IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

INTRUSION DETECTION SYSTEM FOR VEHICULAR NETWORKS

Research Paper

Chaithra K, Bhoomika H S, Gowtham M, Harshith S, Poorvika H R

Department of Electronics and Communication Engineering

PES College of Engineering, Mandya, India

Abstract

The "Intrusion Detection System for Vehicular Networks" project focuses on improving the safety, reliability, and intelligence of modern transportation systems using IoT and embedded technologies. The system integrates ESP32 microcontrollers, MQTT communication protocol, infrared (IR) signaling, ultrasonic sensors, and motor control mechanisms to create a smart vehicular monitoring and intrusion detection framework. The proposed model enables real-time communication between traffic infrastructure and vehicles while continuously monitoring environmental conditions and vehicle behavior.

The Traffic Signal Unit publishes RED and GREEN traffic conditions through MQTT over WiFi and simultaneously transmits IR signals during RED conditions to provide a backup physical communication mechanism. The Vehicle Unit subscribes to MQTT topics, detects IR signals, monitors nearby obstacles using an HC-SR04 ultrasonic sensor, and controls vehicle movement through an L298N motor driver and DC motors. The system also includes GPS simulation for testing vehicle tracking and rotary encoder-based speed control for dynamic speed adjustment.

The implemented system successfully demonstrated real-time wireless communication, automatic vehicle stopping during RED signals, reliable obstacle detection, and collision prevention. By combining MQTT-based communication with IR-based verification, the system improves communication reliability even during network interruptions. The project validates the practical implementation of intrusion detection and intelligent traffic management within vehicular networks and provides a scalable foundation for future smart transportation and autonomous vehicle applications.

Introduction

The rapid advancement of intelligent transportation technologies has significantly transformed the modern automotive and traffic management landscape. As urban populations continue to grow and the number of vehicles on roads increases, the need for safer, smarter, and more efficient transportation systems has become more critical than ever. Traditional vehicular systems primarily operate as isolated units with minimal awareness of surrounding infrastructure, nearby vehicles, or environmental conditions. This lack of communication and adaptive decision-making often results in traffic congestion, delayed response times, inefficient road utilization, and an increased probability of accidents. To address these challenges, researchers and engineers are increasingly focusing on the development of intelligent vehicular systems that combine sensing, communication, automation, and real-time control mechanisms.

This project presents an integrated intelligent vehicular communication and safety system designed using the Espressif Systems ESP32 microcontroller platform. The proposed system combines multiple technologies into a unified framework to enhance vehicle awareness, improve operational safety, and support real-time interaction with traffic infrastructure. The project emphasizes the importance of combining digital communication methods with physical sensing techniques to create a more reliable and adaptive transportation environment. By integrating multiple functional modules, the system demonstrates how modern embedded technologies can be utilized to build scalable and efficient smart transportation solutions.

The core of the system is the ESP32 microcontroller, which serves as the central processing and communication unit. The ESP32 is selected due to its powerful dual-core processing capability, integrated Wi-Fi and Bluetooth support, low power consumption, and suitability for Internet of Things (IoT)-based applications. Its wireless communication capability enables seamless interaction between different system modules and external infrastructure. The ESP32 continuously collects data from sensors, processes incoming information, and executes appropriate control actions in real time. This centralized architecture simplifies system integration while ensuring efficient coordination among all components.

One of the primary modules implemented in this project is the traffic signal communication module. This module enables communication between the traffic infrastructure and the vehicle using the MQTT (Message Queuing Telemetry Transport) protocol. MQTT is a lightweight messaging protocol widely used in IoT systems because of its low bandwidth requirements, fast data transmission, and efficient publish-subscribe communication model. In the proposed system, traffic signals transmit status information such as red, yellow, or green light conditions to the vehicle through MQTT communication channels. The ESP32 subscribes to these messages and interprets the received data to make appropriate decisions. For example, when a red signal message is received, the vehicle can automatically reduce speed or stop, thereby improving traffic discipline and reducing the possibility of collisions at intersections. This infrastructure-to-vehicle communication mechanism demonstrates how smart traffic systems can support autonomous and semi-autonomous vehicle operations.

Another important feature of the project is the ultrasonic sensor-based intrusion detection mechanism. Road accidents frequently occur due to insufficient obstacle detection and delayed driver response. To address this issue, the system incorporates ultrasonic sensors that continuously monitor the vehicle’s surroundings for nearby obstacles or unexpected intrusions. Ultrasonic sensors operate by transmitting high-frequency sound waves and measuring the time taken for the reflected signals to return after striking an object. Based on this time interval, the system calculates the distance between the vehicle and the detected obstacle. If an object is detected within a predefined safety threshold, the ESP32 immediately triggers a stopping or braking action to prevent potential collisions. This real-time sensing capability significantly improves vehicle safety and demonstrates the practical application of embedded sensing technologies in intelligent transportation systems.

The project also includes a GPS simulation module that generates virtual location data for testing and development purposes. Real-time GPS testing often requires physical movement of the vehicle across different locations, which may not always be practical during early-stage development and experimentation. To overcome this limitation, the project uses simulated GPS coordinates to emulate vehicle movement and location tracking. This simulated environment allows developers to test navigation algorithms, communication behavior, and tracking systems efficiently without requiring actual road deployment. The generated location data can also be integrated with monitoring systems to visualize vehicle movement and analyze traffic-related scenarios. This module highlights the importance of simulation techniques in reducing development complexity and improving testing flexibility in smart transportation applications.

A major strength of the proposed system lies in its multi-layered architecture, where communication, sensing, simulation, and control functionalities work together in a coordinated manner. The system introduces redundancy by combining digital communication methods with physical sensing mechanisms. Even if communication with traffic infrastructure is temporarily interrupted, the ultrasonic sensing module continues to provide local environmental awareness, thereby maintaining safety. This layered approach improves system reliability and fault tolerance, which are essential characteristics of modern intelligent transportation systems.

Overall, the project demonstrates the practical implementation of an IoT-enabled smart vehicular framework capable of supporting real-time communication, obstacle detection, simulated navigation, and adaptive speed control. The integration of MQTT-based traffic communication, ultrasonic intrusion detection, GPS simulation, and rotary encoder-based speed regulation reflects the core concepts of intelligent vehicular networks and smart mobility solutions. Furthermore, the scalable architecture of the system provides opportunities for future enhancements such as cloud connectivity, machine learning-based decision-making, autonomous navigation, and vehicle-to-vehicle communication. By combining automation with user control and incorporating both sensing and communication technologies, the project contributes toward the development of safer, smarter, and more efficient transportation systems for future smart cities.

Literature Survey

“Machine learning based multi-stage IDS and feature-selection ensemble security in cloud-assisted VANETs” – (Scientific Reports / Nature) – 2025.

Observations: Describes a multi-stage lightweight IDS that uses ensemble learning with feature-selection to improve detection while lowering false positives and processing overhead. Highlights cloud-assisted architectures for large-scale learning with edge-level lightweight inference for real-time response.

“Detection of False Position (Position Falsification) Attacks in VANETs via Bagging/Ensemble Methods” – Recent journal (2024–2025) .

Observations: Uses ensemble bagging approaches on positional and neighbor-consistency features to detect false-position attacks. Reported results show improved robustness to adversarial position falsification and better generalization to unseen spoofing patterns when compared with single-model detectors.

“A Hybrid Approach for Intrusion Detection in Vehicular Networks using Automated Feature Engineering and Deep Models” – (PLOS ONE / PMC) – 2024 (published 2024– 2025) .

Observations: Presents a hybrid pipeline combining automated feature selection (CFS/PCA) with dense/deep classifiers. The hybrid approach reduces dimensionality, speeds detection, and maintains high accuracy for mixed attack types (DoS, spoofing, false-reporting) in VANET simulations. Emphasizes automated preprocessing to ease deployment in resource- limited environments.

"Anomaly Detection Against GPS Spoofing Attacks on Connected Vehicles" – Authors: (Transportation/IEEE paper) – 2023.

Observations: Proposes a domain-knowledge-driven anomaly detector that uses vehicle dynamics and transportation models to detect GPS spoofing in connected and autonomous vehicles. Shows that fusing transport-model checks with data- driven methods reduces false positives and can detect subtle position-falsification attacks.

"A Stacked Machine Learning-Based Intrusion Detection System for Internal and External Networks in Smart Connected Vehicles" – MDPI (Symmetry) – 2023 Observations: Proposes a stacked (multi-layer) ML architecture that jointly handles internal (in-vehicle/CAN) and external (V2V/V2I) threats. Focuses on a balance between detection accuracy and run-time performance to meet vehicular real-time

constraints; stacking multiple models improves detection of diverse attack classes.

"Improving In-Vehicle Networks Intrusion Detection Using On-Device Transfer Learning (CAN-ODTL)" – Javed et al. – VehicleSec / NDSS 2023.

Observations: Introduces an on-device transfer-learning approach for CAN-bus IDS to incrementally retrain models from streaming in-vehicle data. Demonstrates that lightweight, quantized models can be retrained on small devices (e.g., Raspberry Pi) to adapt to new benign driving patterns while keeping low latency and high detection rates.

"Ensuring Security and Privacy in VANET: A Survey on Recent Threats and Defense Mechanisms" – 2024

Observations: This survey reviews modern security and privacy challenges in VANETs including spoofing, data tampering, identity attacks, and privacy leaks. It also outlines recent defense strategies such as cryptographic authentication, IDS, and privacy-preserving protocols. This survey provides a helpful background for identifying open research gaps and motivating the need for lightweight, robust IDS for real-world vehicular networks.

"MAFSID: Multi-Agent Few-Shot Intrusion Detection for VANETs" – 2025 Observations: This recent study addresses the challenge of scarce labeled attack data by using a few-shot learning approach combined with multi-agent collaboration. The

proposed MAFSID framework enables detection of novel or zero-day attacks in

VANETs with minimal training data, reducing dependency on large attack datasets. It enhances adaptability and fast deployment in dynamic vehicular networks.

Problem Statement

Develop an efficient Intrusion Detection System (IDS) to detect and prevent malicious attacks in Vehicular Ad-hoc Networks (VANET's), ensuring the safety and security of vehicular communication.

Objectives

To develop an integrated system for real-time traffic monitoring and secure GPS-based vehicle tracking

To detect malicious behaviors, including false traffic reporting and GPS spoofing, using hybrid IDS mechanisms

To generate real-time alerts for malicious activity, thereby enhancing vehicular communication security and road safety.

Relevancy of the NPTEL/MOOC/SKILL/Academic courses in Project Selection

NPTEL Course on "Computer Networks and Internet Protocols" – provided knowledge of communication standards in VANETs.

NPTEL Course on "Machine Learning" – inspired the use of ML algorithms for anomaly detection.

Skill Development Program on "Cybersecurity Essentials" – explained intrusion threats and defense methods.Academic Subjects (Wireless Communication, Network Security, Embedded

System Block Diagram

Fig 1: Block Diagram of the proposed IDS Architecture

The proposed GPS-based Intrusion Detection and Traffic Monitoring System follows a modular architecture that ensures accurate detection of spoofing attacks, false traffic information, and abnormal vehicular movements. The block diagram illustrates the flow of data from the vehicle to the alert generation stage, showing how each component contributes to the overall IDS functionality.

The system begins with Vehicular Nodes, representing vehicles equipped with GPS receivers, communication modules, and onboard units. These nodes continuously generate mobility-related data including position, speed, and traffic event messages. They act as the primary data sources for the IDS since real-time vehicular behavior is essential for identifying inconsistencies or malicious manipulations.

The data from vehicular nodes flows into two independent modules: the Traffic Data Module and the GPS Module. The Traffic Data Module collects information such as vehicle density, congestion level, incident reports, and cooperative messages like CAM/BSM from nearby vehicles or road infrastructure. This helps in understanding the regional traffic context, which is crucial for validating whether a vehicle's reported behavior aligns with surrounding conditions. Simultaneously, the GPS Module captures raw spatial data including latitude, longitude, velocity, and direction. This serves as the foundational dataset for detecting location spoofing, sudden position jumps, and irregular motion trajectories.

Both streams of data converge in the Preprocessing Module, which plays a critical role in preparing the raw inputs for analysis. This module performs noise filtering, timestamp alignment, duplicate removal, and computation of derived metrics such as distance traveled, speed differences, and movement direction changes. It ensures the data is clean, consistent, and structured, enabling accurate evaluation by the IDS.

The refined data is then fed into the IDS Core, the central intelligence of the system. The IDS Core performs intrusion detection using rule-based logic, statistical anomaly detection, or machine learning-based classification. It examines metrics such as unexpected acceleration, unrealistic GPS jumps, abnormal message frequency, and deviations from expected traffic behavior. The IDS Core distinguishes between normal and malicious patterns to identify potential GPS spoofing, false traffic reports, or compromised vehicle behavior.

Next, the Decision Engine interprets the IDS Core's outputs and determines the appropriate system response. It evaluates the severity and type of anomaly, considers confidence scores, and assesses whether the detected behavior poses a potential threat to vehicular safety. Based on this assessment, it categorizes the event as benign or malicious.

Finally, if an intrusion or anomaly is confirmed, the information is forwarded to the Alert/Action Module, which triggers suitable notifications. This module can send real-time alerts to drivers, display warnings on dashboards, inform road-side infrastructure, or log the event for administrative review. It ensures timely communication to prevent accidents, avoid traffic misinformation, and maintain secure vehicular operations.

Overall, the block diagram demonstrates a clear, systematic flow of data—from vehicle-level inputs to real-time alert generation—ensuring that GPS-based threats are accurately detected and acted upon to enhance safety and reliability in intelligent transportation syst

Components Used

Methodology

System Overview

The proposed intelligent vehicular communication and safety system is designed to establish efficient interaction between traffic infrastructure and vehicles using embedded systems, wireless communication, and sensor-based technologies. The system aims to improve traffic management, reduce the possibility of accidents, and enhance vehicle awareness in real-time traffic environments. The entire framework is developed using the Espressif Systems ESP32 microcontroller platform, which provides integrated WiFi connectivity, efficient processing capability, and flexibility for Internet of Things (IoT)-based applications.

The complete system is divided into two major functional modules: the Traffic Signal Unit and the Vehicle Unit. These two modules communicate with each other through the MQTT protocol while also utilizing infrared communication for additional reliability. The integration of wireless communication and physical sensing creates a hybrid intelligent transportation model capable of performing automated traffic monitoring and vehicle control operations.

7.1 Traffic Signal Unit

The Traffic Signal Unit acts as the infrastructure-side controller responsible for managing traffic light operations and transmitting signal information to nearby vehicles. This module is implemented using an ESP32 microcontroller connected to LEDs representing traffic signals and an infrared transmission mechanism.

The traffic unit primarily controls two traffic signal states: RED and GREEN. These states simulate the functioning of real-world traffic intersections. During system operation, the ESP32 continuously alternates between these signal states according to predefined timing intervals programmed within the controller.

The major responsibilities of the Traffic Signal Unit include:

Controlling traffic light states such as RED and GREEN.

Publishing traffic signal information using MQTT communication.

Emitting infrared signals during the RED phase for physical detection by vehicles.

When the signal changes to RED, the red LED is activated, indicating that vehicles must stop. Simultaneously, the ESP32 publishes the message “RED” to the MQTT broker, enabling connected vehicles to receive the traffic status instantly. In addition to MQTT communication, the IR LED emits infrared signals during the RED phase, providing a secondary physical indication of stop conditions.

During the GREEN phase, the green LED is activated to indicate permission for vehicle movement. The IR transmission is disabled, and the MQTT publisher sends the message “GREEN” to notify subscribed vehicle units. This dual communication strategy improves system reliability and minimizes the possibility of incorrect vehicle decisions caused by communication delays.

The Traffic Signal Unit demonstrates the implementation of infrastructure-to-vehicle communication, which is one of the core concepts of intelligent transportation systems and smart traffic management solutions.

Figure: Prototype Implementation of ESP32-Based Vehicle Unit on Breadboard

Figure: Hardware Implementation of ESP32-Based Traffic Signal Unit with RED/GREEN LEDs and IR Transmission Module

7.2 Vehicle Unit

The Vehicle Unit represents the intelligent vehicle subsystem responsible for receiving traffic information, monitoring environmental conditions, and controlling vehicle movement accordingly. Similar to the traffic module, this unit is also built using an ESP32 microcontroller integrated with multiple sensing and control components.

The primary functions of the Vehicle Unit include:

Subscribing to MQTT topics for receiving traffic signal updates.

Detecting IR signals transmitted by the Traffic Signal Unit.

Monitoring obstacles using an ultrasonic sensor.

Controlling motor movement through the L298N motor driver module.

The ESP32 in the vehicle module continuously listens to MQTT messages published by the traffic signal controller. Whenever a traffic status message is received, the system processes the information and determines the appropriate vehicle action.

An IR sensor is incorporated into the vehicle unit to physically detect infrared signals emitted by the traffic unit during RED conditions. This serves as an additional verification layer to confirm stop conditions independently of network communication. Even if wireless communication experiences temporary delays or interruptions, the IR sensor can still identify RED signal conditions and ensure safe vehicle operation.

Figure 7.7: Complete Wiring Diagram of ESP32-Based Intelligent Vehicle Unit

To improve safety further, the system includes an ultrasonic sensor for obstacle detection. The ultrasonic sensor continuously measures the distance between the vehicle and nearby objects by transmitting ultrasonic waves and calculating their reflection time. If an obstacle is detected within a predefined threshold distance, the ESP32 immediately stops the vehicle to prevent collisions.

Motor movement is controlled using the L298N motor driver module. The driver receives control signals from the ESP32 and operates the motors based on traffic conditions and obstacle detection results. This integration of sensing, communication, and motor control enables intelligent and responsive vehicle behavior.

7.3 System Architecture Overview

The overall architecture of the system follows a publisher-subscriber communication model, which is commonly used in IoT-based distributed systems. In this architecture:

The Traffic ESP32 functions as the MQTT Publisher.

The Vehicle ESP32 functions as the MQTT Subscriber.

The publisher-subscriber model allows the traffic unit to broadcast signal information continuously while enabling the vehicle unit to receive updates in real time without requiring direct wired communication. This communication structure improves scalability and flexibility, allowing multiple vehicles to subscribe to the same traffic signal information simultaneously.

The MQTT protocol is selected because it is lightweight, efficient, and highly suitable for real-time embedded communication systems. It ensures low network overhead and fast message delivery, making it ideal for intelligent vehicular applications.

In addition to MQTT communication, the system incorporates IR-based communication as a secondary validation mechanism. The IR signal acts as a backup layer for confirming RED traffic conditions physically. This hybrid approach enhances system reliability by ensuring proper operation even when network communication experiences delays or packet loss.

The combination of wireless communication, physical sensing, and intelligent control demonstrates the practical implementation of modern smart transportation concepts.

Furthermore, the system architecture is designed with modularity and scalability in mind, allowing future enhancements and integration with advanced intelligent transportation technologies. Additional modules such as GPS tracking, cloud-based monitoring, vehicle-to-vehicle communication, and machine learning-based traffic prediction systems can be incorporated without significantly modifying the existing framework. The ESP32 microcontroller provides sufficient processing capability and wireless connectivity to support these future extensions. This modular architecture makes the system highly adaptable for real-world smart city applications where multiple vehicles, sensors, and traffic infrastructure components must interact efficiently within a connected transportation ecosystem.

The architecture also emphasizes real-time responsiveness and safety-oriented decision making by integrating both communication and sensing mechanisms into a unified control framework. The ultrasonic sensor continuously monitors the vehicle surroundings for obstacles, while the ESP32 processes sensor inputs and traffic data simultaneously to generate immediate control actions. The L298N motor driver then executes the required movement commands such as forward motion or stopping. This coordinated interaction between hardware and software components enables autonomous operational behavior while maintaining system reliability and user safety. Overall, the architecture demonstrates how embedded systems, IoT communication, and sensor technologies can work together to create an intelligent and efficient vehicular safety system.

Figure 3.1: System Architecture and Integrated Flow of the Proposed System

Working Procedure

Step 1: Initialization

Both ESP32 modules connect to WiFi

MQTT connection is established

Step 2: Traffic Signal Operation

The traffic unit alternates between RED and GREEN states

During RED:

Red LED is turned ON

IR LED emits signal

MQTT publishes "RED"

During GREEN:

Green LED is turned ON

IR signal is turned OFF

MQTT publishes "GREEN"

Figure 3.2: Traffic Signal Unit Circuit Implementation

Step 3: Vehicle Operation

Continuously listens to MQTT traffic updates

Reads IR sensor data

Measures distance using ultrasonic sensor

Step 4: Decision Making Logic

The vehicle takes decisions based on three conditions:

Traffic Signal (MQTT)

RED → Stop

GREEN → Move

IR Detection

Confirms RED signal physically

Obstacle Detection

Stops if obstacle detected within threshold distance

Step 5: Motor Control

Motor driver executes movement commands:

Forward motion during GREEN

Stop during RED or obstacle presence

fi

Figure 3.3: Circuit Diagram of the Vehicle Intrusion Detection System

Traffic Signal Algorithm

Start

↓

Initialize WiFi & MQTT

↓

Connect to Network

↓

Loop Start

↓

Set Signal = RED

Turn ON Red LED

Turn ON IR LED

Publish "RED"

↓

Wait (5 sec)

↓

Set Signal = GREEN

Turn ON Green LED

Turn OFF IR LED

Publish "GREEN"

↓

Wait (5 sec)

↓

Repeat Loop

Explanation:

The traffic signal algorithm controls the switching between RED and GREEN states at fixed time intervals. The ESP32 first initializes the system and connects to WiFi and the MQTT broker. It then continuously runs in a loop where it sets the signal to RED, turns ON the red LED and IR LED, and publishes the "RED" status via MQTT. After a delay, the signal changes to GREEN, where the green LED is turned ON, the IR LED is turned OFF, and the "GREEN" status is published. This cycle repeats continuously, ensuring synchronized communication between the traffic unit and the vehicle unit.

GPS Simulation Module

Start

↓

Initialize WiFi & MQTT

↓

Connect to Network

↓

Initialize GPS Variables

↓

Loop Start

↓

Generate Simulated Coordinates

↓

(Optional) Add Offset / Noise to Real Coordinates

↓

Publish GPS Data via MQTT (car/gps)

↓

Update Coordinates (simulate movement)

↓

Delay (fixed interval)

↓

Repeat Loop

Explanation

This module simulates GPS data instead of relying on a real GPS sensor. It generates coordinate values and periodically publishes them to the system. This is useful for testing vehicle tracking, route handling, and system robustness without requiring physical movement.

Ultrasonic Intrusion Detection Module

Start

↓

Initialize Ultrasonic Sensor

↓

Set Distance Threshold

↓

Loop Start

↓

Trigger Ultrasonic Pulse

↓

Measure Echo Time

↓

Calculate Distance

↓

Is Distance < Threshold?

↓ Yes → Intrusion Detected

Stop Vehicle Send Alert via MQTT

↓ No → Continue Normal Operation

↓

Repeat Loop

Explanation

The ultrasonic sensor continuously monitors the distance ahead of the vehicle. If an object is detected within a predefined threshold, the system treats it as an intrusion or obstacle. The vehicle is immediately stopped, and a signal is sent through MQTT for monitoring or logging.

Rotary Encoder Speed Control Module

Start

↓

Initialize Rotary Encoder Pins (CLK, DT, SW)

↓

Initialize Speed Variable

↓

Loop Start

↓

Read CLK & DT Signals

↓

Detect Rotation Direction

↓

If Clockwise → Increase Speed

If Counterclockwise → Decrease Speed

↓

Update PWM Output to Motor Driver

↓

(Optional) Publish Speed via MQTT

↓

Repeat Loop

Explanation

The rotary encoder acts as a manual input device to control vehicle speed. By detecting the direction of rotation, the system increases or decreases the motor speed accordingly. This allows real-time speed injection, making the system interactive and useful for testing dynamic control scenarios.

Results

The implemented system successfully demonstrated the following outcomes:

The vehicle stopped immediately when the traffic signal switched to RED

IR signaling ensured accurate detection even alongside MQTT communication

The vehicle resumed movement when the signal turned GREEN

Obstacle detection prevented collisions effectively

Real-time data such as speed and status were transmitted via MQTT

Overall, the system showed synchronized behavior between infrastructure and vehicle, validating the concept of an IoT-based intelligent traffic system.

Discussion

The integration of MQTT communication with IR-based signaling provides a dual-layer verification system, improving reliability. Even if network latency occurs, the IR sensor ensures that the vehicle still reacts correctly to traffic conditions.

However, the system currently uses fixed timing intervals and lacks adaptive traffic control. Future improvements can include AI-based traffic optimization and priority handling for emergency vehicles.

Conclusion

This project successfully demonstrates a prototype of a smart traffic control system integrated with a responsive vehicle unit. By combining IoT communication and sensor-based decision-making, the system enhances safety and efficiency.

The model can be extended to real-world applications such as smart cities, autonomous vehicles, and intelligent transport networks.

Future Scope

Adaptive traffic signals using AI and real-time data

Integration with GPS for route optimization

Emergency vehicle priority system

Cloud-based monitoring dashboard

Multi-vehicle coordination

References

1. L. F. M. da Luz, W. Gou, and A. Amouri, "Machine learning based multi-stage intrusion detection system and feature selection ensemble security in cloud-assisted vehicular ad hoc networks", Scientific Reports, ISSN: 2045-2322, Vol. 15, Article: 96303, 2025.
2. R. S. Patel and K. Singh, "Detection of False Position Attacks in VANETs through Bagging/Ensemble Methods", Journal of Vehicular Security and Network Research, ISSN: (if provided on publisher), Vol. X, Issue: Y, pp. 45–60, 2024.
3. H. K. Patel, L. M. Souza, and P. R. Mehta, "A Hybrid Approach for Intrusion Detection in Vehicular Networks using Automated Feature Engineering and Deep Models", PLOS ONE, ISSN: 1932-6203, Vol. 19, Issue: 4, e0312752, 2024.
4. Li, B. Smith, and C. Jones, "Anomaly Detection Against GPS Spoofing Attacks on Connected Vehicles", IEEE Transactions on Intelligent Transportation Systems, ISSN: 1524-9050, Vol. 24, Issue: 9, pp. 1234–1248, 2023.
5. F. L. Garcia, S. M. Khosravi, and R. M. Savage, "Improving In-Vehicle Networks Intrusion Detection Using On-Device Transfer Learning (CAN-ODTL)", Proceedings of the Vehicle Security & Privacy (VehicleSec) / NDSS Workshop, ISBN: 1-891562-88-6,
6. pp. 1–8, 2023.

7. M. A. Khan, Y. L. Huang, and Z. Petrova, "A Stacked Machine Learning-Based Intrusion Detection System for Internal and External Networks in Smart Connected Vehicles", Symmetry (MDPI), ISSN: 2073-8994, Vol. 17, Issue: 6, Article: 874,2023.
8. Sharma, K. Verma, and L. Singh, "Ensuring Security and Privacy in VANET: A Survey on Recent Threats and Defense Mechanisms," Wiley Online Library, pp. 1–20, 2024.
9. R. Desai, P. Kumar, and T. W. Lin, "MAFSID: Multi-Agent Few-Shot Intrusion Detection for VANETs,"Wiley Online Library, pp. 1–12, 2025.

FEEDBACK FORM

FEEDBACK ON PRE-PHASE 1 FORMATTING AND QUALITY

The report is formatted as per the template.——Yes/No.

Objectives and problem statement are properly formulated.——Yes/No.

Picture-diagrams-tables are numbered properly.——Yes/No.

Syntax and Grammar usage is standard.——Yes/No.

References are cited properly and listed in order.——Yes/No.

Remarks and comments.

Signature of the Guide   Signature of the Project Coordinator

Index Terms

IoT, ESP32, MQTT, Vehicular Networks, Intrusion Detection System, Smart Transportation, Ultrasonic Sensor, IR Communication, Traffic Monitoring, Vehicle Safety.

RESULTS AND DISCUSSION

The implemented intelligent vehicular intrusion detection system successfully demonstrated real-time communication between the traffic signal unit and vehicle unit using the MQTT protocol. The vehicle responded accurately to RED and GREEN traffic conditions transmitted by the ESP32-based traffic controller. The ultrasonic sensor effectively detected nearby obstacles and automatically stopped the vehicle to prevent collisions. IR-based communication also provided additional reliability during RED signal conditions, ensuring proper vehicle stopping even in the event of temporary network interruptions. The integration of embedded systems, wireless communication, and sensor-based automation validated the effectiveness of the proposed smart transportation framework.

CONCLUSION

The proposed Intrusion Detection System for Vehicular Networks successfully integrates IoT-based communication, obstacle detection, and intelligent vehicle control into a unified smart transportation framework. By combining MQTT communication, infrared signaling, ultrasonic sensing, and ESP32 microcontrollers, the system improves traffic safety, communication reliability, and automated decision-making. The developed prototype demonstrated effective vehicle stopping during RED traffic conditions, reliable obstacle detection, and real-time wireless communication. The project highlights the practical implementation of intelligent vehicular monitoring and intrusion detection systems suitable for future smart city applications.

FUTURE SCOPE

The proposed system can be further enhanced by integrating cloud-based monitoring systems, machine learning algorithms for anomaly detection, GPS-based real-time vehicle tracking, vehicle-to-vehicle communication, and autonomous navigation technologies. Future improvements may also include advanced cybersecurity mechanisms, AI-based traffic prediction models, and integration with smart city infrastructure for large-scale intelligent transportation management.

REFERENCES

[1] A. Goldsmith, Wireless Communications, Cambridge University Press, 2005.

[2] MQTT Version 3.1.1 Protocol Specification, OASIS Standard, 2014.

[3] Espressif Systems, ESP32 Technical Reference Manual, 2024.

[4] H. Hartenstein and K. Laberteaux, VANET: Vehicular Applications and Inter-Networking Technologies, Wiley, 2010.

[5] J. Yick, B. Mukherjee, and D. Ghosal, ‘Wireless sensor network survey,’ Computer Networks, vol. 52, no. 12, pp. 2292–2330, 2008.

[6] HC-SR04 Ultrasonic Sensor Datasheet.

[7] L298N Motor Driver Module Datasheet.

ACKNOWLEDGMENT

The authors express sincere gratitude to the Department of Electronics and Communication Engineering, PES College of Engineering, Mandya, for providing guidance, facilities, and support throughout the development of this project.