计算机科学与探索 2008 2 (2): 113-122 ISSN: 1673-9418 CN: 11-5602/TP

综述·探索

无线传感器网络中的广播认证协议

赵 鑫+, 王晓东, 周兴铭

国防科技大学 计算机学院，长沙 410073

收稿日期 修回日期 网络版发布日期 2008-4-20 接受日期

摘要 在总结广播认证协议理想属性的基础上，对现有基于数字签名技术和对称加密技术的广播认证协议优缺点进行了分析讨论，并指出其对无线传感器网络广播认证协议设计的借鉴价值。将广播认证协议中的参数初始化和密钥更新等与密钥管理相关的问题归结为认证系统的完备性问题，并指出现有技术方案在解决该问题时存在的缺陷。初步探讨了无线传感器网络广播认证协议分级安全功能支持的意义，并给出了相应的方案设计思路。

关键词 无线传感器网络 广播认证 哈希链 哈希树 数字签名 一次性签名

分类号

Broadcast authentication protocols in wireless sensor networks

ZHAO Xin+, WANG Xiaodong, ZHOU Xingming

College of Computer Science， National University of Defense Technology， Changsha 410073，China

Abstract

With the summary about ideal properties of broadcast authentication protocols， the performance of proposed broadcast authentication protocols based on digital signature and symmetric cryptography is analyzed. It highlights some mechanisms in these protocols when designing broadcast authentication protocols in wireless sensor networks. The notion of integrality problems of broadcast authentication protocols， meaning relative key management problems of these protocols such as distribution of bootstrap parameters and update of keys， is presented. Furthermore， it also concludes the limitation of existing methods. It’s considered valuable to support multiple security levels for broadcast authentication protocols in wireless sensor networks. A design of such protocols is also proposed.

Key words wireless sensor networks broadcast authentication hash chain hash tree digital signature one time signature

DOI:

通讯作者 赵 鑫 xinzhao_remerci@nudt.edu.cn