10}=\{x_2',x_3',x_4',x_8',x_{11}'\},$$
$$B_{11}=\{x_1',x_3',x_4',x_5',x_9'\}.$$

每个节点密钥分片组需要的存储能力为

5 个密钥分片 $=2.5$ 个基本密钥 <3 个基本密钥.

节点之间共享的密钥分片个数等于 2,可以按照不同顺序合成多个基本密钥.如 B_1 与 B_7 共享密钥分片 x_5' 和 x_{10}',可以合成基本密钥 $x_5'x_{10}'$ 或 $x_{10}'x_5'$.

KS_sBIBD$_{\text{Hadamard}}$ KPS 带来了两个改进:

1) 通过密钥分片,扩大了 sBIBD$_{\text{Hadamard}}$ KPS 的网络支持能力,可以近似认为扩大 d 倍;

2) 通过密钥合成提高了密钥强度. sBIBD$_{\text{Hadamard}}$ 在商定密钥时,节点对可以在共享的 λ 个基本密钥中选择,而在共享 λ' 个密钥分片的 KS_sBIBD$_{\text{Hadamard}}$ 中,可以合成个基本密钥,共享密钥强度提高了/λ 倍.由排列组合的数学知识可知,随 λ' 增长的速度是相当快的,例如表 4 中,在 $d=7$ 时,λ' 大于 262 后,共享密钥强度就已超过了密钥空间的大小 $2^{56}=72057594037927936$.

表 4 以使用 56 位加密密钥的 DES 标准加密算法为例,对比了密钥分片度数为 7 时,KS_sBIBD$_{\text{Hadamard}}$ KPS 和 KS_Cextend_sBIBD$_{\text{Hadamard}}$ KPS 对最大支持网络尺寸的扩大和对密钥强度的提高.

Table 4 Improvement in Network Size and Key Intensity by Key Slicing

表 4 密钥分片对网络规模和共享密钥强度的提高

Cextended_sBIBD$_{\text{Hadamard}}$			KS_Cextended_sBIBD$_{\text{Hadamard}}$		
Number of Nodes	Key Chain Length	Key Intensity	Number of Nodes	Key Chain Length	Key Intensity
38	10	4	278	10(70)	6041824588800
302	76	37	2126	76(532)	$2^{56}<P\binom{7}{265}$
398	100	49	2798	100(700)	2^{56}
798	200	99	5598	200(1400)	2^{56}
1150	288	143	8190	288(2016)	2^{56}

Notes: Key chain length is caculated as the multiple of a DES key, and numeric within the parenthesis means slicing degree.

相对式(1),(2),在 KS_sBIBD$_{\text{Hadamard}}$ 中,N,m 和 β 存在的近似线性关系变为

$$N\approx 2d\ m\approx 4d\beta. \tag{3}$$

随着 d 的增大,网络尺寸以较大的线性倍数增长.例如取 128 位的 AES 密钥和 $d=16$ 的分片度数,在密钥组容量为 $128\times 128\text{bit}=4\text{KB}$ 时,可以实现支持 8190 个节点,任意节点对可以选取 2^{128} 个共享密钥.

2.5 分析与评价

本节从密钥预分配模型常用的几个指标对 sBIBD$_{\text{Hadamard}}$ KPS 及其扩展方案进行分析和评价.

2.5.1 构造复杂性

sBIBD$_{\text{Hadamard}}$ KPS 系列密钥预分配方案基于组合数学方法,方案的复杂性在于哈达玛矩阵的构造.我们引入两种朴素的方法构造哈达玛矩阵:

1) 基于有限域的构造法

设 p 为素数,且 $p+1$ 是 4 的倍数.设 a 为有限域 $GF(p)=\{0,1,2,\cdots,p-1\}$ 的一个生成元,记 $GF(p)=\{0,a^0,a^1,\cdots,a^{p-2}\}$,定义函数 $f:GF(p)\to\{0,-1,1\}$:

$$f(b)=\begin{cases}0, & b=0,\\ (-1)^i, & b=a^i,\end{cases}\quad b\in GF(p).$$

则下列的 $p+1$ 阶方阵是哈达玛矩阵:

$$\boldsymbol{H}=\begin{pmatrix}1 & 1 & 1 & 1 & 1 & \cdots & 1\\ 1 & -1 & f(1) & f(2) & f(3) & \cdots & f(p-1)\\ 1 & f(p-1) & -1 & f(1) & f(2) & \cdots & f(p-2)\\ 1 & f(p-2) & f(p-1) & -1 & f(1) & \cdots & f(p-3)\\ \square & \square & \square & \square & \square & & \square\\ 1 & f(1) & f(2) & f(3) & f(4) & \cdots & -1\end{pmatrix}.$$

2) 基于低阶哈达玛矩阵的笛卡儿积构造法

设 $\boldsymbol{H}_m=(a_{ij})$,$\boldsymbol{H}_k=(b_{ij})$分别是 m,k 阶哈达玛矩阵,则 $\boldsymbol{H}_m$ 和 $\boldsymbol{H}_k$ 的笛卡儿积 $\boldsymbol{H}_{mk}=(a_{ij}\boldsymbol{H}_k)$ 是 $m\times k$ 阶哈达玛矩阵.

对不是非常巨大的素数,方法 1)中生成元 a 有表可查;而确定 $f(y)$,$y=0,\cdots,p-1$ 即计算出 a^i,$i=0,\cdots,p-2$,需要 $p-2$ 次乘法和 $p-2$ 次取模运算,n 阶哈达玛矩阵构造的计算复杂度为 $O(n)$. 方法 2)需要 m^2k^2 次乘法运算,n 阶哈达玛矩阵构造的计算复杂度为 $O(n^2)$. 本文根据上述两种方法对哈达玛矩阵的存在性进行了计算,结果表明哈达玛矩阵是广泛存在的,并且相对于其大小而言,阶数的跳跃幅度不大.

特别值得提出的是,$\mathrm{sBIBD}_{\mathrm{Hadamard}}$ 系列密钥预分配方案在哈达玛矩阵构造完毕后,无需额外运算就可以由哈达玛矩直接得到区组矩阵,也就确定了节点的密钥组组成和密钥索引向量.

而 Symmetric Design 方案未给出得到区组矩阵的具体过程. 本文认为其使用的由正交拉丁方及其完备组映射到仿射平面再得出区组矩阵的方案.

2.5.2 共享概率

$\mathrm{sBIBD}_{\mathrm{Hadamard}}$ KPS 的密钥共享概率为 1. 在扩展方案中,基于密钥分片的 $\mathrm{KS\_sBIBD}_{\mathrm{Hadamard}}$ 没有损失概率. 在基于补集设计的 $\mathrm{Cextended\_sBIBD}_{\mathrm{Hadamard}}$ 和 $\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$ 中,由于 $\mathrm{sBIBD}_{\mathrm{Hadamard}}$ 和其补集设计存在良好的对称性,基于补集设计的扩展能够保持很高的共享概率,其共享概率为 $1-(1/N)$(N 为节点数). 在 Symmetric Design KPS 设计中也利用了补集区组设计 $\mathrm{sBIBD}(n^2+n+1,n^2,n^2-n)$. Symmetric Design 从 $\mathrm{sBIBD}(n^2+n+1,n^2,n^2-n)$ 的每个区组中随机选取一个大小为 $n+1$ 的子集,作为新的区组补充到 $\mathrm{sBIBD}(n^2+n+1,n+1,1)$ 中,扩充成新的 KPS,作者称之为 Hybrid Symmetric Design. 由于部分引入了随机预分配模型,Hybrid Symmetric Design 在扩充节点数目占全部节点数比例较大时,共享概率损失会较大.

随机预分配模型和 Hybrid Symmetric Design 的概率计算中隐含了节点邻居度的要求. 在 $\mathrm{sBIBD}_{\mathrm{Hadamard}}$ 中,任意两个节点直接共享密钥,对节点度数没有依赖性;在 $\mathrm{Cextended\_sBIBD}_{\mathrm{Hadamard}}$ 和 $\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$ 中对节点邻居度的要求不小于 2.

表 5 和表 6 将 $\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$ 与 Basic Random 及 Hybrid Symmetric Design 方案进行了对比. 与 Hybrid Symmetric Design 比较时按密钥组长度不大于 Hybrid Symmetric Design,节点数不小于 Hybrid Symmetric Design 的标准,取密钥分片大小为 1 字节进行构造. 扩充比例表示节点数中通过补集设计扩展的节点所占比例,用以观察共享概率损失. 在 $\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$ 中取最大的比例 50%.

Table 5 Contrast on Sharing Probabilities of $\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$ with Basic Random

表 5 $\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$ 与 Basic Random 共享概率对比

Key Chain Length	Number of Nodes	Neighbor Degree	Key Sharing Probabilities	
			$\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$	Basic Random
14	886	29	0.998867	0.2012
24	1534	37	0.999347	0.3171
38	2430	42	0.999588	0.4534
54	3454	47	0.999710	0.5758
72	4606	51	0.999783	0.6812

Table 6 Contrast on Sharing Probabilities of $\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$ with Hybrid Symmetric Design

表 6 $\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$ 与 Hybrid SymmetricDesign 共享概率对比

Key Chain Length	Number of Nodes (extentding ratio)		Hybrid Symmetric Design	
	Key Sharing Probabilities	$\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$	Hybrid Symmetric Design	$\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$
14	250(27%)	254	0.89	0.996016
24	750(27%)	758	0.89	0.998675
38	1500(6%)	1502	0.97	0.999333
54	3000(5%)	3022	0.98	0.999669
72	5250(3%)	5278	0.99	0.999810

Notes: Key chain length is caculated as the multiple of a AES key, and the neighbor degree of $\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$ is setted to 2.

可以看出,$\mathrm{KS\_Cextended\_sBIBD}_{\mathrm{Hadamard}}$ KPS 能够保证很高的共享概率,并且具有良好的稳定性,对节点的邻居度数依赖性也很小.

2.5.3 密钥路径长度

密钥路径长度是衡量密钥预分配模型的重要指标,过长的密钥路径长度不仅导致过多的通信开销,

而且会带来安全性的下降. 表 7 对比了 KS_Cextended_sBIBD$_{Hadamard}$与 Basic Random 和 Hybrid Symmetric Design 的平均密钥路径长度.

Table 7 Contrast on the Average Path Length of KS_Cextended_sBIBD$_{Hadamard}$ with Other Schemes

表 7 KS_Cextended_sBIBD$_{Hadamard}$与其他方案平均密钥路径长度对比

Number of Nodes	Key Chain Llength	Neighbor Degree	Average Key Path Length		
			Hybrid Symmetric Design	KS_Cextended_sBIBD$_{Hadamard}$	Basic Random
250	14	29	1.14	1.003984	1.31
750	24	37	1.15	1.001325	1.33
1500	38	42	1.04	1.000667	1.34
3000	54	47	1.03	1.000331	1.35
5250	72	51	1.01	1.000190	1.35

Notes: Key chain length is caculated as the multiple of a AES key, and the neighbor degree of KS_Cextended_sBIBD$_{Hadamard}$ is setted to 2.

sBIBD$_{Hadamard}$系列方案还有一个重要特性就是最大密钥路径为 2,即只要存在一个公共邻居就可以建立密钥路径. 一般的密钥预分配评价并不特别考虑最大密钥路径,因为在传感器网络实际部署时,可以依靠节点密度来保证较大的节点邻居度数,此时平均密钥路径长度基本能够代表实际的密钥路径长度. 但是,对有些节点密度较小或容易造成小范围孤立的场景,最大密钥路径指标是相当有参考价值的.

2.5.4 最大支持的网络规模

设给定密钥组长度为 m,单位为基本密钥,Symmetric Design 方案的数学结构对应了 sBIBD$(n^2+n+1, n+1, 1)$,因此其支持的网络尺寸为

$$max\,N_{Symmetric\ Design} = (m-1)^2 + (m-1) + 1 = m^2 - m + 1. \quad (4)$$

sBIBD$_{Hadamard}$结构对应 sBIBD$(n-1, n/2-1, n/4-1)$,其补集设计结构对应 sBIBD$(n-1, n/2, n/4)$,Cextended_sBIBD$_{Hadamard}$的结构对应(sBIBD$(n-1, n/2-1, n/4-1) \cup$ sBIBD$(n-1, n/2, n/4)$,因此其支持的网络尺寸为

$$4m - 2 \leqslant max\,N_{Cextended\_sBIBDhadamard} = 2(n-1) \leqslant 4m. \quad (5)$$

为描述简单,取 $max\,N_{Cextended\_sBIBDhadamard} = 4m$. 在 m 不是特别小的前提下是不影响评价结果的.

KS_Cextended_sBIBD$_{Hadamard}$的结构与 Cextended_sBIBD$_{Hadamard}$一样,而密钥分片将支持的节点数扩大了 d 倍(密钥分片度数),其支持的网络尺寸为

$$max\,N_{KS\_Cextended\_sBIBDhadamard} = 4dm. \quad (6)$$

Basic Random 能支持的网络尺寸需要根据要求的共享概率来计算,并且对节点的平均度数存在要求,我们假定平均度数满足要求,按照共享概率近似为 1 来计算 Basic Random 支持的网络尺寸.

相比而言,Symmetric Design 对网络规模的支持最强,与密钥组长度成平方关系,而 KS_Cextended_sBIBD$_{Hadamard}$节点数目与密钥组长度成线性倍数,也大大超过了随机预分配方案. 表 8 取基本密钥为 128b 的 AES 密钥,密钥分片大小为 8b,$d=16$,对比了各自的网络规模:

Table 8 Contrast on the Network Size of KS_Cextended_sBIBD$_{Hadamard}$ with Else Scheme

表 8 KS_Cextended_sBIBD$_{Hadamard}$ KPS 与其他方案的网络规模对比

Key Chain Length	Number of Nodes		
	Hybrid Symmetric Design	KS_Cextended_sBIBD$_{Hadamard}$	Basic Random
24	750	1534	100
38	1500	2430	250
54	3000	3454	500
72	5250	4606	750
102	10303	6558	1800

2.5.5 共享密钥强度

sBIBD$_{Hadamard}$系列方案通过密钥分片实时合成共享密钥的方法,大大扩大了共享密钥选择空间. 密钥强度的增强从 3 个方面提高了系统安全性:

1) 扩大密钥选择空间提高了密钥变换的能力和程度,增加了系统抵抗密钥分析特别是基于明文样本统计分析攻击的能力;

2) 大的共同密钥选择空间使得可以不用基于已有密钥进行密钥传输或密钥协商来实现密钥更新,提高了密钥更新的安全性;

3) 大的共同密钥选择空间增大了实时合成公共密钥时密钥分片的排列顺序数,通过变换排列顺序的方式,使得妥协节点即使拥有相同密钥分片,也难以对其他正常节点之间的安全通信造成威胁.

Basic Random 和 Symmetric Design 方案都只能实现单个共享密钥,q-Composite Random 可以实现多个共享密钥,但是共享概率难以提高.

2.5.6 密钥建立的能量消耗

$\text{sBIBD}_{\text{Hadamard}}$系列方案的能量消耗主要发生在密钥建立时,包括通信能耗、计算能耗和存取能耗.

以 $\text{KS_sBIBD}_{\text{Hadamard}}$方案为例,设节点数为 N,密钥组长度为 m,密钥分片度数为 d,按式(3)取 $N=2dm$. 每个传感器节点的能耗产生和计算如下:

1) 交换密钥索引向量

$\text{KS_sBIBD}_{\text{Hadamard}}$的共享密钥发现采用类似于 Basic Random 的密钥 ID 对比方法,区别在于用由区组矩阵导出的密钥索引向量代替密钥 ID 列表.

记传感器节点发送和接收一个 bit 的通信能耗为 ω,则 $\text{KS_sBIBD}_{\text{Hadamard}}$的通信能耗为

$$ComCost\_KS = 2N(\omega). \tag{7}$$

Basic Random 方案相应的能耗可以计算为

$$ComCost\_BR = 2 \times m \log_2 N = \frac{N}{d} \log_2 N(\omega). \tag{8}$$

$ComCost\_KS$ 是数量级 $O(N)$的,而 $ComCost\_BR$ 则是数量级 $O(N\log_2 N)$的.

2) 密钥合成

Basic Random 通过循环对比得到共享密钥的 ID 列表,计算复杂度为 $O(m)$,计算单元长度为 $\log_2 N$. 而 $\text{KS_sBIBD}_{\text{Hadamard}}$通过将双方的密钥索引向量进行一次逻辑与得出共享密钥的索引向量,取同样的计算单元,则计算复杂度为 $O\left(\frac{N}{\log_2 N}\right) = O\left(\frac{m}{\log_2 m}\right) < O(m)$.

记传感器节点的基本字长为 s,基本密钥长度为 $K(s)$,密钥分片长度为 $K/d(s)$,$\text{KS_sBIBD}_{\text{Hadamard}}$取 d 个密钥分片合成一个基本密钥,需要 $K = d \times (K/d)$个存取操作. 在 Basic Random 方案中,需要一次基本密钥的存取,同样需要 K 个存取操作.

由上述分析可知,$\text{KS_sBIBD}_{\text{Hadamard}}$没有在计算和存取操作上带来太多的额外开销. 并且在传感器节点的能耗中,通信能耗占主要部分,而由式(7),(8)可知,随着节点数的增加(m 相应增长),$\text{KS_sBIBD}_{\text{Hadamard}}$在通信能耗上体现出较大的优势. 从总体上说,$\text{KS_sBIBD}_{\text{Hadamard}}$的能耗是可以接受的.

3 结束语

密钥预分配是无线传感器网络的主要密钥管理方式. 在现有方案中,基于概率的随机预分配方案存在共享概率和密钥路径长度无法得到确定性保证的问题,并且在节点密钥组长度受限的情况下难以支持较大规模的网络;已有确定性方案大多计算复杂,与本文类似的基于组合数学方法的 Symmetric Design 实现了确定性的密钥共享,并且可以按密钥组长度成平方增长扩大网络规模,但是只能保证共享一个密钥. 本文基于哈达玛矩阵构造对称平衡不完全区组设计,实现了新的密钥预分配方案 $\text{sBIBD}_{\text{Hadamard}}$ KPS 系列方案. 改进了现有多数方案只能共享单个密钥的问题,提出了共享密钥实时合成方法,在节点密钥组物理长度不变的前提下,大大扩大了共享密钥选择空间,提高了安全强度;实现了同等节点密钥组长度和密钥强度要求情况下,比现有支持多密钥共享方案更高的共享概率和更小的密钥路径长度. 最后使用补集设计方法和密钥分片方法对其扩展,实现了对较大网络规模的支持,并在一定程度上优化了能耗.

参 考 文 献

[1] I F Akyildiz, W Su, Y Sankarasubramaniam, *et al*. A survey on sensor networks [J]. IEEE Communications, 2002, 40(8): 102-114

[2] Sun Liming, *et al*. Wireless Sensor Networks [M]. Beijing: Tsinghua University Press, 2005 (in Chinese)
(孙利民, 等. 无线传感器网络[M]. 北京:清华大学出版社, 2005)

[3] Cui Li, Ju Hailing, *et al*. Overview of wireless sensor networks [J]. Journal of Computer Research and Development, 2005, 42(1): 163-174 (in Chinese)
(崔莉, 鞠海玲, 等. 无线传感器网络研究进展[J]. 计算机研究与发展, 2005, 42(1): 163-174)

[4] H Chan, A Perrig. Security and privacy in sensor networks [J]. IEEE Computer, 2003, 36(10): 103-105

[5] A Perrig, J Stankovic, D Wagner. Security in sensor networks [J]. Communications of the ACM, 2004, 47(6): 53-57

[6] Hu Lei, *et al*. Handbook of Applied Cryptography [M]. Beijing: Publishing House of Electronics Industry, 2005 (in Chinese)
(胡磊, 等. 应用密码学手册[M]. 北京:电子工业出版社, 2005)

[7] Zeng Weini, Lin Yaping, *et al*. A group key management scheme based on distributed rekeying authority in sensor networks [J]. Journal of Computer Research and Development, 2007, 44(4): 606-614 (in Chinese)
(曾玮妮, 林亚平, 等. 传感器网络中一种基于分布式更新权限的组密钥管理方案[J]. 计算机研究与发展, 2007, 44(4): 606-614)

[8] L Eschenauer, V D Gligor. A key-management scheme for distributed sensor networks [C]. In: Proc of the 9th ACM Conf on Computer and Communications Security. New York: ACM Press, 2002. 41-47

[9] Haowen Chan, Adrian Perrig, Dawn Song. Random key predistribution schemes for sensor networks [C]. In: Proc of 2003 IEEE Symp on Research in Security and Privacy. New York: ACM Press, 2003. 197-213

[10] D Liu, P Ning. Establishing pairwise keys in distributed sensor networks [C]. In: Proc of the 10th ACM Conf on Computer and Communications Security. New York: ACM Press, 2003. 52-61

[11] S A Camtepe, B Yener. Combnatorial design of key distribution mechanicsms for wireless sensor networks [C]. In: Proc of the 9th European Symp on Research in Computer Security. Berlin: Springer, 2004. 293-308

[12] J Lee, D R Stinson. Deterministic key predistribution schemes for distributed sensor networks [C]. In: Proc of the 11th Int'l Workshop on Selected Areas in Cryptography. Berlin: Springer, 2004. 1-14

[13] Wenliang Du, Jing Deng. A pairwise key predistribution scheme for wiress sensor networks [C]. In: Proc of the 10th ACM Conf on Comuer and Communications Security. New York: ACM Press, 2003. 42-51

[14] Yang Zhensheng. Combinatorial Mathematics and the Algorithms [M]. Hefei: University of Science and Technology of China Press, 1997 (in Chinese)
(杨振生. 组合数学及其算法[M]. 合肥:中国科学技术大学出版社, 1997)

[15] Li Fanchang, *et al*. Combinatorial Theory and the Applications [M]. Beijing: Tsinghua University Press, 2005 (in Chinese)
(李凡长, 等. 组合理论及其应用[M]. 北京:清华大学出版社, 2005)

[16] I Anderson. Combinatorial Designs: Construction Methods [M]. Chichester, England: Ellis Horwood Ltd, 1990

Xia Geming, born in 1973. Ph. D. candidate in computer science of the National University of Defense Technology, Changsha, China. His current research interests include wireless sensor networks, information security and mobile computing.

夏戈明,1973 年生,博士研究生,主要研究方向为无线传感器网络、信息安全和移动计算.

Huang Zunguo, born in 1958. Associate professor and master supervisor in computer science of the National University of Defense Technology, Changsha, China. His current research interests include computer networks and information security.

黄遵国,1958 年生,副教授,硕士生导师,主要研究方向为计算机网络和信息安全.

Wang Zhiying, born in 1956. Professor and Ph. D. supervisor in computer science of the National University of Defense Technology, Changsha, China. His current research interests include computer architecture, information security and microprocessor designs.

王志英,1956 年生,教授,博士生导师,主要研究方向为计算机体系结构、信息安全和微处理器设计.

Research Background

For its wonderful applied foreground, wireless sensor network turns into a research hotspot nowadays. A great deal of works have been carried out to study the fundamental problems of wireless sensor networks, including the security. For security of wireless sensor networks, the main topic is the key pre-distribution. There are many key pre-distribution schemes for wireless sensor networks, constructed by various methods such as probabilistic subset, bivariate polynomial, generating matrix of a MDS code, and so on. This paper presents a novel scheme based on combinatorial mathematics. The scheme named $sBIBD_{Hadamard}$ KPS is constructed on the symmetric balanced incomplete block design using Hadamard matrix. The $sBIBD_{Hadamard}$ KPS improves itself than the most scheme in existence on a higher sharing probability and a shorter average key path length with the same size of key chain, and it can make the pair nodes share more than one key, and do all that without asking for a node neighbor degree more than 2. By carrying out a particular method of compositing the common key in time for the pair nodes, it enhances the security by enlarging the key space for key analysis. Furthermore, $sBIBD_{Hadamard}$ KPS expands itself to support many more nodes by two means named complementary set design and key slicing.