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

陈燕俐,杨庚.适合于无线传感器网络的混合式组密钥管理方案[J].通信学报,2010,(11):56~64

适合于无线传感器网络的混合式组密钥管理方案

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
陈燕俐	
杨庚	

中文摘要：

针对无线传感器网络中经常出现节点加入或退出网络的情况，提出了一种安全有效的混合式组密钥管理方案。多播报文的加密和节点加入时的组密钥更新，采用了对称加密技术；而系统建立后，组密钥的分发和节点退出后的组密钥更新，采用了基于身份的公钥广播加密方法。方案可抗同谋、具有前向保密性、后向保密性等安全性质。与典型组密钥管理方案相比，方案在适当增加计算开销的情况下，有效降低了节点的存储开销和组密钥更新通信开销。由于节点的存储量、组密钥更新开销独立于群组大小，方案具有较好的扩展性，适合应用于无线传感器网络环境。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭