

黄杰, 黄蓓. 无线传感器网络中一种基于公钥的密钥分配方案[J]. 通信学报, 2011, (10): 52~58

无线传感器网络中一种基于公钥的密钥分配方案

DOI:

中文关键词:

英文关键词:

基金项目:

作者

单位

[黄杰, 黄蓓](#)

摘要点击次数: 358

全文下载次数: 294

中文摘要:

无线传感器网络的大规模使用一直受到安全性的困扰, 其中密钥分配是其关键技术之一, 为此, 产生了大量非常有价值的研究成果, 但这些成果主要集中在对称密钥的研究上, 但无法彻底解决密钥分配的安全问题。为此本文提出了一种基于公钥的密钥预分配方案, 基站利用一系列原始公钥和单向散列函数产生公钥集合, 并为每个节点随机分配公私钥对和保存的密钥集合。利用随机图论的相关原理证明, 该方案与传统的密钥预分配方案相比, 既保证了网络的安全, 又兼顾了网络和节点的资源有限的实际, 在连通性不变的前提下, 其网络安全性和网络的扩展性大幅度提高。

英文摘要:

[查看全文](#) [查看/发表评论](#) [下载PDF阅读器](#)

[关闭](#)

版权所有: 通信学报

地址: 北京东城区广渠门内大街80号通正国际大厦6层602室 电话: 010-67110006-869/878/881 电子邮件: xuebao@ptpress.com.cn

技术支持: 北京勤云科技发展有限公司