

文章编号:1001-9081(2008)01-0085-03

## 基于矩阵格的传感器网络密钥预配置方案

张学锋<sup>1</sup>, 姜皇普<sup>2</sup>, 王永栓<sup>2</sup>

(1. 邢台广播电视台教务处, 河北 邢台 054000; 2. 燕山大学信息科学与工程学院, 河北 秦皇岛 066004)

(huangpujiang66@163.com)

**摘要:**为了提高传感器网络的安全性能,在密钥管理中提出了矩阵池、矩阵格的概念,将密钥的预配置建立在多个密钥矩阵之上,并将加密传输机制应用到密钥的传输过程中,以提高密钥传输过程中的安全性。通过借鉴 Blom 的预配置方案,设计出一个应用于传感器网络的高效密钥对预配置方案。

**关键词:**密钥管理;密钥预配置;密钥矩阵;无线传感器网络

**中图分类号:** TP393    **文献标志码:**A

### Matrix grid-based key pre-distribution in sensor networks

ZHANG Xue-feng<sup>1</sup>, JIANG Huang-pu<sup>2</sup>, WANG Yong-shuan<sup>2</sup>

(1. Studies Affairs Office, Xingtai Radio & TV University, Xingtai Hebei 054000, China;

2. College of Information Science and Engineering, Yanshan University, Qinhuangdao Hebei 066004, China)

**Abstract:** To solve the security problem of wireless sensor networks, the concept of matrix pool and matrix grid were put forward, upon which our key pre-distribution scheme was built. And in the matrix grid based scheme, encryption was introduced into the process of key transfer. Using Blom's key pre-distribution for reference, an efficient key pre-distribution scheme was presented for sensor networks.

**Key words:** key management; key pre-distribution; key matrix; Wireless Sensor Networks( WSN )

近年来,随着传感器网络的应用的日益广泛,很多传感器网络中的密钥管理方案被提出来。文献[1]提出了两个成对的密钥预配置方案:随机的多项式的密钥方案和一个基于格的多项式密钥预配置方案。这些方案是建立在多项式上的密钥预配置协议,通过采用多项式密钥池加强了基础的基于多项式的密钥预配置方案。但是这些方案都需要进行很复杂的计算。在传感器网络里还有很多其他的成对密钥预配置方案,例如:文献[2]的密钥管理方案(下面称 Blom 方案),文献[3,4]提出的多空间的密钥管理方案和基于位置的建立成对密钥的方案。

由于传感器网络的可用资源极其有限,所以传感器网络的密钥预配置方案应当在节省节点和网络资源的情况下提高网络的安全性能。在 Blom 方案中,提出了一种利用密钥矩阵来进行密钥预配置的方案。这种方案的最终结果是在每个节点上配置与网络节点数目相同的密钥数目。因此这种方案在节点资源的利用、网络的可扩展性、网络的安全性能等方面都存在不足。本文以 Blom 方案为基础,提出了一种基于矩阵格的方案,弥补了 Blom 方案的不足,称之为基于矩阵格的密钥预配置方案。

### 1 相关概念

为了便于以后的理解,首先介绍一下相关概念。

#### 1.1 密钥矩阵

如图 1 所示,在密钥的预配置阶段,存在一个离线的安装服务器。这个服务器可以在一个有限域  $GF(q)$  上产生  $(\lambda+1) \times N$  矩阵  $G$ , 其中  $N$  是网络中点个数。矩阵  $G$  是公开的,任何节点,即使是恶意节点都可能获得该矩阵。之后,安装服务器在一个有限域  $GF(q)$  上随机产生一个  $(\lambda+1) \times (\lambda+1)$  的对称矩阵  $D$ , 计算  $N \times (\lambda+1)$  矩阵  $A = (D \cdot G)^T$  (其中

$(D \cdot G)^T$  是  $(D \cdot G)$  的转置矩阵), 矩阵  $D$  是需要保密的, 只有安装服务器知道, 某个合法节点只能获得矩阵  $(D \cdot G)^T$  的某一行。因为  $D$  是一个对称矩阵, 所以有下列结论:

$$A \cdot G = (D \cdot G)^T = G^T \cdot D^T \cdot G = \\ G^T \cdot D \cdot G = (A \cdot G)^T$$

也就是说  $A \cdot G$  是一个对称矩阵。如果设  $K = A \cdot G$ , 则  $K_{ij} = K_{ji}$ , 这里  $K_{ij}$  是  $K$  第  $i$  行第  $j$  列的元素。图 1 说明了密钥  $K_{ij} = K_{ji}$  是如何产生的。为了完成上述计算, 节点  $i$  和节点  $j$  应当能够独立地计算密钥  $K_{ij}$  和  $K_{ji}$ 。将矩阵  $A$  的第  $k$  行,  $G$  的第  $k$  列  $R$  分配给节点  $i$ , 将矩阵  $A$  的第  $m$  行,  $G$  的第  $m$  列  $C$  分配给  $j$ 。当节点  $i$  和节点  $j$  之间进行密钥发现时, 首先交换矩阵  $G$  的份额, 然后它们就可以利用自己存储的  $A$  的份额独立地计算  $K_{ij}$  (或  $K_{ji}$ ) 了, 其中  $G$  的份额可以以明文方式传送, 因为  $G$  是公开的。现在就可以利用  $K_{ij}$  (或  $K_{ji}$ ) 作为节点  $i$  和  $j$  之间的密钥了。

如果矩阵  $G$  的  $\lambda+1$  列是线性无关的, 则此方案被证明是  $\lambda$  安全的, 也就是说, 只有节点  $i$  和  $j$  可以计算出  $K_{ij}$  和  $K_{ji}$ , 除非网络中有大于  $\lambda$  个节点被俘获。

下面举一个矩阵  $G$  的例子。首先我们必须保证  $G$  的  $\lambda+1$  列都是线性无关的。因为  $GF(q)$  中的每一个元素都代表了一个密钥对, 所以如果我们的密钥是 64 位, 那么  $q$  应当是大于  $2^{64}$  的最小素数。假设  $s$  是  $GF(q)$  中的一个本元, 那么  $GF(q)$  中的每一个非零元素都可以用  $s$  的方幂表示。 $G$  可以被设置成如下形式:

$$G = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ s^1 & s^2 & s^3 & \cdots & s^N \\ (s^1)^2 & (s^2)^2 & (s^3)^2 & \cdots & (s^N)^2 \\ \vdots & \vdots & \vdots & & \vdots \\ (s^1)^\lambda & (s^2)^\lambda & (s^3)^\lambda & \cdots & (s^N)^\lambda \end{bmatrix}$$

收稿日期:2007-07-11;修回日期:2007-09-28。

作者简介:张学锋(1967-),男,河北邢台人,硕士,主要研究方向:数据库安全、网络安全; 姜皇普(1982-),男,河北沧州人,硕士研究生,主要研究方向:无线网络安全; 王永栓(1982-),男,河北沧州人,硕士研究生,主要研究方向:PKI。

因为  $G$  是一个范德蒙德矩阵, 所以  $s^1, \dots, s^N$  是线性无关的。实际上, 矩阵  $G$  可以由  $GF(q)$  的本元  $s$  来生成。这样, 当安装服务器分配  $G$  的第  $k$  列到节点  $i$  时, 只需要分配  $s$  的  $k$  次方到节点  $i$  就可以了, 需要时由  $i$  节点生成  $G$  的第  $k$  列。

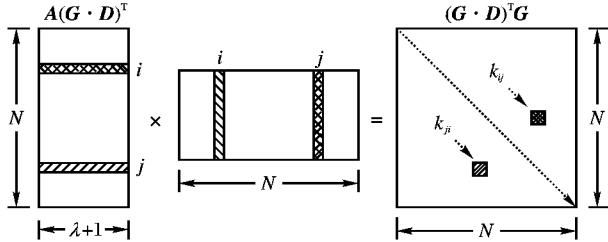


图 1 矩阵

可以利用节点获得的矩阵  $D$  的列数(或者是矩阵  $A$  的行数)来表示的节点 ID。例如获得  $D$  的第  $k$  列的节点 ID 为  $k$ 。

### 1.2 Blom 密钥预配置方案

安装服务器产生  $G, D, A$  矩阵。对于每一个传感器节点, 安装服务器在矩阵  $A$  中选择一个空闲行  $R$ , 在矩阵  $G$  中选择与  $R$  对应的列  $C$ , 然后安装服务器将  $\{ID, R, C\}$  部署到传感器点。当节点  $i$  和节点  $j$  之间进行密钥发现时, 首先交换矩阵  $G$  的份额, 然后它们可以利用自己存储的  $A$  的份额独立的计算  $K_{ij}$ (或  $K_{ji}$ )了, 其中  $G$  的份额可以以明文方式传送, 因为  $G$  是公开的。现在就可以利用  $K_{ij}$ (或  $K_{ji}$ )作为节点  $i$  和  $j$  之间的密钥了。

Blom 的密钥预配置方案在许多方面还存在限制。这个方案是  $t$  安全的, 它最多可以容忍网络中有  $t$  个节点被俘的情况, 这时每个节点的存储量为  $2(t+1) \text{ lb } q$ 。当网络的规模很大时, 需要增大  $t$  的值来保证网络的安全性, 此时节点所需的存储量会急剧增加。Blom 的预配置方案中, 当矩阵  $G, D, A$  确定后, 网络的规模就确定了, 网络中所能容纳的节点数目是固定的。这种规模确定的网络无法实现网络的扩展, 当网络中的节点数目达到饱和时, 就会拒绝任何新节点加入网络。基于矩阵池的方案可以解决以上问题。

## 2 基于矩阵池密钥预配置方案

如图 2 所示, 将矩阵池定义如下: 假设传感器网络中有  $N$  个节点, 则节点集合为  $U = \{user_1, user_2, \dots, user_N\}$ 。安装服务器生成  $G$  矩阵的集合  $S_G = \{G_1, G_2, \dots, G_W\}$  和  $S_D = \{D_1, D_2, \dots, D_W\}$  ( $W$  值将在以后的研究中进行讨论), 从而生成  $A$  矩阵集合  $S_A = \{A_1, A_2, \dots, A_W\}$ 。

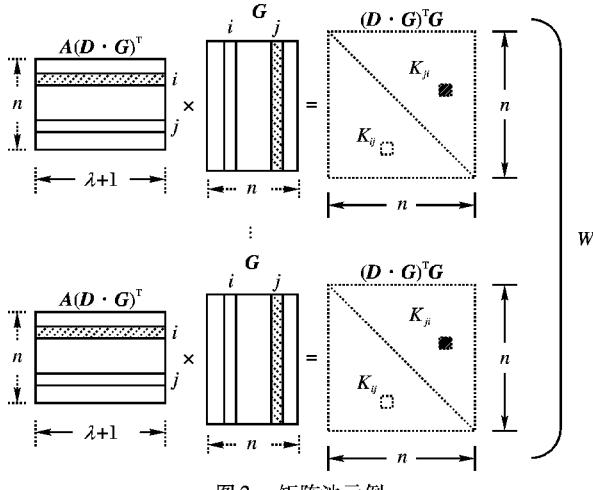


图 2 矩阵池示例

对于节点  $i (i \in U)$ , 安装服务器随机地从  $W$  个  $A$  矩阵中选择  $M (M < W)$  个矩阵  $S'_A = \{A'_1, A'_2, \dots, A'_M\}$ , 从每个选

出的  $A$  矩阵中随机选择一未被分配的行, 构成  $S_R = \{R_1, R_2, \dots, R_M\}$ 。并且选出与  $S_A$  相对应的  $M$  个  $G$  矩阵, 从中选出与  $S_R$  对应的列集合  $S_C = \{C_1, C_2, \dots, C_M\}$ 。此时节点  $i$  的 ID 可以表示为  $ID = \{(p_1, q_1), (p_2, q_2), \dots, (p_M, q_M)\}$ , 其中  $p_i$  表示  $S_A$  中的某个矩阵,  $q_i$  表示的某一列。这样每一个节点都可以用它的 ID 来唯一标识。

基于矩阵池的方案的共享密钥发现和会话密钥发现过程与基于矩阵格方案是基本相同的(请参考 3.3 节和 3.4 节)。但是基于矩阵池的方案中, 实际的矩阵份额分配并不能保证每个矩阵被等机会分配, 这样网络就有可能是非连通的。为了解决以上问题, 本文提出了一种基于矩阵格的密钥预配置方案。

## 3 基于矩阵格的预配置方案

### 3.1 矩阵格的概念

矩阵线: 一组矩阵  $G, D, A$ 。

矩阵线份额: 矩阵  $A$  的第  $i$  行和矩阵  $G$  的第  $i$  列。

矩阵格: 如图 3 所示, 由矩阵线构成的二维网格。假设一传感器网络有  $N$  个节点, 基于格的密钥预配置方案如下: 利用  $2m$  个矩阵线构造一个  $m \times m$  的二维格  $F = \{f_i^r, f_i^c\}_{i=0, \dots, m-1}$ , 其中  $m > \lceil \sqrt{N} \rceil$ 。如图 4 所示: 格中的每一行都与一个矩阵线  $f_i^r$  相关联, 每一列都与一个矩阵线  $f_i^c$  相关联。安装服务器给网络中的每一个节点分配格中的一个交叉点。在坐标  $(i, j)$ , 安装服务器给相应传感器分配矩阵组  $f_i^r$  和  $f_i^c$  的份额。最终, 传感器节点可以在此基础上进行多项式份额发现和密钥传输路径发现。

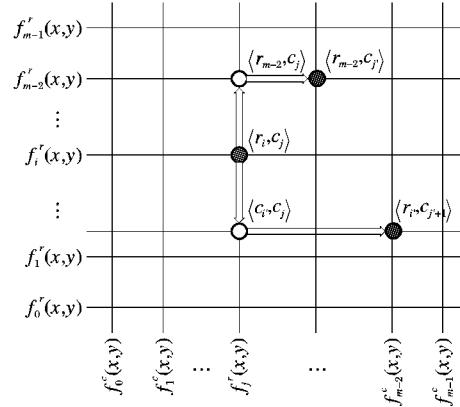


图 3 矩阵格

为方便起见, 利用节点坐标表示节点的 ID。令  $l = \lceil \text{lb } m \rceil$ , 这样任何横坐标、纵坐标都可以用  $l$  位的二进制位串表示。然后我们就可以用表示节点横、纵坐标的  $2l$  位二进制位串来表示节点的 ID 了。例如, 我们可以把利用坐标  $(i, j)$  得到的节点 ID =  $\langle i, j \rangle$ 。有时为了方便表示, 我们用  $\langle c_i, r_j \rangle$  表示传感器节点的 ID, 其中  $c_i, r_j$  分别是节点 ID 的前  $l$  位和后  $l$  位。

### 3.2 多项式子集分配

节点被部署之前, 在一个有限域  $F_q$  上, 安装服务器随机地生成由  $2m$  矩阵线组成的矩阵格  $F = \{f_i^r, f_i^c\}_{i=0, \dots, m-1}$ 。对于每一个传感器节点, 安装服务器选择一个空闲的交叉点  $(i, j)$  并将它分配给此节点。这样, 此传感器节点的 ID 可表示为  $ID = \langle i, j \rangle$ 。然后, 安装服务器将  $\{ID, f_i^r, f_i^c\}$  部署到传感器节点上。为便于将来的路径发现, 我们要求交叉点的分配在格的有限区域内尽量集中, 如图 4 所示, 交叉点的分配遵循一定的规则。很容易看出, 如果点  $\langle i, j \rangle$  和点  $\langle i', j' \rangle$  已经被分配,

则点 $\langle i, j \rangle$ 和点 $\langle i', j \rangle$ 也必须已经被分配。

### 3.3 共享密钥发现

为了与节点 $j$ 建立一个密钥对,节点 $i$ 首先检验是否存在 $c_i = c_j$ 或者 $r_i = r_j$ 。如果 $c_i = c_j$ ,两节点 $i, j$ 都拥有多项式份额 $f_{c_i}^e$ ,它们就可以利用基于多项式的密钥预配置方案直接建立密钥对。同样,如果 $r_i = r_j$ ,它们都拥有多项式份额 $f_{r_i}^e$ ,并建立相应的密钥对。如果以上两个条件都不成立,节点 $i, j$ 只能通过路径发现去建立密钥对了。

### 3.4 路径发现

如果条件 $c_i \neq c_j$ 和 $r_i \neq r_j$ 同时成立,节点 $i, j$ 就必须通过路径发现去建立密钥对。我们发现中间节点 $\langle c_i, r_j \rangle$ 和 $\langle c_j, r_i \rangle$ 都可以同时与节点 $i, j$ 通过共享密钥发现建立密钥对。如果没有被俘节点,根据节点的密钥预分配算法,我们可以保证任意两节点之间至少存在两个节点可以用作中间节点,并且利用中间节点我们可以建立 $i$ 和 $j$ 之间的密钥对。例如:假设 $i$ 节点是 $h$ 节点和 $j$ 节点的中间节点,节点 $\langle i, j \rangle$ 和 $\langle i', j' \rangle$ 可以帮助 $\langle i, j \rangle$ 和 $\langle i', j' \rangle$ 建立一个密钥对。同时可以注意到,节点 $i, j$ 可以在进行交互之前确定可能的中间节点。

## 4 性能分析

每个节点有两个矩阵份额,每个矩阵都被 $m$ 个不同的节点共享,因此每个节点能够与 $2(m-1)$ 个其他节点建立共享密钥。最终,一个节点能够与某一个节点建立共享密钥的概率 $p$ 为:

$$\frac{2(m-1)}{N-1} \approx \frac{2(m-1)}{m^2-1} = \frac{2}{m+1}$$

根据前面的路径发现方法,如果不存在被俘节点,可以保证每两个节点都可以建立一个密钥对。

在存储量方面,本方案中每个节点需要存储2个矩阵线的份额,其存储量为 $4(\lambda+1) \text{ lb } q$ 。在Blom的方案中,节点所需的储量为 $2(\lambda'+1) \text{ lb } q$ 。其中 $\lambda'$ 远大于 $\lambda$ 。如果Blom方案中的 $\lambda'$ 与本方中的 $\lambda$ 取值相同,则Blom网络的安全性能是相当低的。图4假设网络节点数目是20 000,横坐标表示被俘节点的数目,纵坐标表示在一定数目节点被俘的情况下,节点之间存在的不安全链路在总链路中所占的比例。图4(a)是Blom方案在 $\lambda' = 2000$ 的情况下,存储量为 $4002 \times \text{lb } q$ ,当被俘节点数目超过2 000时,网络中的所有链路都被俘获。图4(b)是Blom方案在 $\lambda' = 6000$ 的情况下,存储量为 $12002 \times \text{lb } q$ ,当被俘节点数目超过6 000时,网络中的所有链路都被俘获。图4(c)是Blom方案在 $\lambda' = 16000$ 的情况下,存储量为 $32002 \times \text{lb } q$ ,当被俘节点数目超过16 000时,网络中的所有链路都被俘获。图4(a)、(b)的情况下节点的存储量已经很大,但是网络的安全性能依然很差。图4(c)虽然安全性能相对于图4(a)、(b)有很大的提高,但是节点的存储量已经达到了 $32002 \times \text{lb } q$ ,超出了节点的承受能力。图4(d)是当 $\lambda$ 等于150时本方案的安全性能。图4(d)中节点的存储量为 $604 \times \text{lb } q$ ,远小于Blom方案,但是安全性能却远远高于Blom方案。

基于矩阵池的预配置方案在密钥的预分配环节上是不同的,但是在共享密钥的发现和路径发现环节上采用相同的方法。因此理论上基于密钥池的方案在节点存储量、通信量、网络的安全性和可扩展性方面与基于矩阵格的方案是相同的。但是这种随机方案并不能保证每次网络进行密钥预分配时,每个密钥矩阵都能以绝对相等的概率被使用到,所以整个网络的连通性是不能保证的,进而会影响网络的其他性能。最

终基于矩阵格的方案解决了这些不足。

根据Blom方案,基于矩阵格的方案中,每个节点的储量为 $4(\lambda+1) \text{ lb } q$ (其中 $\lambda$ 为矩阵线的门限值),所以本方法的空间复杂度为线形对数阶 $O(N \lg N^{\frac{1}{2}})$ 。我们主要用算法时间复杂度的数量级(即算法的渐近时间复杂度)评价一个算法的时间性能。每进行一次密钥计算,需要进行 $N(\lambda+1)^2 \text{ lb } q$ 次乘法运算,所以方法的时间复杂度为 $O(N^2 \lg N^{\frac{1}{2}})$ 。

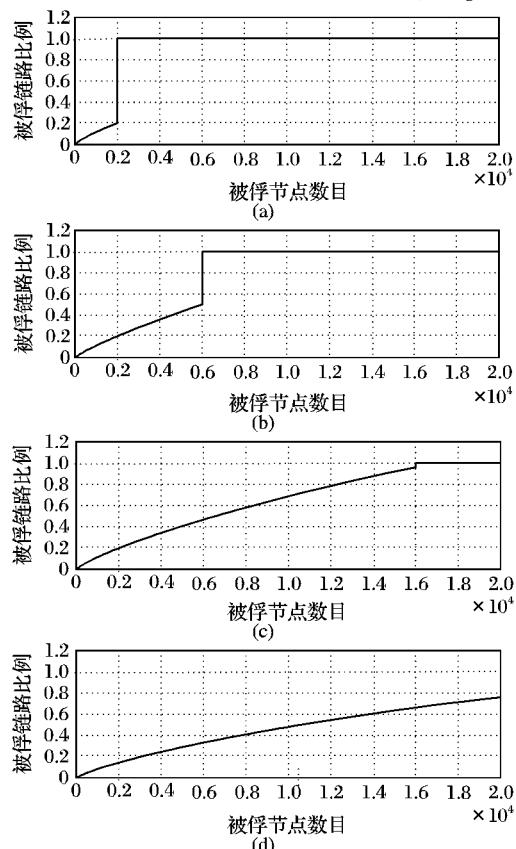


图4 被俘节点数目于被俘链路比例关系

## 5 结语

本文提出了一种基于矩阵格的应用于传感器网络的密钥预配置方案。该方案采用矩阵格的方式,提高了网络的可扩展性,减少了节点在预配置时的信息存储量。并且在密钥的传送过程中采用了加密传输机制,提高了密钥传输地安全性。相对于Blom方案,该方案可以减少网络安全性能对网络资源的依赖性。同时,其安全性能相对以前的方案又有很大提高。

### 参考文献:

- [1] LIU DONG-GANG, NING PENG. Establishing pair wise keys in distributed sensor networks [C]// Proceedings of the 10th ACM Conference on Computer and Communications Security. New York: ACM Press, 2003: 52–61.
- [2] BLOM R. An optimal class of symmetric key generation systems [C]// Lecture Notes in Computer Science 209. Germany: ACM Press, 1985: 335–338.
- [3] DU W, DENG J, HAN Y S, et al. A pair-wise key pre-distribution scheme for wireless sensor networks [C]// Proceedings of the 10th ACM Conference on Computer and Communications Security. New York: ACM Press, 2003: 42–51.
- [4] LIU DONG-GANG, NING PENG. Location-based pairwise key establishments for static sensor networks [C]// Proceedings of ACM Workshop on Security in Ad Hoc and Sensor Networks. New York: ACM Press, 2003: 72–82.