STM JOURNALS

Journal of
Telecommunication, Switching Systems and Networks

ISSN: 2454-6372
Volume 11, Issue 1, 2024
January–April
DOI (Journal): 10.37591/JoTSSN

http://engineeringjournals.stmjournals.in/index.php/JoTSSN/index

Research JoTSSN

Remote Keyless Entry Implementation Using CAN Protocol

J. Ravindra[1,*], P.V. Krishna Reddy[2], R. Upendra[2], N. Sunil Kumar[2]

Abstract

The coming of the Controlling Area Network (CAN) protocol has totally transformed the car industry, enabling smooth communication between various electronical control units (ECUs) within modern vehicles. Using this strong communication framework, our project centers on the execution of a Remote Keyless Entry (RKE) system, providing improved security and ease to vehicle owners. This project aims at designing and developing a complex RKE system employing the CAN protocol, which allows wireless entry to vehicles through coded signals. By amalgamating CAN-powered ECUs like the body control unit (BCU) and the key dongle, our solution promises reliable and secure communication between the key fob and the vehicle, making user interaction simpler. The suggested RKE system consists of two prime components: the key dongle and the vehicle's BCU. The key dongle dispatches coded signals to the BCU via the CAN bus, triggering keyless entry functions like locking, unlocking, and remote beginning. Through careful coding techniques and validation mechanisms, our system alleviates the danger of unauthorized access, securing the vehicle against theft or manipulation. Moreover, embedding the RKE system using the CAN protocol proposes scalability and intercommunication, enabling smooth integration with existing vehicle nets and future improvements. By complying with industry norms and best practices, our solution ensures compliance with a broad array of vehicle makes and manufacturers, thus enhancing its practicality and marketability. To sum up, the Remote Keyless Entry Implementation Using CAN Protocol project stands as a notable leap forward in automotive security and ease. By utilizing the power of the CAN protocol, our solution offers a strong, efficient, and user-friendly approach to remotely accessing vehicles, heralding a fresh age of clever and secure automotive systems.

Keywords: RKE, ECU, CAN communication, BCM, CAN cable, Arbitration, IVN Bed, CAN High and CAN Low.

***Author for Correspondence**
J. Ravindra
E-mail: ravindrajanga@gmail.com

[1]Assistant Professor, Department of Electronics and Electrical Engineering, Bapatla Engineering College, GBCRD, Mahatmajipuram, Bapatla, Andhra Pradesh, India.
[2]Research Scholar, Department of Electronics and Electrical Engineering, Bapatla Engineering College, GBCRD, Mahatmajipuram, Bapatla, Andhra Pradesh, India.

Received Date: May 12, 2024
Accepted Date: May 24, 2024
Published Date: June 04, 2024

Citation: J. Ravindra, P.V. Krishna Reddy, R. Upendra, N. Sunil Kumar. Remote Keyless Entry Implementation Using CAN Protocol. Journal of Telecommunication, Switching Systems and Networks. 2024; 11(1): 30–38p.

INTRODUCTION

In today's automotive landscape, the integration of advanced technologies has become paramount in enhancing both the security and convenience of vehicle operations. Among these technologies, the implementation of Remote Keyless Entry (RKE) systems stands out as a cornerstone in modern vehicle access solutions. The traditional mechanical key systems are gradually being replaced by sophisticated electronic counterparts, offering users seamless access to their vehicles with enhanced security features. Our project, "Remote Keyless Entry Implementation Using CAN Protocol," delves into this paradigm shift, recognizing the importance of leveraging the Controller Area Network (CAN)

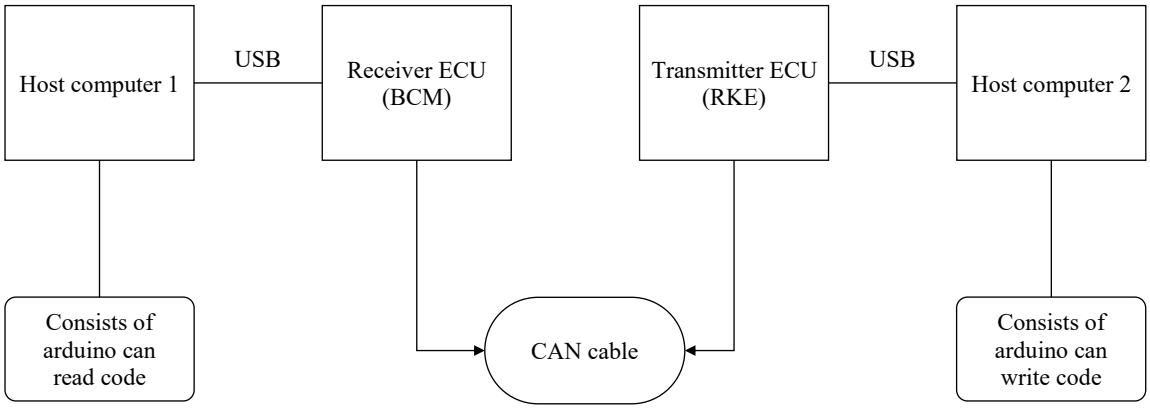

Figure 1. Block diagram of correction of overall hardware.

protocol to revolutionize the way vehicles are accessed and secured. By exploring the intricacies of CAN communication and its application in RKE systems, we aim to contribute to the advancement of automotive technology, offering users a more efficient, secure, and user-friendly means of accessing their vehicles remotely [1].

Furthermore, the widespread adoption of CAN protocol in automotive electronics underscores its significance as a robust and reliable communication standard. As vehicles become increasingly interconnected and reliant on electronic systems, the CAN protocol emerges as a fundamental framework for facilitating seamless communication between various electronic control units (ECUs) within the vehicle. Leveraging the inherent benefits of CAN, such as high reliability, low latency, and robust error handling, our project seeks to harness the full potential of this protocol to enhance the performance and security of RKE systems. By establishing a secure communication channel between the key fob and the vehicle's body control module (BCM), we can ensure that access commands are transmitted swiftly and securely, minimizing the risk of unauthorized access or interception [2].

Moreover, the integration of RKE systems using CAN protocol not only enhances vehicle security but also offers unparalleled convenience to users. Gone are the days of fumbling for keys or manually unlocking doors; with our system, users can remotely lock, unlock, and even start their vehicles with the press of a button on their key fob. This seamless integration of technology into everyday driving experiences epitomizes the evolution of automotive design, catering to the demands of modern consumers for connectivity, convenience, and safety. As we embark on this journey to redefine vehicle access mechanisms, we envision a future where RKE systems using CAN protocol become standard features in vehicles, ushering in a new era of smart and secure automotive solutions [3].

Here, this block diagram as shown in Figure 1 shows the connections of the overall hardware.

LITERATURE REVIEW

The reference project “On the Security of Remote Keyless Entry for Vehicles” significantly advances the understanding and enhancement of RKE system security. By dissecting challenge-response mechanisms, it offers critical insights into fortifying against potential threats such as relay attacks and signal spoofing, thereby bolstering the security of vehicles and occupants against unauthorized access or theft. However, while security remains paramount, our project “Remote Keyless Entry Implementation Using CAN Protocol” takes a slightly different angle by prioritizing safety features alongside implementation considerations. Our focus on safety aims to ensure not only the security but also the physical well-being of vehicle users, incorporating measures to prevent accidents and mitigate risks associated with remote entry functionalities. By integrating safety features seamlessly with RKE systems through the CAN protocol, our project contributes to advancing automotive technology in a holistic manner. [Patel, M. L. Das and S. Nandi *2018 IEEE*].

In juxtaposition to the security-centric approach of the reference project, our emphasis on safety underscores the multifaceted nature of modern automotive systems, where security and safety converge to provide comprehensive protection for both vehicles and their occupants. By meticulously engineering safety features into the implementation of RKE systems, we not only enhance the security posture but also mitigate potential risks associated with remote entry functionalities. This holistic approach aligns with the evolving landscape of automotive technology, where innovations in security and safety work synergistically to address the dynamic challenges of vehicle security and user protection [4-8].

By leveraging bidirectional communication, the system can establish a continuous exchange of data between the key fob and the vehicle, enabling real-time feedback and interaction. Furthermore, putting advanced authentication procedures in place adds security levels by guaranteeing that only people with permission can enter the car. While our project may not incorporate bidirectional communication or advanced authentication mechanisms as the referenced project does, it focuses on leveraging the efficiency and reliability of the CAN protocol for seamless integration of RKE functionalities within vehicles [Kinzig, Johannes. "Design and Implementation of a remote keyless entry system using state of the art bidirectional communication and authentication mechanisms" [9].

Both projects share the common goal of enhancing the functionality and security of remote keyless entry systems, albeit through different technological strategies. While the referenced project emphasizes bidirectional communication and advanced authentication mechanisms for robust security, our project prioritizes the utilization of the CAN protocol for efficient communication between components within the vehicle. Despite these differences, both projects contribute to the advancement of automotive technology by addressing key challenges in remote keyless entry implementation. By exploring distinct technological approaches, these projects offer valuable insights into the diverse methods available for enhancing the functionality, security, and integration of RKE systems within modern vehicles [10-14].

MAIN OBJECTIVE

In our project, "Remote Keyless Entry Implementation Using CAN Protocol," we have developed a comprehensive system that integrates remote keyless entry functionalities into vehicles through the efficient communication protocol known as the Controller Area Network (CAN). Our focus lies on implementing nine key functions crucial for modern vehicle security and convenience: lock, unlock, tailgate open, search, panic alarm, emergency unlocking, auto-lock, auto-unlock, and beep. These functions cater to various user needs, from basic security measures like locking and unlocking to additional features such as tailgate control and panic alarms for emergency situations.

The implementation revolves around two Electronic Control Units (ECUs): a receiver and a transmitter. The receiver ECU, installed within the vehicle, interfaces with the CAN bus to receive commands and data from the transmitter ECU. The transmitter ECU, typically integrated into a key fob or remote device, sends control signals and user inputs to the receiver ECU via the CAN bus. The user and the car may communicate seamlessly thanks to this bidirectional communication, which makes remote access safe and practical.

By leveraging the CAN protocol for communication between ECUs, our project ensures robust and reliable data transmission within the vehicle's network. The CAN cable serves as the physical connection between the transmitter and receiver ECUs, enabling efficient data exchange while maintaining compatibility with existing automotive infrastructure. Overall, our project represents a significant advancement in modernizing automotive systems, providing users with advanced features while maintaining reliability and security.

METHODOLOGY

CAN Protocol

A key component of contemporary automotive systems, the Controller Area Network (CAN) communication protocol allows for dependable and effective data interchange between Electronic Control Units (ECUs) inside automobiles. Designed initially by Bosch in the 1980s, CAN has since become the de facto standard for in-vehicle networking due to its robustness, scalability, and real-time capabilities. Unlike traditional point-to-point communication systems, CAN employs a multi-master, serial bus architecture, enabling multiple ECUs to communicate simultaneously without a central controller. For the demanding automotive environment, this decentralized strategy improves fault tolerance and system resilience.

CAN operates on a message-based communication model, where ECUs transmit data in the form of frames onto the bus. Each frame contains an identifier that prioritizes messages based on their importance, ensuring timely delivery of critical information. In order to preserve data integrity and dependability, CAN also offers error detection and correction techniques like cyclic redundancy check (CRC). With transmission speeds ranging from a few kilobits per second to several megabits per second, CAN accommodates various applications within vehicles, from simple sensor readings to high-speed control tasks.

Furthermore, CAN's versatility extends beyond automotive applications, finding utility in industries such as aerospace, industrial automation, and medical devices. Its widespread adoption and robust performance have solidified CAN as a foundational technology for enabling seamless communication and integration of complex systems. As automotive technology continues to evolve towards autonomous driving and connected vehicles, CAN remains instrumental in facilitating the convergence of electronics and mobility, ensuring vehicles operate safely, efficiently, and intelligently. Two Wired Communication is shown in Figure 2.

CAN arbitration as shown in Figure 3 is a fundamental aspect of the Controller Area Network (CAN) protocol that governs how multiple nodes on the bus compete for access to transmit their messages. In a CAN network, multiple nodes may attempt to transmit messages simultaneously. To prevent data corruption due to collisions, CAN uses a prioritization mechanism known as arbitration to determine which node has the right to transmit its message at any given time.

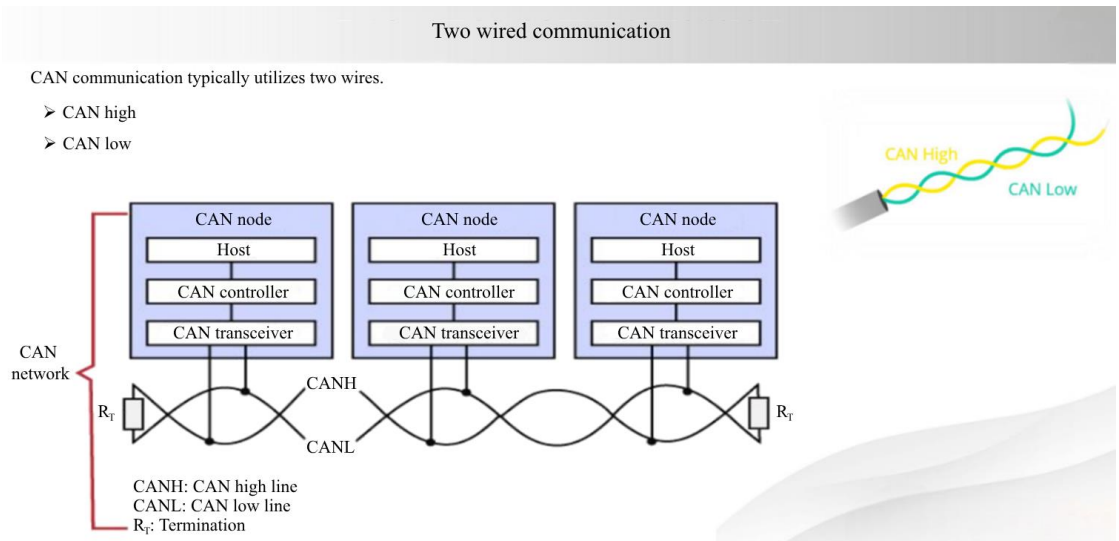

Figure 2. Two wired communication.

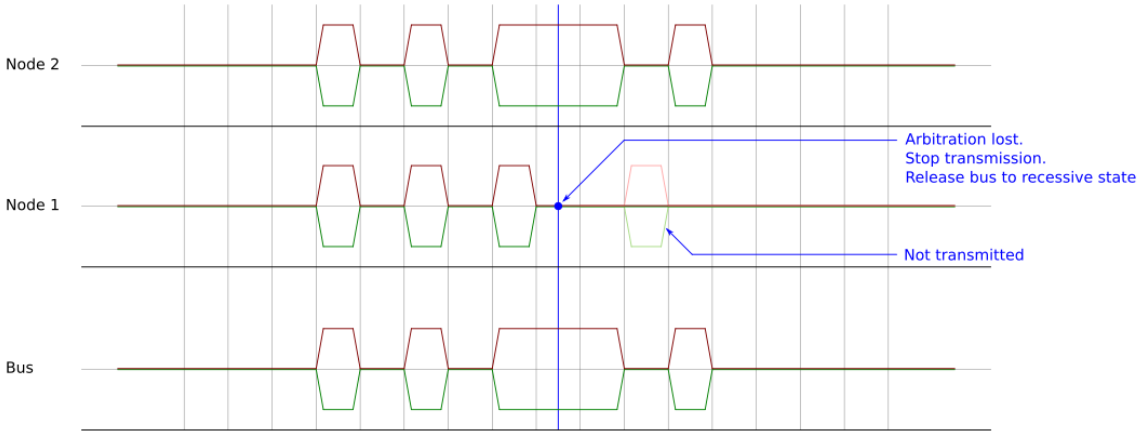

Figure 3. CAN arbitration.

Here's how CAN arbitration works:

1. *Message priority:* The CAN bus assigns a unique identity (ID) to every message. Higher priority communications are indicated by lower identifier number values. Accordingly, a message with a lower ID has a greater transmission priority.
2. *Bit-wise arbitration:* When multiple nodes try to send messages at the same time, they keep an eye on the bus to look for differences between the bits that are sent and received.. This is known as bit-wise arbitration. Nodes compare the bits they transmit with the bits they read from the bus.
3. *Dominant bits vs. Recessive bits:* A dominant bit (logic 0) in CAN takes precedence over a recessive bit (logic 1). Therefore, if a transmitting node detects a dominant bit on the bus while transmitting a recessive bit, it knows that another node with higher priority is attempting to transmit a message. The transmitting node then halts its transmission to allow the higher-priority message to be transmitted.
4. *Non-destructive arbitration:* CAN arbitration is non-destructive, meaning that the higher-priority message is transmitted successfully without corrupting the lower-priority message. This is achieved because the lower-priority message detects the dominant bit on the bus and stops transmitting.
5. *Priority-based access:* The message with the highest priority (lowest ID) is guaranteed to be the first to reach the bus and be transmitted thanks to the arbitration process. Lower-priority messages wait until the bus is idle before attempting to transmit again.

System Architecture

Figure 4 shows IN-VEHICLE TEST (IVN) BED The IVN Test Bed comprises six digital switches, six push buttons, eight analog switches, an ultrasonic sensor, an Arduino Mega 2560 Board connected to pin number 53, twelve LEDs, an LCD display, a buzzer, additional ports for integrating extra sensors, a DC motor, and a CAN cable connector.

CAN CABLE is seen in Figure 5. Because CAN is a serial, multimaster, multicast protocol, any node can transmit a message (multimaster) and any node can receive and act upon the message (multicast) while the bus is available. The transmitter is the node that sends the message, while the receiver is any node that does not send a message.

Figure 6 shows the connection diagram of the total hardware. This represents the block diagram we mentioned in the introduction.

Outputs

Figure 7 shows the output of lock function, whenever the lock pushbutton is pressed in the transmitter ecu (RKE) the receiver will receive the lock request from RKE and checks all the conditions mentioned if all the conditions are satisfied lock function will be enabled with a buzzer sound and led on indication.

Figure 4. IN-VEHICLE TEST(IVN) BEDS.

Figure 5. CAN cable.

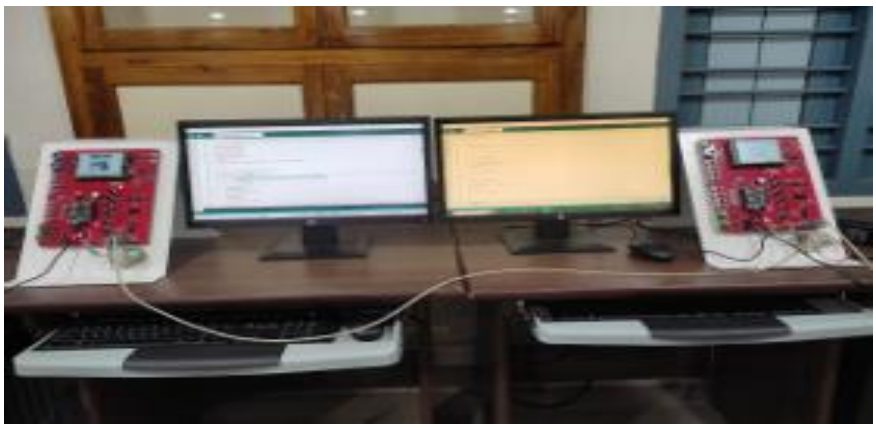

Figure 6. Connecting two IVN test bed using can cable.

Figure 7. Output of lock function.

Figure 8. Output of unlock function.

Figure 8 shows the output of unlock function, whenever the unlock pushbutton is pressed in the transmitter ecu (RKE) the receiver will receive the unlock request from RKE and checks all the conditions mentioned if all the conditions are satisfied unlock function will be enabled with a buzzer sound and led on indication.

Figure 9 shows the output of tailgate open function, whenever the Tailgate open pushbutton is pressed in the transmitter ecu (RKE) the receiver will receive the Tailgate open request from RKE and checks all the conditions mentioned if all the conditions are satisfied Tailgate open function will be enabled with a buzzer sound and led on indication.

Figure 10 shows the output of panic alarm function, whenever the unlock pushbutton is pressed in the transmitter ecu (RKE) the receiver will receive the panic alarm request from RKE and checks all the conditions mentioned if all the conditions are satisfied panic alarm function will be enabled with a buzzer sound and led on indication.

Figure 11 shows the output of beep function, The receiver will receive the unlock request from RKE and checks all the conditions mentioned if all the conditions are satisfied unlock function will be enabled with a buzzer sound and led on indication.

Figure 12 shows the output of the emergency unlock, whenever the Emergency pushbutton is pressed in the transmitter ecu (RKE) the receiver will receive the Emergency request from RKE and checks all the conditions mentioned if all the conditions are satisfied Emergency function will be enabled with a buzzer sound and led on indication.

Figure 9. Output of tailgate open function.

Figure 10. Output of panic alarm function.

Figure 11. Output of beep function.

Figure 12. Output of the emergency unlock.

Figure 13. Output of auto unclock function.

Figure 14. Output of auto lock function.

Figure 13 shows the output of auto unclock function, The receiver will receive the Auto unlock request from RKE and checks all the conditions mentioned if all the conditions are satisfied Auto unlock function will be enabled with a buzzer sound and led on indication.

Figure 14 shows the output of auto lock function, The receiver will receive the Auto lock request from RKE and checks all the conditions mentioned if all the conditions are satisfied Auto lock function will be enabled with a buzzer sound and led on indication.

Here transmitter was RKE and receiver was BCM (Body Control Module). CAN write code was implemented on transmitter (RKE) and CAN read code was implemented on receiver (BCM). We dumped the codes into in vehicle network test beds and connected them using a can cable. In this whenever we press push buttons in the transmitter ECU i.e. RKE function request will be transmitted from RKE and the receiver will receive the request and it will check the conditions if all the conditions are true it will give the output.

In this we get display outputs for eight functions. Those are lock, unlock, tailgate open, panic alarm, beep, emergency unlocking, auto lock, auto unlocking. The above images lock, unlock, tailgate open are basic functions of a car and next emergency unlocking, panic alarm are for emergency functions executed through transmitting the can message. The remaining three functions beep, auto lock, auto unlock are mainly for safety purpose which are executed through body control module itself and these three functions does not need any transmitter message for execution.

CONCLUSION

In conclusion, the implementation of remote keyless entry (RKE) using the Controller Area Network (CAN) protocol rep resents a significant advancement in automotive technology. Throughout this project, we successfully integrated RKE functionalities with the CAN protocol, leveraging its reliability, efficiency, and real time communication capabilities. Our project showcased the seamless communication between the remote key fob and the vehicle's control unit (VCU) via the CAN bus, enabling functionalities such as locking, unlocking, and starting the vehicle remotely. By utilizing Arduino Uno, Arduino Mega 2560 microcontrollers, and Top way SG Tools, we demonstrated the feasibility of implementing RKE systems with CAN protocol in a practical setting.

REFERENCES

1. A. I. Alrabady and S. M. Mahmud, "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs," IEEE transactions on vehicular technology, vol. 54, no. 1, pp. 41–50, 2005.

2. F. Bersani and H. Tschofenig, "The eap-psk protocol: A pre-shared key extensible authentication protocol (eap) method," Tech. Rep., 2007.
3. C. Böhm, M. Hofer, and W. Pribyl, "A microcontroller sram-puf," in 2011 5th International Conference on Network and System Security. IEEE, 2011, pp. 269–273.
4. N. T. Courtois, G. V. Bard, and D. Wagner, "Algebraic and slide attacks on keeloq," in Fast Software Encryption: 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers 15. Springer, 2008, pp. 97–115.
5. T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani, "On the power of power analysis in the real world: A complete break of the keeloq code hopping scheme," in Advances in Cryptology–CRYPTO 2008: 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings 28. Springer, 2008, pp. 203–220.
6. F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock it and still lose it—on the ({In) Security} of automotive remote keyless entry systems," in 25th USENIX security symposium (USENIX Security 16), 2016.
7. J.-R. Lin, T. Talty, and O. K. Tonguz, "On the potential of bluetooth low energy technology for vehicular applications," IEEE Communications Magazine, vol. 53, no. 1, pp. 267–275, 2015.
8. S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," ACM Transactions on Embedded Computing Systems (TECS), vol. 3, no. 3, pp. 461–491, 2004.
9. N. Semiconductor, "Nrf52832 product specification," Nordic Semiconductor, 2017.
10. P. Smith, "Comparing low-power wireless technologies," Tech Zone, Digikey Online Magazine, Digi-Key Corporation, vol. 701, 2011.
11. P. Štembera and M. Novotny, "Breaking hitag2 with reconfigurable hardware," in 2011 14th Euromicro Conference on Digital System Design. IEEE, 2011, pp. 558–563.
12. R. Verdult, F. D. Garcia, and B. Ege, "Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer," in Supplement to the Proceedings of 22nd USENIX Security Symposium (Supplement to USENIX Security 15), 2015, pp. 703–718.
13. J. Patel, M. L. Das and S. Nandi, "On the Security of Remote Key Less Entry for Vehicles," *2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Indore, India, 2018, pp. 1-6, doi: 10.1109/ANTS.2018.8710105.
14. Kinzig, Johannes. "Design and Implementation of a remote keyless entry system using state of the art bidirectional communication and authentication mechanisms."

