

基于超高频 RFID 的被动生物识别电子锁

邹祥^{1,2}, 韩劲松², 曲宇航¹, 肖剑³, 许贤⁴

(1. 西安交通大学计算机科学与技术学院, 陕西 西安 710049;

2. 浙江大学网络空间安全学院, 浙江 杭州 310007;

3. 长安大学电子与控制工程学院, 陕西 西安 710064;

4. 浙江大学建筑工程学院, 浙江 杭州 310085)

摘要: 提出了一种利用人体内部的生物特征来进行认证的生物识别电子锁设计方法, 简称为 PBLock。该方法通过人手指与无源式射频标签的接触, 利用后向散射的射频信号传递人体指尖阻抗特征来实行认证。这样的认证方式的优势在于, 由于人体阻抗不易采集, 加之与设备 (RFID 标签) 的硬件特征充分融合, 大大增加了攻击者复制和克隆的难度。为保证系统的可用性和高效性, 利用标签天线剪切式认证优化机制, 有效提升了人体阻抗敏感度。同时, 利用 RFID 系统的电磁能量优势讨论了被动驱动的可行性。实验评估结果表明, PBLock 的认证准确率可达 96%, 平均单次认证的时间开销是 1.4 s。另外, 从实际环境出发提出了攻击模型, 通过深入分析发现, PBLock 可以有效防止伪造攻击、模仿攻击和重放攻击, 为新型生物识别电子锁的应用安全提供重要保证。

关键词: 生物识别电子锁; 阻抗生物特征; 射频识别; 近场耦合

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021022

Passive biometric electronic lock via UHF RFID

ZOU Xiang^{1,2}, HAN Jinsong², QU Yuhang¹, XIAO Jian³, XU Xian⁴

1. School of Computer Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China

2. School of Cyber Science and Technology, Zhejiang University, Hangzhou 310007, China

3. School of Electronics and Control Engineering, Chang'an University, Xi'an 710064, China

4. College of Civil Engineering and Architecture, Zhejiang University, Hangzhou 310085, China

收稿日期: 2020-07-01; 修回日期: 2020-09-23

通信作者: 韩劲松, hanjinsong@zju.edu.cn

基金项目: 国家自然科学基金 (61872285, 61772413); 浙江大学网络空间国际治理研究基地, 浙江省引进培育领军型创新创业团队 (2018R01005); 浙江省重点研发计划 (2019C03133, 2017YFC0806100); 国家社科基金重大项目 (20ZDA062); 西安市科技计划项目 (201805045YD23CG29(1))

Foundation Items: The National Natural Science Foundation of China (61872285, 61772413), The Research Institute of Cyberspace Governance in Zhejiang University, Leading Innovative and Entrepreneur Team Introduction Program of Zhejiang (2018R01005), The Key R&D Program of Zhejiang Province, China (2019C03133, 2017YFC0806100), Major Projects of the National Social Science Foundation (20ZDA062), Xi'an Science and Technology Plan Project (201805045YD23CG29(1))

论文引用格式: 邹祥, 韩劲松, 曲宇航, 等. 基于超高频 RFID 的被动生物识别电子锁[J]. 网络与信息安全学报, 2021, 7(2): 126-140.

ZOU X, HAN J S, QU Y H, et al. Passive biometric electronic lock via UHF RFID[J]. Chinese Journal of Network and Information Security, 2021, 7(2): 126-140.

Abstract: A biometric lock design method was proposed based on the internal features of human body, namely PBLock. It used the backscattered RF signals to collect the impedance characteristics of human fingertips through the contact between human fingers and tags. The advantage of such authentication method is that the human impedance was not easy to be stolen, and it was fully integrated with the hardware characteristics of the device (RFID tags), which greatly increased the difficulty for the attacker to copy and clone. To ensure the availability and efficiency of the system, an optimization authentication mechanism was proposed by cutting tag antenna, which effectively improved the impedance sensitivity. Moreover, the feasibility of passive drive was discussed by using the electromagnetic energy advantage of RFID system. Through a large number of experimental evaluations, the authentication accuracy of PBLock can reach 96%, and the average time cost of a single authentication is 1.4 seconds. Some attack models were presented based on practical environment. The results show that PBLock can effectively prevent counterfeiting attack, impersonation attack and replay attack, which provides an opportunity for the secure application of new biometric electronic locks.

Keywords: biometric lock, impedance biometric, radio frequency identification, near field coupling

1 引言

锁一直是保证人们财产和隐私安全的重要工具和手段。针对锁的攻击与破坏,从未停止过。传统制锁工艺和锁定方法主要有机械和密码两种方式。从安全的角度看,这两类锁的安全性保证分别可以归入“用户拥有什么”和“用户知道什么”两类。然而,随着技术的发展,这两种方式都面临着日益严峻的挑战。

机械锁需要额外携带开锁钥匙来匹配锁芯,这种开锁方式由于安全性达不到用户的要求,应用范围已日趋缩小。虽然当前市场标准的C级锁已经能够做到防止强扭工具开启锁芯,但用户携带钥匙的要求给使用带来了不便。更严重的是,如果钥匙丢失或被复制,锁的安全性就无法保证。密码锁的出现较好地解决了上述问题。然而,一方面由于用户有可能遗忘密码,另一方面随着现有计算能力的增强,使用暴力破解等方法,可以在很短的时间内将不安全的弱密码破解,使密码锁的安全问题面临极大的考验。锁的安全隐患给人们造成了大量的财产损失。因此,寻找一种不易被复制、不需要用户过多操作和参与,并且具有高安全性保证的上锁方法,成为信息化时代制锁领域一个亟须解决的问题。

近年来,智能门锁得到了广泛应用,其中载有指纹或者人脸生物识别技术,能够以人体固有的、可区分的生理特征作为安全凭证,属于“用户是什

么”或“用户做什么”的范畴。对比于传统机械锁和密码锁方式,生物识别技术的优势在于:

① 不需要用户携带钥匙或者记住密码口令;② 生物特征不易被复制和传递;③ 用户的生物特征伪造和篡改困难。

然而,生物识别技术也面临着日益严峻的安全威胁和挑战。目前主流的智能门锁主要基于指纹和人脸识别。但近些年来的研究^[1-5]发现使用超高清摄像头或者采集模具可以比较容易地窃取并伪造相应的生物特征信息。智能门锁存在安全问题,手指纹或者人脸特征存在于人体表面,因此容易被摄像机采集含有人手、人脸的图像或视频流,再利用特殊的电脑合成和渲染技术,就可以伪造人体的生物特征。另外,生物识别电子锁中的认证模块往往需要较大的能量来驱动,且主要基于电池供电。更严重的是,一旦电量耗尽将出现锁无法打开的窘境,因此需要安装体积庞大的电池或经常更换电池,这就给系统带来了额外的开销和负担。

面对以上问题和挑战,本文提出了一种新型的被动式生物识别电子锁系统,简称为PBLock。它采用一种新的基于人体阻抗的生物信息认证模式,具有抗窃取、人机融合认证的特点,极大提高了系统的安全性。PBLock采用了反向散射的方式采集信息,避免了因电池能量耗尽造成系统瘫痪的隐患。PBLock的出发点是利用人体对无线射频识别标签的偶极子天线增加一个额外的阻抗。由于人体之间的阻抗差异^[6-7],偶极子天线的匹配

阻抗会对电磁波产生不同的反射效果,通过提取反射的电磁波信号中人体阻抗对应的特征就可以认证用户。同时,PBLock 利用天线的近场耦合来进一步加强人体阻抗生物特征的唯一性,使用超级电容存储射频能量并驱动离合器。图1展示了PBLock 的设计原型。射频识别(RFID, radio frequency identification)阅读器发射射频信号,被动标签反向散射信号,当用户的指尖触摸一个剪切了一部分天线的标签,该标签反向散射的信号被阅读器读取并进行特征提取与认证。当特征匹配通过时,阅读器发射特定功率射频信号,控制电路的偶极子天线接收这个射频能量并被邻近的剪切标签近场耦合干扰,偶极子天线产生独特的电压指纹,通过控制电路中微控制器识别并匹配这个电压指纹,当匹配通过时驱动锁的离合器开锁。

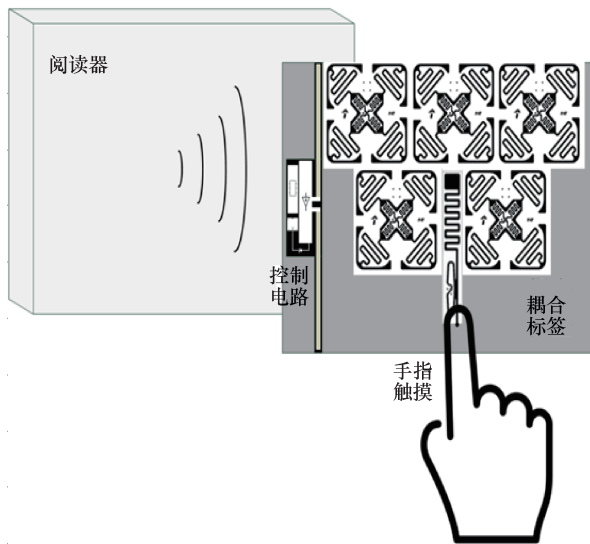


图1 PBLock 设计原型
Figure 1 Illustration of PBLock prototype

然而实现上述系统面临一些挑战:如何设计标签让人体的触摸具有唯一性;考虑到人手触摸的标签只有一个,如何增加特征的数量;商用RFID 阅读器的射频发射功率只有1 W,因此控制电路偶极子天线的接收功率密度非常低,从而导致控制单元能量匮乏。针对第一个挑战,本文利用改变剪切标签的手指触摸天线长度和标签阵列的布局来提升人体触摸下的特征分辨率,保证数据的唯一性。针对第二个挑战,本文使用耦合标签扩充剪

切标签特征数量。针对第三个挑战,本文利用锁在常开和常闭时不需要工作的特性,来获取收集能量的机会。

本文使用的RFID 设备均为商用系统,如阅读器为Impinj 420,阅读器天线为定向的圆极化天线Laird A9028,标签为主流商用被动标签。锁端的微控制器采用MSP430 单片机实现。本文还设计了一个硬件电路来实现天线耦合和能量收集。为了评估系统性能,邀请了12 名志愿者参与了本文的系统实验。

本文具有如下贡献。

(1) 探究了一种基于人体阻抗的被动生物识别电子锁系统,解决了传统生物识别电子锁具有繁杂性和易被偷窃的问题。

(2) 利用标签间的近场耦合效应扩展了特征数据的维度,同时提出双边认证方法,在阅读器端和锁端进行双重认证,使用锁端的天线与剪切标签的近场耦合特性抵御了重放攻击。

(3) 使用商用RFID 系统和便宜的硬件电路构建了系统原型,系统的认证成功率达到96%,防御成功率达到100%。

2 相关工作

(1) 生物认证

生物认证已经广泛应用于人们的日常生活中,如手机的指纹开锁、Face ID、虹膜认证^[8]、手掌或手指静脉认证^[9-11]、声纹认证^[12]等。生物认证的原理是提取人体表面的特征并与提取注册的特征进行匹配。这种认证方式不需要用户携带钥匙,也不需要用户提前记住密码,因此方便了人们的日常生活。然而,最近的研究显示了这种生物特征的不安全性。黑客可以通过高清摄像头捕捉用户指纹并攻击,提出了一种修改摄像头采集指纹,防止指纹通过公共摄像头泄露的方法,然而使用私人摄像头偷窃指纹难以被防御。REN 等^[13]说明了声音可以通过录音设备捕捉并重放,提出了一种利用扬声器失真认证声纹的方法,但这种方法难以抵御高保真扬声器。因此,相对于上述生物特征而言,人体阻抗不可偷窃、不可伪造、难以被设备捕捉,安全性更高。

(2) 行为认证

文献[14]研究使用用户的行为作为特征进行用户认证。基于步态^[15-18]的认证方法受到较大的关注,采集用户的步态长度、走路频率等,通过一段时间的数据采集,进行用户的持续认证。Kong 等^[19]利用用户手势提取行为指纹,通过统计用户的手指间距、挥动频率等,把用户的日常行为习惯当作用户特征来认证。然而,这种方法需要大的数据集用来训练模型,而且需要采集用户一段时间的数据做持续认证。显然这种持续认证方式不适合锁认证。

(3) 活体认证

由于静态特征认证的局限性,活体认证加入了人体活动特征,安全性更高。Lin 等^[20]利用射频信号采集人体心脏跳动时腔体的收缩和扩张频率以及幅度来认证用户,这种内在特征难以被攻击者窃取,因此拥有较高的安全性。人体的口腔活动^[21-22]也能用于活体认证,利用口腔的差异性,捕捉声音在人体口腔的反射来认证用户。这种特征解决了静态特征容易被偷窃的问题。但是这种认证方式同样面临认证时间的问题,系统需要采集一段时间的数据用于认证人体的活动特征,保证人体的活动状态特征能够被采集。

3 研究背景

传统的电子锁由3部分组成:生物信息采集模块、中央处理单元和控制驱动模块^[23]。为了凸显锁的普遍性,本文同样采用这种结构,生物信息采集模块用于采集人体阻抗特征,中央处理单元用于认证锁端,控制驱动模块用于驱动电机。为了提取人体阻抗特征,传统的指纹提取设备和人脸特征提取设备并不能反映阻抗信息,因此引入了RFID技术,运用标签天线阻抗与人体阻抗的关系,使用标签的反向散射信号表征人体阻抗。为了方便理解,下面将介绍RFID技术的一些背景知识。

3.1 商用 RFID 标签天线增益

在商用RFID系统中,阅读器和标签通过电磁波的反向散射进行通信。商用标签的天线被设计成一种偶极子结构,并使用弯折结构降低天线空间,天线的长度为电磁波的半波长(16 cm)以

获得最大的频率响应。当剪切标签天线时,由于频率响应改变,因此标签对阅读器的响应增益会变低,从而导致阅读距离变短。一般而言,可以使用弗里斯公式表示标签从阅读器的发射天线接收到的功率,如式(1)所示。

$$P_{RX} = P_{TX} G_{TX} G_{RX} \left(\frac{\lambda}{4\pi r} \right)^2 \quad (1)$$

其中, λ 表示电磁波波长, r 是发送端和接收端的距离, G_{TX} 和 G_{RX} 分别表示发射端天线和接收端天线的功率增益。因此,在波长、距离和发射端功率不变的情况下,标签的接收功率是与接收标签的天线增益有关的。此外,全向天线的增益是跟天线长度相关的,如式(2)所示。

$$G = 10 \lg \left(2 \frac{L}{\lambda} \right) \quad (2)$$

其中, L 表示天线的长度。也就是说,天线的增益可以通过改变天线的长度而变化。

3.2 阅读器的读取距离

图2表示了不同天线增益标签的阅读器的读取距离。假设固定阅读器发送功率、距离和天线增益,标签芯片最低需要100 μ W(也就是-10 dBm)的能量来激活,标签距离阅读器大约为3 m。标签内部需要消耗一定电量来进行信号解调与调制,如图2中两条红色虚线所示,上虚线为标签芯片电路接收到的-10 dBm能量,经过内部消耗-5 dBm能量后反向散射电磁波。正常情况下,标签天线与电磁波波长匹配,反射的电磁波会被阅读器接收到,如图中接收信号强度为-60 dBm。如果剪切了一半标签,则由于天线长度与波长不匹配,从而导致反向散射信号强度减弱,如图2蓝色绿色斜线所示。当人体触摸剪切了一半天线的标签时,由于人体阻抗的作用,反向散射信号强度会有一定上升,如图2绿色斜线所示。商用阅读器的接收功率都有一个阈值,也就是说当反向散射信号强度低于阈值时不会接收,除非缩短标签到阅读器的距离从而加大信号强度。设置阅读器阈值为-70 dBm,如图2所示,剪切标签只有当距离小于1 m时阅读器才能读到,而人体触摸后读取距离接近2 m,即可以使用读取距离来度量人体阻抗或者固定阅读距离,使用接收信号强度来代表人体阻抗。

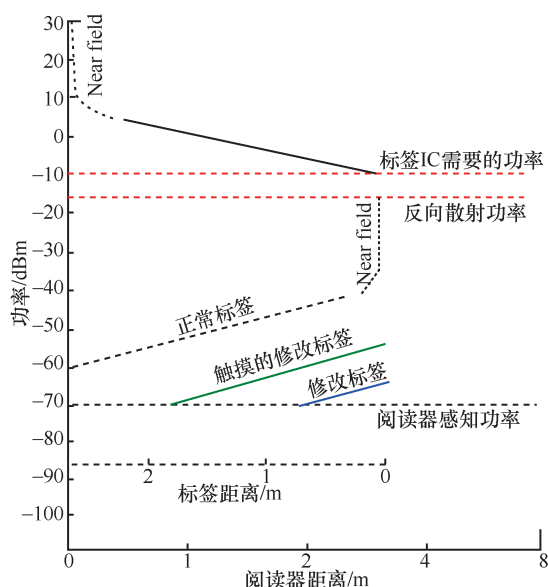


图2 不同天线增益标签的读取距离
Figure 2 Reading distance of different antenna gain tags

3.3 天线近场耦合效应

一些相关工作已经展示了标签天线之间的耦合效应^[24-26]，也就是说，天线工作时其中流动的电流会产生磁场，从而影响另一个标签的感应电流。利用这种原理，一方面在剪切标签附近放置受耦合效应影响的普通标签，用来增加阻抗特征维度；另一方面用于双边认证，在剪切标签旁边放置锁的能量收集天线，剪切标签同时又会影响天线的耦合电压，由于近场耦合效应的影响，这个电压带有人体阻抗特性。

4 系统模型

本节建立了一个标签和人体的阻抗模型，介绍了标签提取人体阻抗的原理与攻击模型，并提出了认证面的概念，用来量化认证方法的安全性。

4.1 阻抗模型

传统商用标签主要包括3部分：天线、阻抗匹配和集成电路芯片，为了方便阐述，用等效电路表示一个普通的商用标签，如图3所示。等效电路同样包括3部分，天线可以用一系列电阻电容电感表示，阻抗匹配可以用 π 型匹配电路表示，芯片可以用电阻电容表示。此时的阻抗匹配电路对应天线的阻抗，具有最高的能量响应。当用手触摸天线，引入一个额外的阻抗时，匹配电路不能拥有最佳的电磁耦合效率，因此，当手指触碰标签裸露的天线时会降低其反向散射功率。而当

剪掉一部分天线后，天线一端变短，人体则可以等效为阻抗^[6]，也就是图3中的电阻 R'' 、电容 C'' 和电感 L'' ，因此当人体触摸剪切标签端时会加入一部分阻抗到天线端，从而增强反向散射信号。

假设使用 Z_{IC} 和 Z_{AN} 分别表示标签芯片和天线的阻抗，匹配电路用以匹配这两个阻抗，以使负载功率最大，因此标签天线的电流可以表示为

$$I = \frac{V}{Z_{IC} + Z_{AN}} \quad (3)$$

其中， V 表示阅读器射频信号引起的源电压。当剪切部分天线并以人体手指替代时，由于标签电流的改变，射频信号的幅值和相位也会变化。

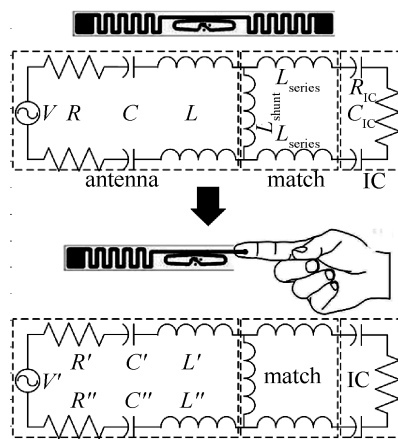


图3 标签等效电路
Figure 3 Equivalent circuit of tag

4.2 攻击模型

考虑到攻击者试图偷窃隐私信息或者伪造合法用户来执行未经授权的操作，本文分析了4种攻击模型。

(1) 伪造攻击。攻击者可能知道用户的指尖外形，用其他材料伪造合法用户所认证的手指，以此骗过系统的认证。

(2) 模仿攻击。攻击者可能知道合法用户认证的姿势和区域，以此模仿合法用户，使用相同的姿势和手指来进行欺骗。

(3) 重放攻击。攻击者通过窃听得到阅读器和标签之间的通信信号，并重放这个信号企图开启系统。

(4) 试错攻击。假设攻击者知道开锁的原理，并尝试改变各种信号来攻击系统，就像密码锁一样尝试各种密码的排列组合方式。

4.3 认证面

常用的生物特征认证方法都需要专用设备传感器捕捉用户的特征,如手指纹采集传感器或者面部采集传感器,这些传感器都有一个和用户交互的接口用于采集用户的特征。一般而言,这些接口都需要采集完整的生物特征来生成独特的用户特征,以手指纹为例,假设其特征点(交叉点、分叉点等)都是由传感器采集到的,每个特征点都有位置、类型、方向和特征间关系的特征矩阵。通常,手指纹拥有 70 个特征点并以此组成 490 个特征,同理,通过摄像头采集的脸部特征也会组成特征矩阵用来认证。

本文提出了认证面的概念,即采集的特征点越多认证越严格,认证方式也就更安全。一般来说,人脸的特征点比手指纹多,因此人脸相较于手指纹认证来说安全性更高。然而,像手指纹和人脸的特征点容易被超清摄像头捕捉,从而泄露生物特征。本文介绍了人体阻抗的生物特征(不易被偷窃、抗伪造能力强)。然而,相较于传统的基于生物表面的特征点提取方法,人体阻抗特征点较少,因此本文引入标签耦合方法提高特征点。

5 系统设计

本节详细介绍了本文系统的设计。首先是系统概述,然后实验验证了修改标签的理论模型,选择最佳修改天线尺寸,随后介绍了标签阵耦合,并提出本文的认证算法,最后介绍了锁的控制逻辑电路。

辑电路。

5.1 系统概述

本系统主要由 4 部分构成:修改标签、数据采集与处理、用户认证和驱动控制,如图 4 所示,锁端包含修改的标签,耦合的标签和能量收集的偶极子天线及电路,阅读器采集标签信息并认证,阅读器端认证通过后发射随机功率给锁端,判断电压是否与注册过的相匹配,最终完成双端认证并进行驱动控制。

(1) 修改标签。首先需要剪切标签的部分天线,让人体阻抗发挥更大的感知性能,为了方便触摸,增加了一个连接到标签天线的导体,这使触摸区域被固定,从而提供了一个指尖的恒定阻抗。

(2) 数据采集与处理。阅读器传输一个遵循 EPC Gen2 标准协议的信号,标签返回包含电子产品编码(EPC, electronic product code)的反向散射信号,阅读器采集这个标签信号并进行异常点去除。

(3) 用户认证。采集到的数据包括标签反向散射信号的时间戳、信号幅值和相位,当然还有标签的 EPC。在阅读器端使用时间序列信号差作为数据特征,运用支持向量机(SVM, support vector machine)进行分类认证。在锁端运用电压阈值作为认证手段。

(4) 驱动控制。当阅读器认证通过后发送一定功率的载波信号给锁端,天线后收集这个电磁

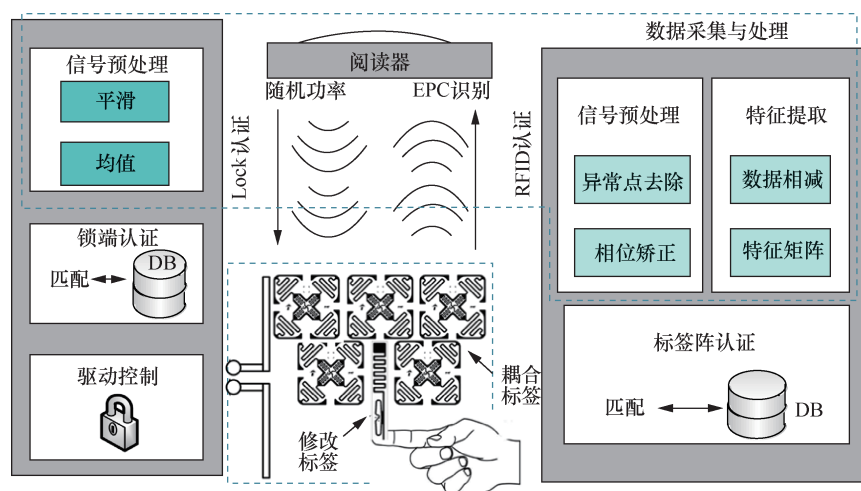


图 4 系统结构
Figure 4 System structure

能量,同时用电压值作为认证特征,当认证通过后控制器驱动离合器开锁。

5.2 标签的数据特征

RFID 通信距离与天线增益成正比关系,同样,当固定阅读距离时天线增益与接收功率成正比关系。因此,可以用阅读距离或者接收功率来表征标签天线的阻抗。

(1) 标签的天线长度

主要影响指尖阻抗的组织是血液和肌肉,较小影响的是皮肤、脂肪、神经、血管、皮质骨和松质骨^[6]。指尖的血液和肌肉不会快速变化,因此本文使用固定的指尖区域触摸标签天线。

理论上,剪切标签增加部分天线时,标签的天线增益会先上升,当天线长度增加到阻抗匹配时,增益达到最大,然后增益会下降,相应地,阅读距离也会先上升后下降。本文进行了一个验证性实验,选用两种不同大小的标签,分别是 Impinj E41-B 和 Alien 9629,先剪切了标签一半的天线,然后使用一定宽度的锡箔纸作为导体,延伸被剪切天线的断面,阅读器的发射功率设定为 15 dBm,导体的长度从 0.5 cm 到 20 cm,间隔为 0.5 cm。由图 5 红色线条可以看到,两个标签的反向散射信号强度呈现先上升后下降的趋势,即验证了上述理论。

同时,使用指尖触摸了导体的尾端,为了固定触摸区域,采用绝缘胶带覆盖住导体,在胶带中间开了一个小孔。从图 5 蓝色线条中可以明显地看到,当触摸标签时,在导体长度较小时,或者大于某一个值时,这两种标签的阅读距离都有差异。比较这两种标签,本文选择了差异性更大的 Impinj E41-B 标签。可以看到这种标签在导体长度小于 4 cm 或者大于 10 cm 时,在用户触摸或者不触摸时差异性较大;而导体长度在 4 cm 到 10 cm 之间时,阅读距离相似。根据这个实验,得到了修改标签有能力来区分指尖的触摸和这个区分性只发生在导体长度小于 4 cm 或者大于 10 cm 时这两个结论。基于此,本文选择了导体长度为 2 cm 进行下文的实验。

(2) 标签天线耦合

如上文所述,人体的阻抗能够改变标签的反向散射信号,但对于不同人,单一的标签没有足

够的认证面来确保特征的多样性,本文引入天线耦合的方法来增加认证面。考虑到模块大小和耦合性能,使用了不同的标签来验证耦合效果,分别是 Alien 9629 和 Impinj H47 标签,使用一个修改标签,周围放置 5 个耦合标签。

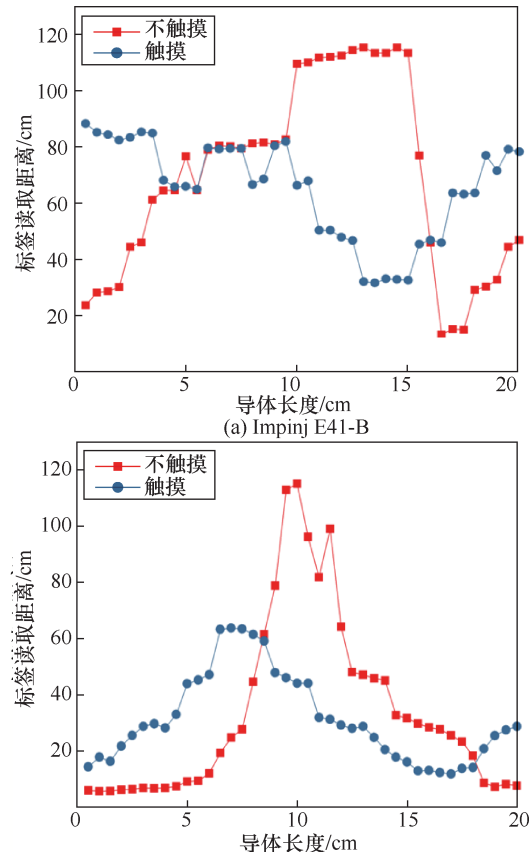


图 5 不同导体长度下的标签读取距离
Figure 5 Reading distance under different conductor length

需要注意的是,应尽可能扩大认证面,提升数据安全性,因此需要计算数据的最大数据特征量。从上面的实验中可以得到导体长度小于 4 cm 或者大于 10 cm 时拥有较好效果,因此可以每 0.5 cm 改变导体的长度作为一项数据特征,从而得到 19 种导体长度。耦合标签同样会增加特征数量,每个耦合标签都可以根据放置位置不同得到不一样的耦合特征,以修改标签的半边天线作为耦合,则每间隔 0.1 cm 移动,共移动 4 cm,一共有 160 种位置特征。另外,再加上阅读器的功率变化,每隔 0.5 dBm,可以从 20 dBm 变化到 30 dBm,标签与阅读器的距离可以每隔 5 cm 从 1 m 变化到 2 m,则一共有 400 种特征。这样总共可以得

到 1 216 000 个特征，也就是说最多可以支持这么多个阻抗相同的用户。

本文选用两名志愿者来进行实验，使用 Impinj H47 和 Alien 9629 标签作为耦合标签紧贴着修改标签，修改标签使用剪切了一半天线的 Impinj E41-B 标签并使用 2 cm 的导体延伸剪切天线，以便于手指触摸。阅读距离设为 1 m，发射功率设为 15 dBm，使用阅读器端软件收集标签反向散射数据。

如图 6 所示，收集了两名志愿者的信号强度和相位数据，其中左边两个表示在 Impinj H47 和 Alien 9629 标签作为耦合标签时志愿者 1 的阻抗特征图，右边两个为志愿者 2 的特征图，上两行为幅值信号，下两行为相位信号，取所有数据的最小和最大值作为颜色最深和颜色最浅区域。通过比较可以看到两人数据有很大差异，而且使用不同耦合标签依然有很大的区别，其中耦合标签的差异性表现出更大的数据差异性，这是因为不同的耦合标签拥有更大的标签天线差异性。下面，将介绍如何提取数据特征并进行认证。

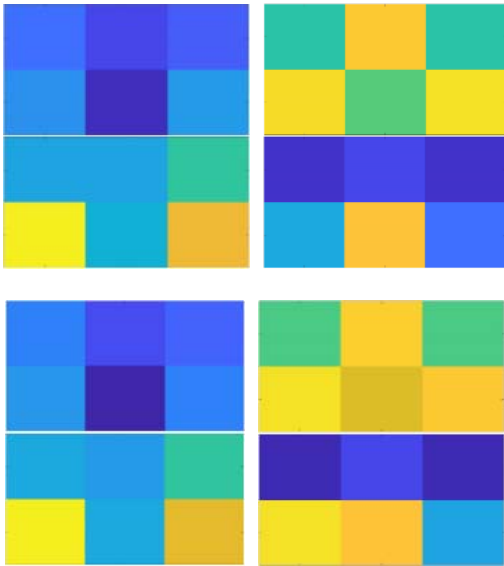


图 6 不同志愿者的阻抗特征的可视化图

Figure 6 The visualization result of the impedance characteristics with different volunteers

5.3 双边认证

一般情况下，传统的认证方式只发生在阅读器端，即采集标签数据，通过阅读器认证标签的合法性。但这种认证方法很难抵御重放攻击，因

为标签的反向散射信号总会发送给阅读器端。本文提出了双边认证，不只需要在阅读器端认证，标签端也需要做认证，这大大抵御了简单的重放攻击，同时，会在下文介绍如何在两边都认证的情况下抵御这种攻击。

5.3.1 标签阵认证

本文介绍了标签阵的认证，从阅读器端采集的数据进行处理并分类。阅读器可以得到标签的 EPC、RSS 和 Phase，当用户不触摸修改标签时，由于标签被剪切掉一半天线，因此反向散射信号低于阅读器接收功率阈值，阅读器只会得到耦合标签的数据。当用户触摸修改标签时，因为额外的阻抗，会使标签被阅读器读取到。处理数据时存在一些问题。

① 由于设备和多径的影响，数据存在异常点，即使采集的数据较为稳定，但数据存在跳变。

② 相位是一个周期数值，当标签位置处于波长整数倍的距离时，标签的相位会在 0 和 2π 之间跳变，这是由于标签的轻微抖动或者硬件的偏差引起的。

为了解决上述问题，本文首先使用异常点消除方法保证数据的稳定性，其次提出相位校准的方法消除这种跳变。最后，提取数据差的特征作为分类器的输入，用来认证用户。使用支持向量机来验证合法用户，使用 one class SVM，RBF 核函数，防止过拟合参数选择 0.01，当合法用户有多人时可以使用多分类模型。

(1) 异常点消除

异常点会使数据出现大偏差，从而导致分类失败，因此异常点消除非常重要。使用一个时间窗求均值的方法来消除异常点，因为总体来说正常点总是占大多数的。当数据点大于这个均值(0.5)时，去除这个数据点，达到消除异常点的目的。如图 7 左边所示，异常点消除后数据变得连续。

(2) 相位矫正

当标签位置在一个波长距离左右晃动时，标签的相位值会在 0 和 2π 之间随机跳变，这会引入不必要的误差。同样，求出数据的最大值和最小值，如果极值差大于 $0.9 \times 2\pi$ 则判断发生了相位跳变，消除与现在数据均值差大于 π 的值，对消除后的数据求均值，把消除的点替换为这个均值，

反之亦然。如图7右边所示,相位校正后数据变得连续。

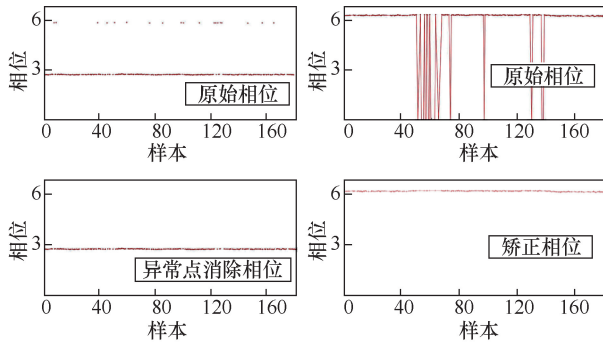


图7 异常点与相位跳变及矫正效果

Figure 7 Calibration of outliers and phase randomly jumps

5.3.2 锁端认证

当阅读器端认证通过后,阅读器发射特定功率的电磁波,通过锁端的天线进行能量收集的同时进行认证。微控制器是一个资源受限的设备,因此认证方法不能太复杂,只能在阅读器端进行更复杂的认证算法。

本文设计了一款锁端的硬件来实现能量收集和认证的目的。锁端包括天线、升压电路和能量收集模块,同时,使用单片机采集天线耦合的电压值用来认证。天线使用偶极子天线,使用一个 6.8 nH 的电感进行阻抗匹配,使用 RB751S40 肖特基二极管和 7 pF 电容组成超高频升压电路,能量收集电路使用 TPS73601 芯片达到稳定的 5 V 输出,经过一个 $5.5 \text{ V}/0.1 \text{ F}$ 的超级电容进行能量收集。

并制作了 PCB,焊接了元器件,总体花费不超过 50 元。硬件原理和实物如图8所示,最上面的是原理图,包括匹配电路、超高频升压电路和稳压电路,中间的是 PCB 板正面,主要排布升压电路,最下面的是 PCB 背面,排布稳压电路。

把修改标签靠近接收功率天线,连接上微控制器来进行锁端认证。如第2节所述,修改标签的阻抗变化会影响天线的耦合能量。本文进行了以下实验来验证这个假设。首先,调整阅读器的发射功率,查看天线的耦合电压是否随着发射功率而变化;随后,验证了不同用户触摸修改标签,天线的耦合电压发生变化。

如图9(a)所示,当调整阅读器发射功率时,天线的电压会随着发射功率呈线性的变化,这是因为在固定距离下,发射功率和接收功率呈线性关系。当固定发射功率,同一个人触摸和不触摸修改标签时,如图9(b)所示,原始采样点完全看不清差别,而进一步取滑动窗口做数值平均时,可以看到数据变得清晰可辨,图9(c)取20个值的窗口,图9(d)取了200个值的窗口,而数据也逐渐变得可以分清,因此使用数据均值可以分辨不同的用户。综上,可以使用电压指纹分辨不同的用户,用来做锁端的认证。

双边认证能够较好地抵御重放攻击,其原理在于双向认证和近场耦合。如果攻击者只重放反向散射信号,并对阅读器端重放攻击时,由于阅读器端接收到了正确的标签信号,因此可能被认

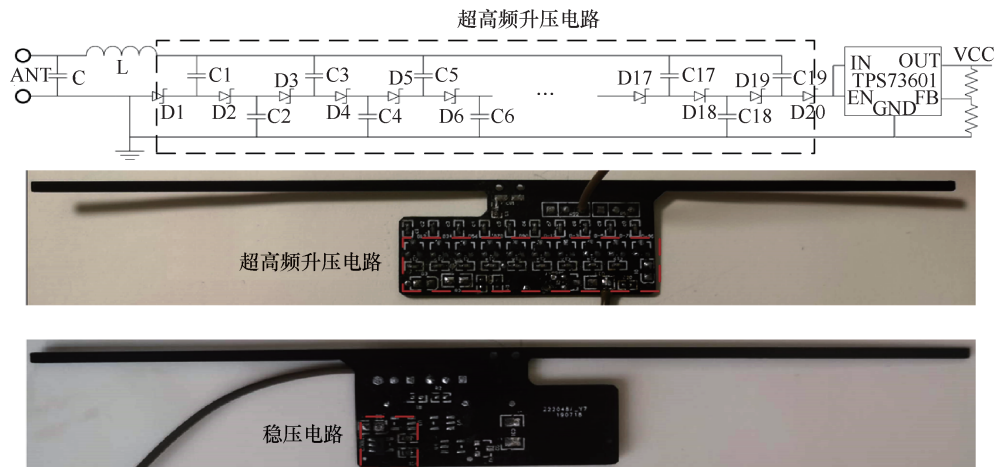


图8 硬件原理和实物

Figure 8 Hardware schematic and circuit prototype

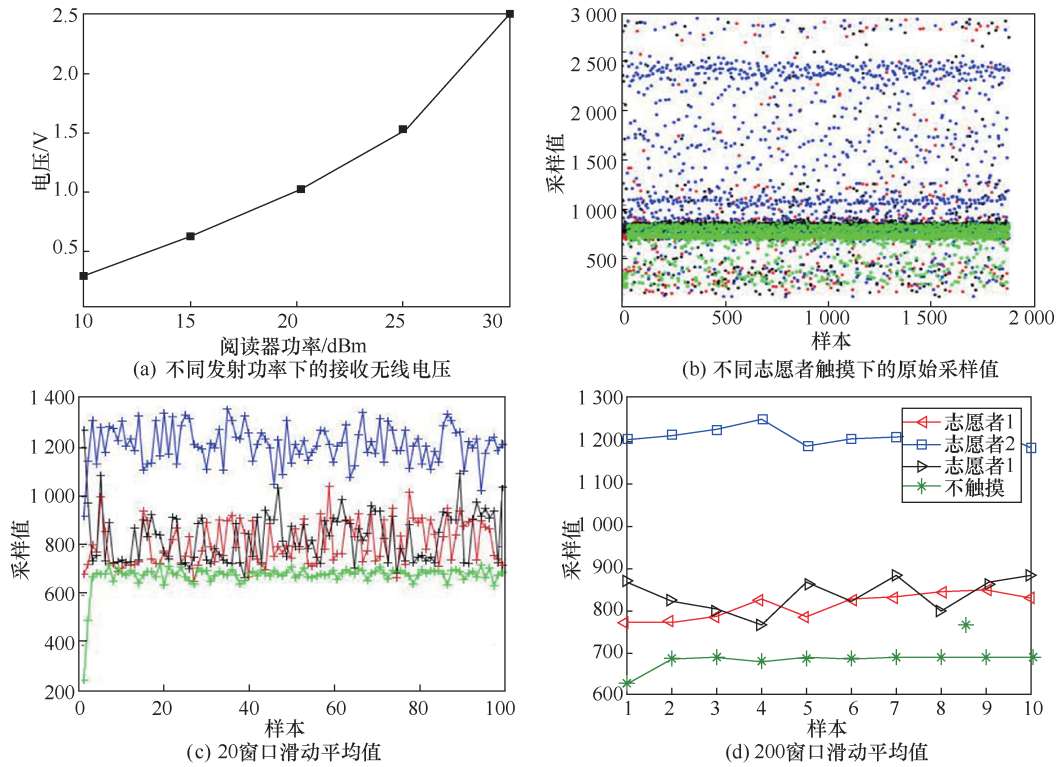


图9 不同发射功率的电压和触摸下的耦合电压采样值
Figure 9 Voltages of different transmitting powers and the coupling voltage samples

证通过。但是，锁端也需要认证，不仅需要阅读器发送正确的功率，而且需要合法用户触摸修改标签，以此耦合天线，使其拥有正确的电压值。即使攻击者能够同时重放双边的认证信号，天线也需要耦合修改标签，以达到认证电压。因此即使认证信号被重放，但由于近场耦合效应，没有合法用户触摸修改标签，锁端的认证也不会通过。

5.4 能量分析

为了能够实现无源生物识别电子锁，需要考虑在锁端对电磁能量进行能源管理，一方面降低锁的能量开销，另一方面提升能量采集效率。本文设置阅读器传输功率为 30 dBm，使用一个 0.1 F 的超级电容储存能量，阅读器和锁的距离为 20 cm，阅读器天线增益为 8 dBi，标签天线增益为 2 dBd，使用式(1)可以求出天线的耦合能量为 0.016 3 J/s，而超级电容可存储的能量计算如式(4)所示。

$$E = 0.5CU^2 \quad (4)$$

其中， C 表示电容量， U 表示电容额定电压。因此，能够得到电容的最大存储能量为 1.512 5 J，充满这个超级电容需要 1.512 5/0.016 3 s，约为 93 s。

使用低压直流电机驱动离合器开锁。驱动电机需要在短时间内开启离合器，因此需要大电流完成这个操作，而超级电容正好能够输出大电流驱动电机。超级电容的最大存储能量为 1.512 5 J，即只要驱动电机功率小于 1.5 W。

6 实验评估

本文建立了一个系统原型来评估其性能。

(1) 实验设置

系统主要由 3 部分组成：标签阵、阅读器和控制电路。其中，控制电路有偶极子天线、硬件电路和微控制器。使用两种耦合标签（Alien 9629 和 Impinj H47）验证系统性能，阅读器采用商用 RFID 阅读器 Impinj 420，阅读器天线为定向圆极化天线 Laird A9028，系统工作频率为 924.38 MHz。微控制器采用 MSP430FR5969 开发版，调整开发版为使用外部电源模式，使用 0.1 F 的超级电容存储能量。阅读器端采集数据的软件采用符合 EPC Gen2 标准协议的 C#代码，软件运行在 Intel Core i7-7700 CPU 和 8 GB RAM 的计算机上。实验环

境为一般的办公室环境,图10展示了真实环境的实验设置。锁端贴在木板一端,阅读器放在另一端来模拟真实环境的门禁,实际场景中锁端和阅读器应该放在木板一侧,只需要把导体延伸出来即可。当认证时,用户只需要用指尖按压延伸出的导体,标签与阅读器的距离越近越好,实验设置该距离为20 cm。阅读器连续的采集标签的EPC和相位幅值数据,一旦阅读器端认证通过,则触发锁端微控制器的中断,退出睡眠模式,并进行认证。

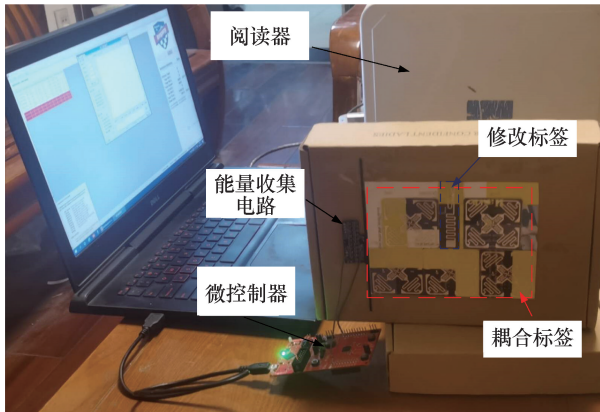


图10 实验设置
Figure 10 Experiment setup

(2) 度量方式

为了表示系统性能,本文采用了两种度量方式,即认证成功率(ASR)和防御成功率(DSR)。认证成功率表示系统成功认证授权用户的概率,可以用认证成功的样本数除以总的认证样本数,更高的ASR表示更好的系统认证性能,如式(5)所示。

$$ASR = \frac{N_{accept}}{N_{authentication}} \quad (5)$$

防御成功率表示系统成功抵御未授权用户攻击的概率,可以用防御成功的样本数除以总的攻击样本数,更高的DSR表示更好的系统防御性能,如式(6)所示。

$$DSR = \frac{N_{defence}}{N_{attack}} \quad (6)$$

6.1 系统认证性能

验证分类器的性能时需要注意的是,在认证前,系统先检查标签的EPC,如果EPC与注册时相同则开始认证。

评估分类器使用不同训练数据的性能,邀请

了12名志愿者参与本文的实验,其中有7个男性和5个女性。在最严苛的环境下进行评估,使用相同的标签阵和设备,因为如果使用不同的标签阵和评估环境,认证分辨率会更高,如第5节所说拥有1 216 000种特征。对每个人收集5 000条数据,使用20个数据为一个窗口,求出每个窗口中各个标签的均值,最后使用不同标签的差值作为特征。用第一名志愿者的数据评估在不同训练数据个数时系统的准确率、精确率、召回率和F1值。准确率是分类正确的样本占总样本个数的比例,精确率指实际为正的样本占被预测为正的样本的比例,召回率指预测为正的样本所占实际为正的样本的比例,F1值是精确率和召回率的调和平均值。使用100个正样本和100个负样本来确保不同类别样本的比例保持均衡。

如图11所示,当使用少量的训练数据进行训练时,系统的性能没有得到充分的展示;当训练数据达到80时,系统性能达到最优。

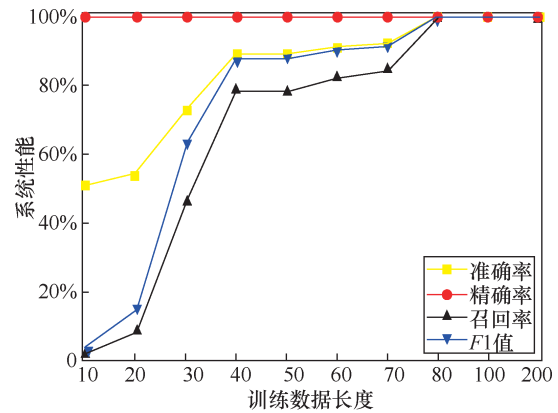


图11 训练数据长度与系统性能的关系
Figure 11 The relationship between training data and system performance

本文使用训练数据长度为200来保证系统更大的准确率,以此模型评估其区分不同人的性能,使用100个测试样本来计算ASR。图12展示了评估结果,M表示男性,F表示女性,系统的平均认证成功率为96%,而且大多数的用户认证成功大于98%,相对于女性来说,男性的认证成功更高。其次,使用其他11名志愿者作为攻击者,评估系统抵御其他人攻击的能力,计算出系统可以完全防御其他人的攻击,这12名志愿者对其他人的DSR均为100%。一般来说,相比认证

成功率，人们更关心系统不被他人攻破的概率，如果认证失败可以重新认证，而一旦攻击者解锁了用户密码则会泄露隐私信息。

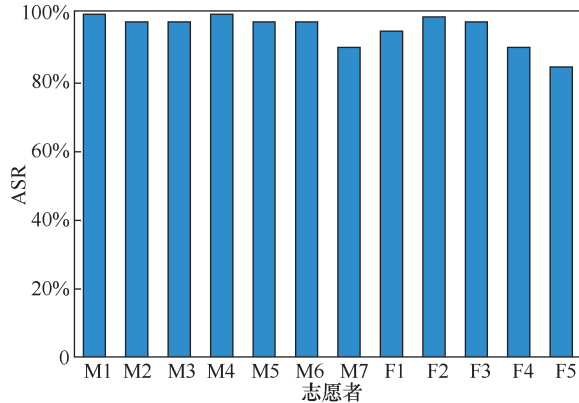


图 12 12 名志愿者的认证成功
Figure 12 ASR performance of 12 volunteers

6.2 各种因素的影响

系统使用人体阻抗作为认证特征，那么就需要考虑可能改变人体阻抗的因素。

选择了人们日常生活中可能佩戴的首饰来进行评估，如手表和戒指。当然，如果一次性喝大量的水也有可能改变阻抗。因此使用 SVM 训练在人体不佩戴首饰时的模型，再让志愿者分别在右手佩戴手表或者戒指，右手同时佩戴手表和戒指，最后让志愿者一次性喝 500 mL 的水，来评估可能改变人体阻抗的因素对系统性能的影响。再使用佩戴了首饰的数据来训练模型，使用佩戴相同首饰的数据测试系统准确率。如图 13 所示，可以看到手表和戒指对系统具有较大的影响，这可能是这些首饰对标签的反向散射信号有干扰。人体喝的水对系统影响较小。

针对这种现象，让志愿者佩戴手表或戒指后再采集数据，使用佩戴首饰的数据来训练模型，计算系统的准确率。如图 13 中最右边两列所示，观察到当使用佩戴手表或者戒指的模型来认证佩戴相应首饰的用户时，系统有较好的认证准确率。因此当用户认证时最好去掉手臂附近的金属物或者在佩戴首饰时也进行注册，确保系统认证性能。

6.3 系统认证时间

在用户开锁体验中认证时间也是一项重要的指标。商用 RFID 系统的采样率大约为 70 Hz^[27]，当采集大量数据时需要更多的时间，而且样本数越

多越需要更多的特征提取时间和指纹匹配时间，因此采集的数据量对于认证时间具有很大的影响。使用不同的采集数据量来评估系统认证时间，模型使用数据长度为 200，改变认证数据长度，在不同的数据长度下测量了 20 次。

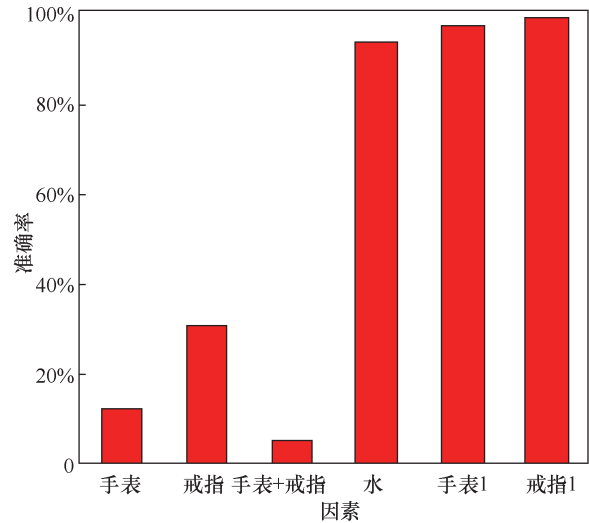


图 13 各种因素对系统的影响
Figure 13 Impact with various factors

图 14 展示了不同数据量下系统的认证性能，可以看到在 5 条数据、10 条数据、15 条数据和 20 条数据下，系统的平均准确率均在 95% 以上。通过采集样本数和系统采样率，可以计算出系统认证时间，当样本数为 5 时，实际采集原始数据约为 100 条，采集时间约为 1.4 s，这对于大多数认证场景是可以忍受的。

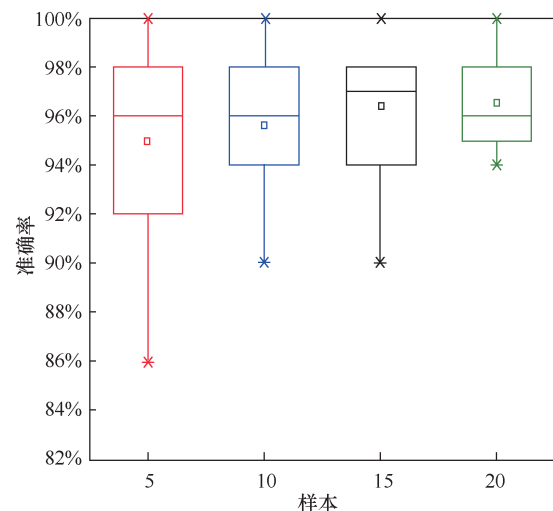


图 14 认证数据量对系统性能影响
Figure 14 The impact of testing data on system performance

6.4 系统充能时间

日常生活中,当用户开启锁后,会有一段不进行开锁操作,因此这段时间给系统充能提供了机会。如第5节所说,系统收集能量时间与阅读器发射功率,阅读器与锁的距离以及超级电容的容量有关。FCC规定超高频RFID阅读器的发射功率不得超出1 W,超级电容器容量为0.1 F,在距离为20 cm时可以算出充电时间约为93 s。本文评估了在0.2 m距离下系统收集的能量随时间的关系,并与离合器的驱动电机功率做出权衡。

如图15所示,超级电容的能量基本与充电时间呈现线性关系,6 min可以充85 mJ的能量,该值远小于理论值,这可能是由真实器件损耗、接收电路的不完美和稳压器的损耗产生的,因此需要后续工作的改进。使用充满电的超级电容驱动FF-030PK直流电机,观察到电机可以工作20 s,其能满足离合器需求。

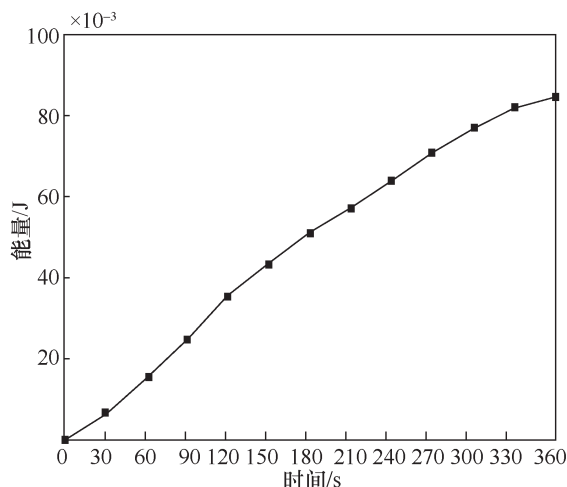


图15 收集能量与时间关系

Figure 15 Relationship between time and collecting energy

7 安全分析

本节分析了一些常见的攻击模型,并讨论系统该如何抵御这些攻击。

7.1 伪造攻击

攻击者可能提前知道合法用户的指尖形状,并使用其他材料伪造手指。这种攻击方法常用于攻击指纹认证方案,攻击者使用高清照相机拍摄到用户指纹并使用模具伪造手指纹^[1]。本文

使用DragonSkin高性能固化硅胶制作了假手指,模具使用低温蜡材料。首先加热软化模具,然后用手指按压模具,等冷却后再使用伪造材料填充模具,冷却后再取出伪造手指。使用真人和伪造手指触摸系统的修改标签,训练集使用开模的真人数据,测试集使用伪造手指,均为食指,由于假手指与人体手指的阻抗完全不同,认证成功率为0,因此系统能够完全抵御伪造攻击。

7.2 模仿攻击

攻击者可能知道合法用户认证的姿势和区域,以此模仿合法用户。由于使用的是人体阻抗来进行认证,不同人的阻抗是不同的,本文的实验也验证了这点(如图12所示)。实验时志愿者的姿势是基本相同的,而系统的认证准确率可以达到96%,防御成功率为100%,因此系统能够防御模仿攻击。

7.3 重放攻击

攻击者首先窃听系统通信信号,然后重放这个信号来欺骗系统。由于一般的认证方式只发生在阅读器端,攻击者完全有可能窃听阅读器采集的信号,因此给重放攻击提供了机会。而本文采用双边认证,在双端都需要进行信号认证,同时引入天线近场耦合,这完全防止了攻击者在用户可视范围外进行窃听的可能。

7.4 试错攻击

攻击者可能知道锁的原理,窃听并修改信号幅值或相位,尝试匹配系统的认证信号。如本文在第5节所述,系统在不同配置下的特征值可达1 216 000,而且还不包含在改变耦合标签的情况下,不同的耦合标签可以得到完全不同的信号值,如图6所示。因此,相比于密码锁的10个数字的排列组合,这种基于电磁波的认证方式安全性更高。

8 结束语

本文针对传统生物认证锁的生物特征安全性问题,提出了一种基于人体阻抗的生物认证方式,使用RFID商用被动标签的天线阻抗和人体阻抗对标签反向散射信号的影响,提取出与人体阻抗相关的特征并进行认证。同时,

为了增强系统安全性, 提出了双边认证方案, 利用触摸标签对偶极子天线的近场耦合效应, 提取出耦合电压来进行锁端认证。并分析了系统能量收集性能, 对4种攻击模型提出了抵御方案。本文实验有12名志愿者参与, 平均认证成功率达到96%。

参考文献:

- [1] CAO K, JAIN A K. Hacking mobile phones using 2D printed fingerprints[R]. Michigan State University Tech. MSU-CSE-16-2, 2016.
- [2] MOSHNYAGA V G, SHIOYAMA J, HASHIMOTO K. A camera-based approach to prevent fingerprint hacking[C]//IEEE International Workshop on Signal Processing Systems. 2018.
- [3] BOWYER K W, DOYLE J S. Cosmetic contact lenses and IRIS recognition spoofing[J]. Computer, 2014, 47(5): 96-98.
- [4] ERDOGMUS N, MARCEL S. Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect[C]//Proc IEEE 6th Int Conf Biometrics Theory Appl Syst. 2013.
- [5] RUIZ-ALBACETE V, TOME-GONZALEZ P, ALONSO-FERNANDEZ F, et al. Direct attacks using fake images in IRIS verification[C]//Proc 1st Eur Workshop Biometrics Identity Manage. 2008.
- [6] KIBRET B, TESHOME A K, LAI D T, et al. Analysis of the human body as an antenna for wireless implant communication[J]. IEEE Transactions on Antennas and Propagation, 2016, 64(4): 1466-1476.
- [7] ARAI N, SASAKI K, MURAMATSU D, et al. Variation of impedance in transmission channel of human body communication[C]//International Symposium on Medical Information and Communication Technology. 2017: 49-53.
- [8] SHAHRIAR H, HADDAD H M, ISLAM M, et al. An iris-based authentication framework to prevent presentation attacks[C]//Computer Software and Applications Conference. 2017: 504-509.
- [9] MIRMOGAMADSADEGHI L, DRYGAJLO A. Palm vein recognition with local binary patterns and local derivative patterns[C]//International Joint Conference on Biometrics. 2011.
- [10] MIURA N, NAGASAKA A, MIYATAKE T. Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification[J]. Systems & Computers in Japan, 2004, 35(7): 61-71.
- [11] ARORA P, SRIVASTAVA S, HANMANDLU M, et al. Robust authentication using dorsal hand vein images[J]. IEEE Intelligent Systems, 2019, 34(2): 25-35.
- [12] BOLES A, RAD P. Voice biometrics: deep learning-based voiceprint authentication system[C]//Service Oriented Software Engineering. 2017: 1-6.
- [13] REN Y, FANG Z, LIU D, et al. Replay attack detection based on distortion by loudspeaker for voice authentication[J]. Multimedia Tools and Applications, 2019, 78(7): 8383-8396.
- [14] YANG Y F, GUO B, WANG Z, et al. BehaveSense: continuous authentication for security-sensitive mobile Apps using behavioral biometrics[J]. Ad Hoc Networks, 2019, 84: 9-18.
- [15] MUSALE P, BAEK D, WERELLAGAMA N, et al. You walk, we authenticate: lightweight seamless authentication based on gait in wearable IoT systems[J]. IEEE Access, 2019: 37883-37895.
- [16] WANG Y X, CHEN Y N, BHUIYAN M Z A, et al. Gait-based human identification using acoustic sensor and deep neural network[J]. Future Generation Computer Systems, 2018, 86: 1228-1237.
- [17] ZENG Y, PATHAK P H, MOHAPATRA P, et al. WiWho: wifi-based person identification in smart spaces[C]//Information Processing in Sensor networks, IPSN. 2016.
- [18] ZHANG J, WEI B, HU W, et al. Wi-Fi-ID: human identification using Wi-Fi signal[C]//Distributed Computing in Sensor systems, DCOSS. 2016.
- [19] KONG H, LU L, YU J, et al. Finger pass: finger gesture-based continuous user authentication for smart homes using commodity Wi-Fi[C]//International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc. 2019.
- [20] LIN F, SONG C, ZHUANG Y, et al. Cardiac scan: A non-contact and continuous heart-based user authentication system[C]//IEEE International Conference on Mobile Computing and Networking. 2017.
- [21] CHAUHAN J, SENEVIRATNE S, HU Y, et al. Breathing-based authentication on resource-constrained IoT devices using recurrent neural networks[J]. IEEE Computer, 2018, 51(5): 60-67.
- [22] ZHANG L, TAN S, YANG J. Hearing your voice is not enough: an articulatory gesture based liveness detection for voice authentication[C]//ACM Conference on Computer and Communications Security, CCS. 2017.
- [23] OH S, YANG J, BIANCHI A, et al. Devil in a box: installing backdoors in electronic door locks[C]//Conference on Privacy Security and Trust, 2015: 139-144.
- [24] ZHAO C, LI Z, LIU T, et al. RF-Mehndi: a fingertip profiled RF identifier[C]//International Conference on Computer Communications, INFOCOM. 2019.
- [25] HAN J S, QIAN C, WANG X, et al. Twins: device-free object tracking using passive tags[C]//International Conference on Computer Communications, INFOCOM. 2014.

[26] DING H, HAN J S, QIAN C, et al. Trio: utilizing tag interference for refined localization of passive RFID[C]//International Conference on Computer Communications, INFOCOM. 2018.

[27] LI P, AN Z L, YANG L, et al. Towards physical-layer vibration sensing with RFIDs[C]//IEEE Conference on Computer Communications, INFOCOM. 2019.



曲宇航（1996-），男，陕西西安人，西安交通大学硕士生，主要研究方向为移动计算、RFID。

[作者简介]



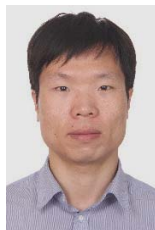
邹祥（1992-），男，陕西西安人，西安交通大学博士生，主要研究方向为移动计算、物联网安全。



肖剑（1975-），男，甘肃庆阳人，长安大学副教授，主要研究方向为智能感知与系统。



韩劲松（1975-），男，山东泰安人，浙江大学教授、博士生导师，主要研究方向为物联网安全。



许贤（1981-），男，浙江杭州人，浙江大学教授、博士生导师，主要研究方向为建筑结构智能监测。