A Hexagon-Based Key Distribution Scheme for Wireless Sensor Networks

YAO Xuan-xia[1], ZHENG Xue-feng[1*], WU Tao[2]

(1. School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China;
2. Department of Computer Science, China Women's University, Beijing 100101, China)

Abstract: In order to improve the secure connectivity & expansibility and decrease memory costs, an efficient hexagon-based grouping key pre-distribution scheme is put forward by using secret binding. In this scheme, the polynomial-based key pre-distribution scheme is used to generate pair-wise keys for the neighboring nodes in one group, and the binding secret generated by a HMAC is employed to establish the common key for the neighboring nodes in different groups. Furthermore, the process of establishing pair-wise key is limited in the beginning of the network deployment, and the pair-wise key establishment in the process of the network updating needs to be verified by the base-station. In addition, by analyzing the relations among the radius of the cell, secure connectivity, memory costs and other parameters, the most appropriate value of the cell's radius is found, which can optimize the hexagon-based key pre-distribution scheme.

Key words: wireless sensor networks; key distribution; hexagon-based model; HMAC; secret binding
EEACC: 6150P; 6210C

一种基于蜂窝模型的无线传感器网络密钥分配方案

姚宣霞[1], 郑雪峰[1*], 武 涛[2]

(1. 北京科技大学信息工程学院, 北京 100083;
2. 中华女子学院计算机系, 北京 100101)

摘 要: 为了提高网络的安全连通性、可扩展性和降低存储开销, 本文基于蜂窝模型, 采用秘密绑定的思想, 提出了一种有效的分组密钥分配方案。在该方案中, 同一组的节点利用基于多项式的密钥预分配方法建立共享密钥, 组间相邻节点借助HMAC函数绑定的秘密建立共享密钥。并将共享密钥的建立限制在网络部署之初, 网络更新中共享密钥的建立则需要经过基站的确认。此外, 通过分析子区域半径与各个参数的关系, 找出了其最佳取值, 实现了对蜂窝模型密钥管理方案的优化。

关键词: 无线传感器网络; 密钥分配; 蜂窝模型; HMAC; 秘密绑定
中图分类号: TP393.17 **文献标识码**: A **文章编号**: 1004-1699(2008)11-1923-06

随着无线传感器网络(WSN, Wireless Sensor Networks)的发展和应用, 其安全问题得到了广泛地关注, 有效的密钥管理方案是解决其安全问题的关键。而WSN由于节点资源(如存储能力、处理能力和能量等)的局限性, 一般采用密钥预分配方法进行密钥的分配和管理[11]。目前, 关于WSN密钥预分配方法的研究很多, 大体可以分为四类, 即随机密钥预分配方法[1-2]、确定性密钥预分配方法[3]、混合方法[4]和基于组(或位置)[5-10]的密钥预分配方法。其中, 随机密钥预分配方法具有较好的可扩展性, 适用于大规模的无线传感器网络, 但安全连通性较差。确定性密钥预分配方法可以实现很好的安全连通性, 但存储开销较大, 可扩展性较差, 只适用于小规模的无线传感器网络。混合方法试图对随机密钥预分配方法和确定性密钥预分配方法进行折中, 不过仍然不能解决两者固有的问题。基于组的密钥预分配方法利用部署知识对网络中的节点进行分组管理, 具有较好的可扩展性, 适用于大规模无线传感器

收稿日期: 2008-06-19 **修改日期**: 2008-08-28

网络，而且安全连通性也比较好，但现有基于组的密钥预分配方案的存储开销一般都比较大。

本文从提高网络的安全连通性、可扩展性和降低存储开销等角度出发，在吸收现有密钥预分配方法优点的基础上，提出了一种适用于静态无线传感器网络的分组密钥管理方案。

1 相关工作

1.1 密钥管理的目的

在无线传感器网络中，由于节点资源的局限性，远程对等节点之间几乎不进行直接通信，网络中的通信主要是节点与基站之间的通信。一般情况下，节点充当中继作用，只与其邻居节点通信，因此，密钥分配方案只要能为相邻节点建立起共享密钥即可。本方案的目的就是为相邻节点建立共享密钥。

1.2 密钥攻击模型

针对不同的密钥管理方案，有不同的攻击方法，但一般都需要俘获一定数量的传感器节点，通过分析被俘节点中的密钥资料和秘密信息，并推导出节点之间建立共享密钥所需要的秘密资料，从而获得任意两个节点之间的共享密钥。

事实上，在网络刚刚部署的一段时间内，攻击者往往来不及发起攻击，即使他们能够从物理上获取节点，对节点中的信息进行分析也需要花费一定的时间，因此，从安全的角度考虑，可以将节点之间建立共享密钥的时间限制在网络部署之初的这段时间内，并在密钥建立完成后删除相关的密钥资料[12]。

1.3 基于组的密钥预分配方法

基于组的密钥预分配方法[5-10]的理论依据是：在无线传感器网络中，节点的能量非常有限，通信覆盖范围较小，通常只与邻居节点直接通信，因此，可以把大的网络覆盖范围划分为较小的子区域，相应地，把传感器节点也划分成组，将同一组的节点部署在同一子区域中，密钥资料也以组为单位进行分配，这样，同一组节点相邻的可能性就很大，相邻节点建立共享密钥的可能性也很大。可以在提高网络安全连通性的同时，增强网络的可扩展性和节点的抗俘获能力[8]。目前，对基于组的密钥预分配方案的研究主要集中在如何对目标区域进行划分和如何为不同组的相邻节点建立共享密钥。其中，对目标区域的划分主要集中在网格模型[7]和蜂窝模型[9]；组间相邻节点共享密钥的建立以及组内密钥资料的分配[8-9]一般采用基于多项式的密钥预分配方案。

蜂窝模型可以较好地反映无线信号的广播特性，各个子区域之间的关系具有对称性且呈层次状分布，可以用一个子区域在另一个子区域外的第 n 层来表示。例如，在如图 1 中，对 C_3 来说，C_0、C_5、C_{18} 分别在其外第 1 层、第 2 层和第 3 层，反过来，C_3 分别位于 C_0、C_5、C_{18} 外的第 1、2、3 层。因此，本方案使用蜂窝模型对目标区域进行划分。

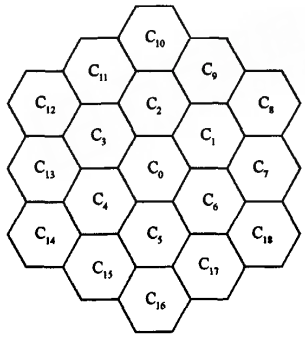

图 1 基于蜂窝模型的分组方法

基于多项式的密钥预分配方案具有很好的安全连通性，适用于小规模的无线传感器网络。因此，在本方案中，组内仍然采用基于多项式的密钥预分配方案。对组间相邻的节点，考虑到存储空间的局限性，借助于 HMAC 函数绑定的秘密为他们建立初始共享密钥。

2 方案描述

2.1 符号说明

在本方案中，假定基站有足够的资源，知道每个组和每个节点的密钥资料。为了便于描述，对一些符号、标记和概念说明如下：

C_i 子区域 i，与组 G_i 相对应。

$<\mathrm{GID}_A, \mathrm{NID}_A>$ 节点 A 的全局标识符，GID_A 是 A 所在组的标识符，NID_A 是节点 A 的组内标识符。

$K_{A,B}$ 节点 A 和 B 的共享密钥。

$E_{Ks}(M)$ 用密钥 Ks 对 M 进行加密。

K_A 节点 A 与基站共享的唯一主密钥，用以保证基站与节点之间通信的安全性。

K_{G_i} G_i 的组密钥，为 G_i 中的节点共享。

K 网络密钥，为网络中所有节点共享。

HMAC(x,y) HMAC 函数，表示以 x 为密钥对 y 进行哈希运算。作用范围是整个网络。

HK_A 节点 A 的隐藏秘密。

$F_i(x,y)$ 组 G_i 的二元 t 次对称多项式。

$KG_{A,i}$ 节点 A 与组 G_i 的绑定秘密。

家乡子区域 节点所在的组对应的子区域。

2.2 初始化

初始化是在部署之前对节点进行的离线操作，由配置服务器完成，包括四项工作。一是根据应用的安全要求、目标区域的大小、节点的通信范围 d_r 和存储容量，确定子区域的半径 R 和秘密绑定的层数 n，将目标区域划分成 x 个半径为 R 的正六边形子区域，将节点分为 x 个组，每个组与一个子区域相对应。二是在有限域 F_q 上为每个组产生一个唯一的二元 t 次对称多项式。三是为节点分配密钥资料。密钥资料包括网络密钥、节点的主密钥、组内多项式的部分值和节点与组间的绑定秘密等。前两者可由配置服务器直接产生。组内多项式的部分值是多项式在节点标识符处取值，例如，对于 G_i 中的节点 A，其组内多项式的部分值为：$F_i(GID_A \oplus NID_A, y)$。绑定秘密需要根据节点的隐藏秘密和待绑定组的组密钥进行计算，A 与组 G_j 的绑定秘密为：$KG_{A,j} = HMAC(KG_j, HK_A)$，其中 $HK_A = HMAC(K_A, K_A)$。假设需要绑定到第 n 层，则对节点家乡子区域外第 1 至 n 层的每个子区域对应的组都要进行秘密绑定，根据蜂窝模型，这样的组共有 $(3n^2+3n)$ 个。由于子区域之间的位置具有对称关系，因此秘密绑定也具有对称性，即如果 G_i 中的节点与 G_j 进行了秘密绑定，那么，G_j 中的节点与 G_i 也有秘密绑定。四是为每个节点设置一个定时器，以将初始密钥的建立过程限制在网络部属之初。

2.3 共享密钥的建立

要为相邻节点建立共享密钥，需要找出每个节点的邻居节点。假定节点间的相邻关系是对称的，即如果 A 为 B 的邻居，则 B 也为 A 的邻居。共享密钥的建立过程就是节点的邻居发现过程。可以分三步进行。

第 1 步，部署完成时，每个节点启动其定时器，广播其邻居发现请求，邻居发现请求包括节点的全局标识符和隐藏秘密的屏蔽值。例如，节点 A 的邻居发现请求为："$GID_A \| NID_A \| (HK_A \oplus K)$"。同时，各节点也接收其相邻节点的邻居发现请求，并利用收到的邻居发现请求建立邻居节点列表。

第 2 步，与邻居列表中的每个节点建立共享密钥。例如，对于 G_i 中的节点 A，假定 B 是其邻居列表中的一个节点。如果 $GID_A = GID_B$，采用基于多项式的密钥预分配方案计算二者的共享密钥，$K_{A,B} = F_i((GID_A \oplus NID_A), (GID_B \oplus NID_B)) = F_i((GID_B \oplus NID_B), (GID_A \oplus NID_A))$。如果 $GID_A \neq GID_B$，假定 B 属于 G_j，有两种情况，一是 G_j 不在 A 的秘密绑定范围内，这时两者都没有与对方所在组的绑定秘密，无法直接建立共享密钥，只要分别从各自的邻居列表中将对方删除即可。二是 G_j 在 A 的秘密绑定范围内，根据初始化阶段的操作可知，A 和 B 中分别存储有 $KG_{A,j}$ 和 $KG_{B,i}$。同时，由于邻居发现请求中包含有邻居隐藏秘密的屏蔽值，因此 A 可计算出 $KG_{B,i} = HMAC(KG_i, (HK_B \oplus K) \oplus K) = HMAC(KG_i, HK_B)$，$B$ 可计算出 $KG_{A,j} = HMAC(KG_j, (HK_A \oplus K) \oplus K) = HMAC(KG_j, HK_A)$，这样可得到他们的初始共享密钥：$K'_{A,B} = KG_{B,i} \oplus KG_{A,j} = KG_{A,j} \oplus KG_{B,i} = K'_{B,A}$。另外，为了防止由于隐藏秘密泄漏造成安全威胁，在组间相邻节点完成初始密钥建立后，应立即协商一个新的共享密钥。一个简单的做法是：由 A 产生一个随机数 r_A 作为二者的共享密钥，并用 $K_{A,B'}$ 将 r_A 加密后发送给 B，B 收到后用 $K_{B,A'}$ 进行解密得到 r_A。

第三步，删除节点中的所有绑定秘密、所有邻居节点的隐藏秘密以及中间密钥资料。

2.4 网络更新

网络更新主要是指网络中出现失效或死亡的节点和向网络中添加新节点。一个节点一旦检测到其某个邻居节点失效或死亡，只需将它从自己邻居节点列表中删除即可。向网络中加入新节点的情况比较复杂，以向 G_i 中增加一个节点 C 为例进行说明。在加入前需要对 C 进行初始化操作，并由基站向其家乡子区域附近的节点发出通知。加入后 C 首先启动其定时器，产生一个随机数 r_C，然后用 r_C 和隐藏秘密 HK_C 进行异或操作构造邻居发现请求"$GID_C \| NID_C \| (r_C \oplus HK_C)$"，对于收到其邻居发现请求的 G_j 中的某个节点 D，如果 D 不是新节点且事先未收到基站的通知，则认为 C 是攻击节点，不予理会，否则需要对该请求处理，有两种情形。

(1) $GID_D = GID_C$，D 根据 C 的标识符和共享多项式的部分值计算出与 C 的共享密钥 $K_{C,D}$，然后将消息"$GID_D \| NID_D \| E_{K_{C,D}}(GID_D \oplus NID_D)$"发送给 C，C 收到后，利用 D 的标识符和共享多项式计算出与 D 的共享密钥 $K_{C,D}$，并对 $E_{K_{C,D}}(GID_D \oplus NID_D)$ 进行解密和验证。

(2) $GID_D \neq GID_C$，D 产生一个随机数 r_D，并将 r_D 和收到的邻居发现请求"$GID_C \| NID_C \| (r_C \oplus HK_C)$"一并用 K_D 进行加密后发送给基站。基站收到后，进行解密，然后根据 K_C 从 $(r_C \oplus HK_C)$ 中恢复出 r_C，计算 $KG_{D,i} = HMAC(KG_i, (r_D \oplus HK_D))$，并将消息"$E_{K_D}(r_C \| KG_{D,i})$"发送给 D。D 收到后进行解密得到 r_C 和 $KG_{D,i}$，用 r_C 与 C 的邻居发现请求消

息中的($r_C \oplus HK_C$)进行异或运算,恢复出 HK_C,计算 $KG_{C,j}=HMAC(KG_j, HK_C)$,得到二者的共享密钥 $K_{C,D}=KG_{D,i}\oplus KG_{C,j}$。然后再向 C 发送消息"($r_D \oplus HK_D$)",C 收到后,可计算出 $KG_{D,i}=HMAC(KG_i,(r_D \oplus HK_D))$,如果 C 与 G_j 进行了秘密绑定,用其绑定秘密 $KG_{C,j}$ 计算 $K_{C,D}=KG_{D,i}\oplus KG_{C,j}$,否则,$C$ 取 $K_{C,D}=KG_{D,i}$,并向 D 发送消息"$E_{K_{C,D}}(r_C+1)$",D 收到后,通过解密对比,也取 $K_{C,D}=KG_{D,i}$。可以看出,新加入的合法节点总能与其邻居节点建立起共享密钥。

3 性能分析

3.1 相邻节点之间建立共享密钥的概率

为计算相邻节点之间建立共享密钥的概率,需要知道一个节点的邻居节点个数和能与之建立共享密钥的邻居节点个数。任意取两个组 G_i 和 G_j 进行考察,设他们的家乡子区域 C_i 和 C_j 中心位置的坐标分别是 (x_i,y_i) 和 (x_j,y_j)。可以计算出 G_i 中的节点与 G_j 中的节点相邻的概率为:

$$p(G_i,G_j)=\begin{cases}0, d\geq(2R+2e+dr)\\ \dfrac{1}{\pi(R+e)^2}\iint\limits_{d_1\leq(R+e+dr)\text{且}d_2\leq(R+e)} f(x,y)\mathrm{d}x\mathrm{d}y, & dr<d<(2R+2e+dr)\end{cases}$$

其中,

$$f(x,y)=\begin{cases}\dfrac{dr^2}{(R+e)^2}, d_1\leq(R+e-dr)\\ 1, d_1\leq(d_r-(R+e))\\ \dfrac{1}{\pi(R+e)^2}\iint\limits_{\substack{\sqrt{(x'-x)^2+(y'-y)^2}\leq dr,\\ \text{且}\sqrt{(x'-x_j)^2+(y'-y_j)^2}\leq(R+e)^2}} \mathrm{d}x'\mathrm{d}y', & |(R+e-dr)|<d1<(R+e+dr)\\ 0, d_1\geq(R+e+dr)\end{cases}$$

$$d=\sqrt{(x_i-x_j)^2+(y_i-y_j)^2},\quad d_1=\sqrt{(x-x_j)^2+(y-y_j)^2},\quad d_2=\sqrt{(x-x_i)^2+(y-y_i)^2}。$$

从 $p(G_i,G_j)$ 的计算公式可以看出,在节点的通信半径 d_r、最大部署误差 e 和子区域半径 R 确定后,两个节点相邻的概率由他们家乡子区域中心之间的距离 d 确定。而根据蜂窝模型,可以方便地用层数 n 和 R 表示出 d,这样,利用高斯积分法就可以求出任两个组中的节点相邻的概率 $p(G_i,G_j)$。

假定每个节点平均有 m 个邻居,那么节点的分布密度为:$w=\dfrac{(m+1)}{\pi\cdot dr^2}$。按照蜂窝模型,每个子区域的面积为$\dfrac{3\sqrt{3}}{2}R^2$,因此,平均情况下每个子区域中节点的个数 N_C 为:$N_C=\dfrac{3\sqrt{3}}{2\cdot\pi\cdot dr^2}\cdot(m+1)\cdot R^2$。这样,对 G_j 中的所有节点,G_i 中的节点 u 能与之直接通信的节点的平均数为:$N_C\cdot p(C_i,C_j)$,网络中能与 u 直接通信的,即 u 的邻居节点的平均数为 n_u,

$$n=N_C\cdot\sum_{\forall j}p(G_i,G_j)。$$

为了计算能与 u 建立共享密钥的邻居节点的个数,将节点的相邻关系分为组内相邻和组间相邻。对于组内相邻的节点,由于共享同一个二元 t 次对称多项式,一定可以建立共享密钥。对于组间相邻的节点,共享密钥的建立依赖于二者是否有与对方所在组的绑定秘密,这由秘密绑定的层数 n 决定。从 $p(G_i,G_j)$ 的计算公式可以看出,当两个节点家乡子区域中心之间的距离 $d\geq(2R+2e+dr)$ 时,他们相邻的概率为 0。也就是说如果两个节点相邻,他们家乡子区域中心之间的距离 d 应满足:$d<(2R+2e+dr)$,而 d 是层数 n 和 R 的函数,因此,可以推出如果一个节点是 u 的邻居节点,那么它的家乡子区域最远在 u 的家乡子区域之外的第 n_m 层,n_m 是 R、e 和 dr 的函数。其中 dr 在传感器节点确定时就确定了,假定 $e=dr$,则 n_m 的取值只与 R 有关。他们之间的关系如图 2 所示。

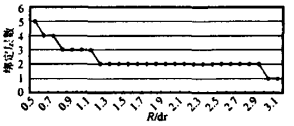

图 2 子区域的半径 R 与最大绑定层数 n_m 的关系

如果用 S_i 表示那些与 G_i 中的节点有秘密绑定的组的集合,根据蜂窝模型,在绑定层数为 n 时,S_i 中应有 $(3n^2+3n)$ 个这样的子区域,那么能与 u 建立共享密钥的节点数为:$n_u'=N_C\cdot\left(\sum\limits_{G_j\in S_i}p(G_i,G_j)+p(G_i,G_i)\right)$,两个相邻节点之间能直接建立共享密钥的概率为:$p=p(u)=\dfrac{n_u'}{n_u}$。显然,$p$ 是绑定层数 n 和子区域半径 R 的函数。他们之间的关系如图 3。

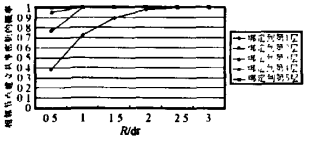

图 3　p 与秘密绑定层数 n 和 R 之间的关系

可以看出，在秘密绑定层数 n 确定的情况下，相邻节点建立共享密钥的概率 p 随 R 的增大逐渐趋向 1。在 R 相同的情况下，p 随着 n 的增加快速增大。当 $n = n_m$ 时，$p = 1$。在实际中，往往需要根据存储空间和 dr 进行综合考虑，找出最佳的 n 和 R，使 p 接近或等于 1。

3.2　存储开销

为了便于分析，将存储开销分为可变存储开销和不变存储开销。其中，可变存储开销随着其它参数（如相邻节点建立共享密钥的概率 p）的变化而变化。在本方案中主要是存储绑定秘密和共享多项式的开销。不变存储开销在方案的安全参数确定后不随其它参数的变化而变化，本方案中主要包括存储网络密钥、主密钥、组密钥等开销。因此，在分析一个方案的存储开销与其他参数的关系时，只需要分析可变存储开销即可，但在对不同方案的存储开销进行对比时，既需要考虑可变开销也需要考虑不变开销中随方案变化的部分。下面首先对本方案中的存储开销与其他参数的关系进行分析，以便于对方案的性能进行优化，然后再与完全基于多项式的密钥预分配方案的存储开销进行对比。

由于组内采用基于多项式的密钥预分配方案，因此每个节点需要存储一个二元对称 t 次多项式的部分值，假设密钥的长度为 128 bit，存储开销为：$mv_1 = (t+1)\mathrm{lb}2^{128} = 128 \cdot (t+1)$。

假设 HMAC 的值也为 128 bit，则存储一个绑定秘密也需要 128 bit。若将秘密绑定到第 n 层，需要存储 $(3n^2+3n)$ 个绑定秘密，所需的存储空间为：$mv_2 = 128 * (3n^2+3n)$。这样，总的可变存储开销为：$mv = (mv_1 + mv_2) = (128 \cdot (3n^2+3n) + 128 \cdot (t+1))$bit。

根据前面的分析可知 n 是 R 的函数，共享多项式的阶 t 由子区域中的节点数决定，为了增强多项式的安全性，要求 $t = 2 \cdot N_C$，这样，可变存储开销 mv 与 R 和平均邻居节点数 m 的关系如图 4 所示。

显然，无论网络的密度多大，当 $R \approx 1.2dr$ 时，可变存储开销都为最小。同时，从图 4 也可以看出，当 $R = 1.2dr$ 时，只需绑定到第 2 层即可使 p 达到 1，因此可以得出，在 $e = dr$ 的情况下，蜂窝模型中子区域的半径 $R \approx 1.2dr$ 是安全连通性和存储开销的最佳点。

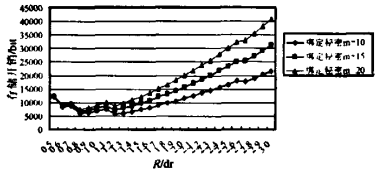

图 4　可变存储开销与 R 和 m 的关系

另外，一般的安全方案都会用到单向哈希函数，本方案使用了一个 HMAC 以根据密钥的不同发挥不同的作用，HMAC 的存储开销与一般的单向哈希函数差别不大，因此，在与其他方案对比时可以不考虑存储 HMAC 的开销。这样，本方案的不变存储开销与完全基于多项式的方案的不变开销就基本相同，他们的差别只在可变开销方面，在节点的平均邻居节点数 m=15 时，两种方案的存储开销如图 5 所示。

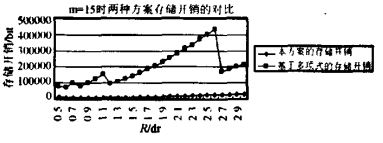

图 5　两种方案存储开销对比

可以看出，本方案的存储开销远远低于完全基于多项式的方案。

3.3　安全性分析

本方案把共享密钥的建立分为初始共享密钥的建立和网络更新时密钥的建立。并将初始共享密钥的建立时间限制在网络刚建立时，在网络更新时采用与基站确认的方法建立享密钥，可以在保障网络可扩展性的同时提高网络的安全性。同时，为了防止推测和伪造，组间绑定秘密以隐藏秘密为参数，在初始共密钥建立完成时立即删除隐藏秘密和绑定秘密等密钥资料，而且对组间相邻节点的初始共享密钥需要立即修改，以增强共享密钥的安全性，减少攻击的可能性。另外，对每组多项式的阶 t 取组中节点平均数的两倍，使得攻击者即使俘获了组内的全部节点也不能恢复出多项式。

总之，在本方案中，一个节点被俘只影响它与邻居节点的通信，不影响其他节点之间的通信，可将攻击限制在节点的通信范围内，安全性较高。

3.4　通信和计算开销

在初始密钥建立阶段需要和邻居节点互换邻居发现请求；组间相邻节点在初始密钥建立完成时需要进行密钥更新和确认；在网络运行过程中，如果有新节点加入，需要和基站进行确认，因此，通信开销较基于多项式的组间密钥建立方案相比要大。但计算开销比较小，主要是一些简单的多项式求值、哈希运算和异或操作。

4 结论

本文利用分组密钥管理技术、秘密绑定的思想和蜂窝模型提出了一种适用于静态无线传感器网络的分组密钥管理方法，该方法具有较好的安全连通性、可扩展性、抗攻击能力和较低的通信开销。通过分析子区域半径与各个参数的关系，找出了最佳 R 值，实现了基于蜂窝模型密钥管理方法的安全最优化。

参考文献：

[1] Eschenauer L and Gligor V D. A Key Management Scheme for Distributed Sensor Networks[C]// Proceedings of 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, ACM Press, November 2002:41-47.

[2] Chan H, Perrig A, and Song D. Random Key Pre-Distribution Schemes for Sensor Networks[C]// Proc. IEEE Symposium on Research in Security and Privacy (SP 2003), 2003:197-213.

[3] Blundo C, De Santis A, Herzberg A, Kutten S, Vaccaro U, and Yung M. Perfectly Secure Key Distribution for Dynamic Conferences[C]// Advances in Cryptology - CRYPTO '92, LNCS 740, 1993:471-486.

[4] Liu D, Ning P. Establishing Pairwise Keys in Distributed Sensor Networks[C]// Proceedings of 10th ACM Conference on Computer and Communications Security (CCS'03), October 2003:52-61.

[5] Chuang Po-Jen, Chao Tun-Hao, Li Bo-Yi. A Scalable Grouping Random Key Pre-distribution Scheme for Large Scale Distributed Sensor Networks[C]// Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05), volume 2, July 2005:535-540.

[6] Liu Donggang, Ning Peng, Du Wenlisng. Group-Based Key Pre-Distribution in Wireless Sensor Networks[C]// Proceedings of the 4th ACM Workshop on Wireless Security. Cologne Germany: ACM Press, 2005, p11-20.

[7] Liu Donggang, Ning Peng. Location-Based Pairwise Key Establishments For Static Sensor Networks[C]// Proc. 2003 ACM Workshop on Security in Ad Hoc and Sensor Networks. 2003,52-61.

[8] Yu Bo, Cao Xiaomei, Han Peng, Mao Dilin, Gao Chuanshan. Flexible Deployment Models For Location-Aware Key Management in Wireless Sensor Networks[C]// APWeb 2006, LNCS 3841,343-354.

[9] Li Guorui, He Jingsha, and Fu Yingfang. Key Pre-Distribution in Sensor Networks[C]// UIC2006, LNCS 4159, 2006, pp 845-853.

[10] Wu S Y and Shieh S P. Adaptive Random Key Distribution Schemes for Wireless Sensor Networks[C]// Proceeding of 2003 Int'l Workshop on Advanced Developments in Software and System Security, Dec. 2003:61-65.

[11] 覃伯平，周贤伟，杨军. 无线传感器网络中密钥管理方案的综合评估[J]. 传感技术学报，2006,19(3):913-916.

[12] 王国军，吕婷婷，过敏意. 无线传感器网络中基于临时初始密钥的密钥管理协议[J]. 传感技术学报，2007,20(7):1581-1586.

姚宣霞(1971-)，女，河南洛阳人，分别于1994 年和 2002 年获得计算机专业学士学位和硕士学位，现任北京科技大学信息工程学院计算机系讲师，同时在职攻读计算机专业博士学位研究生，主要研究方向为网络与信息安全、可信计算、无线传感器网络。目前已在国内外刊物及学术会上发表学术论文多篇。yaoxuanxia@163.com

郑雪峰(1951-)，男，福建福州人，北京科技大学信息工程学院教授、博士生导师，主要研究方向为网络与信息安全，zxfxue@263.net

武 涛(1974-)，女，山西阳泉人，中华女子学院计算机系讲师、博士，主要研究方向为网络与信息安全。

一种基于蜂窝模型的无线传感器网络密钥分配方案

作者： 姚宣霞， 郑雪峰， 武涛， YAO Xuan-xia， ZHENG Xue-feng， WU Tao

作者单位： 姚宣霞,郑雪峰,YAO Xuan-xia,ZHENG Xue-feng(北京科技大学信息工程学院,北京,100083)
， 武涛,WU Tao(中华女子学院计算机系,北京,100101)

刊名： 传感技术学报 ISTIC PKU

英文刊名： CHINESE JOURNAL OF SENSORS AND ACTUATORS

年，卷(期)： 2008，21(11)

引用次数： 0次

参考文献(12条)

1. Eschenauer L. Gligor V D A Key Management Scheme for Distributed Sensor Networks 2002

2. Chan H. Perrig A. Song D Random Key Pre-Distribution Schemes for Sensor Networks 2003

3. Blundo C. De Santis A. Herzberg A. Kutten S, Vaccaro U, Yung M Perfectly Secure Key Distribution for Dynamic Conferences 1993

4. Liu D. Ning P Establishing Pairwise Keys in Distributed Sensor Networks 2003

5. Chuang Po-Jen. Chao Tun-Hao. Li Bo-Yi A Scalable Grouping Random Key Pre-distribution Scheme for Large Scale Distributed Sensor Networks 2005

6. Liu Donggang. Ning Peng. Du Wenlisng Group-Based Key Pre-Distribution in Wireless Sensor Networks 2005

7. Liu Donggang. Ning Peng Location-Based Pairwise Key Establishments For Static Sensor Networks 2003

8. Yu Bo. Cao Xiaomei. Han Peng. Mao Dilin, Gao Chuanshan Flexible Deployment Models For Location-Aware Key Management in Wireless Sensor Networks

9. Li Guorui. He Jingsha. Fu Yingfang Key Pre-Distribution in Sensor Networks 2006

10. Wu S Y. Shieh S P Adaptive Random Key Distribution Schemes for Wireless Sensor Networks 2003

11. 覃伯平. 周贤伟. 杨军 无线传感器网络中密钥管理方案的综合评估[期刊论文]-传感技术学报 2006(3)

12. 王国军. 吕婷婷. 过敏意 无线传感器网络中基于临时初始密钥的密钥管理协议[期刊论文]-传感技术学报 2007(7)

相似文献(10条)

1. 学位论文 李倩 无线传感器网络密钥分配技术研究 2008

无线传感器网络是计算机、通信和传感器三项技术相结合的产物，作为一种新的信息获取和处理技术，目前成为计算机科学领域一个活跃的研究分支。传感器网络由大量的传感器节点组成，这些节点能够协作地实时监测、感知和采集各种环境或监测对象信息，并对其进行处理，传送到用户。基于网络的这些特点，无线传感器网络可以应用于环境、军事、交通、家庭、医疗等各个方面，并且具有广泛的应用前景。 由于传感器节点一般都被布置在恶劣环境、无人区域或者敌方阵营中，加上无线传感器网络本身固有的脆弱性，网络安全引起了人们的极大关注。密钥分配技术是安全管理中重要的方面，能够有效地保证信息在网络中的安全传送，而由于无线传感器网络自身的局限性，传统的适用于有线网络的密钥分配技术在该网络中并不适用，于是新的密钥分配方案成为传感器安全研究的一个重要方面。 本文详细分析现有的无线传感器网络中密钥预分配模型，并对各个模型进行了分类和详细的分析比较，指出了每种方案的优劣及具体使用环境。通过结合随机密钥预分布模型与分簇模型，提出了一种基于分簇的随机密钥预分配模型。本文对新模型的通信过程进行了详细的叙述，并且通过仿真试验验证新模型中节点能量的消耗方面的优势。另外模型在安全性、连通度等方面都比基本模型有很大的提高，更适合应用于大规模的无线传感器网络。

2. 期刊论文 黄海平. 王汝传. 孙力娟. 肖甫. HUANG Hai-ping. WANG Ru-chuan. SUN Li-juan. XIAO Fu 基于逻辑网格的无线传感器网络密钥分配方案 -通信学报2009,30(8)

由于无线传感器网络能源受限、拓扑易变化等特性,需要解决其密钥管理机制涉及到的机密性、完整性、源端认证和无充足空间存储大量密钥信息等问题.针对当前研究工作的一些局限,提出了一种基于逻辑网格的无线传感器网络密钥分配方案,基于层簇式的网络拓扑,描述了系数矩阵求解、密钥设定和具体实现的流程.最后通过与多种现存方法(例如SPIN协议和逻辑密钥树方案)的仿真实验比较,验证了该方案在安全性、存储性和节能性方面的优势.

3. 学位论文 廖兴 无线传感器网络路由协议及密钥分配与管理技术的研究 2008

无线传感器网络无论是在国家安全,还是国民经济诸方面均有着广泛的应用前景。未来,微型、高可靠、多功能、集成化的传感器,微型、大容量的能源,高效、高可靠的网络协议和操作系统,面向应用、低计算量的模式识别和数据融合算法,低功耗、自适应的网络结构,及在现实环境中的各种应用模式,会使传感器网络最终成为现实和数字世界的接口,深入人们生活的各方面,像互联网一样改变人们的生活方式。但在目前的科技水平下,生产低成本、低功耗、体积小的传感器节点,都不可避免的具有能量少(不可更换的电池供电),计算及存储能力有限,仅支持短距离无线通信的特点。如何高效使用能量,最大化网络生存期是传感器网络面临的首要挑战。 目前Multi-Sink无线传感器网络逐渐成为传感器网络领域的研究热点。由于现有的路由协议多

是针对单sink节点的传感器网络提出的,并不适宜于Multi-Sink网络,因此,本文从如何设计高效,高可靠且适宜于Multi-Sink网络的路由协议的问题入手,尝试着设计了一种用于Multi-Sink无线传感器网络的基于标记的路由协议(MS-TBRP)。该协议的核心思想是根据多个sink节点的分布位置,对网络中所有节点按照距离sink节点的跳数进行标记,形成分层的网络拓扑,使用该协议能够为成千上万的传感器节点建立起到sink节点的能量高效的路由。为满足应用的可靠性和多样性需求,针对MS-TBRP协议本文提出了一些有益的改进措施,另外还提出了一种与MS-TBRP搭配使用的能量高效的MAC协议,并利用MS-TBRP的层次划分对无线传感器网络支撑技术作了改进。　　有些应用对于无线传感器网络所采集数据传输的安全有很高的要求,考虑到传感器网络的无线通信环境,缺少基础设施支持,以及节点在能量,计算及存储能力方面有限的特点,本文提出了一种用于分布式无线传感器网络的成对密钥分配与管理方法。它具有能量高效,节省节点存储空间等特点,算法本身也很简单。此外,可以根据需要加入新节点,撤销网络中不安全的节点,或是更新节点的密钥以增强网络的安全性,仿真结果证明了该方法具有很好的可扩展性。　　本文最后对所做的工作进行了总结,并提出了一些需要进一步研究的问题。

4.学位论文 杜薇 无线传感器网络中的密钥分配协议的研究 2009

无线传感器网络WSN（Wireless Sensor Networks）一般是由大量体积小，价格便宜，仅依靠电池供电的具有数据处理、传输以及存储和计算能力的专用传感器节点（Sensor Node）和功能相对强大的基站（Base Station）所组成的网络。传感器节点大多被部署在无人照看地方或者区域，很容易受到监听和物理俘获等攻击，保证无线传感器网络的安全性更是应该首先考虑的问题。由于无线传感器网络所固有的特点，例如受限的计算、通信、存储能力等，使得传统的密钥分配技术很难直接运用于传感器网络中，因此应采用新的适合于无线传感器网络的密钥分配协议，同时也应使其具有容侵的特性。　　本文首先提出的一种新的适用于无线传感器网络的密钥预分配NRKPD协议。NRKPD协议主要将密钥演化的概念运用到密钥预分配协议中。在直接对密钥建立阶段后增加了密钥环演化阶段。这样，每个节点在完成直接对密钥建立后，演化密钥环上的每一个密钥，并删除之前的原始密钥。这样，即便节点被敌手物理俘获时，也能够在很大程度上防止密钥池里的密钥泄露，从而大大降低了由于节点被敌手俘获而对其他安全的网络路径造成的影响。

由于无线传感器网络的不稳定性，如网络延迟等原因，拥有自愈能力的密钥分配协议在无线传感器网络中显得十分重要。本文分析了现有的两种存储量为常数的自愈密钥分配协议：Dutta et al. 协议[38]和Robust. 协议[40]，并给出了对Dutta et al. 协议的两种攻击，并提出了对Dutta et al. 协议[38]的一种修改协MSHKD协议。　　此外本文在MSHKD协议的基础上，给出了一种新的能够抵抗合谋攻击　的自愈密钥分配协议NSKD with RR协议。NSKD with RR协议不仅满足了基本的安全属性，同时也能够有效防止敌手通过俘获一个撤销用户和新用户而获得它们不是合法成员时的群会话密钥。　　接着，本文又给出了一种新的存储量为常数的自愈密钥分配协议CSSKDwith R协议。NCSSKD with R协议满足前向安全、后向安全，同时用户私钥的使用周期不再受到限制。通过对比可以看出本文提出的NCSSKD with R协议更高效和实用。　　最后，利用C++环境，对本文提出的NCSSKD with R协议进行了实验仿真，其运行结果表明了理论的正确性和可行性，明了该协议是一个适用于WSN的高效、可行的自愈密钥分配协议。　关键词：密钥预分配，密钥演化，自愈密钥分配，无线传感器网络

5.期刊论文 李志军.秦志光.王佳昊.LI Zhi-Jun.QIN Zhi-Guang.WANG Jia-Hao 无线传感器网络密钥分配协议研究 -计算机科学2006,33(2)

密钥分配协议对于无线传感器网络的安全起着基础性作用.由于传感器网络大规模、节点资源非常受限、分布式等特点,传统的基于公钥和可信任的密钥分配中心等方式不能实用.本文系统针对传感器网络特点,提出密钥管理协议的需求与性能指标,系统阐述了几种当前比较典型的密钥预分配协议:基于初始信任、随机密钥预分配以及各种改进方案等,分析比较其优缺点,并提出了进一步研究的方向.

6.学位论文 胡松 无线传感器网络安全问题的研究 2009

无线传感器网络是由大量分布在特定区域的无线传感器节点组成的，这些节点具有无线通信、传感、数据处理的能力，并以自组织方式组成无线网络，具有非常广阔的应用前景。在特定的应用领域中，无线传感器网络的安全通信是非常重要的。在无线传感器网络的安全问题研究中，密钥分配策略是目前研究的热点。由于传感器节点自身特点，许多传统的加密算法并不适合传感器网络，研究的热点也主要是密钥的预分配方法。本文分别对传统的ECC加密算法和密钥的预分配方法进行了研究，在此基础上提出了更有效的解决方案。　　本文首先分析和研究了现有的密钥管理方案，其中主要讨论了基于KDC的机制和基于密钥预分发的机制。在基于KDC的机制中，简要的研究了SPINS等方案，在密钥预分发机制中，讨论了经典的Eschenauer-Gligor，q-composite等方案，并进行了仿真，分析了各方案的优点和缺点。在通过对基于位置信息的密钥方案中的最近对密钥方案的分析后，提出了一种基于六边形区域划分模型的节点部署方案和密钥分配策略，并进行了仿真和理论分析。新方案在建立安全通信和节点间建立多跳链接方面都有了一定的改进。在第四章中，本文对传统的公钥算法ECC进行了研究，讨论和分析，并结合具体算法进行了在无线传感器网络中实现，在结合ECC算法的特点的基础上，提出了一种改进的ECC方案。该方案也进行了实现，结合公钥算法自身的特点，对两种方案进行了比较，结果表明改进后的方案在能量和密钥计算时间方面都有了很大的改进。

7.期刊论文 杨庚.王江涛.程宏兵.容淳铭.YANG Geng.WANG Jiang-tao.CHENG Hong-bing.RONG Chun-ming 基于身份加密的无线传感器网络密钥分配方法 -电子学报2007,35(1)

由于无线传感器网络在电源、计算能力和内存容量等方面的局限性,传统的网络密钥分配和管理方法已不适用.本文从基于身份密钥体系出发,提出了一种适用于无线传感器网络的密钥预分配方法.首先简要介绍了身份密钥体系,特别是Boneh-Franklin算法,然后基于身份密钥系统和Diffie-Hellman算法,给出我们的密钥分配方法,并从方法的复杂性、安全性、健壮性和内存需求等方面,与随机算法等进行了分析比较,结果表明我们的算法在这些方面有一定的优势.最后我们讨论了可进一步研究的内容.

8.会议论文 张吉赞 簇状无线传感器网络中基于层次的密钥分配方案 2008

为了解决簇状传感器网络中的密钥分配问题,本文提出了一种新的基于层次的密钥分配方案。在该方案中,基站将成员节点的保密知识下发给相应的簇首,并在簇首的协助下成员节点和邻居节点建立对话密钥.在整个密钥分配过程中,簇成员节点无需保存密钥池。分析比较的结果证明,该方案具有较好的保密性和抗被俘获能力。

9.期刊论文 张建民.刘贤德.徐海峰.ZHANG Jian-min.LIU Xian-de.XU Hai-feng 基于Hash函数的无线传感器网络密钥预分配方案 -计算机应用2007,27(8)

密钥分配是无线传感器网络通信安全的基础.在Echenauer和Gligor的随机密钥预分配方案的基础上,提出了一个基于Hash函数的密钥预分配方案.该方案利用Hash函数来计算出节点中部分的预置密钥,用Hash函数的单向运算特性来增强网络抵抗攻击的能力.分析表明,与现有的密钥预分配方案相比,该方案的计算负载小,安全性能高,更适合于无线传感器网络.

10.学位论文 袁素春 无线传感器网络中密钥管理的研究 2006

无线传感器网络是一种集成了传感器技术、微机电系统技术、无线通信技术和分布式信息处理技术的新兴下一代网络，具有广泛的应用前景和很高的研究价值。　　本文首先对无线传感器网络的体系结构、传感器节点的组成以及无线传感器网络区别于传统网络的特性做了简单的描述。分析了无线传感器网络所面临的安全威胁，给出在这种特定的网络环境下应该考虑的安全目标和信任模型。密钥管理问题是本文重点研究的对象。分别详细介绍了无线传感器网络环境下密钥管理的性能指标，以及几种目前广泛研究的密钥分配机制，包括基于KDC的密钥分配体制、基于公钥密码的分配体制、基于随机概率的密钥预分配体制等。给出了这几种机制下的典型方案，理解各种机制设计的思想，以及它们的性能分析。最后介绍在网络规模极大的情况下，可以采用的群密钥管理方法，它改进了方案可支持的网络规模。接着介绍了一个简单的群密钥管理方案，指出其中的一个安全漏洞，给出一点改进建议。　　结合实习过程中使用的OpenSSLToolkit理解安全套接层SSL协议。描述了协议的握手过程，理解实际应用中是如何实现通信的机密性、认证性和完整性的。给出利用OpenSSLToolkit实现SSL协议的程序设计框架，以及在产品实现过程中遇到的几个问题和解决的方法。