计算机工程与应用 2009 45 (29): 91-93 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

一种无线传感器网络的组密钥管理方案研究

章志明[1]，邓建刚[3]，彭雅丽[1]，余 敏[2]
1.江西师范大学 软件学院，南昌 330022
2.江西师范大学 计算机信息工程学院，南昌 330022
3.江西师范大学 科技处，南昌 330022

收稿日期 2008-5-29 修回日期 2008-8-19 网络版发布日期 2009-10-10 接受日期

摘要 为了在有限资源的无线传感器网络上能安全进行群组通讯，同时考虑到组密钥管理必须满足前向安全性、后向安全性和完整性的安全需求，使用椭圆曲线密码体制的部分步骤和异或运算提出了一种安全有效的组密钥管理方案。与目前现有的群组密钥相比，方案不仅具有较好的效率，并且更适合于无线传感器网络。

关键词 无线传感器网络 组密钥管理 前向安全性 后向安全性
分类号 TP212

Group key management scheme research of wireless sensor networks

ZHANG Zhi-ming[1]，DENG Jian-gang[3]，PENG Ya-li[1]，YU Min[2]

1.College of Software，Jiangxi Normal University，Nanchang 330022，China
2.College of Computer Information Technology，Jiangxi Normal University，Nanchang 330022，China
3.Science and Technology Research Place，Jiangxi Normal University，Nanchang 330022，China

Abstract
To support secure group communications in resource constrained wireless sensor networks，and consider the security requirement of forward security，backward security and integrality that group key management must meet，a security and efficient group key management scheme which only uses elliptic curve cryptosystems and XOR is proposed.Compared with previous group key mana-
gement schemes for wireless sensor networks，this scheme provides more efficiency and is more suitable for wireless sensor networks.

Key words wireless sensor network group key forward security backward security

DOI: 10.3778/j.issn.1002-8331.2009.29.026

通讯作者 章志明 zzm_9650@163.com