计算机工程　2008 34 (5): 153-154,157　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

传感器网络中基于簇的组密钥管理方案

赵治平1，林亚平1,2

(1. 湖南大学计算机与通信学院，长沙 410082；2. 湖南大学软件学院，长沙 410082)

收稿日期　修回日期　网络版发布日期 2008-2-29　接受日期

摘要　针对传感器网络中无长期可信节点的特点，基于传感器网络的簇结构和门限密钥共享机制提出一种新的组密钥管理方案，使得只有组中的合法节点才能存储一个有效的组密钥分量。组密钥更新时，组密钥由节点协同产生并由簇头安全分发。理论分析和仿真实验表明，该方案具有良好的安全性，在组密钥更新时存储开销和通信开销较低。

关键词　传感器网络；簇结构；门限密钥共享机制；组密钥管理

分类号　TP393

DOI:

对应的英文版文章：05-61

通讯作者:

作者个人主页: 赵治平1;林亚平1;2