

Automatic Vehicle Security System with Zigbee Keyless Entry Over CAN Network

Meenakshi R. Talwar¹, Nikhil A. Kulkarni²

¹, Student of Electronics and Communication Engineering, College of KLS VEDIT Haliyal- 581 329, Visvesvaraya Technological University, Jnana Sangama, Belagavi – 590 018, KARNATAKA, INDIA.

², Assistant Professor, Department of Electronics and Communication Engineering, College of KLS VEDIT Haliyal- 581 329, Visvesvaraya Technological University, Jnana Sangama, Belagavi – 590 018, KARNATAKA, INDIA.

ABSTRACT:

The proposed work includes integration of ZigBee Keyless entry system with Controller Area Network (CAN) in vehicles. ZigBee offers wireless Keyless access, while CAN serves as the vehicle's communication backbone. This combination enhances convenience and security of vehicle. This allows security estimate averse to unauthorized access users advanced features while ensuring robust protection. Through meticulous examination, it underscores the feasibility and benefits of this integration, heralding a new era of sophisticated, secure vehicle access and operation in the automotive industry. Through careful analysis, it demonstrates that this integration is both feasible and advantageous, so ushering in a new era of sophisticated and secure vehicle access and operation within automobile industry.

KEYWORDS: CAN protocol, Zigbee protocol, automatic vehicle security.

I. INTRODUCTION

ZigBee is an IEEE 802.15.4 based specification suite for lofty level connection protocol utilize to fabricate personal area network with squat power. Due to its open standard, affordable price, and energy efficient characteristics, it has become a highly desirable wireless connection solution. As a result, it is more satisfaction for required application with low data rates than other technologies. A great number of businesses have implemented intelligent vehicle management systems for high-security zones inside their organizations. Through the use of identification and verification, it grants limited access to cars on the premises, for automated system it is necessary to include a wireless solution that has a low cost. Identifying and authenticating cars that are travelling into such a location, a system that makes use of Zigbee wireless RF modules has been developed.

For each vehicle, the design includes a RF module, a gate side radio frequency (RF) module for gathering vehicle data and a central database listing every car that may interact via radio RF with the gate side module. The vehicular module contains the vehicle's data, including a unique serial number and a password input keypad. The gate side module is capable of functioning as an RF module reader and delivering verification results to individuals who are seated in the watchmen room. Additionally, it functions as a communicator between the respective vehicle modules and the central database. Information To improve convenience while also providing comprehensive protection against theft and unauthorized entry. One such solution that is gaining popularity is the combination of a keyless entry

mechanism that uses ZigBee technology and a Controller Area Network (CAN) that is installed inside of automobiles. This article aims to examine the design and execution of an autonomous vehicle security system that facilitates keyless access via the utilization ZigBee technology and is managed over the CAN network.



Figure 1. Door opening with Zigbee

The traditional dependence on physical keys for accessing and ignition of vehicles has been replaced by wireless alternatives, which provide customers with an unprecedented level of ease and flexibility. Because of its dependability, security features, and energy economy, ZigBee has emerged as a viable solution for keyless entry systems. It is very attainable for automobiles to accomplish seamless reporting between the key fob and the numerous electronic control units (ECUs) accountable for vital operations such as engine control, brakes, and powertrain management if ZigBee technology is integrated with the CAN network. By leveraging the power of wireless communication and implementing stringent security measures, automobile manufacturers are able to provide customers with a sophisticated but secure method of accessing and managing their vehicles. This allows the automotive industry to redefine the norms of convenience and safety that are now in place.

II. PROBLEM STATEMENT

As compared to the conventional door locking system existing in the vehicles. The proposed approach uses different microwave frequencies ranging up to 2.4GHz band, for door locking operation, and 40kbits per channel. Its control networks up to 65,536 nodes. Which in term is hard to generate and trace the duplicates for unauthorized access to operate the door of the vehicle. Generally, ZigBee keyless entry over CAN network is useful to find the actual problem.

III. OBJECTIVES

- **To generate a frequency up to 2.4GHz:** Every time a door opening of car, it brings about newer frequency, the older frequency will not match with recent one.
- **Intrusion detection:** Inform the owner. **Steering lock/ Wheel lock:** It is electronically controlled and activated automatically when car is parked, and Key is outside, or when the car is locked. Steering wheel will not lock if the ignition is on or the car is moving.

- **Automatic head lights:** According to ambient brightness, head lights are ON and OFF, with the help of sensors.
- **Automatic Petrol/Diesel pump:** It's a resourceful apparatus that automatically shuts off when the fuel tank is full.

IV.LITERATURE SURVEY

1. **“Wireless CAN adaptation for ZCU based ZigBee for efficient data transmission and data security”**, by Balaji K J, Manjunath H P, 2024. **Affiliated:** Continental Automotive CAE Conference – **Road to virtual world. Event: International Automotive CAE Conference- road to virtual world, e-ISSN:2688-3627**

This paper explores the integration of wireless control area network CAN technology with ZigBee protocol to efficiency of data transmission security in Zonal Control Unit. by combining ZigBee's with CAN reliability, aims to address challenges while robust security measures. The integration of CAN with ZigBee offers a promising solution to restrictions of traditional wired communication architecture. The adoption of this presents an innovative solution for achieving transmission of data efficiently.

2. **“IOP Conference Series: Earth, 2024- iopscience.iop.org”** by A Sarango, G Vasquez, R Torres-

This article introduces a communication model for vehicle-to-vehicle interactions, utilizing the ZigBee wireless communicational protocol. The implementation involves the creation of a sensor network were exchanged information with connected vehicles. The test result showed that prototype is feasible of reliably and efficiently data interchange between vehicles atop greater distance than 300 meters, with the ZigBee. In inclusion, the prototype was able to warn the driver of potential road hazards and possible collisions at intersections. The finding of this research project demonstrates the potential of ZigBee technology for the maturing of the system.

3. **“Research and Implementation of DM1 based on the J1939”** by Y. Wang L. Guo and T. Tang (2023), IEEE 3rd International Conference on ICCS- International Conference on Computer system, Qingdao, China,2023, pp.163-167.

DOI:10.1109/ICCS59700.2023.10335562.

The J1939 protocol is a communication protocol widely used in automotive electronic network. It supports real time closed loop control among electronics control system in the entire vehicle to be distributed. This paper focuses the overall structural characteristics of J1939 protocol.

Keywords: Protocols; Codes; Automotive electronics; Communication protocol; Storage structure.

4.**“An Automated Smart Centralized Vehicle Security System for controlling the vehicle Thefts/Hacking using IOT and Facial Recognition”** by M. Pathak, K.N. Mishra, S.P. Singh and A. Mishra (2023), 2023 International Conferences on

Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates,2023, pp. 516521.

DOI: 10.1109/ICCIKE58312.2023.1013176.

With the invention of many other features like key card entry that will unlock the car and ignition of the vehicle to start, no key requirements. The application software keeps track over vehicle. **Keywords:** Roads; Security; Vehicle theft; RFI, Face recognition, etc.

5. **“An Intelligent ZigBee algorithm for vehicle monitoring system using wireless sensor Networks”** by P. N. Mosana and T Muchenje

(2022),

International conference on Computational intelligence, NV, USA, 2022 pp.1700-1704.

DOI:10.1109/CSCI58124.2022.00302

WSN could be implemented sensory device for communication technology, home hospital, industrial areas, vehicles, etc. end to end of sensors is growing. When it comes to operating the LED lights of a vehicle, the LIN protocol is also used here. delay of packets, loss of packets, packets collision and bandwidth are some major issues experienced in wireless sensor technology. In this type of study ZigBee routing protocols are studied and analysed. High network latency is identified as one of the shortcomings of ZigBee tree routing protocol. This end-to-end delay of packets routed on tree topology. This study will purpose an algorithm that attempts to improve the original protocol. NTRP is an output of meeting ZTR algorithm. NS-2 simulator will be used to validate the algorithm.

Keywords: ISO; Computational modelling; ZigBee; Routing; WSN, Delays; Algorithms.

V. PROPOSED METHODOLOGY



Figure 2 Block Diagram of automatic vehicle system

The above fig 2 showcases the block diagram of comprehensive automated vehicle security system, and it includes Tx section and Rx section.

The Tx section contains the following part.

- **ZigBee Based key fob:** The system incorporates a ZigBee Keyless Entry System, allowing wireless communication between the vehicle and Key fob. It is a network associated Key using MAC sublayer. For security mechanism it uses 128 bits Keys. The most important network for security function is Key distribution.

The Rx section have the following parts.

- **ZigBee:** It acts as an interface between the Key fob and CAN NETWORK, enabling functions such as locking/unlocking doors and starting the engine.
- **CAN driver:** The security of communication is ensured through strong encryption algorithms and authentication mechanism. It is simple API (Application Program Interface).
- **Arduino UNO:** Additionally, the system features an Arduino controller, responsible for coordinating the overall operation, implementing access control policies, and interfacing with ZigBee gateway and other components.
- **Actuator/ Sensor:** We know that, this device is converting one form of energy to another form, the signals from the controller are actuated and together form a robust and efficient automated vehicle security system.

- **Door mechanism:** the main intension of this objective is to mitigating the threat of uncertified explosion or vehicle theft, if so, door will not open any way. Using ZigBee Keless fob the door open and closed, every time with opening of door ZigBee generated the newer frequencies, it will not match with older one. Seamlessly integrating various components to ensure robust functionality and security. At the core of the system lies the Controller Area Network (CAN) network, serving as the backbone for tied up electronic control units (ECUs) responsible for critical vehicle functions. The system incorporates a ZigBee Keyless Entry System, allowing wireless communication between the vehicle and a key fob. This system operates through a ZigBee Gateway, which acts as an interface between the key fob and the CAN network, enabling functions such as locking/unlocking doors and starting the engine. The security of communication is ensured through strong encryption algorithms and authentication mechanisms.

VI. RESULT and WORKING MODEL

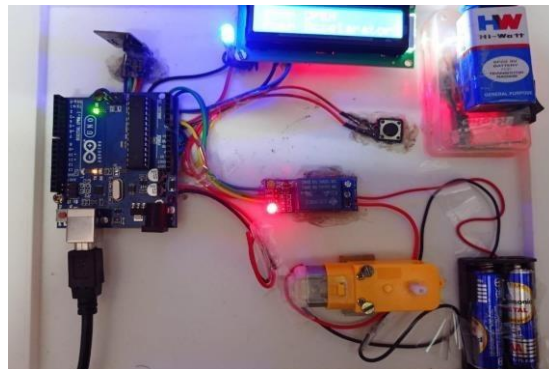


Figure 3 Working model for proposed system

Transceiver and accelerator position ECU:

ZigBee transceiver, accelerator and start switch flag the quickening position of ECU, through UART. The CAN correspondence convention is a CSMA/CA, it is message-based convention, colocation-based convention.

Driving wheel control ECU:

The wheel and driving wheel control ECU gets signal regarding advance qualities from units of other panel relies on the sign and motor wheel controlled by PWM.

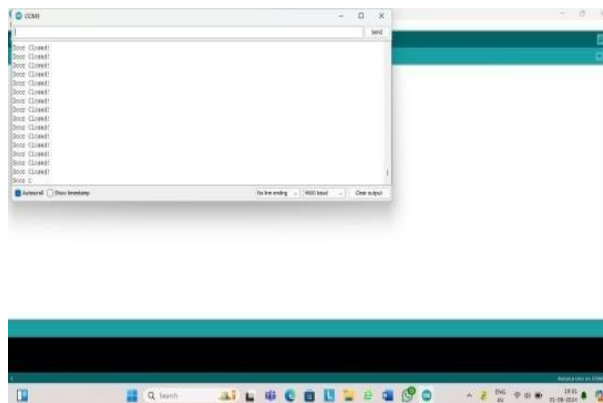


Figure 4 Output of the system during 'door closed', through Arduino.

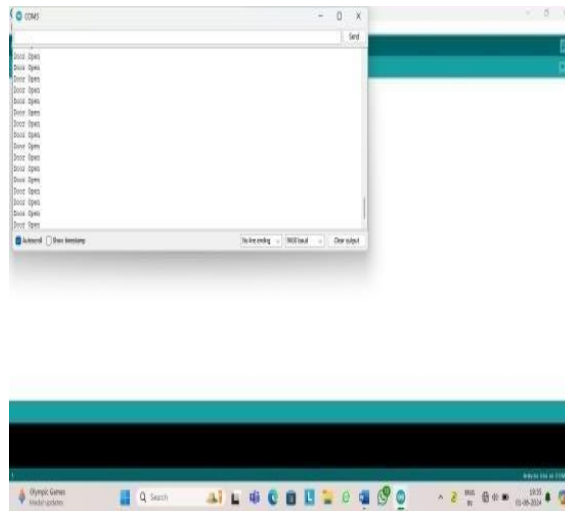


Figure 5 Output of the system during ‘door open’, through Arduino.

OPERATION

In normal vehicle security system having normal keys, you can regenerate that key with duplicate one, using this key the car door will be opened. These vehicles can generate the vehicle radio frequency from 433MHZ to 2.4GHZ, so you can catch this frequency easily. With Zigbee, the frequency band is 2.4GHZ, for every time remote unlocking, it generates the newer frequency, both Tx and Rx side, it contains the algorithm key nodes, you cannot trap the frequency it is called heimglizer effect. Like I2C/UART, in automobile industry CAN protocol introduced, because it’s have only 2 sets of wire CAN HIGH and CAN LOW, within 2 wires you may connect n-number of devices, I2C is master slave, if master sends any information’s the slave will understands and receive the information.

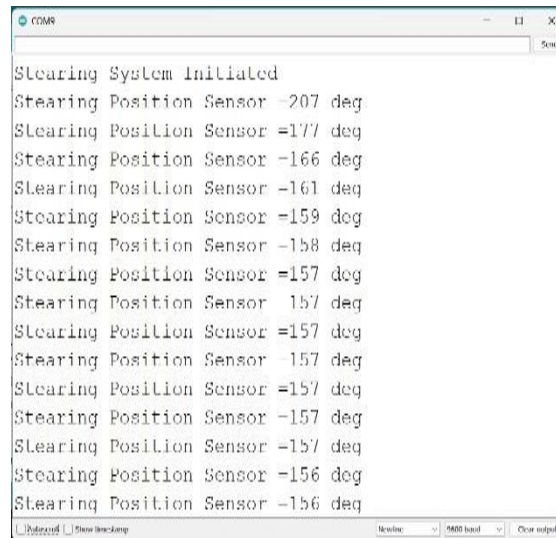


Figure 6 Output of the system, when door closed.



Figure 7 Output of the system, when door opened.

The fig 3 involves such a configuration, fig 4 and 5 illustrates the output of the system during ‘door close’ and ‘door open’ respectively through Arduino controller. The fig 6 and 7 shows door close and open by LCD. Fig 8 informs the steering position.



```

CGMR
Steering System Initiated
Steering Position Sensor =207 deg
Steering Position Sensor =177 deg
Steering Position Sensor =166 deg
Steering Position Sensor =161 deg
Steering Position Sensor =159 deg
Steering Position Sensor =158 deg
Steering Position Sensor =157 deg
Steering Position Sensor =157 deg
Steering Position Sensor =157 deg
Steering Position Sensor =157 deg
Steering Position Sensor =157 deg
Steering Position Sensor =157 deg
Steering Position Sensor =157 deg
Steering Position Sensor =157 deg
Steering Position Sensor =156 deg
Steering Position Sensor =156 deg
  
```

Figure 8 Steering position

In CAN all behaves like master and slave, in the CAN communication if ABS fails it uses the commander like I failed, CAN bus can have the address with ABS and raise the question about failure, whoever connect with CAN (any device) all are knows ABS is failed. In Master Slave this is not possible. In CAN all devices are independent and can raise the question and accept the question, but in Master Slave a particular device accepts and arise the question. In moving vehicle Electro Magnetic Noise (EMF) will be more, in normal I2C if noise generated it considered as bit, like normally high or low, it considers like a signal, it gives an error data, your sending data is different receiving data is different, for avoiding this we are used differential technology ZigBee, its only for communication. CAN is standard automobile protocol, one side is door lock system of car, another side looking like key but not physical key, normal cars having physical keys, if key pressed door will open, but in this system if the band is near to car the door will open, if the remote is within the range the door will close automatically. The signalling information can be visible with the help of Cathode Ray Oscilloscope for changing the frequency, how it communicates, and how 128 bits of CAN shared with frequency and how it is relocated with another frequency.

If any ECU fails, CAN controls the device and it's never failure, it retrieves the data. Each car has its own chassis number, according to this number the frequency will allocate. If thief arrives its zero chances to stolen the car, he doesn't have option to open the car, and immediately the message sent to the owner with the help of GSM.

VII. CONCLUSION

The integration of ZigBee Keyless entry systems with Controller Area Network appears for a significant advancement in automotive security and convenience. By leveraging ZigBee's energy efficient wireless protocol and robust service capabilities of the CAN network, vehicles can carry off seamless and settled access control. This turns up has outlined the system architecture and highlighted the Key components involved in administer ZigBee based Keyless entry over CAN network. As well, it has emphasized the momentousness of robust security measures to safeguard reporting in the middle of Key fobs, ZigBee gateways, and vehicle ECUs, ensuring protection against unauthorized access and malicious attacks. Through a thorough examination of the system design, surety protocols, and potential sake, this arrives s

has demonstrated the feasibility and advantages of adopting ZigBee Keyless entry systems integrated with CAN networks in modern vehicles. By harnessing the power of wireless communication and put into practice robust security measures, automotive manufactures can redefine the standards of convenience and safety in the industry. It offers consumers a sophisticated yet dependable means of accessing and operating their vehicle, enhancing the overall driving experience and paving the way for future evolution in automotive technology.

With the help of this system the proposed applications are implemented.

- Door open/close, with Keyless entry.
- Steering lock
- Automatic headlights.
- Automatic Petrol/ Diesel tank.

VIII. REFERENCES

1. “Wireless CAN adaptation for ZCU based ZigBee for efficient data transmission and data security.” By Balaji K J, Manjunath H P, 2024, Affiliated: Continental Automotive CAE Conference – Road to virtual world. Event: International Automotive CAE Conference- road to virtual world, eISSN:2688-3627
2. “IOP Conference Series: Earth, 2024iopscience.iop.org “by A Sarango, G Vasquez, R Torres-
3. “Research and Implementation of DM1 based on the J1939.” By Y. Wang L. Guo and T. Tang (2023), IEEE 3rd International Conference on ICCS- International Conference on Computer system, Qingdao, China,2023, pp.163-167. DOI:10.1109/ICCS59700.2023.10335562.
4. “An Automated Smart Centralized Vehicle Security System for controlling the vehicle Thefts/Hacking using IOT and Facial Recognition.” By M. Pathak, K.N. Mishra, S.P. Singh and A. Mishra (2023), 2023 International Conferences on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates,2023, pp. 516-521. DOI: 10.1109/ICCIKE58312.2023.1013176.
5. “An Intelligent ZigBee algorithm for vehicle monitoring system using wireless sensor Networks.” By P. N. Mosana and T Muchenje (2022), International conference on Computational intelligence, NV, USA, 2022 pp.1700-1704. DOI:10.1109/CSCI58124.2022.0
6. Rashidi, F. R. (2011).” Car monitoring using Bluetooth security system”. International Conference on Electrical, Control and Computer Engineering 2011 (InECCE), 424-428.
7. Hameed, S. a. (2010). “Car monitoring, alerting and tracking model”: Enhancement with mobility and database facilities. International Conference on Computer and Communication Engineering (ICCCE'10), 1- 5.
8. S. Padmapriya & Esther Annlin Kala James. (2012). “Real Time Smart Car Lock Security System Using Face Detection and Recognition”. International Conference on Computer Communication and Informatics.
9. K S Khangura, N V Middleton and M M Olivier, (1993). “Vehicle Antitheft System Uses Radio Frequency Identification”. IEE. Savoy Place, London, WC2R OBL, UK.
10. Zhixiong Liu and Guiming He, (2005). “A Vehicle Anti-theft and Alarm System Based on Computer Vision”.

11. N. M. Z. Hashim, A. S. Jaafar, N. A. Ali, L. Salahuddin, N. R. Mohamad, “Traffic Light Control System for Emergency Vehicles Using Radio Frequency”, IOSR Journal of Engineering (IOSRJEN) Vol. 3, Issue 7, pp 43-52, 2013
12. N. M. Z. Hashim, M. S. Sizali, “Wireless Patient Monitoring System”, International Journal of Science and Research (IJSR) Volume 2 Issue 8, pp 250-255, 2013.
13. N. M. Z. Hashim, N. A. Ali, A. S. Jaafar, N. R. Mohamad, L. Salahuddin, N. A. Ishak, “Smart Ordering System via Bluetooth”, International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7, pp. 2253-2256, 2013.
14. N. M. Z. Hashim, S. H. Husin, A. S. Ja’afar, N. A. A. Hamid, “Smart Wiper Control System”, International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2 Issue 7, pp. 409-415, 2013.
15. Y. Y. David Flowers, Kim Otten and N. Rajbharti. (2006, 12) Microchip stack for the zigbee protocol. Microchip Technology Inc. [Online]. Available: <http://www.microchip.com>
16. D. Flowers. (2006) Microcontroller Technology Inc. [Online]. Available: <http://www.microcontroller.com>
17. Microchip technology Inc, (2002), MPLAB C18 C COMPILER USER’S GUIDE.pdf.
18. Transfer Multisort Elektronik Company (1990), DISPLAY ELEKTRONIK DEM16217-SYH-LY - Display: LCD; alphanumeric; STN Positive; 16x2; LED; (84x44x8.5mm) Datasheet, pdf.
19. N. M. Z. Hashim, S. N. K. S. Mohamed, “Development of Student Information System”, International Journal of Science and Research (IJSR) Volume 2 Issue 8, pp 256-260, 2013.
20. N. M. Z. Hashim, N. A. M. M. Arifin, “Laboratory Inventory System”, International Journal of Science and Research (IJSR) Volume 2 Issue 8, pp 261-264, 2013.
21. Zigbee Specification, ZigBee Document 053474r06 Version 1.0, Zigbee Alliance Std., Dec. 2004.
22. Wheeler, “Commercial applications of wireless sensor networks using zigbee,” in Communications Magazine, IEEE, vol. 45, no. 4, Toronto, Ont., Canada, Apr. 2007, pp. 70–77.
23. N. Baker, “Zigbee and bluetooth strengths and weaknesses for industrial applications,” Computing & Control Engineering Journal, vol. 16, pp. 20– 25, Apr./May 2005.
24. P.J. Chitamu., (2012). “What is Zigbee,” Zigbee Alliance.
25. National Semiconductor, (2000), LM35 Precision Centigrade Temperature Sensors.