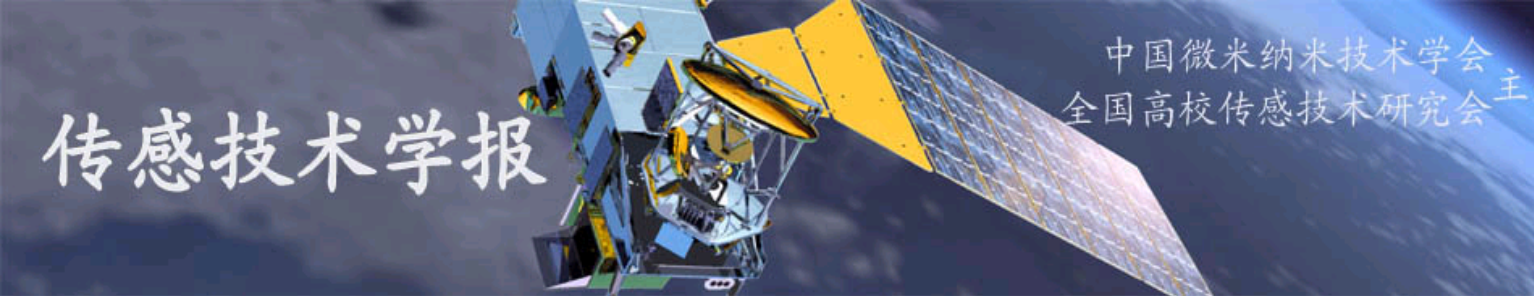

一种新的基于部署知识的WSN密钥分配方案

作　者：袁猷南, 杨明慧, 游林

单　位：浙江省杭州市江干区下沙高教园区杭州电子科技大学通信工程学院通信与信息系统研究所

基金项目：浙江省自然科学基金

摘　要：

在正六边形模型的基础上，利用素域中Blom矩阵和对称多项式的阈值及哈希密钥链的不可逆特性提出了一种新的密钥分配方案。该方案在网络部署之初建立对时，同一区域中节点利用分配的哈希链中的值构造一系列Blom矩阵来建立对密钥并保证相同矩阵的个数不超过各自的阈值，不同区域中相邻节点利用随机分配钥构造出的多项式建立对密钥，从而使得敌方难以破解，增强了抗毁性。仿真结果表明，与Kong和q-composite的方案相比较，本方案能有效提高对密钥的建立率和抗毁性。

关键词：无线传感器网络；随机密钥分配；部署知识；Blom矩阵；多项式；哈希链

A novel scheme of key distribution based on the deployment knowledge of WSN

Author's Name:

Institution:

Abstract:

By using Blom matrices, symmetric polynomial thresholds in prime fields and the irreversibility of hash chains, a novel hexagon-based key distribution scheme for wireless sensor networks is proposed. During the beginning of the node network deployment and pair-wise keys to be established, the distributed hash chain values are used to construct a number below the threshold Blom matrices and so as to generate pair-wise keys among the nodes in the same region. While among the neighboring nodes in different regions, the polynomials constructed by randomly pre-distributed keys are employed to establish pair-wise keys. These designs make the security of the proposed key distribution scheme greatly improved and make enemies harder to break the network. Compared to both Kong' scheme and q-composite's scheme, our simulation results show that the proposed scheme has more efficiently improved the probability of pair-wise key establishment and invulnerability.

Keywords: wireless sensor networks; random key distribution; deployment knowledge; Blom matrix; polynomial; hash chain

投稿时间：**2010-11-07**