信号处理 2012, 28(11) 1595-1601 DOI: ISSN: 1003-0530 CN: 11-2406/TN

应用

物联网移动RFID系统匿名访问控制认证密钥交换协议

朱炜玲, 喻建平

深圳大学ATR国防科技重点实验室

摘要：

针对物联网移动RFID系统标签隐私信息的访问控制以及用户身份隐私保护问题，本文采用身份加密和属性加密相结合的方法，建立了IB-AB-eCK安全模型，设计了基于身份及属性的认证密钥交换协议IB-AB-AKE。基于IB-AB-AKE协议，提出了移动RFID手机与信息服务器之间认证密钥交换协议，实现了在保护移动RFID手机用户身份隐私的同时，根据标签所有者定制的访问控制策略进行标签信息的访问控制认证和会话密钥交换，防止了隐私信息被非法访问。分析表明，IB-AB-AKE协议在IB-AB-eCK模型下是安全的，且在通信次数、通信量及计算量方面具有优势。

关键词： 物联网；射频识别；属性；认证密钥交换；匿名访问控制

An anonymous access control and authenticated key exchange protocol for Mobile RFID systems in the internet of things

ZHU Wei-Ling, YU Jian-Ping

ATR Key Laboratory of National Defense Technology， Shenzhen University

Abstract:

For the access control of a tag’s privacy information and the privacy protection of a user’s identity in Mobile RFID systems in the internet of things, a security model called IB-AB-eCK is introduced, and an identity-based and attribute-based authenticated key exchange (IB-AB-AKE) protocol is proposed in this paper. Based on IB-AB-AKE protocol, an authenticated key exchange scheme is then established between mobile RFID phones and information servers of mobile RFID systems in the internet of things. The scheme not only preserves the identity privacy of the user of mobile RFID phone, but also completes the authentication and agrees upon a session key for the access to the tag’s information according to the owner’s access control policy. The analyses show that IB-AB-AKE protocol is secure in IB-AB-eCK model and it has advantages for communication round, communication traffic and computing complexity.

Keywords: internet of things； radio frequency identification； attribute； authenticated key exchange；anonymous access control

收稿日期 2012-04-22 修回日期 2012-09-11 网络版发布日期 2012-11-25

DOI:

基金项目:

国家自然科学基金(61171072)；深圳市科技计划资助项目(CXB201104210002A)

通讯作者:

作者简介:

作者Email: lynn_zhuwl@hotmail.com

参考文献：

本刊中的类似文章

文章评论

反馈人		邮箱地址	
反馈标题		验证码	9550