电子与信息学报 2010 32 (4): 869-874 ISSN: 1009-5896 CN: 11-4494/TN

论文

一种轻量级的无线传感器网络密钥建立协议

刘 伟, 罗 嵘, 杨华中

清华大学电子工程系 北京 100084

收稿日期 2009-3-19 修回日期 2009-8-13 网络版发布日期 2010-4-7 接受日期

摘要
该文提出了一种适用于无线传感器网络的轻量级密钥建立协议。该协议以预置的瞬时初始密钥为基础，通过优化密钥建立过程中的信息交互，能够获得更好的可扩展性和更低的能量开销。对该协议的完成时间和网络的连通概率的理论分析表明，该协议是可行的。从仿真结果可以看出，该协议在典型的网络规模下可以获得超过97%的连通概率。与同类协议相比，可以在保证足够的连通概率的情况下以更短的时间完成密钥建立。当网络密度为单跳30个节点时，建立时间小于5.2 s。此外，该协议的能量开销只有同类协议的25%，因此更适合应用于资源受限的无线传感器节点。

关键词 无线传感器网络 初始密钥 密钥建立 完全连通概率 协议开销

分类号 TP393

A Lightweight Key Establishment Protocol for Wireless Sensor Networks

Liu Wei, Luo Rong, Yang Hua-zhong

Department of Electronic Engineering, Tsinghua University, Beijing 100084, China

Abstract
In this paper, a lightweight key establishment protocol for wireless sensor networks is proposed. By optimizing information exchanges in the process of key establishment, this temporal initial key based protocol is able to achieve better extensibility and lower energy consumption. Theoretical analysis of finish time and totally connected probability verifies that this protocol is feasible. The simulation results show that, the connected probability is larger than 97% for typical network density. Compared with similar protocols, this protocol needs much less time to finish with enough connected probability. The finish time is less than 5.2s at the network density of 30 nodes per hop. Moreover, energy consumption is only 25% of those of similar protocols, which makes this protocol more suitable for resource constrained sensor nodes.

Key words Wireless sensor network Initial key Key establishment Totally connected probability Protocol overhead

DOI: 10.3724/SP.J.1146.2009.00349

通讯作者 罗嵘 luorong@tsinghua.edu.cn

作者个人主页 刘 伟; 罗 嵘; 杨华中