MOVING OBJECT DETECTION IN VEHICLE-TO-VEHICLE (V2V) COMMUNICATION FOR INTELLIGENT ROAD SAFETY

A Project Report Submitted in Partial Fulfillment
of the Requirements for the Award of the Degree of
BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE & ENGINEERING

by

JYOTIBHUSHAN HAZARIKA (Roll No. 202102021071)

ANGSHUMAN GOSWAMI (Roll No. 202102021060)

KULDIP DAS (Roll No. 202102022097)

PRINCE HAZARIKA (Roll No. 202102021065)

Under the Supervision of

Dr. Pankaj Pratap Singh

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CENTRAL INSTITUTE OF TECHNOLOGY KOKRAJHAR
(Deemed to be University under MoE, Govt. of India)
BTR, KOKRAJHAR, ASSAM 783370
Website: www.cit.ac.in

May 2025

Abstract

In the rapidly evolving domain of intelligent transportation systems, the need for secure, efficient, and real-time Vehicle-to-Vehicle (V2V) communication has become increasingly critical. As autonomous vehicles and advanced driver assistance systems (ADAS) continue to gain prominence, the ability for vehicles to reliably share their perception of the environment is vital for enabling cooperative behavior and improving road safety. This project presents the design and development of a secure V2V communication framework that integrates real-time object detection with cryptographic verification techniques to ensure data authenticity and integrity during transmission.

The proposed system leverages the power of deep learning through the YOLO12 model for accurate and real-time detection of road objects such as vehicles and pedestrians using live camera input in Vehicle A. Once detected, the object information is serialized and signed using RSA digital signatures to safeguard the data against tampering or forgery. This signed data is transmitted over a TCP socket to Vehicle B, which acts as a peer vehicle. On reception, Vehicle B utilizes the corresponding RSA public key to verify the authenticity of the received data before processing it for any critical driving decisions.

This architecture demonstrates a practical approach to achieve secure V2V communication using widely accepted cryptographic standards in combination with real-time computer vision model. This report provides a detailed description of the system architecture, object detection model setup, cryptographic implementation, socket-based communication pipeline, testing methodology, and performance analysis. In addition, this project highlights existing challenges, such as limited computational resources, network latency, and dynamic peer discovery.

Contents

Chapter 1

Introduction

The increasing adoption of autonomous and semi-autonomous vehicles has highlighted the critical need for efficient and secure Vehicle-to-Vehicle (V2V) communication. V2V systems enable vehicles to share information such as detected obstacles, traffic conditions, and potential hazards, thereby improving decision-making and enhancing overall road safety. However, the open and distributed nature of wireless communication channels makes V2V systems highly susceptible to various security threats, including message spoofing, tampering, and impersonation attacks.

To address these challenges, this project proposes a secure V2V communication framework that integrates real-time object detection with RSA-based cryptographic verification. In this system, two vehicles are simulated—Vehicle A performs real-time object detection using the You Only Look Once version 12 (YOLO12) deep learning model fine-tuned for Indian road conditions, and signs the detection results using a private RSA key. The signed data is then transmitted over a TCP socket to Vehicle B. Vehicle B receives the data and verifies its authenticity and integrity using the sender's public RSA key, ensuring that only trusted and unmodified messages are processed.

The key contributions of this project are:

- Integration of YOLO12 for accurate and real-time road object detection.
- Implementation of RSA public-private key cryptography for secure message signing and verification.
- Use of a hybrid communication mechanism combining HTTP (for key exchange) and TCP sockets (for real-time data transmission).

This approach ensures that V2V communication is not only functionally effective but also secure, laying the foundation for trustworthy autonomous driving systems and offering a scalable solution for future intelligent transportation infrastructures.

Chapter 2

Literature Survey

Several studies have explored object detection in autonomous vehicles and the importance of secure communication protocols in connected vehicular networks.

- **YOLO (You Only Look Once)**: Redmon et al. proposed the YOLO[8] framework for real-time object detection. Its speed and accuracy make it suitable for use in intelligent transportation systems where quick detection is critical.
- **RSA Cryptography**: Developed by Rivest, Shamir, and Adleman, RSA[1] is a widely adopted public-key cryptographic method. It is commonly used for secure data transmission and digital signature verification.
- **Secure V2V Communication**: Muhammad et al. emphasized the necessity of secure and authenticated V2V[14] data exchange, focusing on encryption and signature mechanisms to prevent spoofing, impersonation, and data tampering.
- **IDD Dataset**: Roboflow provides a publicly available Indian Driving Dataset (IDD)[11], which is suitable for training object detection models in diverse and real-world driving conditions.

Table 2.1 Summary of Related Works

Authors name	**Problem statement**	**Methodology**	**Future Scope**
Andrija Petrović et al.[7]	Optimize toll booth use to reduce congestion	RNNs, queuing theory, and differential evolution.	Improve vehicle arrival modeling and adaptability
Yakub Kayode Saheed et al.[9]	IoV security lacks transparency and struggles with zero-day attacks.	XAI-based ensemble learning with SHAP, BiLAE, and BMO.	Expand real-time IoV security and adaptive learning
Habib Talha Hashmi et al.[5]	Toll congestion, long queues, and inefficiencies.	YOLOV7, LSTM prediction, and variable speed limits.	Enhance real-time control and low-visibility accuracy
Suryanti Awang et al.[3]	Manual tolls have high errors and costs.	SF-CNNLS for feature extraction and classification.	Improve feature extraction and processing speed.
Elizabeth Arthur et al.[2]	Lack of FHWA-compliant datasets for classification.	Images collected from various sources (Google Images) to capture environmental conditions.	Expand Dataset: Include more geographic diversity to improve.

Chapter 3

Methodology

3.1 System Architecture

The system is designed as a simulation of two vehicles (see fig. 3.1). Vehicle A is responsible for detecting road objects and transmitting the data securely to Vehicle B. Vehicle B verifies the integrity and authenticity of the received data.

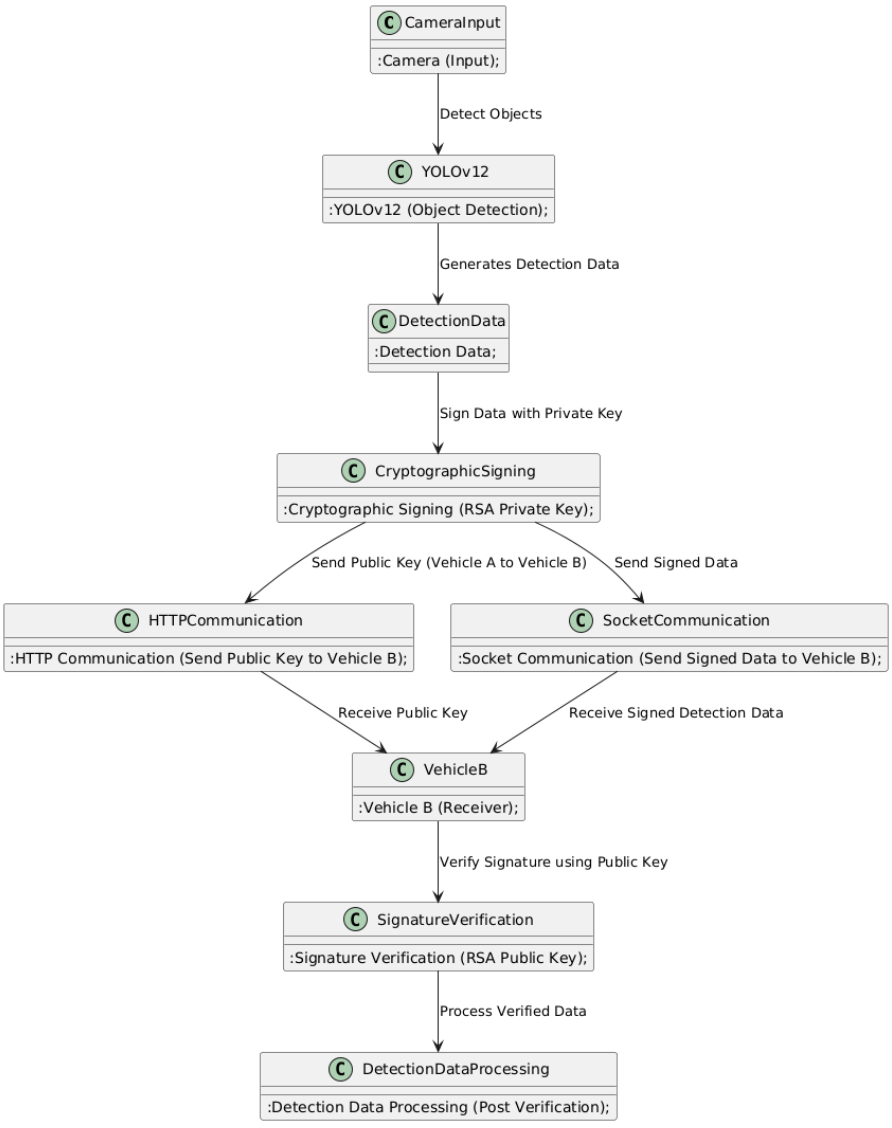

Figure 3.1: System Architecture: Secure V2V Communication Setup

– **Vehicle A (Sender)**: Uses a camera to detect road objects using a pretrained YOLO12

model. Generates RSA[4] keys and shares the public key with Vehicle B. Signs detection data with the private key and transmits it.

- **Vehicle B (Receiver)**: Receives detection data from Vehicle A. Uses the shared public key to verify the digital signature and validate data integrity.
- **Communication Flow**: The initial public key exchange is done over HTTP, while the continuous transfer of detection data is handled through a TCP[1] socket connection.

3.2 Hybrid Approach

This section explains the two primary components of the system: object detection using YOLO12 and secure Vehicle-to-Vehicle (V2V) communication using RSA cryptography.

3.2.1 Object Detection Using YOLO12

YOLO12[12] is a deep learning model designed for real-time object detection. The model divides an image into a grid and makes predictions for each grid cell. It outputs bounding boxes and class probabilities for each object detected in the image.

In this project, the YOLO12 model was trained on a custom dataset obtained from Roboflow's Indian Driving Dataset (IDD)[11]. This dataset contains labeled images with various road objects such as cars, pedestrians, and traffic signs. The trained model is capable of detecting these objects in real-time through a video feed captured by a camera.

The following steps describe the object detection process (see fig. 3.2):

1. **Input Image:** A camera captures a frame from the real-time video stream.
2. **Detection:** YOLO12 processes the image and predicts bounding boxes for detected objects. It also assigns class labels (e.g., car, pedestrian) and calculates the confidence score.
3. **Result Generation:** The detection results are formatted into a structured JSON object that includes:
   - Object label (e.g., "car", "pedestrian")
   - Confidence score
   - Bounding box coordinates (left, top, right, bottom)
   - Timestamp of detection
4. **Transmission:** The detection results are signed with the private key of Vehicle A and sent over a TCP socket to Vehicle B.

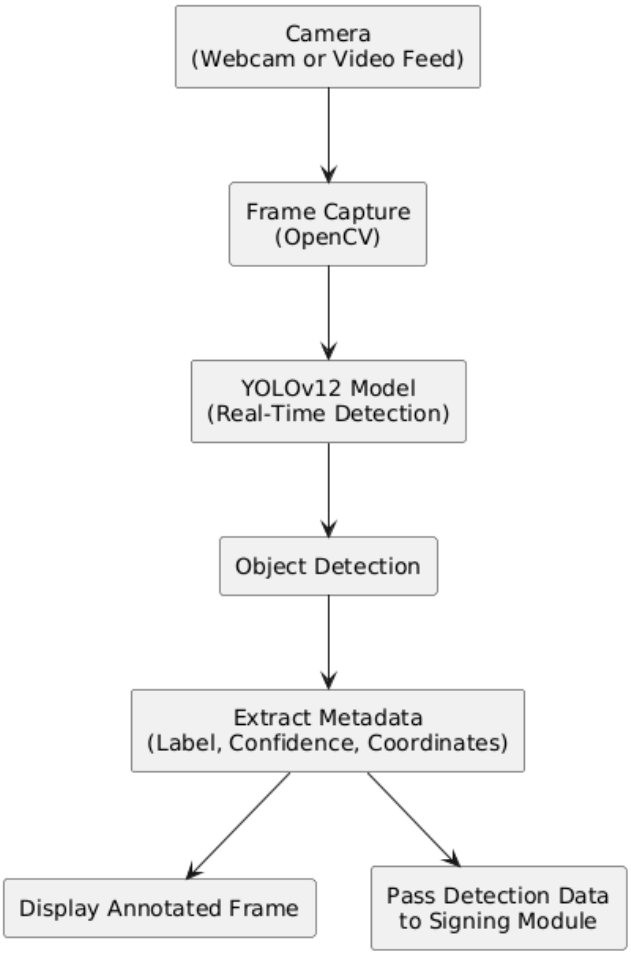

Figure 3.2: Object Detection Workflow Using YOLO12: From camera input to labeled detection output.

The model's ability to detect objects quickly and accurately is crucial for ensuring that Vehicle A can provide timely data to Vehicle B for decision-making.

3.2.2 Vehicle-to-Vehicle (V2V) Communication

In this project, V2V[6] communication was established between two vehicles (Vehicle A and Vehicle B) using a secure communication protocol. This involves the exchange of detection data, verified with RSA digital signatures, to ensure authenticity and integrity.

3.2.3 Key Generation and Exchange

Each vehicle generates a pair of public and private keys using RSA cryptography[10]. The public key is shared with the other vehicle, while the private key remains confidential.

The key generation process involves the following steps:

- Vehicle A generates a private-public key pair using RSA. The private key is used for signing detection data, and the public key is shared with Vehicle B for signature verification.
- Vehicle A sends its public key to Vehicle B over an HTTP POST[4] request. This allows Vehicle B to securely verify any signed data that it receives from Vehicle A.

– Vehicle B receives Vehicle A's public key and stores it for future verification of signatures.

3.2.4 Digital Signature Mechanism

Once the objects are detected, Vehicle A generates a payload containing the detection data, including:

– A list of detected objects, including their labels and bounding box coordinates
– The confidence score for each object
– A timestamp of when the detection occurred
– The Vehicle ID (e.g., "Vehicle A")

Vehicle A then signs this payload using its private key. The signature is computed as the hash of the payload, which is then encrypted with the private key to ensure that only Vehicle A could have generated the signature.

Once the data is signed, Vehicle A sends the detection data and the digital signature to Vehicle B over a TCP socket.

3.2.5 Verification at Vehicle B

When Vehicle B receives the detection data from Vehicle A, it performs the following steps:

– Vehicle B decodes the signature and the detection data.
– Vehicle B computes the hash of the received detection data.
– Vehicle B uses Vehicle A's public key to decrypt the signature and compares it with the computed hash to verify the authenticity of the data.
– If the signature is valid, Vehicle B processes the data (e.g., displaying detected objects on the screen). If the signature is invalid, Vehicle B discards the data as tampered.

This mechanism ensures that only legitimate detection data from Vehicle A is processed by Vehicle B, preventing data manipulation or impersonation attacks.

3.3 Implementation

The implementation of the secure V2V communication system is divided into several modules: object detection, key generation and exchange, and data transmission.

3.4 Setup and Environment

The following tools and libraries were used in the project:

– **YOLO12**: The YOLO12[15] model was used for real-time object detection.
– **OpenCV**: OpenCV was used for camera capture and real-time video stream processing.
– **RSA (cryptography module)**: Python's cryptography library was used to generate RSA keys, sign data, and verify signatures.

- **Socket Programming**: TCP[10] sockets were used to establish communication between Vehicle A and Vehicle B.
- **HTTP (requests module)**: The requests module was used to exchange public keys between vehicles over HTTP.

3.4.1 Vehicle A - Sender

Vehicle A's implementation includes the following steps:

1. **Camera Capture**: Vehicle A captures video input from a webcam using OpenCV.
2. **Object Detection**: YOLO12[8] processes each frame to detect road objects.
3. **Payload Creation**: The detection results are formatted into a JSON payload, which includes the object labels, confidence scores, bounding box coordinates, and timestamp.
4. **Digital Signing**: The payload is signed using Vehicle A's private key.
5. **Transmission**: The signed detection data is sent to Vehicle B over a TCP[1] socket.

3.4.2 Vehicle B - Receiver

Vehicle B's implementation involves the following steps:

1. **Listening for Incoming Data**: Vehicle B listens for incoming data on a specified TCP port.
2. **Data Reception**: Upon receiving data, Vehicle B decodes the signature and payload.
3. **Signature Verification**: Vehicle B uses Vehicle A's public key to verify the signature of the received payload.
4. **Processing**: If the signature is valid, Vehicle B processes the data (e.g., displaying the detected objects).
5. **Data Discarding**: If the signature is invalid, Vehicle B discards the data.

Chapter 4
Result and Analysis

The secure Vehicle-to-Vehicle (V2V)[4] communication system was successfully implemented, integrating YOLO12[13] for real-time object detection and RSA cryptography for secure data exchange. This section outlines the outcomes of the system, including the performance of object detection, the security measures in place, and the challenges encountered during implementation.

4.1 Object Detection Performance

The object detection system based on YOLO12 was able to detect road objects with high accuracy and real-time speed. The system detected objects such as cars, pedestrians, traffic signs, and obstacles reliably across different road conditions. The following results were observed during testing:

- **Detection Speed**: The YOLO12 model processed each frame in real time, providing low-latency object detection. This is crucial for V2V communication, as the system must react quickly to ensure safety.
- **Accuracy**: The detection accuracy was evaluated using standard metrics such as mAP (mean Average Precision), which measures how accurately the model detects and classifies objects. The trained YOLO12 model achieved a high mAP[15] score, ensuring that it correctly identified objects with minimal false positives and false negatives. (see Fig. 4.1 & 4.2)
- **Object Types**: YOLO12 successfully identified a variety of objects, including vehicles, pedestrians, traffic signals, and other road obstacles.

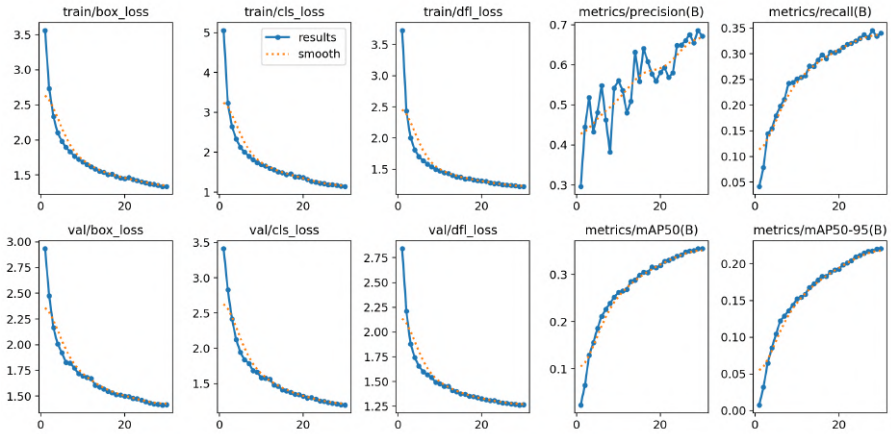

Figure 4.1: Precision Matrix showing class-wise detection precision across different road objects such as vehicles, pedestrians, and traffic signs.

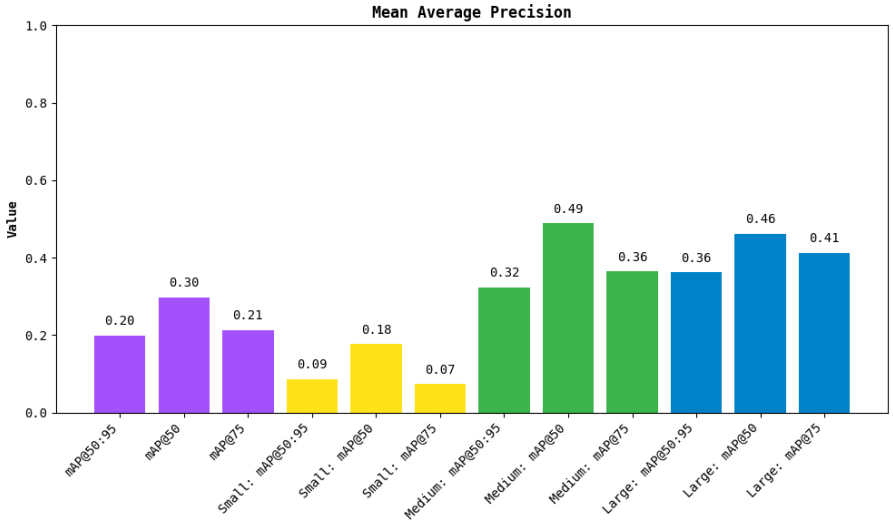

Figure 4.2: mAP Curve representing the model's average precision across various IoU thresholds, indicating overall detection accuracy.

4.1.1 Detected Objects

During the testing phase, the YOLO12 model was used to detect various road objects such as pedestrians, traffic signs, and vehicles. The following images show the detected objects in the real-time video feed. (Fig. 4.3)

Figure 4.3: Detected results.

These results demonstrate that YOLO12 is well-suited for real-time object detection in a V2V communication system.

4.2 Security and Integrity of Data Transmission

The integration of RSA digital signatures in the system ensured the authenticity and integrity of the transmitted data. The key points regarding the security performance are as follows:

- **Signature Verification**: Vehicle B successfully verified the integrity of the data received from Vehicle A using the public key. This process ensured that the data had not been altered during transmission and was indeed sent by the correct vehicle.
- **Prevention of Spoofing and Tampering**: The use of RSA signatures prevented spoofing, where an attacker might attempt to impersonate Vehicle A, and tampering, where an attacker might modify the detection data in transit. Any attempt to alter the detection payload during transmission resulted in a verification failure at Vehicle B.
- **Authenticity of Data**: Since only Vehicle A could have signed the data using its private key, Vehicle B could trust the authenticity of the detection data.

The combination of object detection with YOLO12 and secure communication using RSA signatures provided a robust security mechanism, making the V2V communication system reliable and resistant to common attacks.

4.2.1 Socket Communication and Data Transmission

The communication between the two vehicles (Vehicle A and Vehicle B) was established using TCP sockets, ensuring low-latency and continuous data transmission. The key points regarding the socket communication performance are:

- **Low Latency**: The socket connection allowed for continuous, real-time data transfer with minimal delay. This is essential in a V2V communication system, where vehicles need to exchange information quickly to avoid accidents.
- **Reliable Data Transmission**: The TCP[10] protocol ensured reliable transmission of detection data from Vehicle A to Vehicle B, with retransmissions occurring if data packets were lost.
- **Data Integrity**: The system ensured that the data remained intact during transmission, with the added layer of RSA digital signature verification guaranteeing that the received data was not altered.

Overall, the socket communication provided a stable foundation for the real-time exchange of object detection data between the vehicles.(Fig. 4.4 - 4.7)

Figure 4.4: Object Detection and V2V Testing

Figure 4.5: Vehicle A sending data to Vehicle B

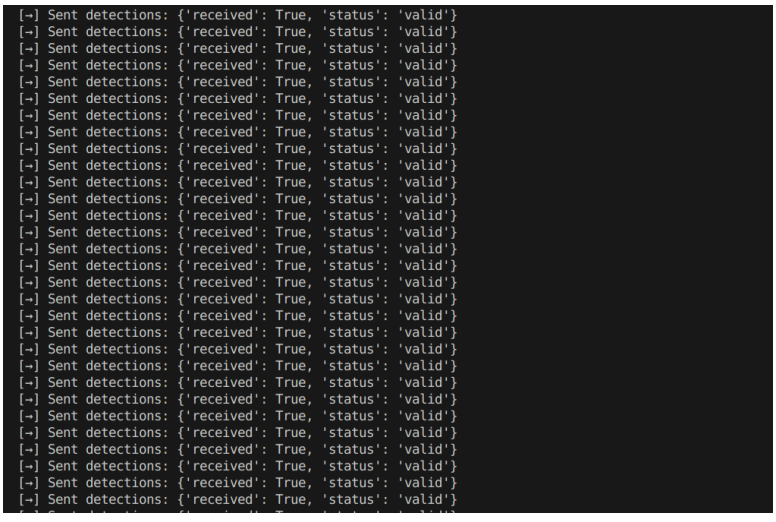

Figure 4.6: Vehicle A sending data to Vehicle B

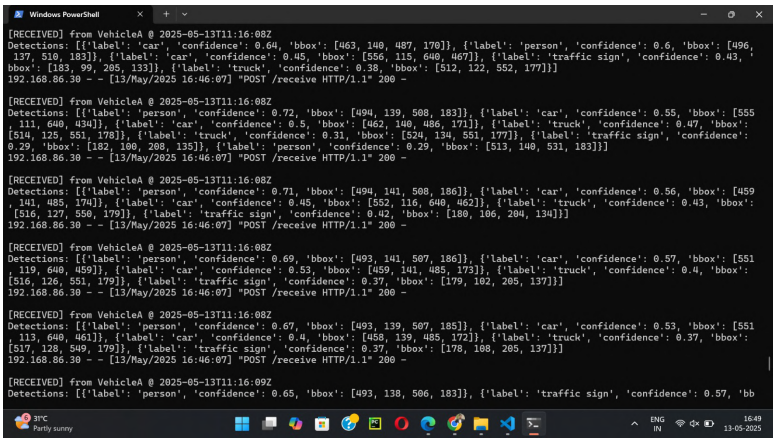

Figure 4.7: Vehicle B receives data from Vehicle A

4.3 Challenges Encountered

During the implementation of the system, several challenges were encountered:

- **Computational Resources**: One of the major challenges encountered during the project was the limitation of computational resources, which restricted our ability to train large-scale deep learning models and perform real-time inference efficiently. This necessitated optimization strategies and reliance on pre-trained models to balance performance and feasibility.
- **Camera Input Variability**: The performance of the YOLO12 model varied depending on the quality and resolution of the camera input. Lower-quality cameras resulted in reduced accuracy in object detection, especially in low-light conditions or high-speed scenarios.

These challenges were addressed through optimizations in the network protocols and improvements in the object detection pipeline.

Chapter 5
Conclusion and Future Work

This project successfully demonstrates a secure Vehicle-to-Vehicle (V2V) communication system that integrates real-time object detection using YOLO12 and secure data transmission using RSA cryptography. The system effectively addresses several critical issues in V2V communication, including object detection, data integrity, and authenticity, through a combination of computer vision and cryptographic techniques.

5.1 Conclusion

The results confirmed that the system is capable of detecting various moving road objects with moderate level accuracy and speed, making it suitable for real-time applications in intelligent transportation systems. The integration of RSA-based digital signatures ensured the authenticity and integrity of the transmitted data, preventing impersonation and tampering. Socket programming enabled real-time communication between vehicles with low-latency data transfer.

In summary, the system demonstrated the feasibility of combining real-time object detection with secure communication for V2V applications, offering a robust solution to ensure safer and more efficient autonomous driving. The work also concludes the potential enhancements, including implementation on moving vehicles, integration with RSA256 cryptography for security management, and deployment in more complex traffic environments to validate real-world robustness.

5.2 Future Work

While the system was successful, several areas for enhancement and further development have been identified. Future work on this project could focus on improving performance, scalability, and security:

- **Support for Multiple Vehicles and Dynamic Vehicle Discovery**: The current system is designed for communication between two vehicles. Future work could expand the system to support communication between multiple vehicles in a network, enabling collaborative decision-making and sharing of detection data.
- **Implementation On Moving Real Vehicle**: : Implement the V2V communication system on real vehicles using onboard cameras and embedded devices (e.g., Raspberry Pi) to enable real-world object detection and blockchain-based data verification in dynamic traffic environments.

These future enhancements would further elevate the system's capabilities, making it more adaptable, scalable, and secure for real-world deployment in autonomous vehicles.

References

[1] Abdullah Alghamdi and Farhan A Khan. Authentication and encryption protocol with revocation and reputation for 5g-v2x communication. *Journal of King Saud University - Computer and Information Sciences*, 2023.

[2] Elizabeth Arthur, Armstrong Aboah, and Ying Huang. A novel fhwa-compliant dataset for granular vehicle detection and classification. *IEEE Access*, 2024.

[3] Suryanti Awang and Nik Mohamad Aizuddin Nik Azmi. Automated toll collection system based on vehicle type classification using sparse-filtered convolutional neural networks with layer-skipping strategy (sf-cnnls). In *Journal of Physics: Conference Series*, volume 1061, page 012009. IOP Publishing, 2018.

[4] Misbah Fatima, Hafsa Malik, and Asim Ahmad. Enhancing security in vehicle-to-vehicle communication: A comprehensive review. *Electronics*, 6(1):20, 2023.

[5] Habib Talha Hashmi, Sameer Ud-Din, Muhammad Asif Khan, Jamal Ahmed Khan, Muhammad Arshad, and Muhammad Usman Hassan. Traffic flow optimization at toll plaza using proactive deep learning strategies. *Infrastructures*, 9(5):87, 2024.

[6] Andreas Hülsing and Job Rijneveld. Drive (quantum) safe! towards post-quantum security for vehicle-to-vehicle communication. *IACR Cryptology ePrint Archive*, 2023:003, 2023.

[7] Andrija Petrović, Mladen Nikolić, Uglješa Bugarić, Boris Delibašić, and Pietro Lio. Controlling highway toll stations using deep learning, queuing theory, and differential evolution. *Engineering Applications of Artificial Intelligence*, 119:105683, 2023.

[8] Joseph Redmon, Santosh Divvala, Ross Girshick, and Ali Farhadi. You only look once: Unified, real-time object detection. *arXiv preprint arXiv:1506.02640*, 2016.

[9] Yakub Kayode Saheed and Joshua Ebere Chukwuere. Xaiensembletl-iov: A new explainable artificial intelligence ensemble transfer learning for zero-day botnet attack detection in the internet of vehicles. *Results in Engineering*, 24:103171, 2024.

[10] Dmitry Ulybyshev and Binu Babu. Secure data communication in autonomous v2x systems. In *IEEE International Congress on Internet of Things (ICIOT)*. IEEE, 2018.

[11] Girish Varma, Anbumani Subramanian, Anoop M. Namboodiri, Manmohan Chandraker, and C. V. Jawahar. IDD: A dataset for exploring problems of autonomous navigation in unconstrained environments. *CoRR*, abs/1811.10200, 2018.

[12] Chen Wang, Yu Zhang, and Min Liu. Yolov12: Attention-centric real-time object detectors. *arXiv preprint arXiv:2502.12524*, 2024.

[13] Lei Xue and Jun Song. Yolo-vehicle-pro: A cloud-edge collaborative framework for object detection in autonomous driving under adverse weather conditions. *arXiv preprint arXiv:2410.17734*, 2024.

[14] Wei Zhang, Xiaofei Wang, and Jun Li. 5g-based v2v broadcast communications: A security perspective. *Vehicular Communications*, 29:100332, 2021.

[15] Shiyu Zhuang and Zhen Qin. Yolo-z: Improving small object detection in yolov5 for autonomous vehicles. *arXiv preprint arXiv:2112.11798*, 2021.