基于有限几何构造密钥预分配方案

姚泓杨　严付伟灏　姚沂姗
中国民航大学

[摘　要]无线传感器网络被广泛应用于各个行业，密钥预分配是无线传感器网络中极具挑战性的安全问题之一，本文基于n维向量中$n-1$维子空间和1为子空间之间的包含关系构造了一个密钥预分配方案，该方案的连通性达到最大值1,当捕获节点数目较少时，方案的损失概率也非常低，与其它一些已有的密钥预分配方案相比，该方案具有良好的连通性和抗毁性。

[关键词]无线传感器网络；密钥预分配；组合设计；向量空间
【DOI】10.12252/j.issn.2096-6288.2021.10.2246

一、研究背景

无线传感器网络可用于遥测外部环境中的一些物理数据，并通过无线通信的方式将测试结果发回测试台站，近年来，无线传感器络在各行各业上都得到了广泛的应用。军事方面，对于危险的战场搜集信息，包括侦察敌情、监控兵力、装备和物资，判断生物化学攻击等多方面用途。

1.农业方面：农作物中的害虫、土壤的酸碱度和施肥状况等；

2.工业方面：挪威是一个盛产石油的国家，他们在石油管道上分布大量了传感器，监测管道是否正常工作，也监测管道周围环境是否对石油管道构成威胁（例如盗窃石油）；

3.环境的监测和保护：可以跟踪候鸟和昆虫的迁移，研究环境变化对农作物的影响，监测海洋、大气和土壤的成分等；

4.预防自然灾害：办公场所及森林的防火；

5.老人保健：在国外，利用传感器对高龄人士的健康监测，引起了越来越多的重视。

在传感器网络的应用中，有时候需要信息的保密性。例如战场上采集到的信息，人的健康状况等隐私信息。在传感器网络的使用环境中，敌方（或者攻击者）不仅可以接收传感器之间相互传递的信息，而且能够捕获一定数量的传感器，还可能打开传感器的防护措施，得到传感器中存储的信息，为了保证信息的安全，需要采用密码技术。为此，首先要解决的问题是密钥交换问题，因为传感器之间要秘密通信，一定有公共的会话密钥。公钥密码非常完美地解决了会话密钥的交换和管理问题，但是由于绝大多数的公钥密码都是建立在特定的数学难题的基础上，相应的加密和解密算法要涉及到复杂的与大整数计算有关的操作，因而计算速度比较慢。另一方面，在传感器网络的应用中，往往需要成千上万个传感器，为了降低成本，所采用的都是价格比较低廉、计算能力比较弱、存储性能比较小的传感器。因此，在这些低端的处理器上实现公钥密码算法，至少对目前来说是不合适的。

另一种做法是采用密钥预分配方案，即在传感器散布到测试现场之前，先往每一个传感器中存储一些密钥或者密钥材料。对于存储密钥材料的情形，每一对传感器需要花费一定的计算量来产生会话密钥。对于前者，则要为每个会话密钥进行编号，当传感器散布到测试现场之后，每个传感器与自己周围（即每个传感器的通信范围之内，称之为通信半径）的传感器交换彼此存储的密钥编号，从而可以确定是否有公共的会话密钥，如果有公共的会话密钥，就可以选择其中一个进行安全通信，这时我们称这两个传感器之间有一个安全联接。如果两个传感器需要通信，它们不在彼此的通信范围之内，或者在彼此的通信范围之内但没有公共密钥，这时需要寻找一个通信路径来达到安全通信的目的。

对于传感器网络中的密钥预分配方案来说，往往从以下四个方面来刻划方案的好坏：第一、传感器中所存储密钥的个数k。参数k表明了方案对传感器硬件的要求，如果k越大，则对传感器的存储空间要求就越高，从而传感器的成本也相对较高。第二、方案所能够支持的传感器最大数目b，它刻划了方案所能支持的传感器网络的规模。第三、安全连通概率p，即传感器网络中任意一对传感器之间存在公共密钥的概率。它衡量了密钥预分配方案的通信效率，我们希望连通概率越高越好。第四、损伤概率fail(1)当一个传感器被敌方捕获后，该传感器中存储的密钥将不能在传感器网络中使用，这时如果一对传感器的公共密钥恰好全部包含在被捕获的传感器中，则这一对传感器之间的安全连接被破坏，那么损伤概率概率定义为

fail(1)=损失的连接数/原来的的连接数

损伤概率fail(1)表达了传感器网络的稳健性，我们希望它越小越好。

根据给节点分配密钥方法的不同，无线传感器网络的密钥预分配方案有以下两种划分，即概率不确定型密钥预分配方案和基于组合结构的确定型密钥预分配方案。

Eschenauer和Gligor最早为无线传感器网络提出了一种随机型的密钥预分配方案。该方案的过程如下：先从已选定的对称密码算法的密钥空间中随机产生一个足够大的密钥池，假定有p个密钥，并对每一个密钥编号。为传感器网络中的每个传感器随机选择k个互不相同的密钥，将这k个密钥及相应的编号存储在传感器中。当传感器散布到测试场所时，每个传感器与相邻的传感器（称两个传感器相邻，是指它们彼此地对方的通信范围之内）相互交换密钥的编号，看是否有公共的密钥，如果有公共密钥，就可以进行安全通信。如果没有公共的密钥，则寻找是否存在一条安全通信链。

假定一个传感器网络中有n个传感器，任意两个传感器之间有公共密钥的概率为p，令d=p(n-1)。则表明在整个传感器网络中，对于每一个传感器来说，平均有d个传感器与该传感器有公共密钥。另一方面，Eschenauer研究了传感器网络在

应用中的一种实际情况：由于每个传感器的通信功能有限，每个传感器只能和它通信范围内的有限几个传感器进行安全通信，他们利用概率图论的方法，研究了在这种情况下传感器网络的实际连通概率。

相比于随机型的密钥预分配方案，确定型的密钥预分配方案方面的文章相对比较少最早由Camtepe等人提出，并利用射影平面中的射影直线构造了一类安全连通概率为$p=1$的密钥预分配方案。后来Lee和Stinson对这种方法做了进一步的推广，并利用 Transversal Design构造了一类密钥预分配方案。

二、基础知识

（一）基本定义

1.所有的密钥预分配方案都可大致分为以下三个阶段：

密钥预分配：将所有密钥编号然后预先将密钥与编号分配给节点。

共享密钥发现：发现节点间的公共密钥（共享密钥可直接建立通信）。

密钥路径建立：无共享密钥节点可通过共享密钥节点作中间密钥建立通信。

2.密钥预分配方案一般从网络容量、密钥量。连通概率和损失概率四个方面来衡量是否具有可行性。

网络容量：方案所支持的最大传感器数目；

密钥量：（密钥链/密钥环的大小）：每个节点所能储存的密钥数量；

连通概率：方案中任意2个传感器节点建立能够直接通信的概率（越大越好）；

损失概率：当s个节点被捕获时，一条随机链接被破坏的概率，通常用fail(s)来表示。

3.所有的节点只储存一个密钥，所有节点利用同一个密钥k_1建立通信。连通概率p=1。

4.假如网络中有n个节点，每个节点存储与其他n-1个节点的共享密钥一旦未被捕获，该节点失效，其余连接不被破坏且每一节点密钥存储量过大连通概率p=1。

（二）组合设计

X 是一个有限集，$X=\{x_1,\ldots,x_n\}$ 是一个点集，$\mathcal{B}=\{B_1,\ldots,B_b\}$ 称为区组集，$\mathcal{B}$ 是 X 子集的集合，对任意 $x\subseteq X$，x 的度是指包含点 x 的区组数。若 x 中所有点有相同的度 r，则称 $(X,\mathcal{B})$ 是正则的，$(X,\mathcal{B})$ 的秩为所含元素个数最多的区组的大小，如果所有的区组秩都相同且等于 k，$(X,\mathcal{B})$ 则称是一致的。

例：$X=\{1,\ldots,9\}$，$\mathcal{B}=\{123,456,147,369,357,249,348,159,789,267,168,258\}$。

$|X|=9$　　$|\mathcal{B}|=12$

$r=4$　　$rank=3$

$(X,\mathcal{B})$ 既正则又一致。

定义2.1　令 X 和 $\mathcal{B}$ 是两个不相交的有限集合，I 为 X 与 $\mathcal{B}$ 之间的二元关系，即 $I\subseteq X\times\mathcal{B}$，三元组 $D=(X,\mathcal{B},I)$ 为一个关联结构。X 中的元素叫点，$\mathcal{B}$ 中的元素叫区组，I 叫关联结构。设 $x_i\in X$，$B_j\in\mathcal{B}$，若 $(x_i,B_j)\in I$，则称点 x_i 与区组 B_j 关联，并记作 x_iIB_j。

当 $D=(X,\mathcal{B},I)$ 为有限关联结构时，通常记 $|X|=v$，$|\mathcal{B}|=b$。为方便起见，用 $X(B)$ 表示与一给定的区组 B 关联的点的集合，$\mathcal{B}(x)$ 表示与一给定的点 x 关联的区组的集合，记 $|X(B)|=k$，$|\mathcal{B}(x)|=r$。另用 σ 表示与两个不同的区组同时关联的点数。

定义2.2　令 v,k,λ,t 均为正整数，且 $v\geq k\geq 2$，$\lambda\geq 1$，$t\leq k$。$D=(X,\mathcal{B},I)$ 是一个关联结构，二元组 $(X,\mathcal{B})$ 是一个平衡不完全区组设计或者 $(v,k,\lambda)-BIBD$，简记如果满足下列条件：

(1) $|X|=v$，$|\mathcal{B}|=b$；

(2) 对任意的 $B\in\mathcal{B}$，$|B|=k$；

(3) X 中的任意两个不同的点恰与 $\mathcal{B}$ 的 λ 个区组关联；

组合设计中每个点 x 对应一个密钥，点集 X 对应密钥池，每个区组对应每个节点，其中区组数 $|\mathcal{B}|$ 则是节点数，区组大小 $|B_i|(B_i\in\mathcal{B})$ 则是密钥量，$|B_i\cap B_j|\geq 1$ 表示节点 N_i 与 N_j 有共享密钥。

以攻击模型为例：当 s 个节点被捕获，考虑如何才能使得未捕获的两个节点之间的链接断开。被捕获的 s 个节点对应的区组为 $B_1,\ldots,B_s$，若两个未被捕获的节点 N_i,N_j，则他们对应的区组为 B_i,B_j，当 $B_i\cap B_j\subseteq\bigcup_{k=1}^{s}B_k$ 时，N_i 和 N_j 之间的链接断开。

三、方案设计

设 V 是一个 n 维向量空间，若

$X=\{x|\ x$ 为 V 的一维子空间$\}$

$\mathcal{B}=\{B$ 为 V 的 $(n-1)$ 维子空间$\}$

此时 X 为点集，$\mathcal{B}$ 为区组集。

对 $x\in X$，$B\in\mathcal{B}$，定义 x 与 B 关联当且仅当 $x\subseteq B$，即 x 与 B 关联当且仅当一维子空间包含在 $(n-1)$ 维子空间中。

对任意 $B\in\mathcal{B}$，

$$X(B)=\{x|x\subseteq B\}$$

对任意 $x\in X$，

$$\mathcal{B}(x)=\{B|x\subseteq B\}$$

根据以上构造计算可得

$$v=|X|=\begin{bmatrix}n\\1\end{bmatrix}=\frac{\prod_{i=n}^{n}(q^i-1)}{\prod_{i=1}^{1}(q^i-1)}=\frac{q^n-1}{q-1},\quad b=|\mathcal{B}|=\begin{bmatrix}n\\n-1\end{bmatrix}=\frac{\prod_{i=2}^{n}(q^i-1)}{\prod_{i=1}^{n-1}(q^i-1)}=\frac{q^n-1}{q-1}。$$

密钥环 k 即为 $n-1$ 维子空间中所包含的一维子空间个数，故

$$k=|X(B)|=\begin{bmatrix}n-1\\1\end{bmatrix}=\frac{q^{n-1}-1}{q-1}。$$

对任意一个密钥 k 都存在于个r节点中，故

$$r=|\mathcal{B}(X)|=\frac{q^{n-1}-1}{q-1}。$$

考虑 X 两个不同的点与 B 中多少个区组关联密钥，即两个不同的1维子空间 x_1,x_2 包含在多少个 $n-1$ 维子空间中，由维数公式

$$dim(v_1+v_2)=dim(v_1)+dim(v_2)-dim(v_1\cap v_2)$$

可知 $\dim(x_1+x_2)=2$，因此

$$\lambda=\begin{bmatrix}n-2\\ n\text{-}1\text{-}2\end{bmatrix}=\begin{bmatrix}n-2\\ n-3\end{bmatrix}=\frac{q^{n-2}-1}{q-1}。$$

综上本文构造了一个平衡不完全区组设计。接下来分析基于该组合设计的密钥预分配方案的一些参数。

考虑两个不同的区组有多少个公共点，即 $n-1$ 维子空间所包含的1维子空间的数目。设 B_1,B_2 为 V 中的两个不同的 $n-1$ 维子空间，则由维数公式可知 $\dim(B_1\cap B_2)=n-2$，因此

$$\delta=\begin{bmatrix}n-2\\ 1\end{bmatrix}=\frac{q^{n-2}-1}{q-1}$$

本方案中任意两个节点都有共享密钥，因此连通概率为

$$p=1$$

节点 N_i 和节点 N_j 通信时，并不以它们之间的公共密钥作为会话密钥 k，而是将 δ 个公共密钥按照一定的顺序排列。经过Hash函数复合而成一个新的密钥 $k=Hash(k_1\|\ldots\|k_8)$。考虑本方案的损失概率，即计算捕获 δ 个节点之后，两个未被捕获的节点之间断开的概率为

$$fail(s)=(1-(1-\frac{r}{b})^s)^\delta。$$

即

$$fail(s)=(1-(1-\frac{r}{b})^s)^\delta=\left[1-q^{vn-s}\left(\frac{q-1}{q^n-1}\right)^s\right]^{\frac{q^{n-2}}{q-1}}。$$

四、方案分析

广义四边形：

对 X 中的每一个点，恰好有 B 中的 $t-1$ 直线经过，而且对于 X 中任意两个不同的点，B 中最多有一条直线同时经过这2个点；

每条直线上恰有 $1+s$ 个点，而且任意2条不相同的直线最终交于 X 的一个点；

对 $x\in X,L\in B$，如果点 x 不在直线 L 上，则存在唯一的一个点 $y\in X$ 及唯一的一条直线 $M\in B$，使得点 x 在直线 M 上，而直线 M 经过点 y，点 y 在直线 L 上。

连通概率：

$$p=\frac{k(r-1)}{b-1}$$

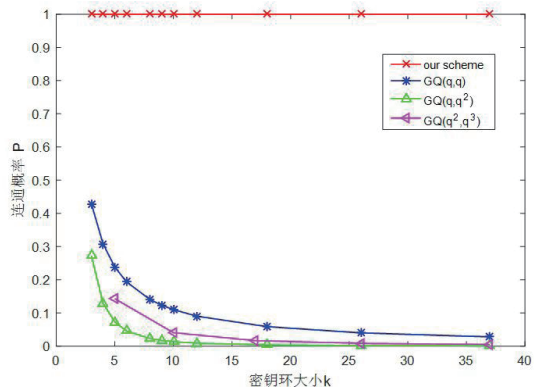
损失概率：

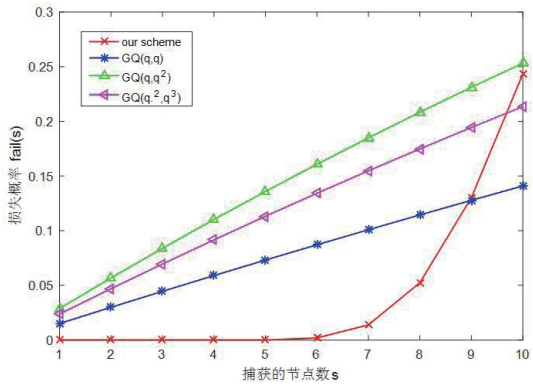
$$fail(1)=\frac{r-2}{b-2},fail(s)=\left(1-\frac{n-2}{n^2-2}\right)^s_1$$

密钥预分配方案诸参数：

方案	v	b	k	r	连通概率	损失概率
Our scheme	$\frac{q^n-1}{q-1}$	$\frac{q^n-1}{q-1}$	$\frac{q^{n-1}-1}{q-1}$	$\frac{q^{n-1}-1}{q-1}$	1	$\left[1-q^{sn-s}\left(\frac{q-1}{q^n-1}\right)^s\right]^{\frac{q^{n-2}}{q-1}}$
$GQ(q,q)$	$(q+1)(q^2+1)$	$(q+1)(q^2+1)$	$q+1$	$q+1$	$\frac{q+1}{q^2+q+1}$	$1-\left(\frac{q^3+q^2}{q^3+q^2+q-1}\right)^s$
$GQ(q,q^2)$	$(q+1)(q^3+1)$	$(q+1)(q^3+1)$	$q+1$	q^2+1	$\frac{q+1}{q^3+q+1}$	$1-\left(\frac{q^4+q^3-q^2+q}{q^4+q^3+q-1}\right)^s$
$GQ(q^2,q^3)$	$(q^2+1)(q^5+1)$	$(q^2+1)(q^5+1)$	q^2+1	q^3+1	$\frac{q^2+1}{q^5+q+1}$	$1-\left(\frac{q^7+q^5-q^3+q^2}{q^7+q^5+q^2-1}\right)^s$

由matlab基于广义四边形的密钥预分配方案作图得出广义四边形与本文中方案比较连通概率和损失概率：





经过对比发现本文中提出的密钥预分配方案连通概率更高，损失概率更小，显然方案更好。

五、结语

随着网络安全的普及，研究传感器网络的连通性、安全性、节点间的通信延迟、节点能储存的密钥量、网络最大节点数、可认证性、网络通信的能耗等衡量标准之间的关系越来越多。目前为止，每种密钥预分配方案的分析还只是停留在对少数几种性能方面的比较，对除捕获攻击外的攻击手段下，网络的安全性分析的结果甚少。本文基于n维向量空间中子空间之间的包含关系构造了一个密钥预分配方案，使连通率对比其他的更高，损失率则更低。

参考文献：

[1]董武军，王学理.密钥预分配方案与正交阵列.湖南大学博士学位论文.20090216