计算机应用 2007 27 (08): 1904-1906 ISSN: 1001-9081 CN: 51-1307/TP

网络与信息安全

基于Hash函数的无线传感器网络密钥预分配方案

张建民[1];刘贤德[1];徐海峰[1]

华中科技大学 光电子工程系[1]

收稿日期 2007-2-2 修回日期 网络版发布日期 2007-8-27 接受日期

摘要 密钥分配是无线传感器网络通信安全的基础。在Echenauer和Gligor的随机密钥预分配方案的基础上，提出了一个基于Hash函数的密钥预分配方案。该方案利用Hash函数来计算出节点中部分的预置密钥，用Hash函数的单向运算特性来增强网络抵抗攻击的能力。分析表明，与现有的密钥预分配方案相比，该方案的计算负载小，安全性能高，更适合于无线传感器网络。

Abstract Key distribution plays a fundamental role in Wireless Sensor Networks (WSN). A key pre-distributing protocol based on Hash function was proposed, which extended the ideas of the probabilistic key pre-distribution scheme put forward by Echenaue and Gligor. In this scheme, some of the pre-distribution keys in the nodes were computed by Hash function. With the advantage of one way Hash function, this scheme could enhance the ability of network to resist attacks. Compared with other schemes, this one has less computing overhead and higher security performance, which is more suitable for WSN.

关键词 无线传感器网络 密钥分配 Hash 函数

Key words Wireless Sensor Network (WSN);key distribution;Hash function

分类号

DOI:

通讯作者:
张建民 zjm1996@163.com

作者个人主页: 张建民 刘贤德 徐海峰