基于分簇的 WSN 多项式随机密钥管理方案

王培东，董修岗

（哈尔滨理工大学 计算机科学与技术学院，黑龙江 哈尔滨 150080）

摘 要：结合多项式的密钥预分配方案和基于分簇管理的随机预分配方案，提出了一种改进的密钥管理方案，并在该方案中添加距离参数来提高无线传感器网络的安全性。对该方案的分析和评估结果表明，该方案提高了无线传感器网络的安全性，并能降低节点的存储空间和计算开销。

关键词：无线传感器网络；分簇管理；二元多项式；距离参数

中图分类号：TP212 **文献标识码**：A **文章编号**：1674-7720(2012)09-0047-03

The WSN polynornial random key management scheme based on cluster

Wang Peidong, Dong Xiugang

(College of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China)

Abstract: An improved key management scheme is proposed by combining the polynomial key pre-distribution scheme and cluster-based random pre-distribution scheme, and adding the distance parameter into the scheme to increase the secunity of WSN. Through assessment and analysis of the scheme, it indicates that the secheme increases the security of WSN and is able to reduce storage space and computational overhead.

Key words: WSN; clustering management; bivariate polynomial; distance parameter

无线传感器网络 WSN(Wireless Sensor Network)通常被部署在野外，尤其是在军事上的应用，节点面临着各种各样的攻击，很容易被俘获，导致其所包含的机密信息可能完全曝露给攻击者。由此可见，WSN 的通信安全问题是一个具有挑战性的课题。

近年来，关于无线传感器网络安全的研究已经取得很大的成果[1]，在密钥管理方面更为突出。例如，随机密钥预分布模型(E-G)[2]、在 E-G 模型基础上的随机密钥对模型[3]以及 Blundo 等人在有限域 $F(q)$ 上提出的基于对称二元多项式随机密钥预分配方案[4]，但都存在一些不足，有待改进。本文在分簇管理密钥和多项式密钥管理研究的基础上，提出了一种新的密钥方案。

1 相关知识

Blundo 等提出的基于对称二元多项式计算的密钥预分配管理方案为网络中的任意两个节点生成密钥对。该方案的基本思想是：首先由基站在有限域 $F(q)$ 生成一个对称二元多项式：

$$f(x,y)=\sum_{i,j=0}^{k}a_{ij}x^iy^j \quad 0\leqslant i,j\leqslant k$$

其中，a_{ij} 在足够大范围内取值，以便满足密钥选取，f 必须满足对称性，即 $f(x,y)=f(y,x)$。把整个无线传感器网络分成若干簇，每个簇由一个簇头和若干普通节点组成，节点通过感知周边环境获得信息并传递给簇头，簇头再把这些数据传递给基站。

2 改进后的密钥分配方案

本文提出的密钥管理方案结合了基于多项式的密钥预分配方案和基于分簇管理的随机预分配方案，在密钥生成过程中采取二元多项式的形式并在二元多项式中添加一个距离参数，生成一种新的有效的密钥管理方案。

在基站生成密钥池前，基站首先向全网发一个洪泛广播，得到全网节点的个数和节点地理位置，基站根据这些地理位置信息把整个通信区域划分成 M 个小区域，每个区域为一簇。每个簇内节点个数分别为 $N_1,N_2\cdots N_M$，每个簇中选取较强的一个节点作为簇头，并假设簇头和基站的距离为 d_n，则二元多项式重新定义为：

$$f(x,y)=\sum_{i,j=0}^{t}a_{ij}x^iy^jd_n \quad 0\leqslant i,j\leqslant t$$

其中，$t=\max\{N_1,N_2\cdots N_M\}$。

2.1 密钥预分配阶段

基站通过一次洪泛广播把整个网络的节点分成 M 个簇，并选举出簇头节点，同时基站产生一个大的密钥池。簇头节点获取密钥的步骤如下：基站向节点随机地从密钥池中取得大量密钥直接放入到节点存储数据的区域，然后每个簇的簇头节点向本区域内的普通节点发出带有到基站距离 d_n 信息的洪泛广播；区域内普通节点接收到本次广播，与存储在自身节点通信数据区域初始密钥环上的二元 t 次多项式相比较；节点把自身二元 t 次多项式中不带有本域内簇头节点距离 d_n 的密钥从初始密钥环上丢掉，然后，把剩余的密钥组成新的密钥环并将其存储于节点密钥存储区域。

2.2 密钥发现阶段

区域内每个节点向本区域内邻居节点发出要求建立通信信道的广播，广播节点自身密钥环上的密钥。邻居节点接收到广播后，比照自身节点上是否有相同的密钥，如果有，则建立通信，该密钥就为初始可信通信信道上的共享密钥；如果密钥环上没有相同的密钥，则转发该信息向自身的邻居节点，邻居节点采取同样的方式查询，直到发现并成功建立可信通信信道；若该信息在本区域内都转发完仍没有解密成功，则舍弃掉该信息，孤立发出此项通信信息的节点，把该节点划分为恶意节点。本区域内节点密钥发现阶段完成，建立可信区域通信网络，簇头节点由于存储的密钥环肯定在基站密钥环上存在，则簇头节点和基站建立可信的通信信道。

2.3 密钥更新阶段

以区域内已经建立通信的 3 个节点 A、B、C 为例。

这 3 个节点均可以采集信息或者转发其他节点采集的信息。若节点 A 采集到或者接收到信息 X，则取信息 X 的前 N 位 X_n 存入节点 A 的密钥存储区域，然后对信息 X 加密发送到节点 B。节点 B 启用自身定时器并解密得到信息 X，同样，取信息 X 的前 N 位即 X_n 存入节点 B 的密钥存储区域，作为标示节点 A 的当前状态。节点 A 继续接收并收集新的信息 Y，节点 A 取上次存储的 X_n 和 Y 加密并发送到节点 B。节点 B 接收到密文后首先检查通信时间是否在规定的时间内，如果不在规定时间内，则抛弃此密文并认为节点 A 已坏，不再接收节点 A 的信息；若通信时间在规定时间内，则节点 B 解密此信息，并取解密后消息的前 N 位与已存入节点 B 的 X_n 对比，若相同，则接收该信息并对该信息做上述循环，否则，舍弃该信息并认为节点 A 为恶意节点，不再接收节点 A 的信息，完成密钥更新。

3 方案分析与评估

本方案在 MATLAB 7.0 上进行仿真验证，规定在 100×100 矩阵里随机布置节点。表 1 给出了相关符号所代表的含义。

表 1 符号约定

符号	含义描述	符号	含义描述
N	WSN 中节点总数	n	划分区域个数
$K_{d,j}$	第 d 个区域第 j 个节点的内存位数	f_d	第 d 个区域
$N_{d,j}$	第 d 个区域内第 j 个节点	K_{ab}	相同区域内节点 a 和 b 之间的密钥

3.1 安全性分析

本文提出的新方案的安全性分析主要是分析其抗捕获的能力，而分析一种对称密钥建立方案的抗捕获性，主要是分析当网络中有部分节点被捕获时，其他非被捕获节点之间链路的安全性是否受到影响。本密钥管理方案每一个特定区域内的形式为：

$$f(x,y)=\sum_{i,j=0}^{t}a_{ij}x^iy^jd_n \quad 0\leqslant i,j\leqslant t$$

其中，d_n 在特定区域内的值是一定的。要求保证每个 a_{ij} 完全不同且对节点都完全保密，每个节点中至少存储一个二元 t 次多项式，保存由本节点计算后的一元 t 次多项式 $f(ID,y)$，通过广播得到邻居节点的 ID'，将由多项式计算获得的 $f(ID,ID')$ 作为两个节点之间通信密钥。由于本方案首先作了分簇管理，簇内每个节点存储的二元 t 次多项式都是不相同的，并且 t 的取值为所有簇中节点个数最多的簇中节点的个数。假设敌方捕获节点时一直捕获的是节点最多簇，只有捕获该簇内所有节点才有可能把该簇内的节点密钥破解，但是也只会影响本簇内的节点，并不会影响其他簇内节点的安全通信；若捕获节点不是节点最多的簇，即使敌方把本簇内所有节点捕获，也不会破解该二元 t 次多项式。

3.2 网络连通性分析

节点如果在相同的区域内能够保留的都是具有一定相同特征的密钥，则这片区域内的网络连通性增强，密钥发现概率提高。本文提出的密钥管理方案在进行密钥的存储时，首先尽可能多地选取密钥，然后在每个簇内对密钥进行筛选，只选择其中具有某一簇内特征的密钥，从而提高了相邻节点发现彼此密钥的概率。

图 1 为 3 种方案在 MATLAB 上的仿真对比图，设计比较参数为：N=1 000，n=10，f_d=3，$N_{d,j}$=4，取距离参数 d_n=4。

3.3 内存需求分析

在密钥分配中本文已经分析到，初次选过密钥以后，根据距离参数的需要，对节点存储在数据区的密钥进行甄别选取，把不符合规定的密钥将从节点中直接删除，通过该方式降低了密钥占用节点的存储空间。

假设邻居节点个数相同的情况下，3 种密钥管理方案占用内存仿真对比图如图 2 所示。设计比较参数为：令 N=1 000，n=10，f_d=3，$N_{d,j}$=4，$K_{d,j}$=32。

《电子技术应用》 www.ChinaAET.com

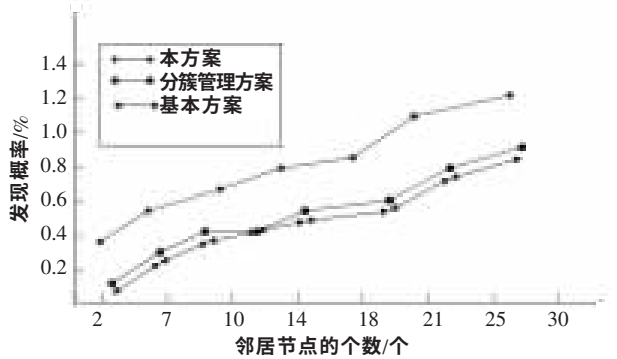

图1 网络连通性对比图

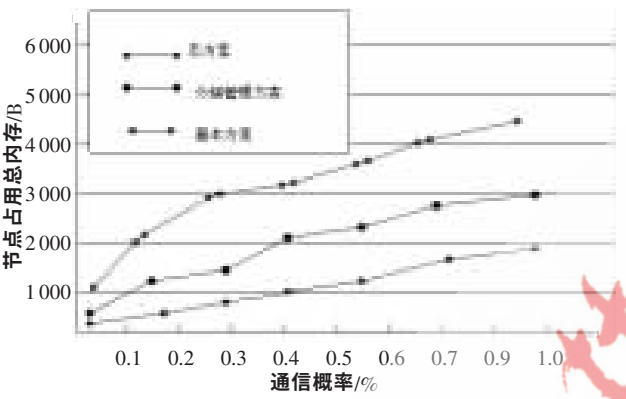

图2 内存占用对比图

3.4 能量消耗分析

在一个无线传感器网络中，数据的发送、接收和融合3部分所消耗的能量占据了节点消耗总能量的90%以上，减少任何一部分的能量消耗对整个网络来说都有很大的改进。在节点进行通信期间，减少通信次数和数据融合次数可以减少能量消耗，因此本方案加入密钥更新机制，在密钥的更新过程中密钥参与运算，通过字符的截取和追加来进行密钥更新，即利用上一次通信的内容作为下一次通信的密钥，不需要进行复杂运算并且减少了数据融合的次数，从而达到了节省节点能量的目的。

本文结合分簇管理密钥方案和多项式密钥管理方案，提出了一种新的安全、高效的无线传感器网络密钥管理方案。与以前方案相比，本方案在节省存储空间和降低能源消耗的同时，提高了网络的连通性和节点发现率。性能分析和仿真结果显示，基于分簇的WSN多项式随机密钥管理方案在满足安全需求的前提下，能为WSN高效地建立节点间密钥对和基站密钥，并在提高了网络通信概率的同时减小了密钥占用内存的问题。

参考文献

[1] CHOI S, SARANGAN V, TROST S. Key management in wireless sensor networks with internetwork sensor roaming [C]. Proceedings of the 33rd IEEE Conference on Local Computer Networks. Montreal, Quebec, Canada: [s. n.], 2008: 328-335.

[2] RIAZ R, ALI A, KIM KH, et al. Secure dynamic key management for sensor networks [C]. Proceedings of the Innovations in Information Technology, Dubai: IEEE Press, 2006.1-5.

[3] 杨顺，李乔良.分层无线传感器网络密钥管理研究[J].微计算机信息，2010，26(10-3)：57-59.

[4] 肖德贵，杨金，罗娟.基于多项式和分组的无线传感器网络密钥管理方案[J].计算机应用研究，2009，26(2)：680-682.

(收稿日期：2012-01-05)

作者简介：

王培东，男，1953年生，教授，主要研究方向：嵌入式应用技术，无线传感器网络。

董修岗，男，1987年生，硕士研究生，主要研究方向：无线传感器网络安全。

《电子技术应用》 www.ChinaAET.com