计算机工程与科学 2012, 34(2) 25-30 DOI: ISSN: 1007--130X CN: 43-1258/TP

论文

WSN中一种基于身份的短签名广播认证协议

杨〓露，游〓林，杨明慧

（杭州电子科技大学通信工程学院，浙江 杭州 310018）

摘要：

广播认证是传感器网络中很重要的安全服务，它允许发送者通过安全的方式广播信息给多个节点。无线传感器网络中的μTESLA、M μTESLA等基于消息认证码的广播认证协议存在一些不足，加上最近的研究显示，基于双线性对的加密算法可应用于资源有限的传感器节点。本文介绍一种高效的基于身份的无证书短签名协议，它拥有目前最短的签名长度160bits，计算量相比其他公钥签名低得多，还能提供认证多个基站的广播信息的功能。基于MICA2DOT平台对其通信和计算能量消耗进行分析，以及对该协议的其他性能的分析，得出该协议引入的能量消耗小，满足广播认证的一些重要性质，适合无线传感器网络环境。

关键词： 无线传感器网络 广播认证 身份 短签名 双线性对

An Identity Based Short Signature Broadcast Authentication Protocol in WSNs

YANG Lu，YOU Lin，YANG Ming hui

(School of Communications Engineering,Hangzhou Dianzi University,Hangzhou 310018,China)

Abstract:

Broadcast authentication is a critical security service in sensor networks, since it allows a sender to broadcast messages to multiple nodes in a secure way. In wireless sensor networks, the broadcast authentication schemes based on message authentication code, like μTESLA and M μTESLA, have some disadvantages. Recent research results have shown that bilinear pairing based cryptography is applicable on resource constrained sensor nodes. This paper introduces an efficient identity based certificateless short signature scheme. The size of signature generated by this scheme is approximately 160 bit long, which is the shortest signature so far. And the computation cost is much less than that of other public key signatures. It also provides the feature that it can authenticate the broadcast messages from multi base stations. Based on the MICA2DOT platform, the energy consumptions on communications and computation are analyzed. And the protocol's other performances are also analyzed. The protocol proposed in this paper can effectively reduce resource cost and satisfy some cardinal properties of broadcast authentication, so it adapts the characteristics of wireless sensor networks.

Keywords: wireless sensor network；broadcast authentication；identity；short signature；bilinear pairing

收稿日期 2011-01-22 **修回日期** 2011-04-10 **网络版发布日期** 2012-02-25

DOI:

基金项目:

浙江省自然科学基金资助项目（Y1100818）；浙江省自然科学基金杰青团队项目（R1090138)

通讯作者:

作者简介:

作者Email:

参考文献：

本刊中的类似文章

1. 孟中楼, 王殊1, 王骐1, 赵峰2.K连通的分簇式无线传感器网络拓扑控制算法研究[J]. 计算机工程与科学, 2010,32(2): 11-14
2. 胡富平, 王殊, 刘威, 李安.落信道下认知传感器网络频谱检测方法研究[J]. 计算机工程与科学, 2010,32(3): 7-10
3. 赵鑫，王晓东.无线传感器网络快速广播认证协议研究[J]. 计算机工程与科学, 2010,32(4): 106-109
4. 杨东勇，陈晓倩，顾东袁.一种节能的无线传感器网络路由协议的设计与实现[J]. 计算机工程与科学, 2010,32(4): 110-113
5. 张炼冬,汪秉文.无线传感器网络在粮情测控系统中的应用[J]. 计算机工程与科学, 2010,32(4): 114-118
6. 阳娣兰[1] 谢政[2] 陈挚[2] 肖满生[3] 徐桢[4].无线传感器网络中能耗均衡的覆盖控制算法[J]. 计算机工程与科学, 2008,30(12): 15-18
7. 李敏 殷建平 伍勇安 程杰仁.无线传感器网络密钥管理方案综述[J]. 计算机工程与科学, 2008,30(12): 27-31
8. 张红莉，黄守明.一种基于MA的无线传感器网络IDS模型研究[J]. 计算机工程与科学, 2010,32(5): 18-20
9. 黄海平，王汝传，孙力娟，沙超.应用移动Agent的无线传感器网络能量管理机制[J]. 计算机工程与科学, 2010,32(6): 9-12
10. 杨修兰 蒋泽军 王丽芳.基于LDAP和双因素身份认证的统一认证[J]. 计算机工程与科学, 2008,30(7): 27-29
11. 张丽 赵洋 史丽敏.基于OTP的增强型身份认证系统的研究与设计[J]. 计算机工程与科学, 2008,30(6): 16-17
12. 温俊 蹇强 蒋杰 窦文华.保证覆盖的无线传感器网络梯度部署方法[J]. 计算机工程与科学, 2008,30(6): 86-90
13. 吴迪 胡钢 倪刚 张卓 李威.无线传感器网络多路径簇头链分簇式路由算法[J]. 计算机工程与科学, 2008,30(6): 101-105
14. 伍勇安 殷建平 李敏.无线传感器网络连通忌覆盖问题及其解决方案综述[J]. 计算机工程与科学, 2008,30(11): 155-158
15. 孙勇.NET下使用虚拟Token的安全认证方案[J]. 计算机工程与科学, 2008,30(4): 15-16
