计算机应用 2009, 29(09) 2351-2354 DOI: ISSN: 1001-9081 CN: 51-1307/TP

信息安全

安全有效的无线传感器网络匿名通信方案

章志明[1],邓建刚[2],邹成武[2],余敏[2]

1. 江西师范大学
2.

摘要： 随着无线传感器网络(WSN)的广泛应用，在某些场合不仅需要保证传送信息的安全性，还需要保证节点在传送信息过程中的匿名性和私有性，如何设计出安全有效的无线传感器网络匿名通信协议已成为当前研究的热点。使用双线性函数的双线性对，哈希函数和异或运算提出了一种可验证安全的无线传感器网络匿名通信方案，方案不仅能满足匿名通信的基本要求，而且大大提高系统的计算复杂度和存储复杂度，更适合无线传感器网络。

关键词： 无线传感器网络 匿名通信 节点身份 双线性对 Wireless Sensor Network (WSN) anonymous communication node-ID bilinear pairing

Secure and effective anonymous communication scheme for wireless sensor network

Abstract: With the widespread applications of large scale distributed Wireless Sensor Network (WSN), in some situations, the security of WSN involves not only the security of sending data by sensors, but also the anonymity and privacy during the sending process. How to design a secure efficient anonymous communication scheme for wireless sensor network has become a research hotspot. Using bilinear pairing, hash function and different operation, a scheme of validated secure anonymous communication was proposed. Through the analysis and improvement, this scheme can not only satisfy the basic requirement of anonymous communication, but also improve distinctly the complexity of computation and storage, and it is more suitable for wireless sensor network.

Keywords:

收稿日期 2009-02-03 修回日期 2009-03-20 网络版发布日期 2009-09-01

DOI:

基金项目:

国家级基金

通讯作者: 章志明

作者简介:

作者Email:

参考文献：

本刊中的类似文章

1．王玲玲 张国印 马春光.一种基于双线性对的可验证无证书环签密方案[J]. 计算机应用, 2007,27(9): 2167-2169

2．张学军 王育民 .高效的基于身份的代理盲签名[J]. 计算机应用, 2006,26(11): 2586-2588

3．刘军龙 王彩芬 .基于身份的可截取门限签名方案[J]. 计算机应用, 2006,26(8): 1817-1820

4．王天银 蔡晓秋 张建中 .对一种门限代理签名方案的密码分析及改进[J]. 计算机应用, 2006,26(7): 1631-1633

5．徐丽娟 徐秋亮 郑志华.基于身份的指定验证人的门限代理签名方案[J]. 计算机应用, 2007,27(5): 1058-1061

6．徐吉斌 叶震.一种可公开验证的基于身份的签密方案[J]. 计算机应用, 2007,27(6): 1553-1555

7．王泽成 斯桃枝 李志斌.改进的带签名者意向的结构化多重签名方案[J]. 计算机应用, 2008,28(1): 71-73

8．高伟 李飞 徐邦海.依托BLS签名的基于身份盲签名方案[J]. 计算机应用, 2008,28(11): 2827-2828

9．杜焕强 吴铤 叶春涛.基于身份的代理盲签名[J]. 计算机应用, 2007,27(11): 2715-2717

10．张学军.高效的使用双线性对的自认证公钥签名[J]. 计算机应用, 2009,29(2): 355-356

11．樊玫玫 彭长根.一种基于身份的多方公平交换协议[J]. 计算机应用, 2009,29(2): 367-369

12．彭长艳 张权 唐朝京.基于IBC的TLS握手协议设计与分析[J]. 计算机应用, 2009,29(3): 633-637

13．吴晨煌 陈智雄 王海明 沈毅军.一个无证书代理签名方案的安全性分析及改进[J]. 计算机应用, 2009,29(4): 944-946,

14．樊睿 王彩芬 蓝才会 左为平.新的无证书的代理签名方案[J]. 计算机应用, 2008,28(4): 915-917

15．quietloner.高效的动态安全组播密钥协商方案[J]. 计算机应用, 2008,28(8): 1943-1945

16．张玉磊 王彩芬 张永洁 程文华 韩亚宁.基于双线性对的高效无证书签名方案 [J]. 计算机应用, 2009,29(05): 1330-1333

17．耿永军 张延红 崔国华.基于身份的结构化重签名方案 [J]. 计算机应用, 2009,29(09): 2339-2341

文章评论

反馈人		邮箱地址	
反馈标题		验证码	6920
