Original Article
ISSN (Online): 2350-0530
ISSN (Print): 2394-3629

International Journal of Research - GRANTHAALAYAH
March 2025 13(3), 337–342

DESIGN AND IMPLEMENTATION OF RADIO-CONTROLLED CAR LOCK SYSTEM

Asif Abbas [1], Deepak Kumar [1], Vipul Narayan[1]

[1] Computer Science and Engineering Department, Galgotias University, Greater Noida, India

Received 25 February 2025
Accepted 28 March 2025
Published 17 April 2025

Corresponding Author
Asif Abbas, 14asifcr7@gmail.com

DOI
10.29121/granthaalayah.v13.i3.2025.6056

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

With the increasing incidents of vehicle theft, tradi- tional security systems have proven inadequate in countering modern-day threats. This paper presents a radio-controlled car locking system that enhances vehicle security using ad- vanced technological measures. The proposed system features radio-controlled locking mechanisms, encrypted communication, backup power solutions, and real-time alerts. These features provide an effective security solution that balances both conve- nience and safety. Additionally, the system is designed to integrate seamlessly with modern vehicle security protocols, providing a comprehensive approach to theft prevention.

Keywords: Vehicle Security, Radio-Controlled Lock, Theft Prevention, Real-Time Alerts, Encryption, Rolling Code Technol- Ogy

1. INTRODUCTION

Vehicle theft has emerged as a significant concern in urban areas, with traditional security mechanisms failing to provide adequate protection against sophisticated theft techniques. Ex- isting vehicle security systems often rely on mechanical locks, alarms, and GPS tracking, which are either easily bypassed or reactive rather than preventive Jones et al. (2017).

This research focuses on the design and implementation of a radio-controlled car locking system that addresses these vul- nerabilities. The proposed solution integrates radio-frequency identification (RFID), rolling code encryption, and real-time monitoring to provide a robust security mechanism. By em- ploying encrypted signal transmission and real-time alerts, the system ensures that unauthorized access is promptly detected and prevented.

2. BACKGROUND

The rise in vehicle theft cases has prompted the development of advanced security systems. Traditional methods such as me- chanical locks and basic alarm systems are no longer sufficient due to advancements in theft techniques. Modern vehicles require security solutions that are proactive and capable of thwarting sophisticated attacks Wang et al. (2015) Huang and Xu (2017).

Radio-controlled car locking systems have gained attention due to their convenience and effectiveness. These systems use radio frequency (RF) signals to remotely lock and unlock vehicles. However, the security of these systems is often compromised by signal interception and replay attacks. To address these issues, rolling code encryption and real-time monitoring have been proposed as effective countermeasures Smith and Patel (2019).

3. SYSTEM COMPONENTS

The proposed system consists of several key components:

- Central Control Unit: A microcontroller-based unit that processes incoming signals and controls the locking mechanism.
- RF Communication Module: Handles the transmission and reception of encrypted RF signals.
- Power Management Unit: Ensures uninterrupted opera- tion with a battery backup system.
- Mobile Application Interface: Allows users to monitor and control the system in real-time.
- Sensors and Actuators: Detects unauthorized access attempts and operates the locking mechanism Kumar and Jain (2020) Brown and Davis (2019).

4. METHODOLOGY

The proposed system follows an agile development ap- proach, incorporating iterative design, testing, and validation. The core components of the system include:

- Radio-Controlled Locking Mechanism: Uses encrypted RF signals to operate the vehicle lock remotely.
- Rolling Code Encryption: Implements dynamic codes to prevent replay attacks.
- Real-Time Alerts: Sends instant notifications to the owner's mobile device upon unauthorized access at- tempts.
- Backup Power Solutions: Ensures continued operation during power failures.
- Integration with Existing Security Protocols: Enhances compatibility with contemporary vehicle security frame- works.

1) System Architecture

The system architecture consists of a central control unit, RF communication module, power management unit, and a mobile application interface. The central control unit is equipped with a microcontroller that processes incoming signals and commands the locking mechanism. The RF communication module handles the

transmission and reception of encrypted signals. The power management unit ensures that the system remains operational during power outages by switching to backup power sources. The mobile application interface allows users to monitor and control the locking system in real-time Lee and Kim (2020) Garcia and Martinez (2020).

2) Hardware Design

The hardware design involves selecting appropriate compo- nents for the central control unit, RF communication module, and power management unit. The central control unit uses a microcontroller with sufficient processing power and memory to handle encryption algorithms and signal processing. The RF communication module includes a transceiver that supports the required frequency range and communication protocols. The power management unit comprises a battery backup system and a power monitoring circuit to ensure uninterrupted operation Sharma and Kumar (2019) Rappaport et al. (2019).

3) Software Development

The software development process includes writing firmware for the microcontroller and developing the mobile application. The firmware is responsible for handling signal reception, encryption, and controlling the locking mechanism. The mobile application is developed using a cross-platform framework to ensure compatibility with both Android and iOS devices. The application provides a user-friendly interface for monitoring and controlling the locking system Mathew and Thomas (2018) Kim and Lee (2020) Zhang and Liu (2020).

4) Implementation

The implementation phase involved the development of the hardware and software components of the system. The hardware components were designed and assembled, followed by the development of the firmware for the microcontroller. The mobile application was developed using a cross-platform framework to ensure compatibility with both Android and iOS devices. Extensive testing was conducted to validate the functionality and reliability of the system under various scenarios.

1) Assembly and Integration: The hardware components were assembled and integrated into a single unit. The mi- crocontroller, RF communication module, and power manage- ment unit were connected according to the designed circuit. The sensors and actuators were also integrated into the system to detect unauthorized access attempts and operate the locking mechanism.
2) Firmware Development: The firmware was developed to handle signal reception, encryption, and control the locking mechanism. The rolling code encryption algorithm was imple- mented to generate dynamic codes for secure communication. The firmware was tested for reliability and efficiency in processing signals and controlling the locking mechanism.
3) Mobile Application Development: The mobile appli- cation was developed using a cross-platform framework to ensure compatibility with both Android and iOS devices. The application provides a user-friendly interface for monitoring and controlling the locking system. Features such as real- time alerts, system status monitoring, and remote control were implemented in the application.

5) Testing and Validation

The system was subjected to rigorous testing to evaluate its performance under different conditions. The testing phase included:

1) Signal Interference Testing: Ensuring the system's reliability in environments with high RF interference.
2) Encryption Robustness Testing: Assessing the re- silience of rolling code encryption against replay and brute force attacks.
3) Power Failure Simulation: Verifying the seamless tran- sition to backup power sources during power outages.
4) User Experience Testing: Gathering feedback from users on the usability and functionality of the mobile application and overall system.

The results from these tests were analyzed to identify any potential weaknesses and make necessary improvements to the system.

5. RESULTS AND DISCUSSION

The implementation of the proposed system was tested under various scenarios to evaluate its effectiveness. Results demonstrated a significant improvement in security, with en- crypted communication preventing unauthorized access at- tempts. Comparative analysis with traditional security systems highlighted the advantages of integrating rolling code encryp- tion and real-time monitoring.

1) Performance Evaluation

The system's performance was evaluated based on several criteria, including response time, reliability, and security. The response time of the system was measured from the moment a signal was sent to the time the locking mechanism was activated. The system demonstrated a quick response time, ensuring timely locking and unlocking of the vehicle.

The reliability of the system was tested by subjecting it to various environmental conditions, including high RF interference and power outages. The system maintained con- sistent performance, with the backup power solutions ensuring uninterrupted operation during power failures.

2) Security Analysis

The security analysis involved testing the system against various attack vectors, including signal hijacking, relay at- tacks, and brute force attempts. The rolling code encryption effectively mitigated replay attacks, while the encrypted RF communication ensured that signals could not be easily inter- cepted or duplicated. Real-time alerts provided an additional layer of security by notifying the vehicle owner of any unauthorized access attempts.

3) User Experience

User feedback was collected to evaluate the usability and convenience of the system. The mobile application interface was rated highly for its intuitive design and ease of use. Users appreciated the real-time alerts and the ability to control the locking mechanism remotely. The backup power solutions were also well-received, as they ensured uninterrupted opera- tion of the system.

4) Limitations and Future Work

While the proposed system offers significant improvements in vehicle security, there are some limitations that need to be addressed. The reliance on RF communication makes the system vulnerable to jamming attacks, which can disrupt the signal transmission. Additionally, the cost of implementing the system may be a barrier for widespread adoption.

Future work will focus on enhancing the system's resilience to jamming attacks by incorporating alternative communica- tion channels such as Bluetooth and Wi-Fi. Further research will also explore the integration of artificial intelligence (AI) for threat detection and blockchain technology for secure access control. These enhancements aim to provide a more robust and comprehensive security solution.

6. CONCLUSION

The study presents a radio-controlled car lock system that enhances vehicle security through encrypted RF communica- tion, rolling code technology, and real-time alert mechanisms. The proposed solution not only prevents unauthorized access but also reduces reliance on traditional security measures that are easily compromised. Future work will explore fur- ther enhancements, including AI-based threat detection and blockchain-based access control for improved security mea-sures.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

The authors would like to thank Galgotias University for providing the necessary resources and support to conduct this research. Special thanks to the faculty members who provided valuable insights and feedback during the development of the system.

REFERENCES

Brown, L., & Davis, D. (2019). RF Signal Security in Vehicle Access Systems. Ieee Transactions on Vehicular Technology, 68 (7), 6283-6292.

Garcia, P., & Martinez, N. (2020). AI-Based Threat Detection in Vehicle Security Systems. IEEE Access, 8, 146789-146800.

Huang, W., & Xu, Z. (2017). Security Analysis of Radio-Controlled Car Lock Systems. Journal of Network and Computer Applications, 98, 45-53.

Jones, A., Smith, B., & Roberts, C. (2017). Vehicle Theft: An Urban Epidemic. Journal of Criminal Justice, 45 (1), 34-45.

Kim, H., & Lee, J. (2020). Smart Security Solutions for Connected Vehicles. Internet of Things Journal, 7 (11), 10815-10828. https://doi.org/10.1109/JIOT.2020.3030522

Kumar, R., & Jain, M. (2020). Microcontroller-Based Remote Control Systems for Automotive Applications. Journal of Automation and Control Engineering, 8 (2), 76-83.

Lee, M., & Kim, S. (2020). Blockchain-Based Vehicle Security Systems. Journal of Information Security and Applications, 52, 1-10.

Mathew, A., & Thomas, S. (2018). Integration of Vehicle Automation and Security Protocols. IEEE Transactions on Intelligent Transportation Systems, 20 (12), 4562-4573.

Rappaport, T., Heath, R., & Daniels, R. (2019). RFID Advancements in Vehicle Security Systems. IEEE Communications Surveys & Tutorials, 21 (3), 2321-2345.

Sharma, K., & Kumar, V. (2019). Enhancing Vehicle Security with Bluetooth Technology. IEEE Communications Magazine, 57 (8), 62-67.

Smith, J., & Patel, A. (2019). Rolling Code Systems for Automotive Security. International Journal of Advanced Research in Electrical, Electronics, and Instrumentation Engineering, 8 (4), 1124-1130.

Wang, J., Liu, C., & Zhang, Y. (2015). Radio Frequency Identification (RFID) and Remote Keyless Entry Systems: A Review. Ieee Transactions on Consumer Electronics, 61 (2), 234-240.

Zhang, F., & Liu, X. (2020). Advanced Encryption Techniques for Vehicle Security. Ieee Transactions on Information Forensics and Security, 15, 3125-3138.