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

关志涛1,徐月1,伍军2.传感器网络中基于三元多项式的密钥管理方案[J].通信学报,2013,(12):71~78

传感器网络中基于三元多项式的密钥管理方案

Ternary polynomial based key managementscheme for wireless sensor network

投稿时间： 2013-07-23

DOI：10.3969/j.issn.1000-436x.2013.12.008

中文关键词：无线传感器网络 密钥管理 分簇 三元多项式 更新认证数

英文关键词:wireless sensor network key management cluster ternary polynomial distance parameter

基金项目:国家自然科学基金资助项目（61001197）；中央高校基金资助项目（JB2012087）

作者	单位
关志涛1，徐月1，伍军2	1. 华北电力大学 控制与计算机工程学院，北京112206；2. 早稻田大学 国际信息通信研究院，日本 东京 169-0051

中文摘要:

提出一种新的密钥管理方案KMTP(key management based on ternary polynomial)。基站为每个节点建立唯一性标识，保证节点合法性；基于三元多项式设计簇内和簇间密钥预分配算法，可以保证秘密多项式的破解门限值分别大于簇内节点和分簇总数，理论上难以破解；通过构造安全连通邻接表，设计簇间多跳路由选择算法，保证通信阶段的安全；引入更新参数和更新认证数，保证密钥更新阶段的安全。仿真表明，相比已有方案，KMTP开销较小，且能够提供更高的安全性。

英文摘要:

A ternary polynomial based key management (KMTP) scheme was proposed, which is effective in cluster based wireless sensor networks. Firstly, the base station will give each node one unique identifier to ensure the validity of the node. Then, algorithm of the inner-cluster and inter-cluster key pre-distribution based on the ternary polynomial of the same order was stated, which can ensure the value of the cracking threshold is bigger than the number of nodes of a cluster and all clusters separately, which means it’s very hard to be cracked even all nodes of a cluster or all clusters are compromised. To assure the communication security, inter-cluster multi-hop routing mechanism was designed based on constructing secure conjunct neighbor table. Finally, the updating parameter and the updating authentication number were introduced in rekeying phase. The analysis shows that the proposed scheme can meet the security requirement of key management, and it also has less computation cost and storage cost than the existing schemes.

查看全文 查看/发表评论 下载PDF阅读器

关闭