# 一种新的无线传感器网络密钥预分配方案

蹇 波[1],陈文杰[2],郭永辉[3],罗长远[3]
JIAN Bo[1],CHEN Wen-jie[2],GUO Yong-hui[3],LUO Chang-yuan[3]

1.解放军重庆通信学院,重庆 400035
2.联勤部二十二分部司令部自动化工作站,昆明 650032
3.解放军信息工程大学 电子技术学院,郑州 450004
1.Institute of Signal Communication,Chongqing,PLA,Chongqing 400035,China
2.22nd Subsection of Joint Logistics,Kunming 650032,China
3.Institute of Electronic Technology,PLA Information Engineering University,Zhengzhou 450004,China
E-mail:jiancomnet@126.com

**JIAN Bo,CHEN Wen-jie,GUO Yong-hui,et al.New key pre-distribution scheme for wireless sensor networks.Computer Engineering and Applications,2009,45(30):101-103.**

**Abstract:** Because of the limitation of resources in Wireless Sensor Network(WSN).This paper presents a new key pre-distribution scheme based on plane grid.It not only reduces cost of storage and power,but also ensures that all neighbors' nodes can establish pairwise keys directly.But the safety performance is poor.Then the scheme is extended to tridimensional grid.A novel key pre-distribution is proposed,which is called tridimensional grid key pre-distribution scheme.The results of analysis indicate that the scalability and resilience of the scheme is much better.

**Key words:** Wireless Sensor Network(WSN);key pre-distribution;plane grid;tridimensional grid

**摘 要:**针对无线传感器网络资源有限的特点,给出了一种基于平面格的密钥预分配方案,该方案存储开销与能量消耗较小,能确保所有邻近节点直接建立对偶密钥,但安全性能较差。然后将方案扩展到三维格上,提出了基于三维格的密钥预分配方案,分析结果表明方案具有较好的可扩展性与抵抗攻击的能力。

**关键词:**无线传感器网络;密钥预置;平面格;三维格
**DOI:**10.3778/j.issn.1002-8331.2009.30.030 **文章编号:**1002-8331(2009)30-0101-03 **文献标识码:**A **中图分类号:**TP393

## 1 引言

无线传感器网络是微电子技术、通信技术和计算机技术相结合的产物,具有广阔的应用前景。同时,WSN 面临诸多安全挑战,如窃听、欺骗、注入、重放、拒绝服务(DoS)、HELLO 扩散法、陷阱区等安全威胁[1],提供高效的密钥管理方案对 WSN 的安全具有重要意义。

由于 WSN 受到能量、内存、计算能力和通信带宽等方面的限制,密钥管理面临着诸多困难和挑战。Echenauer 和 Gligor[2]提出了 WSN 随机密钥预分配方案(E-G 方案),其较好处理了存储空间和安全性的关系,但由于采用概率密钥预置模型,存在一定的概率使得网络不连通。Chan[3]等对 E-G 方案进行了扩展,提出了 $q$-composite 随机密钥预分配方案,研究结果表明改变 $q$ 的值可以使网络被破坏的可能性限定在一定范围之内,但当小部分节点妥协时,将会对很大部分的对偶密钥造成影响。Liu[4]等给出了一种基于多项式池的密钥预置模型,并提出两种新的密钥预置算法:随机子集指派和基于超立方体指派密钥预置算法,前者无法保证两节点之间一定存在一条密钥路径,后者虽然能保障密钥路径的建立,但节点之间直接建立对偶密钥的概率低,导致节点在间接密钥建立过程中通信开销过大。

为了有效地提高节点之间直接建立对偶密钥的概率,降低网络的开销,增强网络抗攻击能力,提出了一种基于平面格密钥预分配方案-PGKP(Plane Grid Key Pre-distribution scheme),方案存储开销较小,直接对偶密钥建立概率高,但是安全性较差,在此基础上,将方案扩展到三维格,给出了基于三维格的密钥预分配方案-TGRP(tridimensional grid key pre-distribution scheme),方案具有较强的可扩展性与抵抗攻击的能力,但同时降低了网络直接建立对偶密钥的概率。

在说明方案之间,给出该文所用主要英文符号的含义:

$n$:传感器网络节点数量;

$S$:密钥池;

**基金项目:**国家高技术研究发展计划(863)(the National High-Tech Research and Development Plan of China under Grant No.AA07003004)。

**作者简介:**蹇波(1982-),男,硕士研究生,主要研究方向为无线传感器网络安全;陈文杰(1981-),男,主要研究方向为信息安全评估;郭永辉(1967-),男,博士,副教授,主要研究方向为装备保障与管理、现代仿真理论与应用、自然语言处理与机器学习;罗长远(1973-),男,博士,副教授,主要研究方向为装备工程、无线通信安全。

**收稿日期:**2008-11-17 **修回日期:**2009-03-09

$k$:密钥池中的密钥;

$m$:密钥环大小;

$ID_A$:节点 $A$ 的标识,同时为 $k$ 的标识;

$n'$:平均邻近节点个数;

$K_{AB}$:节点 $A$ 与 $B$ 间的对偶密钥;

∪:两个集合相并;

$\lceil x \rceil$:对数 $x$ 向上取整。

## 2 基于平面格的密钥分配方案

假设 WSN 中每个节点是平面格上的一个点,节点在密钥预置过程中保存两条相互垂直密钥线上的密钥。PGKP 方案主要包括以下两个部分。

### 2.1 平面格密钥池的生成与密钥预置

服务器产生 $n$ 个密钥$\{k_1,k_2,\cdots,k_n\}$,并为所有节点产生唯一标识 $ID_A=(x_i,y_j)$,标识与密钥之间一一对应,则密钥池 $S=\{k_1,k_2,\cdots,k_n\}\cup\{ID_1,ID_2,\cdots,ID_n\}$。任意节点 $A(x_i,y_j)$选取与标识为$(x_i,y_h)$和$(x_h,y_j)$密钥线对应的 $2\lceil\sqrt{n}\rceil-1$ 个密钥(如图 1 所示),其中 $h=1,2,\cdots,\lceil\sqrt{n}\rceil$,将 $2\lceil\sqrt{n}\rceil-1$ 个密钥和对应的节点标识存入节点中。

### 2.2 直接对偶密钥的建立

节点在布置到目标区域后,如果任意节点 $A(x_i,y_j)$需要与节点 $B(x_k,y_g)$之间建立对偶密钥,则节点 $A$ 通过如下方法来得到与节点 $B$ 之间的对偶密钥:

每个节点广播 $ID$,节点 $A$ 在收到节点 $B$ 的标识后,查找出 $C(\min(x_i,x_k),\max(y_j,y_g))$对应的密钥 $k_{C(x_i,y_g)}$(如图 1 中箭头所示),则与 $B$ 的对偶密钥:$K_{AB}=k_{C(x_i,y_g)}$。同理,节点 $B$ 可以找出与 $A$ 的对偶密钥 $K_{BA}$,显然 $K_{AB}=K_{BA}$。

**定理** 1 WSN 中任意节点 $A(x_i,y_j)$与节点 $B(x_k,y_g)$直接建立对偶密钥概率 $P_{AB}=1$。

**证明** 由于节点 $A$、$B$ 为网格中的一个点,$A$、$B$ 均存储了一对相互垂直的密钥线,若 $x_i\neq x_k$、$y_j\neq y_g$,则由平面上两条直线不平行则相交可得,$A$、$B$ 一定存在两个与 $A$、$B$ 互异的交点,那么 $A$、$B$ 中一定存储了两个相同的密钥,故 $A$、$B$ 可以直接建立对偶密钥,若 $x_i\neq x_k$、$y_j=y_g$或者 $x_i=x_k$、$y_j\neq y_g$,则 $A$、$B$ 有相同的密钥线,那么 $A$、$B$ 亦可以直接建立对偶密钥。若 $x_i=x_k$、$y_j=y_g$,则与节点标识唯一性相矛盾,故此情况不存在。因此节点 $A$、$B$ 一定能直接建立对偶密钥。

## 3 基于三维格的密钥预分配协议

为了进一步降低网络的存储开销,提高网络的安全性,将方案扩到了三维格上。TGKP 方案主要包括以下三个部分。

### 3.1 三维格密钥池的生成与密钥预置

服务器产生 $n$ 个密钥$\{k_1,k_2,\cdots,k_n\}$,并为所有节点产生唯一标识 $ID_A=(x_i,y_j,z_k)$,标识与密钥之间一一对应,则密钥池 $S=\{k_1,k_2,\cdots,k_n\}\cup\{ID_1,ID_2,\cdots,ID_n\}$。部署服务器为任意节点 $A(x_i,y_j,z_k)$选取与标识为$(x_i,y_j,z_h)$、$(x_i,y_h,z_k)$和$(x_h,y_j,z_k)$密钥线对应的 $3\lceil\sqrt[3]{n}\rceil-2$ 个密钥(如图 2 所示),其中 $h=1,2,\cdots,\lceil\sqrt[3]{n}\rceil$,将$\lceil\sqrt[3]{n}\rceil-2$ 个密钥和对应的节点标识存入节点中。

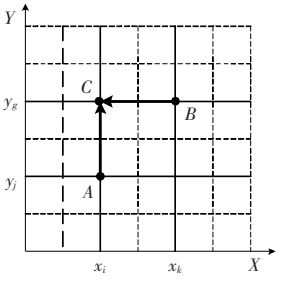

图 1 平面格密钥图

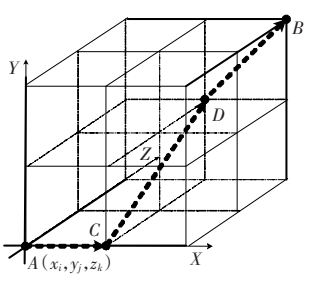

图 2 三维格密钥图

### 3.2 直接对偶密钥的建立

节点在布置到目标区域后,任意节点 $A(x_i,y_j,z_k)$需要与节点 $B(x_g,y_h,z_v)$之间建立对偶密钥,若节点 $A$ 和 $B$ 标识中的 $x$、$y$、$z$ 至少有一个相等,那么 $A$ 和 $B$ 一定处于同一平面或者同一条直线上,因此节点 $A$ 和 $B$ 可以通过 2.2 节方式直接建立对偶密钥。若节点 $A$ 和 $B$ 标识中的 $x$、$y$、$z$ 均不相等,则节点 $A$ 和 $B$ 不能直接建立对偶密钥。

**定理** 2 WSN 中任意节点 $A(x_i,y_j,z_k)$与 $B(x_g,y_h,z_v)$之间直接密钥建立的概率为 $P_{AB}=(3n^{2/3}-3n^{1/3})/(n-1)$。

**证明** 由于节点 $A$、$B$ 为网格中的一个点,若 $A$ 和 $B$ 和能直接建立对偶密钥,那么 $A$ 和 $B$ 标识中的 $x$、$y$、$z$ 至少有一个相等,因此能与 $A$ 直接建立对偶密钥的节点必须在平面 $x=x_i$、$y=y_j$、$z=z_k$ 中,这样的节点共有 $3n^{2/3}-3n^{1/3}$ 个,故任意节点 $B$ 与 $A$ 直接密钥建立的概率:

$$P_{AB}=\frac{C(3n^{2/3}-3n^{1/3},1)}{C(n-1,1)}=\frac{(3n^{2/3}-3n^{1/3})}{(n-1)}$$

### 3.3 密钥路径的发现

节点 $A$ 和 $B$ 标识中的 $x$、$y$、$z$ 均不相等,则节点 $A$ 和 $B$ 之间可以按照如下方法建立间接对偶密钥:

节点 $A$ 找到任意节点 $C$,节点 $A$ 和 $C$ 之间具有直接对偶密钥,节点 $C$ 找到任意节点 $D$,节点 $C$ 和 $D$ 之间具有直接对偶密钥,而节点 $D$ 和 $B$ 之间也具有直接对偶密钥,那么 $A\leftrightarrow C\leftrightarrow D\leftrightarrow B$(如图 2 中虚线所示)为节点 $A$ 和 $B$ 之间的一条密钥径。

## 4 方案的性能分析

本章将通过与 E-G 方案的比较,分析所提出 PGKP 方案与 TGKP 方案的存储开销、能量消耗和安全性。

### 4.1 方案存储开销分析

理想的 WSN 存储开销是节点仅保存其邻近节点通信密钥和节点标识。假设所有密钥长度相等,单个密钥存储开销为 $e_k$,以下对 E-G 方案、PGKP 方案与 TGKP 方案的存储开销进行分析比较。

在 E-G 方案中,网络达到 $c$ 以上的安全连通概率与相邻节点间建立安全链路的概率 $p$ 存在以下关系[2]:

$$p=[\frac{n-1}{n}]\times\frac{\ln n-\ln(-\ln(c))}{n'}$$

当 $n$ 较大时,$(n-1)/n$ 近似为 1,要求网络安全连通概率 $c=0.999\,9$ 时,上式可简化为:

$$p=\frac{\ln n+9.21}{n'}$$

单个节点存储密钥数量 $m$ 与网络规模存在以下关系:

$$m=np=n\times\frac{\ln n+9.21}{n'}$$

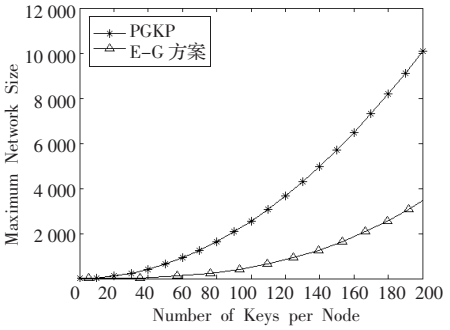


图 3　最大网络规模

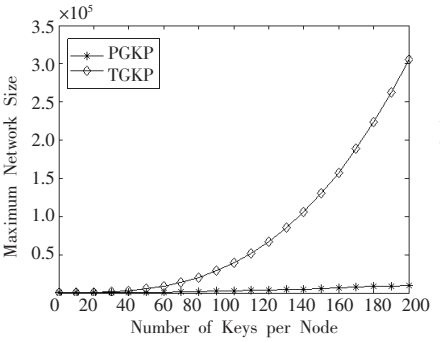


图 4　最大网络规模

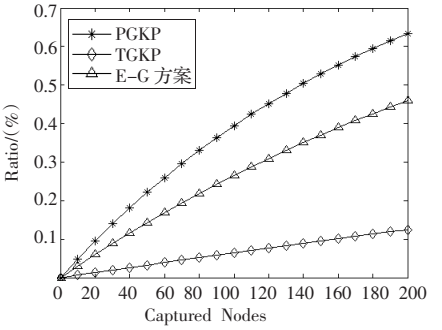


图 5　通信链路被破解与被捕获节点之间关系

因此,E-G 方案单个节点存储开销为 $n\times(\ln n+9.21)e_k/n'$。PGKP 方案中节点保存两条相互垂直的密钥线上共 $2\sqrt{n}-1$ 个密钥和对应的密钥标识,其节点存储开销为 $(2\sqrt{n}-1)e_k$。TGKP 方案中节点保存三条两两相互垂直的密钥线上共 $3n^{1/3}-2$ 个密钥和对应的密钥标识,PGKP 方案节点的存储开销为 $(3n^{1/3}-2)e_k$。

若网络平均邻近节点数量 $n'=\sqrt{n}$,对几种方案网络规模与存储开销关系进行分析对比,结果如图 3、图 4 中所示,从图中可以看出 PGKP 方案好于 E-G 方案支持网络规模,TGKP 方案支持网络规模要明显强于 PGKP 方案和 E-G 方案。

### 4.2　方案能耗分析

传感器节点的电源能量极其有限,要求密钥管理协议的耗能要尽可能少。协议能耗主要包括通信能耗和计算能耗。假设发送和接收一条消息的能耗分别为 $e_S$ 和 $e_R$,节点进行一次密钥查找的计算能耗为 $e_L$,$p$ 为节点间直接建立密钥的概率。表 1 为 E-G 方案、PGKP 方案、TGKP 方案能耗分析。

表 1　节点能耗分析

| | 通信能耗 | 计算能耗 |
|---|---|---|
| E-G 方案 | $e_S+ce_R+(1-p)ce_S$ | $pce_L$ |
| PGKP 方案 | $e_S+ce_R$ | $ce_L$ |
| TGKP 方案 | $e_S+ce_R+(1-p)ce_S$ | $pce_L$ |

从表 1 可以看出,TGKP 方案与 E-G 方案能耗相近,PGKP 方案通信能耗要小于 E-G 方案与 TGKP 方案,而 PGKP 方案计算能耗要大于 E-G 方案与 TGKP 方案。研究表明传感器节点传输信息时要比执行计算时消耗电能更多,传感器将 1 bit 信息传输 100 m 所需要的能量大约相当于执行 3 000 条计算指令消耗的能量[5],因此,TGKP 方案和 E-G 方案能量消耗要大于 PGKP 方案。

### 4.3　方案安全性分析

节点被捕获是无线传感器网络中受到的一种严重安全威胁,攻击者试图通过被捕获的节点获得其他节点的密钥信息。

假设 $K$ 为节点间没有被截获的通信密钥,当某个节点被捕获后,$K$ 没有被捕获的概率[2]是 $1-m/S$,当 $x$ 个节点被捕获时,$K$ 没有被捕获的概率是 $(1-m/S)^x$,因此,密钥被捕获的概率为 $1-(1-m/S)^x$。若 $m$=200,$p$=0.33,不同方案抵抗捕获攻击的能力对比结果如图 5 所示。当被捕获节点数为 100 时,E-G 方案安全链路被破解的概率为 0.25,而 PGKP 方案与 TPKP 方案分别为 0.4、0.06,TPKP 方案的安全性要明显较好,而 PGKP 方案的安全性较差。

## 5　结束语

密钥管理是无线传感器网络安全的热点研究问题。假设每个节点都是平面格上的一个点,提出了 PKGP 方案,分析了其性能。针对 PKGP 方案安全性差的缺点,将其扩展到了三维格上,给出了 TKGP 方案,只需要增加了少量的能耗代价,就可以降低节点的存储开销和提高节点抗攻击能力。

## 参考文献:

[1] Wood A D,Stankovic J A.Denial of service in sensor network[J].IEEE ISNNIP 2005:89-95.

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

[3] Chan H W,Perrig A,Song D.Random key pre-distribution schemes for sensor networks[C]//Proc of the 2003 IEEE Symp on Security and Privacy.Washington:IEEE Computer Society,2003:197-213.

[4] Liu D,Ning P.Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks[C]//Proceedings of the 10th Annual Network and Distributed System Security Symposium.San Diego:ACM Press,2003:263-276.

[5] 李善仓,张克旺.无线传感器网络原理与应用[M].北京:机械工业出版社,2008.

(上接 64 页)

进一步深入,该软件还需要进一步地完善。

## 参考文献:

[1] 陈义群,陈华.基于 MATLAB 的工程物探软件快速开发[J].地球物理学进展,2004(4):802-806.

[2] 周美华,徐静波,王夏琴.基于 MATLAB 的化工课程设计软件开发[J].计算机与应用化学,2001(5):496-498.

[3] 王强,金珩.MATLAB 环境下的数值分析教学软件开发[J].内蒙古民族大学学报,2004(2):176-179.

[4] 飞思科技产品研发中心.MATLAB6.5 辅助神经网络分析与设计[M].北京:电子工业出版社,2003.

[5] 陈杰.MATLAB 宝典[M].北京:电子工业出版社,2007.

[6] Demuth H,Beale M.Neural network toolbox user's guide-neural network toolbox for use with Matlab[Z].The MathWorks,Inc,1992.

[7] Neural Network Toolbox.MathWorks[Z].2000.