传感技术学报
中国微米纳米技术学会
全国高校传感技术研究会 主办

基于Hash函数的RFID安全认证协议的研究

作　者：刘明生, 王艳, 赵新生

单　位：邯郸学院信息工程学院

基金项目：1、河北省自然科学基金；2、邯郸市科学技术研究与发展计划项目

摘　要：

为了改善RFID传感网络中阅读器与标签之间存在的安全隐私问题，通过分析现有安全协议，提出一种新的基于Hash函数的RFID安全认证协议。分析表明，该协议可以有效抵御非法读取、位置跟踪、窃听、伪装哄骗和重放等不安全问题，具有成本低、效率高、安全性高等特点。通过建立协议的理想化模型，利用BAN逻辑形式化分析该协议，在理论上证明其安全性。

关键词：射频识别；安全协议；Hash函数；BAN逻辑

Research on RFID Security Authentication Protocol Based on Hash Function

Author's Name:

Institution:

Abstract:

In order to improve security and privacy between readers and tags in Radio Frequency Identification(RFID)Sensor Networks,an improved RFID security authentication protocol based on hash function is proposed by comparing with several typical current protocols.Analysis shows that this protocol resists spoofing,tracking,eavesdropping impersonation and replay attack and it is low-cost,high-efficiency and good-security.After setting up the idealized protocol model,a process of formal analysis of this protocol is presented and the security is proved theoretically by using the BAN logic.

Keywords: RFID;security protocol;hash funtion;BAN logic

投稿时间：**2011-03-16**

查看pdf文件