Software Engineering and Applications 软件工程与应用, 2022, 11(6), 1339-1343
Published Online December 2022 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2022.116137

Hans汉斯

RFID技术的安全性分析

包红琦，郝　宽，廖祎玮

哈尔滨师范大学计算机科学与信息工程学院，黑龙江 哈尔滨

收稿日期：2022年11月29日；录用日期：2022年12月8日；发布日期：2022年12月28日

摘　要

随着物联网的成熟发展，无线射频识别技术(Radio Frequency Identification, RFID)在物联网相关技术中扮演着至关重要的角色。在万物互联的时代，对RFID技术的应用日益广泛，针对该技术的研究也逐渐受到学者们的广泛关注。然而RFID技术在系统应用的过程中，仍面临了种类繁多的安全隐患，因此，本文对RFID技术面临的安全隐患进行了概述与分析，对未来RFID技术的发展有着重要意义。首先，本文总结了应对RFID技术各类隐患的RFID技术安全方案，主要分为物理安全方案和密码学相关方案。其次，分析了现有结合了密码学相关方案的RFID技术的认证协议。最后，对RFID技术的应用前景与发展趋势进行了总结展望。

关键词

RFID技术，RFID系统安全隐患，安全方案

Security Analysis of RFID Technology

Hongqi Bao, Kuan Hao, Yiwei Liao

College of Computer Science and Information Engineering, Harbin Normal University, Harbin Heilongjiang

Received: Nov. 29th, 2022; accepted: Dec. 8th, 2022; published: Dec. 28th, 2022

Abstract

With the mature development of the Internet of Things, radio frequency identification technology (RFID) plays a vital role in IoT-related technologies. In the era of the Internet of Everything, the application of RFID technology is becoming more and more extensive, and the research on this technology has gradually attracted widespread attention from scholars. However, RFID technology still faces a wide variety of security risks in the process of system application, so this paper summarizes and analyzes the security risks faced by RFID technology, which is of great significance to the future development of RFID technology. First of all, this paper summarizes the RFID technology security solutions to deal with various hidden dangers of RFID technology, which are mainly di-

文章引用: 包红琦, 郝宽, 廖祎玮. RFID 技术的安全性分析[J]. 软件工程与应用, 2022, 11(6): 1339-1343.
DOI: 10.12677/sea.2022.116137

vided into physical security schemes and cryptography-related solutions. Secondly, the existing authentication protocol of RFID technology combined with cryptography-related schemes is analyzed. Finally, the application prospects and development trends of RFID technology are summarized.

Keywords

RFID Technology, RFID System Security Hazards, Security Solutions

1. 引言

随着计算机技术与物联网的成熟发展及广泛应用，射频识别技术逐渐成为业内研究的关注焦点。RFID 技术起源于 20 世纪 40 年代，其理论基础发展于雷达的工作原理。紧接着，于 20 世纪 50 至 70 年代研究学者对 RFID 技术理论基础进行了初步的探索与补充。20 世纪 70 年代至世纪末，RFID 技术步入飞速发展时期，RFID 技术相关产品被大规模地广泛应用。从 2000 年至今，RFID 技术的相关标准及安全问题成为了各行业学者的热点研究问题。与其它同类别的感知技术，如条形码、二维码等技术相比，RFID 技术具有可进行非接触式传感，适应性强，可重复利用率高、形式多样化等优势，因此 RFID 技术也逐渐成为了人们生活中不可或缺的一部分[1]。

虽然该项技术在实际应用的市场已经趋近成熟，但在当前万物互联的时代，用户的数据面临着高度曝光的状态，因此，信息交互便利的同时，数据传递的过程也面临着极大的安全隐患。本文首先对 RFID 技术面临的安全隐患及安全方案进行了概述与分析。其次，对现有 RFID 技术的认证协议系统地进行了安全性分析，最后，对 RFID 技术的应用前景与发展趋势进行了总结展望。

2. RFID 技术应用系统交互的安全隐患

服务器、阅读器以及标签三者构成 RFID 系统，其组成结构如图 1 所示。同时，面向 RFID 技术的系统应用的安全问题以 RFID 系统交互过程中标签与阅读器后端交互的数据机密性问题为主要表现。

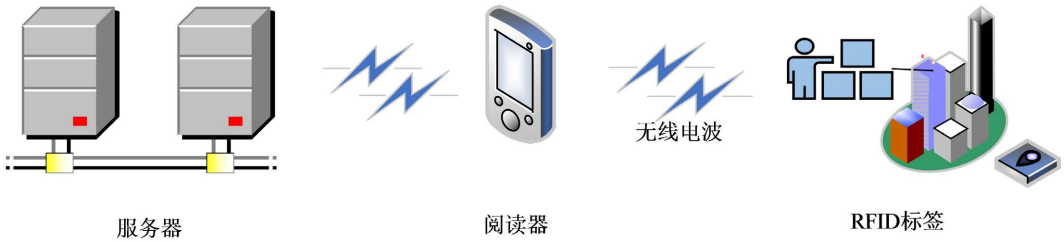

Figure 1. RFID system composition structure diagram
图 1. RFID 系统组成结构图

1) 物理破坏 RFID 标签

常见的通过物理手段破坏 RFID 标签功能及活性的手段有：非法获取标签实体并对标签采取暴力破

坏；使用机器物理屏蔽手段致使标签无法发送信号参与数据交互；监控标签信息；隐藏标签实体等。但这些攻击手段并不能在大规模实施的前提下发起破坏。

2) 篡改标签内容

攻击者通过特殊软件操作处理，捕获标签内的真实数据，随意对标签的数据进行增删改查，甚至可以通过这种攻击方式伪造标签，响应阅读器的交互请求，以此破坏整个 RFID 系统交互的机密安全性。

3) 攻击或伪冒阅读器

在 RFID 交互传输数据的过程中，阅读器充当着必不可少的一个角色，阅读器和标签之间的通信借助无线信号的传输完成彼此的认证，因此部分攻击者伪冒阅读器以获取 RFID 系统交互过程中标签向其发送的关键数据，以此威胁标签乃至整个系统的安全。通过发射带有干扰性质的无线信号甚至可以导致阅读器无法正常收发数据，直接破坏了阅读器参与交互的积极性。

4) 被动监听

RFID 系统交互过程中，由于标签与阅读器是通过无线电波的传输完成数据的交互和身份的认证，因此，部分攻击者选择被动攻击方式的监听技术，在监听了来自标签发送的数据后，对其进行分析以获取标签和阅读器的有效信息。虽然该种攻击方式不影响系统的正常运行，但被获取到的关键信息仍然威胁整个系统的安全性。

3. RFID 技术相关安全方案

针对 RFID 系统交互过程中面临的安全隐患，解决策略分为物理安全方案以及结合密码学相关技术的安全方案。

3.1. 物理安全方案

1) 销毁危险标签

针对安全受到威胁的标签，阅读器可以向危险标签发送销毁指令，常见的即 Kill 指令。一旦标签接收到来自阅读器的销毁命令，标签便会立即执行自我销毁手段，以确保自身数据不被捕获，保护系统传输的数据机密性。但是该类指令为不可逆操作，标签自毁后不能再参与交互，失去活性。

2) 阻塞标签

为防止标签收到来自伪冒阅读器的交互请求后发送关键数据，可以在标签附近增加一个假冒对象，即阻塞标签。阻塞标签实质上可以理解为真正标签的替身，当收到来自假冒阅读器的认证信息，可以自行向其发送错误信息以此对假冒阅读器造成混淆，以此保护真正标签及标签中的关键数据。

3) 法拉第笼

法拉第笼可以从物理手段阻隔屏蔽发送无线信号，即可以保证阻挡来自危险方发送的假冒信息或读取信号，也可以保证标签不会向假冒方发送关键数据。

3.2. 密码学相关安全方案

结合密码学相关技术的 RFID 系统安全方案可以保证 RFID 系统传输交互过程中的数据机密性，大多数学者结合密码学相关技术提出了相关的 RFID 认证协议，针对提出的方案协议不同，对标签的功耗要求及系统性能要求也不同[2]。

1) 基于 Hash 函数的 RFID 认证协议

熊婧等人[3]提出了一种基于 Hash 函数的 RFID 认证协议，协议对标签功耗要求低，认证速率高。但认证过程中的传输数据的前向安全性以及标签窃听等安全隐患仍未得到解决。因此对于标签溯源攻击以及窃听标签关键信息等攻击手段仍存在安全隐患。周静等人[4]提出了基于 Hash 链的双向认证协议，协

议中采取三分认证方式，即阅读器认证传输数据、标签解析来自阅读器的数据以及阅读器认证标签的预置标识，以此提高认证过程的数据的前向机密性。郑欣等人[5]在基于 hash 函数的基础上提出了 RFID 双向认证协议，协议对伪造攻击、重放攻击以及被动窃听等具有良好的抵抗能力。

2) 基于随机数方案的 RFID 认证协议

陈文雄等人[6]提出了一种基于随机数方案机制与 Hash 函数结合的 RFID 认证协议，协议在避免标签跟踪以及窃听关键信息等方面具有良好表现，但在该协议中的 Hash 函数在面对重放攻击市仍然不具备抵抗能力。史志才等人[7]提出随机化加密数据并使其参与哈希运算的加密，以确保认证的高效率运行。谢海宝等人[8]提出的基于伪随机数的 RFID 认证协议采用了伪随机数发生器参与加密的原则，保证了传输数据的新鲜性及不可预测性。郝伟伟等人[9]提出了基于伪随机数方案的 RFID 认证协议，协议采取了异变每一轮参与加密数据的原则，混入了随机数进行加密，确保了数据的随机性，保障了数据的前向安全。

3) 基于逻辑算法的 RFID 认证协议

Yun Tian 等人[10]提出了一种基于逻辑算法的 RFID 认证协议。协议通过引入基于逻辑算法的 Per 函数置换计算加密认证过程，以保证数据的机密性，Per 函数中设置两个指针对第二方输入进行扫描，第一个指针从高位到低位扫描，所遇值为 1，保存第一方输入的值；第二个指针从低位到高位扫描，指针读扫描值为 0，保存第一方输入值，其原理如图 2 所示。基于此逻辑算法加密的 RFID 认证协议，可以确保认证过程中数据的机密性且该协议所使用的逻辑加密函数复杂度不高，因此对标签的功耗要求较低。但 Bagheri 等人[11]提出 RAPP [10]协议对于标签溯源攻击手段及去同步攻击方式等仍不具备抵抗能力。王沅等人[12]提出了一种字合成运算 Syn(X, Y)的加密方式，以此确保认证过程数据传输的安全性，协议对于异步攻击具有良好的抵抗能力。

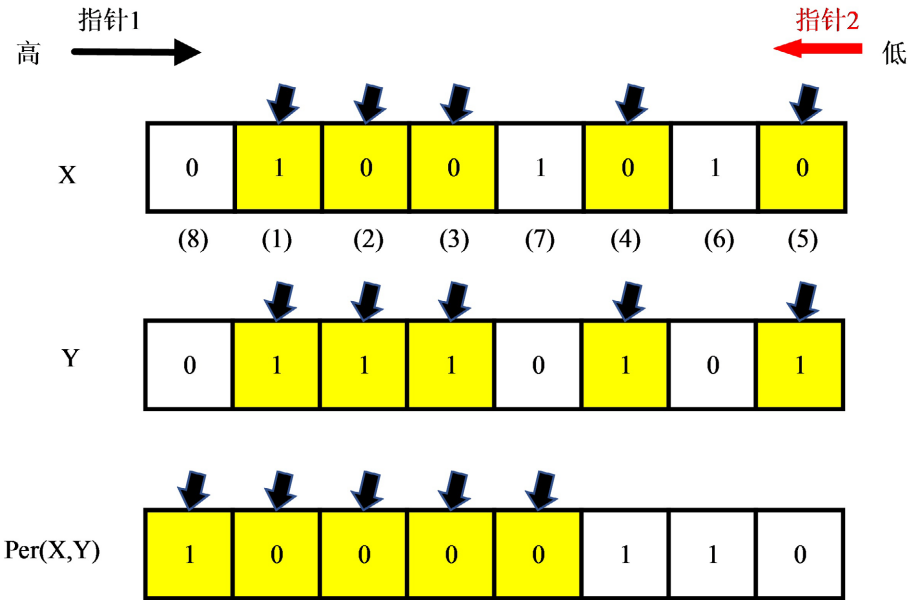

Figure 2. RAPP protocol algorithm schematic
图 2. RAPP 协议算法原理图

4. RFID 技术的应用前景及发展趋势

如何提高传感效率是物联网环境面临的一大挑战，作为应对该挑战的 RFID 传感技术的应用被广泛关注，RFID 技术在基于物联网环境的基础上具有广泛的应用前景，包括但不局限于：

1) 智慧家居。在智慧家居的领域，RFID 技术已经有所应用，但应用规模依旧有可探索空间，结合了 RFID 传感技术的家居生活，能够实现对灯光、家居的远程控制，且操作方便，成本较低，同时提高了生活的便利性和高效性。

2) 智慧出行。现阶段无人驾驶、智慧出行、实时交通等技术正处于大规模推广阶段，将 RFID 技术应用在智慧交通，无人驾驶等场景，可实现人机交互，数据传输，进而提高出行效率。

3) 智慧医疗健康。随着当前大环境医疗水平的提升，配合 RFID 技术，将患者的就诊数据实现加密传输的同时，提高了就诊速率，为精准治疗患者提供科学保障。

另外，RFID 传感技术应用具备可重复利用率较高、适应场景范围较广、操作便捷等优势，因此在物流运输、农业自动化、林业智能化等应用场景也具备了良好的发展趋势。

5. 结语

由于 RFID 技术系统应用的过程中所需要的成本较低，并且操作难度也相对较低，因此伴随着对其应用的前提下，该项技术面临的系统应用的安全隐患也日益显现。本文对 RFID 技术在应用中所面临的安全隐患进行了概括总结，并且总结了应对各类隐患的安全方案，主要分为物理安全方案和密码学相关方案。其中，对现有结合了密码学相关方案的 RFID 技术的认证协议进行了系统性分析。最后，对 RFID 技术的应用前景与发展趋势进行了展望，为日后 RFID 技术的研究提供参考。

基金项目

哈尔滨师范大学研究生培养质量提升工程“新工科背景下创新创业型研究生多维培养模式的研究——以网络安全方向研究生培养为例”和哈尔滨师范大学本科专业人才培养方案研究改革专项(XJGRYK2022012)。

参考文献

[1] 王悦. RFID 安全认证协议研究[J]. 网络安全技术与应用, 2020(5): 42-44.

[2] 李宇松. 浅析 RFID 系统安全防护[J]. 信息网络安全, 2021(S1): 252-254.

[3] 熊婧, 王建明. 基于 HASH 函数的 RFID 安全双向认证协议研究[J]. 中国测试, 2017, 43(3): 87-90, 96.

[4] 周静, 董国超, 邓祖强, 等. 基于随机 Hash 链的双向安全认证 RFID 协议[J]. 计算机与现代化, 2021(3): 46-50.

[5] 郑欣. 一种改进的 RFID 双向认证协议[J]. 网络安全技术与应用, 2021(2): 4-5.

[6] 陈文雄. 基于随机数和 Hash 函数的 RFID 安全协议[J]. 网络安全技术与应用, 2018(4): 17-21.

[7] 史志才, 王益涵, 张晓梅, 陈计伟, 陈珊珊. 一种具有隐私保护与前向安全的 RFID 组证明协议[J]. 计算机工程, 2020, 46(1): 108-113.

[8] 谢海宝, 吕磊. 基于伪随机数发生器的双向认证协议[J]. 计算机技术与发展, 2022, 32(1): 128-133.

[9] 郝伟伟, 吕磊. 基于伪随机数发生器的移动 RFID 双向认证算法[J]. 计算机技术与发展, 2022, 32(5): 93-98.

[10] Tian, Y. (2012) A New Ultralightweight RFID Authentication Protocol with Permutation. *IEEE Communications Letters*: *A Publication of the IEEE Communications Society*, **16**, 702-705. https://doi.org/10.1109/LCOMM.2012.031212.120237

[11] Bagheri, N., Safkhani, M., Peris-Lopez, P., *et al*. (2014) Weaknesses in a New Ultralightweight RFID Authentication Protocol with Permutation-RAPP. *Security and Communication Networks*, **7**, 945-949. https://doi.org/10.1002/sec.803

[12] 王沅. 抗异步攻击的 RFID 认证协议[J]. 计算机应用与软件, 2021(6): 318-323.