

基于蓝牙与密码双模态认证的智能电动车锁系统设计 及安全性研究

陶佳波 应兴聪 刘昌贵 梁志华 李裕华 郑海华
浙江豪钿科技有限公司 318050

【摘要】随着智能交通的快速发展,电动车锁作为保障车辆安全的关键部件,其安全性和便捷性成为了用户关注的焦点。传统的机械锁由于易被破坏,已难以满足现代安全需求。而单一认证方式的智能锁,如纯蓝牙锁或密码锁,虽在一定程度上提升了安全性,但仍存在各自的局限性。因此,本研究提出了一种基于蓝牙与密码双模态认证的智能电动车锁系统,旨在通过集成蓝牙近场通信与动态密码验证技术,实现高安全性与用户友好性的完美平衡。系统硬件以MCU模块为核心,结合旋钮开关、双检测模块及双色灯珠状态指示,软件层面则设计了多模式切换逻辑与加密通信协议。通过一系列严格的测试与分析,验证了该系统的安全性与实用性。工程案例表明,该系统在共享电动车场景中显著降低了非授权开锁事件,同时保持了极低的误操作率。本研究为智能电动车锁的可靠性与安全性提升提供了坚实的理论与技术支撑。

【关键词】智能电动车锁;双模态认证;蓝牙解锁;密码验证;安全性分析;MCU模块

Design and security study of intelligent electric vehicle lock system based on Bluetooth and password dual-mode authentication

Tao Jiabo Ying Xingcong Liu Changgui Liang Zhihua Li Yuhua Zheng Haihua
Zhejiang Haodian Technology Co., LTD. 318050

【Abstract】 With the rapid development of intelligent transportation, electric vehicle locks, as key components to ensure vehicle safety, have become a focal point for users due to their safety and convenience. Traditional mechanical locks, being easily tampered with, can no longer meet modern safety requirements. Single-authentication methods, such as pure Bluetooth locks or password locks, while enhancing security to some extent, still have their limitations. Therefore, this study proposes an intelligent electric vehicle lock system based on dual-mode authentication using Bluetooth and passwords. The aim is to achieve a perfect balance between high security and user-friendliness by integrating Bluetooth near-field communication and dynamic password verification technologies. The system's hardware is centered around an MCU module, combined with a rotary switch, dual detection modules, and dual-color LED status indicators. On the software side, it features multi-mode switching logic and encrypted communication protocols. Through rigorous testing and analysis, the system's security and practicality have been verified. Engineering cases show that the system significantly reduces unauthorized unlocking incidents in shared electric vehicle scenarios while maintaining an extremely low error rate. This research provides solid theoretical and technical support for enhancing the reliability and security of intelligent electric vehicle locks.

【Key words】 intelligent electric vehicle lock; dual-mode authentication; Bluetooth unlock; password verification; security analysis; MCU module

1.引言

1.1 研究背景

电动车作为城市短途出行的首选工具,其便捷性和经济性得到了广大用户的认可。然而,随着电动车数量的激增,防盗问题也日益突出。传统机械锁由于结构简单,易被不法分子利用工具破坏,导致车辆被盗。而智能锁虽然在一定程度上提升了安全性,但单一认证方式仍存在安全隐患。例如,纯蓝牙锁虽然操作便捷,但蓝牙信号易被截获和重放,存在被远程攻击的风险;而密码锁虽然安全性较高,但静态密码易被窥视或通过暴力破解方式获取。因此,如何结合多种认证方式,设计出一种既安全又便捷的智能电动车锁系统,成为了当前研究的热点。

1.2 研究现状

目前,智能锁技术已经取得了显著的发展,并广泛应用于各个领域。在电动车锁领域,主要出现了蓝牙/NFC解锁、生物识别解锁以及动态密码解锁等方式。蓝牙/NFC解锁依赖近场通信技术,具有操作便捷的优点,用户只需将设备靠近电动车锁即可实现解锁。然而,这种解锁方式存在信号被劫持的风险,一旦蓝牙信号被不法分子截获,即可实现远程开锁。生物识别解锁如指纹或人脸识别,具有较高的安全性,因为每个人的生物特征都是独一无二的。但这种方式成本较高,且易受环境干扰,如手指湿润、面部遮挡等都可能影响解锁效果。动态密码解锁需要依赖网络支持,通过生成随时间变化的密码来提高安全性。但这种方式稳定性不足,且存在一定的操作复杂性,用户需要记住并输入不断变化的密码。

双模态认证作为一种结合多种认证方式的技术,可以弥补单一认证模式的缺陷,提高系统的整体安全性。双模态认证要求用户同时满足两种或多种认证条件才能实现解锁,从而大大提高了系统的安全性。然而,目前双模态认证的研究多集中于门禁系统、金融支付等领域,在电动车锁领域的应用较少。因此,本研究旨在设计一种基于蓝牙与密码双模态认证的智能电动车锁系统,以提高电动车的安全性。

1.3 研究目标

针对现有智能电动车锁存在的问题,本研究旨在设计一种基于蓝牙与密码双模态认证的智能电动车锁系统。具体目标包括:设计一种支持蓝牙与密码双模态认证的智能电动车锁硬件架构,该架构应具有较高的安全性和稳定性;提出基于场景自适应的认证模式切换策略,以实现不同场景下的灵活应用,如用户靠近电动车时自动切换为蓝牙模式,远离时切换为密码模式;通过实验测试与案例分析,验证系统的安全性及实用性,包括抗干扰能力、物理攻击防护能力、数据安全机制等;为智能电动车锁的推广与应用提供理论与技术支撑,推动电动车锁技术的进一步发展。

2.系统设计

2.1 硬件架构设计

本系统硬件架构主要由锁体、MCU 模块、旋钮开关、双检测模块、电子开关模块、双色灯珠、降压供电模块以及信号传输模块等组成。各模块之间通过电路连接,共同实现智能电动车锁的功能。

锁体是系统的外壳,负责保护内部电路和机械结构。本研究采用了 304 不锈钢外壳,以提高锁体的结构强度和抗破坏能力。304 不锈钢具有较高的硬度和耐腐蚀性,能够有效抵抗不法分子的物理破坏。

MCU 模块是系统的核心部件,负责信号处理与逻辑控制。MCU 模块接收来自旋钮开关、双检测模块等的信号,根据预设的逻辑进行处理,并控制电子开关模块的通断,实现解锁或锁定功能。同时,MCU 模块还负责与中控仪表进行通信,显示蓝牙连接状态及密码输入界面。

旋钮开关是双模态认证的重要组成部分,用于触发认证模式的选择和确认用户的操作意图。用户通过旋转旋钮开关来选择蓝牙模式或密码模式,并通过按压旋钮开关来确认解锁操作。

双检测模块用于检测用户操作意图的准确性和完整性。第一检测模块检测旋钮开关的位置切换,以触发模式选择。第二检测模块检测旋钮轴向的按压操作,以确认用户的解锁意图。双检测模块的设计可以有效防止误操作或恶意攻击。

电子开关模块控制电路的通断,实现解锁或锁定功能。电子开关模块由 MOS 管与三极管组成,具有较高的稳定性和可靠性。同时,电子开关模块还内置了过压保护电路,以防止短路攻击对系统造成损害。

双色灯珠用于显示系统状态,包括认证成功、认证失败、异常状态等。蓝色灯珠亮起表示认证成功,操作就绪;红色灯珠亮起表示认证失败或异常状态,提醒用户注意。

降压供电模块为 MCU 模块提供稳定的工作电压。由于电动车锁的供电环境较为复杂,电压波动较大,因此降压供电模块的设计具有重要意义。降压供电模块能够将不稳定的输入电压转换为稳定的输出电压,确保 MCU 模块的正常工作。

信号传输模块负责与中控仪表进行通信,显示蓝牙连接状态及密码输入界面。信号传输模块采用无线通信技术,如蓝牙或 Zigbee 等,实现与中控仪表的数据传输。用户可以通过中控仪表查看蓝牙连接状态、输入密码等操作。

2.2 软件逻辑设计

系统软件逻辑设计主要包括模式选择、信号检测、认证执行以及状态反馈等步骤。具体流程如下:

(1) 模式选择: MCU 模块根据蓝牙绑定状态自动切换出厂模式、蓝牙模式或密码模式。在出厂模式下,系统默认处于未绑定状态,用户需要通过特定操作进入蓝牙或密码绑定流程。在蓝牙模式下,用户需要保持设备与中控仪表的蓝牙连接,通过旋钮开关触发解锁操作。在密码模式下,用户需要在无蓝牙连接的情况下,通过旋钮开关触发密码输入界面,输入正确的动态密码后解锁。

(2) 信号检测: 系统通过第一检测模块检测旋钮开关的位置切换,以触发模式选择。当用户旋转旋钮开关时,第一检测模块检测到信号并发送给 MCU 模块。MCU 模块根据信号判断用户选择的认证模式,并切换到相应的模式。同时,系统通过第二检测模块检测旋钮轴向的按压操作,以确认用户的操作意图。当用户按压旋钮开关时,第二检测模块检测到信号并发送给 MCU 模块。MCU 模块根据信号判断用户的解锁意图,并控制电子开关模块的通断实现解锁或锁定功能。

(3) 认证执行: 在蓝牙模式下,系统需要验证设备与中控仪表的蓝牙连接状态以及旋钮开关的触发信号。当用户靠近电动车并触发解锁操作时,系统首先检查蓝牙连接状态。如果蓝牙连接正常且信号稳定,则系统继续检查旋钮开关的触发信号。如果旋钮开关被正确按压且信号有效,则系统控制电子开关模块通断实现解锁功能。在密码模式下,系统需要验证用户输入的动态密码是否正确。当用户触发密码输入界面并输入密码时,系统接收密码并对其进行验证。动态密码基于时间同步算法(TOTP)生成,每分钟更新一次6位密码。系统通过比较用户输入的密码与生成的动态密码是否一致来判断认证是否成功。如果密码一致,则系统控制电子开关模块通断实现解锁功能;如果密码不一致,则系统显示认证失败并提示用户重新输入密码。

(4) 状态反馈: 系统通过双色灯珠实时显示认证结果。在认证成功时,蓝色灯珠亮起表示操作就绪;在认证失败或异常状态下,红色灯珠亮起提示用户。同时,中控仪表会记录用户的操作日志,包括认证时间、认证模式、认证结果等信息。这些日志信息可以用于后续查询和分析,帮助用户了解系统的使用情况并发现潜在的安全问题。

3.安全性分析

3.1 抗干扰能力测试

为了验证系统的抗干扰能力,本研究进行了蓝牙信号抗截获测试和密码防暴力破解测试。在蓝牙信号抗截获测试中,系统采用了 AES-128 加密通信协议,实测在 10 米外的信号强度衰减至-70dBm 以下,无法有效解析数据包。这表明系统具有较高的蓝牙信号抗截获能力。在密码防暴力破解测试中,系统设置了输入错误 3 次后锁定 5 分钟的机制,并触发 MCU 报警机制。这有效防止了不法分子通过暴力破解方式获取密码。

3.2 物理攻击防护

为了抵御物理攻击,本研究在锁体结构强度和电子开关防护方面进行了优化设计。锁体采用 304 不锈钢外壳,具有较高的结构强度和抗破坏能力。经过实测,锁体能够抵抗液压剪 15kN 的剪切力,有效防止了不法分子通过物理破坏方式打开锁具。在电子开关防护方面,系统内置了过压保护电路,防止了短路攻击对系统造成损害。

3.3 数据安全机制

为了保障数据安全,本研究在动态密码生成和中控仪表加密方面进行了优化设计。动态密码基于时间同步算法(TOTP)生成,每分钟更新一次 6 位密码。这提高了密码的复杂性和随机性,有效防止了静态密码被窥视或通过暴力破解方式获取的风险。同时,中控仪表的操作日志通过 SHA-256 哈希算法进行存储,防止了日志数据被篡改或伪造的风险。

4.工程应用案例

4.1 应用场景

为了验证本研究的可行性和实用性,本研究选择了一家共享电动车企业在杭州市进行工程应用案例部署。该企业选择了景区与地铁站周边等高人流量区域作为试点区域,共部署了 2000 套本系统。这些区域电动车使用频率高且人员流动性大,对电动车锁的安全性和便捷性要求较高。

4.2 实施效果

经过 6 个月的实地运行和测试,本系统取得了显著的实施效果。在安全性方面,系统成功抵御了多次非授权开锁尝试,非授权开锁事件的发生率下降了 90% 以上。同时,系统具有较高的抗干扰能力和物理攻击防护能力,有效防止了不法分子的恶意攻击。在用户体验方面,系统平均解锁时间仅为 2.1 秒,大大提高了用户的便捷性和满意度。用户满意度

评分为 4.8/5.0,表明系统得到了用户的广泛认可和好评。在维护成本方面,系统支持远程固件升级功能,减少了现场维护的频率和成本。据统计,年度维护成本降低了 35% 以上。

4.3 问题与改进

尽管本系统取得了显著的实施效果,但在实际应用过程中仍存在一些需要改进的问题。首先,在极端环境下系统的适应性有待提高。例如,在-20℃的低温环境下,蓝牙连接延迟增加,影响了用户的解锁体验。为了解决这个问题,后续版本将优化射频电路的设计,提高系统在低温环境下的连接稳定性和可靠性。其次,在密码输入效率方面存在不足。部分老年用户反映密码输入步骤繁琐且易出错。为了解决这个问题,计划增加语音辅助功能,通过语音提示用户输入密码的步骤和结果,提高系统的易用性和用户体验。

5.结论与展望

5.1 结论

本研究提出了一种基于蓝牙与密码双模态认证的智能电动车锁系统,通过集成蓝牙近场通信与动态密码验证技术,实现了高安全性与用户友好性的平衡。系统硬件以 MCU 模块为核心,结合旋钮开关、双检测模块及双色灯珠状态指示等部件,实现了灵活的操作控制和状态显示。软件层面设计了多模式切换逻辑与加密通信协议,提高了系统的安全性和稳定性。通过抗干扰测试、暴力破解模拟及数据加密分析等一系列严格的测试与分析,验证了系统的安全性和实用性。工程应用案例表明,该系统在共享电动车场景中取得了显著的实施效果,降低了非授权开锁事件的发生率,提高了用户的便捷性和满意度,降低了维护成本。

5.2 未来工作

为了进一步完善本系统并拓展其应用范围,未来的研究工作将主要集中在以下几个方面:一是集成生物识别技术实现三模态认证。通过增加指纹识别或人脸识别等生物识别方式,进一步提高系统的安全性和便捷性。二是探索区块链技术用于分布式密钥管理。利用区块链技术的去中心化和不可篡改性等特点,实现密钥的安全存储和管理。三是优化低功耗设计以延长电池寿命。通过优化系统的电源管理和信号处理算法等措施,降低系统的功耗并延长电池的使用寿命。这些研究工作的实施将进一步推动智能电动车锁技术的发展和

参考文献

- [1]高涵,尹圆圆,赵世勇,等.电动车智能防盗锁装置[J].中国新通信,2019,21(22):130.DOI:10.3969/j.issn.1673-4866.2019.22.110.
- [2]王慧媛,张宝文.基于RFID和手机蓝牙的电动车数字化智能防盗锁[J].中国新通信,2016(2):144-144.DOI:10.3969/j.issn.1673-4866.2016.02.116.
- [3]王明亮.电动车智能锁[J].五金科技,2007,35(3):45.
- [4]杜润秋,陈苇娜.利用RFID技术的智能防盗电动车设计方案探讨[J].科技经济导刊,2016(1):108,75.