通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会



王 潮,胡广跃,张焕国.无线传感器网络的轻量级安全体系研究[J].通信学报,2012,(2):30~35

# 无线传感器网络的轻量级安全体系研究

**DOI：**

**中文关键词：**

**英文关键词：**

**基金项目：**

**作者** **单位**

王 潮，胡广跃，张焕国



**中文摘要：**

结合无线传感器网络现有的安全方案存在密钥管理和安全认证效率低等问题的特点，提出了无线传感器网路的轻量级安全体系和安全算法。采用门限秘密共享机制的思想解决了无线传感器网络组网中遭遇恶意节点的问题；采用轻量化ECC算法改造传统ECC算法，优化基于ECC的CPK体制的思想，在无需第三方认证中心CA的参与下，可减少认证过程中的计算开销和通信开销，密钥管理适应无线传感器网络的资源受限和传输能耗相当于计算能耗千倍等特点，安全性依赖于椭圆离散对数的指数级分解计算复杂度；并采用双向认证的方式改造，保证普通节点与簇头节点间的通信安全，抵御中间人攻击。

**英文摘要：**

查看全文 查看/发表评论 下载PDF阅读器

关闭