KLE Technological University

Creating Value
Leveraging Knowledge

School of
Electronics and Communication Engineering

Minor-1 Project Report

on

SECURING V2X COMMUNICATION

By:

1. **Shreesha Hegde** USN: 01FE21BEC226
2. **Shrinidhi K T** USN: 01FE21BEC136
3. **Rakshan Kulkarni** USN: 01FE21BEC151
4. **Nandish M** USN: 01FE21BEC303

Semester: VI, 2023-2024

Under the Guidance of

Prof. Shraddha Hiremath

K.L.E SOCIETY'S
KLE Technological University,
HUBBALLI-580031
2022-2023

SCHOOL OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that project entitled **" SECURING V2X COMMUNICATION "**is a bonafide work carried out by the student team of **Shreeshah Hegde(01FE21BEC226), Shrinidhi Togaleri(01FE21BEC136), Rakshan Kulkarni(01FE21BEC151), Nandish(01FE21BEC303)"**. The project report has been approved as it satisfies the requirements with respect to the Minor project work prescribed by the university curriculum for BE (VI semester) in School of Electronics and Communication Engineering of KLE Technological University for the academic year 2023-24.

Prof. Shraddha Hiremath	**Dr. Suneeta V Budihal**	**Dr. B. S. Anami**
Guide	**Head of School**	**Registrar**

External Viva:

Name of Examiners	**Signature with date**
1.	
2.	

ACKNOWLEDGMENT

We would like to express our gratitude towards our research guide Prof. Shraddha B Hiremath for her continuous support, encouragement, and guidance. We are grateful to her for setting high standards and giving us the freedom necessary for pursuing the project. .Our special thanks to Dr. Suneeta V Budihal, Head of School, Dr. Ashok Shettar, Vice-Chancellor of KLE Technological University, Hubballi, and Dr. P. G. Tewari, Principal, KLE Technological University, for providing us with an opportunity to undertake this unique course and pursue our desire for research. Finally, we would like to thank all teaching staff, non-teaching staff of the School of Electronics and Communication Engineering for their constant support and motivation for the successful completion of the project and also, we thank all our friends who helped us directly or indirectly in the completion of this project.

-Shrinidhi K T
Shreesha H
Rakshan K
Nandish

ABSTRACT

In the growing field of intelligent transportation systems, vehicle-to-everything (V2X) communication is essential to enable vehicles to interact with each other and with other vehicles infrastructure components. This project presents the development of a secure V2X data transmission system designed to ensure the integrity and authenticity of messages exchanged within this network. Using strong encryption techniques, the proposed system aims to prevent unauthorized access and tampering, thereby ensuring the reliability and security of vehicle data. Key features of the system include implementation of Elliptic Curve Cryptography (ECC) for efficient and robust security, optimized key management protocols for secure and resilient key exchange, and digital signature scheme such as ECDSA for message authentication. In addition, the system also integrates lightweight encryption solutions suitable for resource-constrained environments, ensuring minimal latency and computational costs. By meeting the critical need for secure data communications in V2X networks, the system helps improve road safety, optimize traffic management, and support the development of smart transportation infrastructure and sustainable.

Contents

1 Introduction **9**
- 1.1 Motivation . . . 9
- 1.2 Objectives . . . 10
- 1.3 Literature survey . . . 11
- 1.4 Problem statement . . . 12
- 1.5 Application in Societal Context . . . 13

2 System design **15**
- 2.1 Functional block diagram . . . 15
- 2.2 Final design . . . 16

3 Implementation details **18**
- 3.1 Specifications and final system architecture . . . 18
- 3.2 Algorithm . . . 20
- 3.3 Flowchart . . . 21

4 Optimization **23**
- 4.1 Introduction to optimization . . . 23
- 4.2 Types of Optimization . . . 24
- 4.3 Selection and justification of optimization method . . . 25

5 Results and discussions **26**
- 5.1 optimization . . . 27

6 Alignment with SDG **29**
- 6.1 Targets and Indicators . . . 30

7 Conclusions and future scope **31**
- 7.1 Conclusion . . . 31
- 7.2 Future scope . . . 31

8 References **32**

List of Tables

List of Figures

2.1 Functional Block Diagram 15
2.2 Final Design 17

3.1 Raspberry Pi 2 18
3.2 Nodemcu 19
3.3 mpu6050 20
3.4 Enter Caption 21
3.5 Enter Caption 22

5.1 server and client sharing symmetric key 26
5.2 communicating with encryption after symmetric key calculation 27
5.4 time profiling 27
5.5 packet before optimization 28
5.6 after optimization 28

6.1 SDG 11.2 29

Chapter 1

Introduction

1.1 Motivation

Creating a secure V2X information communication framework is driven by the critical have to be address the developing complexities and challenges of present day transportation. With the approach of associated and independent vehicles, the trade of information between vehicles and foundation has ended up a foundation of next-generation portability arrangements. In any case, this expanded network moreover presents noteworthy security dangers.

The judgment and genuineness of messages traded inside the V2X organize are vital for guaranteeing the security of travelers, the unwavering quality of transportation frameworks, and the assurance of basic infrastructure. Without satisfactory shields, malevolent on-screen characters seem misuse vulnerabilities within the communication framework, possibly driving to disastrous results such as mishaps, activity disturbances, or even sabotage.

By leveraging cryptographic methods, such as encryption and confirmation, able to build up a vigorous security system that secures against unauthorized get to and altering. Encryption guarantees that information transmitted between vehicles and framework remains private, defending delicate data from prying eyes. Verification instruments confirm the personality of communication partners, anticipating pernicious substances from imitating genuine vehicles or foundation components.

Additionally, a secure V2X communication framework ingrains believe within the unwavering quality and judgment of vehicular information, fundamental for cultivating far reaching appropriation and acknowledgment of associated vehicle innovations. Drivers, travelers, and partners must have certainty that the information traded inside the V2X arrange is exact, solid, and free from control.

By tending to the security challenges related with V2X communication, we not as it were relieve dangers but too open the complete potential of associated vehicle advances. More secure streets, decreased blockage, moved forward activity administration, and upgraded transportation effectiveness are fair a few of the benefits that can be realized through the improvement of a secure and strong V2X communication framework. Eventually, this contributes to making more brilliant, more secure, and more maintainable transportation environments for communities around the world.

Listening in:-

Everyone could read sensitive information by just listening in on the communication channel if data secrecy was not necessary. To fix this, just encrypt the messages sent by the car. We will use a symmetric key to accomplish this

Examining Traffic:-

A distinct symmetric key will be used for each session involving two cars, and this key will be shared via the Diffie-Hellmann algorithm. Thus, restricted data can be taken from an encrypted

stream in the same session. But since cars would be changing platoons often, this isn't seen to be a big deal.

Modification of the message:-

It would be best to utilize a channel that uses encryption to prevent anyone from changing the messages' content. An attacker might still alter the encrypted data, rendering the original communication unintelligible, even if we currently utilize encryption.

Replay To prevent message replay by an intruder

A sequence number needs to be appended to all forms of communication between two vehicles. The sequence number will be outdated during a replay-attack, making it clear that this is not an authentic message.

Inversion of Service:-

Communication breaks down when two vehicles overload their connection (for example, by sending a large number of packets at once). There is no way to solve this issue. A Denial-of-Service attack can also be carried out by focusing on a single car. If computationally demanding operations are requested too frequently, the car may become unresponsive and refuse to cooperate. Caching the findings can help with this.

Tracking of locations:-

It is impossible to track from outside this network because each platoon is a local network. The highest level of traceability possible is the ability to save a vehicle's public key, which can be obtained from a Certification Authority, and monitor subsequent encounters with the key.

Hijacking and man-in-the-middle:-

Different symmetric keys are used by every pair of automobiles that communicates. In this manner, traffic can't be hijacked because the hijacker would require the key in order to transmit important messages. It is also impossible to spoof the other entity because all messages are authenticated using its private key.

1.2 Objectives

The objective is to create a vigorous and secure V2X (Vehicle-to-Everything) information communication framework that guarantees the keenness and realness of messages traded between vehicles and foundation. V2X communication includes different intuitive, counting Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Network (V2N). The framework will use progressed cryptographic methods such as encryption, advanced marks, and hashing to secure information from unauthorized get to and altering.

Encryption will change over information into a secure arrange, guaranteeing that as it were substances with the proper unscrambling key can get to the data. Computerized marks will be utilized to confirm the personality of the message sender, guaranteeing that messages are without a doubt from true blue and trusted sources, hence anticipating pantomime. Hashing will change information into a fixed-size hash esteem interesting to the initial substance, making any changes to the information effectively distinguishable.

Guaranteeing the judgment of messages implies that the information remains unaltered amid transmission, which is pivotal for keeping up precise and dependable communications. Realness ensures that the messages start from confirmed and trusted sources, which is imperative for avoiding noxious on-screen characters from infusing wrong or deluding data into the V2X arrange. By joining rigid get to control measures, the framework will confine arrange and information get to to authorized substances as it were, subsequently anticipating unauthorized get to and pernicious exercises.

The system's plan points to supply reliable and reliable information communication, which is fundamental for the unwavering quality of vehicular intuitive. Dependable information communication is basic for making educated choices in real-time, whether for independent driving frameworks or driver-assist innovations. Keeping up the security of vehicular information is

vital, as vehicles progressively depend on exact data to explore, dodge collisions, and optimize activity stream.

Eventually, this secure V2X communication system points to upgrade the by and large unwavering quality and security of vehicular information, which is basic for the compelling working of cleverly transportation frameworks. By keeping up tall guidelines of information astuteness and genuineness, the framework will support secure decision-making forms in vehicles, contributing to more secure roadways and more proficient activity administration. This framework will be essential within the advancement and arrangement of progressed vehicular innovations, guaranteeing that as vehicles ended up more associated and independent, they can do so in a secure and dependable way.

1.3 Literature survey

[?]. Security Concerns for Automotive Communication and Software Architecture:-

• There is a dearth of integrated security solutions in automotive design. General and AUTOSAR-based systems, as well as communication protocols like CAN bus and Ethernet, present security challenges.

• CAN bus and Ethernet are two communication protocols that are essential for in-car connectivity; Ethernet is chosen because of its high bandwidth and cutting-edge technologies.

• Vulnerabilities in the CAN bus that allow for effective assaults on safety-critical ECUs, denial-of-service attacks, and wireless tire pressure monitoring systems are among the security issues with communication protocols.

• Integrity, authenticity, secrecy, and availability are the security criteria for automotive systems; symmetric cryptography is emphasized for message authentication.

• Cross-layer security, scarce resources for security measures, strict design limitations like real-time deadlines, and difficulties with plug-and-play architecture are some of the unresolved issues in vehicle cybersecurity.

• System-level security and hacking access points are two security issues associated with automotive software architecture, which includes sensors, ECUs, buses, and actuators.

[?]. Security Analysis of Intelligent Vehicles: Challenges and Scope:-

• Intelligent vehicles enable communication between infrastructure, gadgets, and other vehicles. This results in the generation of vast amounts of data, which must be securely transmitted to predetermined locations in order to protect user privacy.

• Future cybersecurity research issues for intelligent vehicles will require a security architecture to handle hardware and software components of automotive security challenges.

• Hardware and software security layers provide defense against attacks and vulnerabilities. V2V defenses, in-vehicle protection, and V2X security for data integrity and privacy are all part of the security of intelligent vehicles.

• Hardware security provides trusted execution environments, encryption, and secure booting to protect automotive components like CAN and ECUs from outside threats.

• By protecting operating systems, firewalls, network connectivity, and cryptography operations in intelligent cars, software security improves hardware security.

[3]. Automotive Security State of the Art and Future Challenges:-

• The study examines how, over the past 20 years, the complexity of electrical and software systems in automobiles has increased, emphasizing the growth in the quantity of electronic control units (ECUs) and Bluetooth or Internet connectivity.

• Hardware support is required for various security measures that have been deployed or will be introduced in the future, with a focus on hardware security modules.

• It highlights the significance of looking at the security of each ECU and the entire vehicle architecture due to the larger attack surface.

• The growth of threats in the automobile sector is also covered in the study, ranging from commonplace problems like theft to more dangerous assaults that have the potential to jeopardize safety-critical components in cars.

[4]. Astudy of Authentication Encryption Algorithms (POET, Deoxys, AEZ, MORUS, ACORN, AEGIS, AES-GCM) For Automotive Security :-

• The study contrasts seven lightweight, verified methods for protecting connected and self-driving vehicles against security breaches that could jeopardize public safety.

• To help choose the best algorithm for each application, it categorizes automotive embedded systems according to safety and security standards.

• The POET, Deoxys, AEZ, MORUS, ACORN, AEGIS, and AES-GCM algorithms were among those examined.

• It highlights the characteristics and factors to be taken into account of algorithms like as AES-GCM, AEGIS, ACORN, and MORUS and discusses metrics such nonce misuse resistance and network communications.

• The study highlights how crucial it is to select appropriate and effective algorithms in accordance with system constraints, resources, and requirements.

[5]. Poster: Hardware Based Security Enhanced Framework for Automotives:-

• Using hardware-based security primitives appropriate for automotive safety needs, the study proposes a security-enhanced framework and examines the threat model of the current CANbus communication protocol.

• It solves the security flaw in the CAN protocol as well as the problem of illegal access to cars via key fob hacks.

• To stop unwanted access and lessen replay assaults, the suggested architecture entails shared key generation, encryption with public and private keys, and secure communication between nodes.

• The NSF is funding the effort under grant number 1566530.

[6]. Vehicle to Vehicle Communication: Dedicated Short Range Communication and Safety Awareness:-

• By recommending security specifications and a modified RSA method for emergency warning transmission, the article increases security awareness for V2V DSRC.

• In VANET, emphasizes data privacy by encryption using digital certificates and secret keys.

In order to prevent system destruction, it is necessary to detect and prevent hostile behaviors in the network. Previous efforts on V2V communication security, such as MAC access delay analysis and congestion management approaches, are examined.

[7]. Secure V2V Communication with Identity-based Cryptography from License Plate Recognition:-

• The research focuses on identity-based cryptography and secure vehicle-to-vehicle communication for technologies such as autonomous driving, utilizing license plates for vehicle identification.

• It tests the viability of implementing this technology using Android devices, taking into account the range at which license plates may be identified as well as cryptographic primitives.

• Identity-based cryptography is suggested as a solution to the security issues in V2V communication caused by constrained processing power and bandwidth in the research.

• The significance of security in V2X communication is emphasized by discussing some projects and research efforts in the subject of secure vehicular communication.

1.4 Problem statement

Develop a secure V2X data communication system that ensures the integrity and authenticity of messages exchanged between vehicles and infrastructure using cryp-

tographic techniques. The system should prevent unauthorized access and tampering to maintain the reliability and safety of vehicular data.

1.5 Application in Societal Context

Improving Street Security

A secure V2X communication framework can significantly diminish street mischances and fatalities. By guaranteeing that the information traded between vehicles and foundation is true and tamper-proof, drivers and independent frameworks get exact data approximately street conditions, activity signals, and potential risks. For occasion, real-time alarms almost a sudden impediment on the street or a vehicle making an crisis halt can offer assistance avoid collisions. Bona fide and dependable V2X communications empower vehicles to form better-informed choices, in this manner upgrading the security of all street clients, counting people on foot and cyclists.

Progressing Activity Productivity

Effective activity administration is vital for lessening clog and minimizing travel time in urban zones. A secure V2X framework encourages consistent communication between vehicles and activity administration foundation, such as activity lights and street signs. By guaranteeing the judgment of this communication, activity signals can be powerfully balanced based on real-time activity stream information, diminishing bottlenecks and moving forward the by and large effectiveness of the transportation arrange. Solid V2X communication can too bolster facilitated vehicle developments, such as platooning, where a gather of vehicles voyages closely together at tall speeds with decreased discuss drag, driving to lower fuel utilization and emanations.

Empowering Independent Driving

The progression of independent vehicle innovation intensely depends on the secure and dependable trade of information. Independent vehicles must communicate with each other and with framework to explore securely and proficiently. A secure V2X framework guarantees that the information directing these vehicles is both exact and dependable, anticipating pernicious substances from interferometer with vehicle operations. Usually basic for picking up open believe in autonomous driving innovations, as any helplessness seem lead to security dangers and weaken certainty in these frameworks.

Supporting Keen City Activities

Keen cities point to use innovation to make strides the quality of life for their residents. A secure V2X communication framework may be a foundation of savvy city foundation, empowering different applications that improve urban living. For illustration, it can back brilliantly stopping frameworks that direct drivers to accessible stopping spaces, decreasing time went through looking for stopping and subsequently diminishing blockage and outflows. Moreover, secure V2X communications can encourage the integration of open transportation frameworks with private vehicles, advancing multimodal transportation arrangements that are more productive and ecologically inviting.

Ensuring Protection and Security

Within the computerized age, securing the security and security of people is vital. A secure V2X framework employments cryptographic procedures to guarantee that information isn't as it were ensured from unauthorized get to but moreover anonymized where vital to secure client protection. This implies that whereas vehicles can communicate fundamental data for security and productivity, individual information is kept private, tending to security concerns related with the far reaching sending of connected vehicle innovations.

Financial and Natural Benefits

The execution of a secure V2X communication framework can lead to noteworthy financial benefits by decreasing the costs related with street mishaps, activity clog, and fuel utilization. Besides, by optimizing activity stream and empowering more effective vehicle operations, such

a framework contributes to lower nursery gas emanations, supporting natural supportability objectives.

Chapter 2

System design

In this Chapter, we list out the interfaces.

2.1 Functional block diagram

To secure V2X communication, a strong cryptographic framework is fundamental to guarantee the secrecy, keenness, and realness of the messages traded between vehicles and framework. The framework laid out here leverages the standards of Open Key Framework (PKI) and Elliptic Bend Cryptography (ECC) to supply a secure communication channel. By utilizing littler, more proficient keys given by ECC, and a trusted Certificate Specialist (CA) to issue and manage advanced certificates, we will make a secure environment where as it were authorized hubs can exchange information. Usually basic for the security and unwavering quality of V2X communications, because it avoids unauthorized get to and guarantees that the messages come from a authentic source. We utilize the taking after system to guarantee secure trade of symmetric key and partner is in fact a veritable.

1. Make a CA Key Match: The Certificate Specialist (CA), as a foundation of believe, produces a key match utilizing the **EC SECP256R1* parameters. The private key is safely put away by the CA, whereas the open key is conveyed for signature confirmation purposes.

2. Create D/H Key Combine for Hub 1: Hub 1 makes a Diffie-Hellman (D/H) key match with the **EC SECP256R1* parameters, empowering the secure trade of cryptographic keys over a open organize.

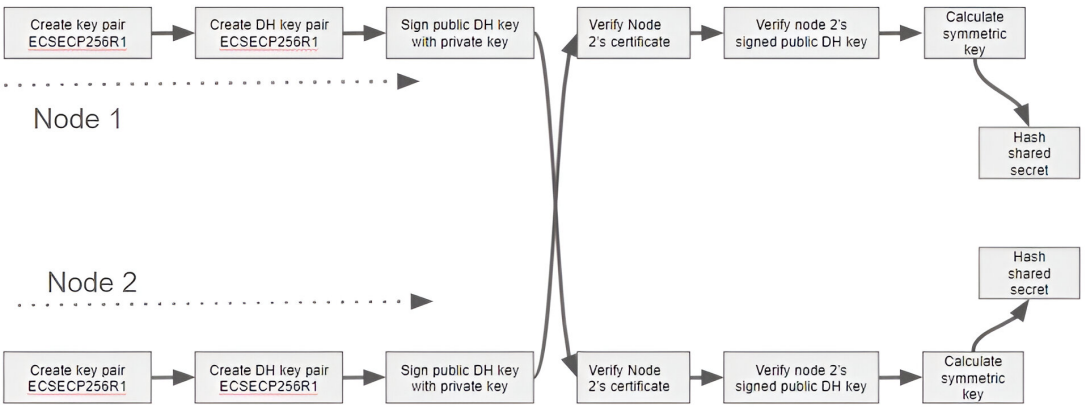

Figure 2.1: Functional Block Diagram

3. Sign Open Key: Hub 1's open D/H key is marked with its private key to make a unquestionable advanced signature, setting up the authenticity of the open key.

4. Trade of Open Keys: Hub 1 and Hub 2 trade their open keys, permitting them to scramble and decrypt messages in a secure way.

5. Confirm Hub 2's Certificate: Hub 2's certificate is confirmed against the CA's open key to affirm its authenticity and guarantee it has not been changed.

6. Confirm Hub 2's Marked Open Key: The signature on Hub 2's open key is confirmed utilizing the CA's open key to confirm its proprietorship.

7. Calculate Symmetric Keys: Symmetric keys are inferred utilizing Hub 1's private key and Hub 2's open key through the ECDH calculation, encouraging a secure communication channel.

8. Hash Shared Mystery: The shared mystery is hashed and truncated to **128 bits* to create a fixed-length encryption key, assist securing the communication prepare.

This system guarantees that each step within the communication prepare is secured, from key era to the ultimate encryption of messages, making V2X communication dependable and secure.

2.2 Final design

1. Components:

- The graph outlines a remote neighborhood zone organize (WLAN) setup. - It includes two Raspberry Pi computers, each prepared with particular components:

- ESP8266 Wi-Fi Module: These are spoken to by the Wi-Fi flag symbols over each Raspberry Pi. The ESP8266 modules empower remote communication.

MPU6050 Sensor: This sensor is associated to each Raspberry Pi. The MPU6050 may be a combination accelerometer and spinner, commonly utilized for movement detecting and introduction following.

2. Communication Stream:

- The two Raspberry Pi units communicate wirelessly through the WLAN. - The double-headed bolt labeled "WLAN" speaks to bidirectional communication between them. Here's how the communication might work:

- One Raspberry Pi (let's call it Pi A) collects information from its MPU6050 sensor (e.g., identifying movement or introduction changes). - Pi A scrambles this information and sends it over the WLAN to the other Raspberry Pi (Pi B). - Pi B gets the scrambled information, unscrambles it, and forms the data (e.g., activating an activity or overhauling a show). - Both gadgets can trade information back and forward in this way.

3. Applications:

- This setup has different applications:

- IoT (Web of Things): Envision utilizing these Raspberry Pi units to screen room temperature, detect movement, or control keen gadgets. - Mechanical autonomy: In mechanical autonomy ventures, comparable communication permits robots to share sensor information or facilitate activities wirelessly. - Farther Detecting: For natural observing, these gadgets may collect information (e.g., mugginess, light levels) and transmit it to a central server.

4. Security Contemplations:

- When transmitting information wirelessly, security is vital. The method might include:

- Key Trade: The exchangecert() step likely alludes to trading security certificates or keys for secure communication.

- Encryption: The "encrypt(data)" step guarantees that information remains private amid transmission.

- Framework Wellbeing Checks: The parallel arrangement checks framework status ("lively" or "dead") and association unwavering quality ("checkconn()").

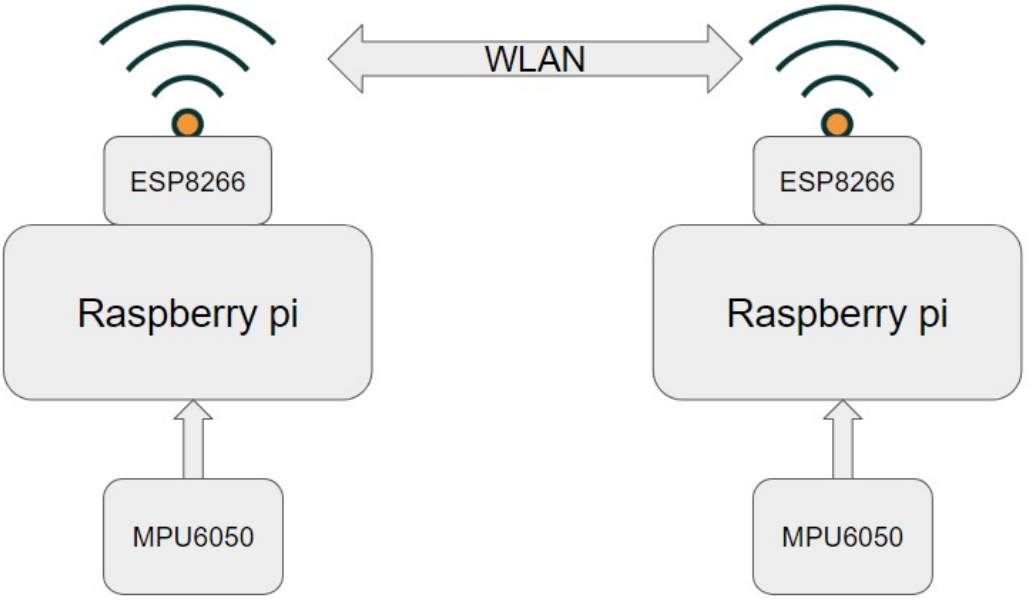

Figure 2.2: Final Design

Chapter 3

Implementation details

3.1 Specifications and final system architecture

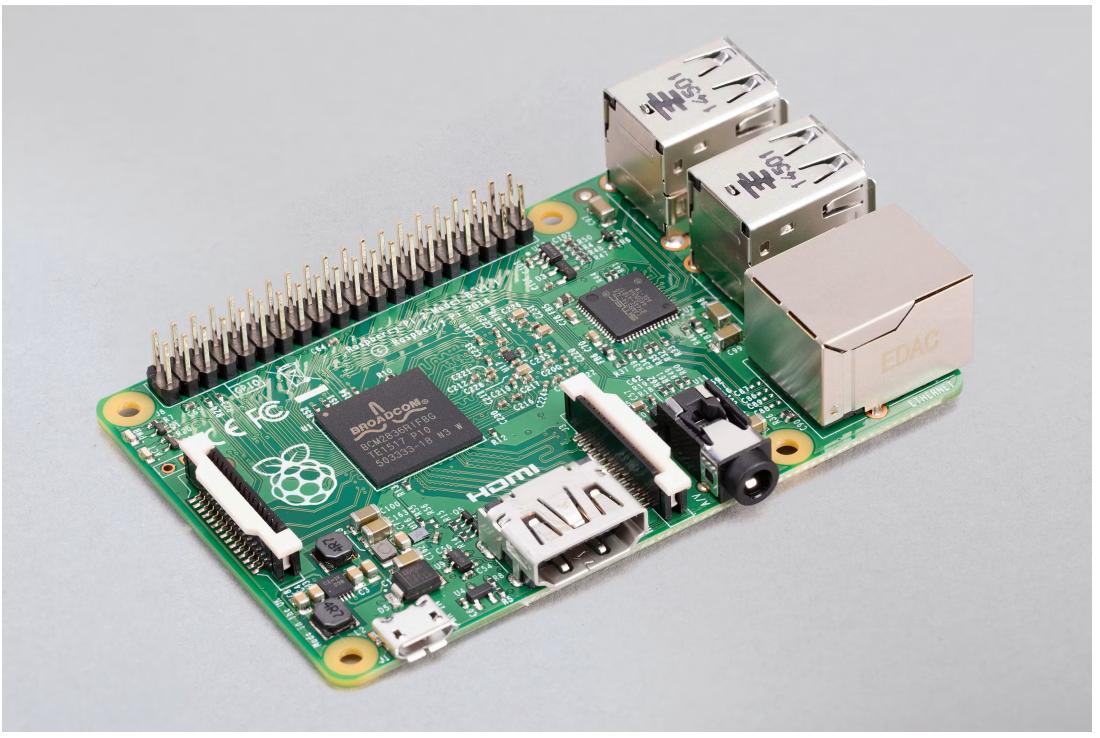

Figure 3.1: Raspberry Pi 2

Specifications
- 900 MHz quad-core ARM Cortex-A7 CPU
- 1 GB RAM
- VideoCore IV 3D graphics core
- Ethernet port
- Four USB ports
- Full-size HDMI output
- Four-pole 3.5 mm jack with audio output and composite video output

• 40-pin GPIO header with 0.1-spaced male pins that are compatible with our 2×20 stackable female headers and the female ends of our premium jumper wires.
• Camera interface (CSI)
• Display interface (DSI)
• Micro SD card slot

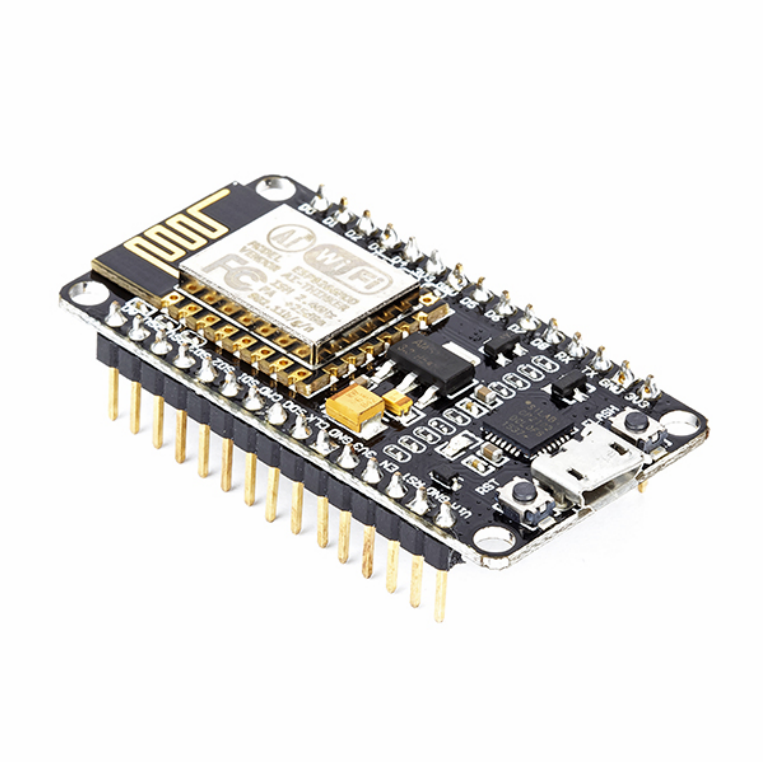

Figure 3.2: Nodemcu

Specifications
• Model: ESP8266-12E
• Wireless Standard: 802.11 b/g/n
• Frequency range: 2.4 GHz - 2.5 GHz (2400M-2483.5M)
• Wi-Fi mode: Station / SoftAP / SoftAP+station
• Stack: Integrated TCP/IP
• Output power: 19.5dBm in 802.11b mode
• Data interface: UART / HSPI / I2C / I2S / Ir
• Remote Control GPIO / PWM
• Supports protection mode: WPA / WPA2
• Encryption: WEP / TKIP / AES
• Power supply: from 4.5 VDC to 9 VDC (VIN) or via micro USB connector
• Consumption: with continuous Wi-Fi transmission about 70 mA (200 mA MAX) - in standby ¡ 200µA
• Operating temperature: from -40°C to +125°C
• Dimensions (mm): 58×31.20×13
Specifications
• Chip: MPU-6050.
• Power supply: 3 5V Onboard regulator.

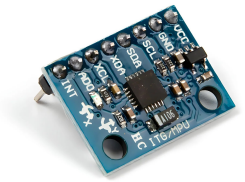

Figure 3.3: mpu6050

- Communication mode: standard IIC communication protocol.
- Chip built-in 16bit AD converter, 16bit data output.
- Gyroscopes range: +/- 250 500 1000 2000 degree/sec.
- Acceleration range: +/- 2g, +/- 4g, +/- 8g, +/- 16g.
- Pin pitch: 2.54mm.

3.2 Algorithm

• Here's an clarification of each step concurring:

1. Start - The method starts here.

2. interface() - Builds up a arrange association between Hub 1 and Hub 2.

3. init-node() Initialize Hub: Stack the node's certificate, private key, and the CA's open key from records.

Reason: Build up the node's personality and empower cryptographic operations.

4. exchange$_{c}ert()$

- Trade Certificates:

- Send Hub 1's certificate to Hub 2. - Get Hub 2's certificate. - Approve the gotten certificate utilizing the CA's open key. - Reason: Guarantee both hubs can verify each other.

5. dh$_{k}ey_{s}hare()$

- Perform Diffie-Hellman Key Trade:

- Produce a DH key match (open and private keys). - Sign the DH open key with the node's private key. - Trade DH open keys and marks with the peer. - Confirm the peer's DH open key and signature utilizing the peer's certificate. - Reason: Set up a shared mystery key safely.

6. calculate$_{s}ym_{k}ey()$

- Create Symmetric Key:

- Compute the shared mystery from the DH key trade and infer a symmetric AES key. - Reason: Utilize the symmetric key for scrambling and unscrambling messages.

7. read$_{s}ensor()$

- Examined Sensor Information:

- Assemble information from the MPU6050 sensor. - Reason: Collect the estimations to be sent to the peer.

8. check$_{c}onn()$

- Choice: Check in the event that the association is lively. - In the event that the association is dead, continue to the halt step. - In case the association is lively, proceed with the communication circle.

9. encrypt(data)

- Scramble Information:

- Utilize the symmetric key to scramble the MPU6050 sensor information. - Reason: Guarantee that the information being transmitted is secret.

10. send(encrypted)

- Send Scrambled Information:

- Transmit the scrambled sensor information to the peer. - Reason: Safely send information to the peer.

11. receive(encrypted)

- Get Scrambled Information:

- Get scrambled information from the peer. - Reason: Safely get information from the peer.

12. decrypt(encrypted)

- Decode Information:

- Utilize the symmetric key to unscramble the gotten messages. - Reason: Guarantee that the received data is clear and bonafide.

13. halt

- Conclusion Handle:

- End the secure communication session when the association is dead. - Reason: Cleanly conclusion the communication session.

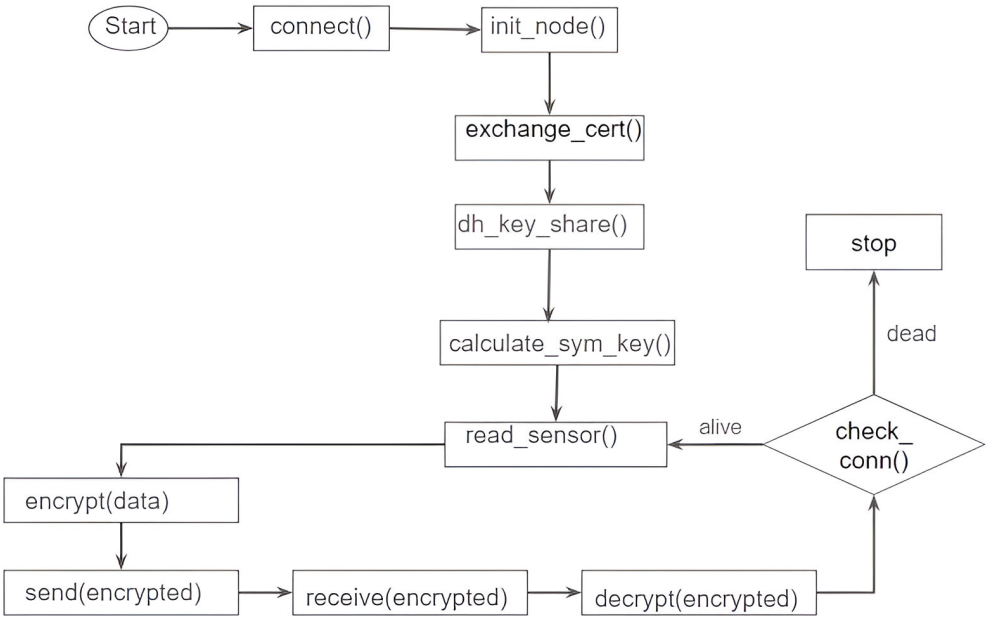

Figure 3.4: Enter Caption

3.3 Flowchart

Initialization Vector (IV) Generation:

An Initialization Vector (IV) is generated. The IV could be a irregular or pseudo-random esteem that's utilized beside a mystery key for information encryption. It guarantees that the same plaintext scrambled numerous times will yield distinctive ciphertexts.

Encryption with AES 128 bit GCM:

The plaintext message is scrambled utilizing the AES (Progressed Encryption Standard) calculation in GCM (Galois/Counter Mode). AES may be a symmetric encryption calculation,

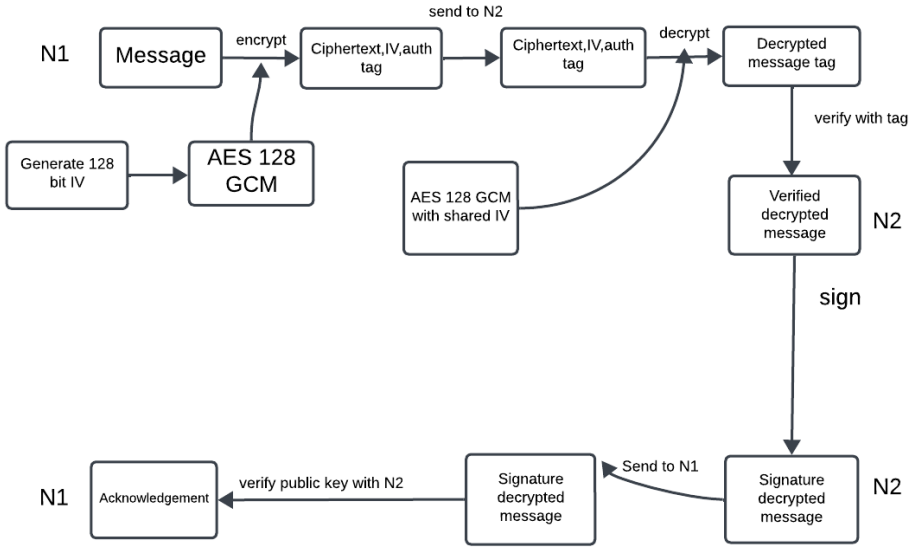

Figure 3.5: Enter Caption

meaning the same key is utilized for both encryption and decoding. GCM mode gives both information secrecy and information keenness by producing an confirmation tag.

Making Verification Labels:

Amid the encryption prepare, an verification tag is made. This tag is utilized to confirm the judgment and realness of the scrambled message. On the off chance that the message is changed in travel, the confirmation tag will not coordinate, demonstrating altering.

Marking Messages:

The scrambled message is marked employing a computerized signature calculation. This guarantees that the message has not been changed and confirms the character of the sender. Computerized marks utilize deviated cryptography, where a private key is used to sign the message, and a comparing open key is utilized to confirm the signature.

Message Transmission:

The scrambled and signed message, along with the IV and authentication tag, is transmitted to the beneficiary.

Receipt Affirmation:

The beneficiary recognizes the receipt of the message. This affirmation can be utilized to affirm that the message was effectively gotten and handled.

Decoding and Confirmation:

Upon accepting the message, the beneficiary employments the IV and the shared mystery key to decode the message utilizing AES 128 bit GCM. The beneficiary moreover confirms the verification tag to guarantee the message judgment. The beneficiary at that point confirms the computerized signature to affirm the sender's personality and guarantee the message has not been altered with. This prepare guarantees secure communication by giving secrecy, judgment, and realness of the messages traded between parties.

Chapter 4

Optimization

4.1 Introduction to optimization

Presentation to Optimization for Secure V2X Information Communication Frameworks

Within the quickly advancing scene of cleverly transportation frameworks, Vehicle-to-Everything (V2X) communication has risen as a foundation innovation, empowering vehicles to communicate with each other and with framework components. The improvement of a secure V2X information communication framework is basic to guarantee the judgment and genuineness of messages traded between vehicles and foundation. Such a framework must use cryptographic procedures to defend against unauthorized get to and altering, in this manner keeping up the unwavering quality and security of vehicular information.

Optimization in this setting includes a multifaceted approach to guarantee that the cryptographic and communication forms are effective, vigorous, and adaptable. The essential objectives of optimization incorporate minimizing computational overhead, decreasing idleness, guaranteeing tall security, and keeping up vitality proficiency, particularly given the asset imperatives normal in vehicular situations.

Key Zones of Optimization

1. Cryptographic Effectiveness:

- Calculation Determination: Choosing cryptographic calculations that offer solid security with negligible computational and memory prerequisites. For occurrence, Elliptic Bend Cryptography (ECC) gives tall security with littler key sizes compared to conventional strategies like RSA, coming about in speedier computations and diminished asset utilization. - Lightweight Cryptography: Executing lightweight cryptographic solutions that are particularly planned for situations with constrained preparing control and vitality assets, guaranteeing that the framework can perform productively without compromising security.

2. Key Administration:

- Productive Key Dissemination: Optimizing key administration conventions to guarantee that keys are dispersed and overseen safely and productively. This incorporates the utilize of Open Key Foundation (PKI) and session key foundation methods to encourage secure and energetic key trades. - Repudiation and Recharging: Creating proficient strategies for disavowing and recharging cryptographic keys to preserve security over time without presenting noteworthy delays or computational burdens.

3. Verification and Judgment Confirmation:

- Computerized Marks: Utilizing optimized advanced signature plans such as the Elliptic Bend Computerized Signature Calculation (ECDSA) to confirm the realness of messages whereas minimizing computational stack. - Group Confirmation: Executing clump confirmation strategies to proficiently confirm different marks at once, diminishing the by and large compu-

tational exertion required.

4. Communication Conventions:

- Low-Latency Conventions: Utilizing communication conventions that are optimized for low idleness and tall unwavering quality, such as the IEEE 1609.2 standard for V2X security administrations. These conventions guarantee that messages are transmitted and gotten rapidly and safely. - Productive Information Transmission: Diminishing the sum of information transmitted without compromising security, utilizing strategies such as information compression and effective encoding strategies.

5. Equipment Speeding up:

- Cryptographic Equipment: Leveraging specialized cryptographic equipment quickening agents to offload seriously cryptographic operations from the most processor, in this manner moving forward generally framework execution. - Trusted Stage Modules (TPMs): Utilizing TPMs for secure capacity of cryptographic keys and execution of cryptographic capacities, improving both security and proficiency.

6. Vitality Productivity:

- Energy-Aware Conventions: Planning conventions that minimize vitality utilization, which is vital for the supportability of vehicular frameworks. This incorporates optimizing the communication conventions to diminish control utilization and executing rest modes to moderate vitality when the framework is sit out of gear. - Obligation Cycling: Overseeing the dynamic and rest cycles of communication modules to guarantee that energy utilization is minimized without relinquishing the opportuneness and unwavering quality of information communication.

4.2 Types of Optimization

Cryptographic Optimization Methods

1. Proficient Cryptographic Calculations:

- Elliptic Curve Cryptography (ECC): ECC gives tall security with littler key sizes compared to conventional calculations like RSA, coming about in quicker computations and lower asset utilization. - Lightweight Cryptography: Planned for resource-constrained situations, such as vehicular systems, lightweight cryptographic calculations guarantee strong security without critical computational overhead.

2. Optimized Key Administration:

- Open Key Foundation (PKI): Effective administration of open and private keys, counting fast and secure key conveyance and disavowal instruments. - Session Key Foundation: Utilizing strategies like Diffie-Hellman for setting up session keys powerfully to guarantee secure communication with negligible computational taken a toll.

3. Advanced Marks and Verification:

- Proficient Computerized Signature Calculations: Utilizing optimized computerized signature plans like ECDSA (Elliptic Bend Advanced Signature Calculation) to guarantee message realness with negligible overhead. - Clump Confirmation: For scenarios where different marks got to be confirmed at the same time, group confirmation procedures decrease the by and large computational exertion.

Organize Optimization Procedures

1. Productive Communication Conventions:

- IEEE 1609.2 Standard: Indicates security administrations for V2X communications, counting message designs and handling methods optimized for moo inactivity and tall unwavering quality. - Devoted Short-Range Communications (DSRC): Optimized for low-latency communication, guaranteeing opportune and dependable message trade.

2. Information Judgment and Alter Location:

- Hash Capacities: Utilizing cryptographic hash capacities (e.g., SHA-256) to guarantee information astuteness. Optimized usage guarantee speedy hash computations. - Message Ver-

ification Codes (MACs): Guaranteeing information judgment and realness with negligible computational overhead through effective MAC calculations.

System-Level Optimization

1. Equipment Speeding up:

- Cryptographic Equipment Quickening agents: Utilizing specialized equipment to quicken cryptographic operations, lessening the computational burden on the most processor. - Trusted Stage Modules (TPMs): Leveraging TPMs for secure key capacity and cryptographic operations, upgrading both security and execution.

2. Vitality Proficiency:

- Energy-Efficient Conventions: Planning conventions that minimize vitality utilization, which is basic for vehicular frameworks with restricted control assets. - Rest Modes and Obligation Cycling: Optimizing the framework to enter low-power states when not effectively communicating, in this manner preserving vitality.

4.3 Selection and justification of optimization method

We have employed algorithm level optimization, which focuses on optimizing initializations, out of all the optimization techniques mentioned above. Because of its simplicity and isolation, algorithmic optimization is frequently easier than protocol- and cryptographic-level optimizations in an embedded security project. Algorithmic optimization is concerned with increasing the efficiency of individual algorithms by selecting or constructing algorithms that are as simple as possible in terms of time complexity and resource utilization. This approach often employs well-established computer science ideas like as loop unrolling, dynamic programming, and efficient data structures, and may be accomplished by straightforward, localized code modifications.

Protocol-level optimizations, on the other hand, need a thorough comprehension of the communication protocols in use as well as the ways in which these protocols interact with other system components and external systems. These improvements have to guarantee compatibility with current systems and standards, which sometimes entails difficult trade-offs between security, latency, and bandwidth. The complex mathematical underpinnings and demanding security requirements of cryptography make optimizations at the cryptographic level considerably more difficult. Cryptographic algorithms must be made more performant while yet remaining resilient to different kinds of assaults. This usually need for in-depth understanding of cryptography and careful balancing to prevent the introduction of vulnerabilities. We are utilizing algorithm-level improvements for the aforementioned reasons.

Chapter 5

Results and discussions

The outcomes of our implementation and some related insights will be covered in this chapter. Timing and memory profiling were performed after a successful key setup to make sure this could be used in real-time applications.

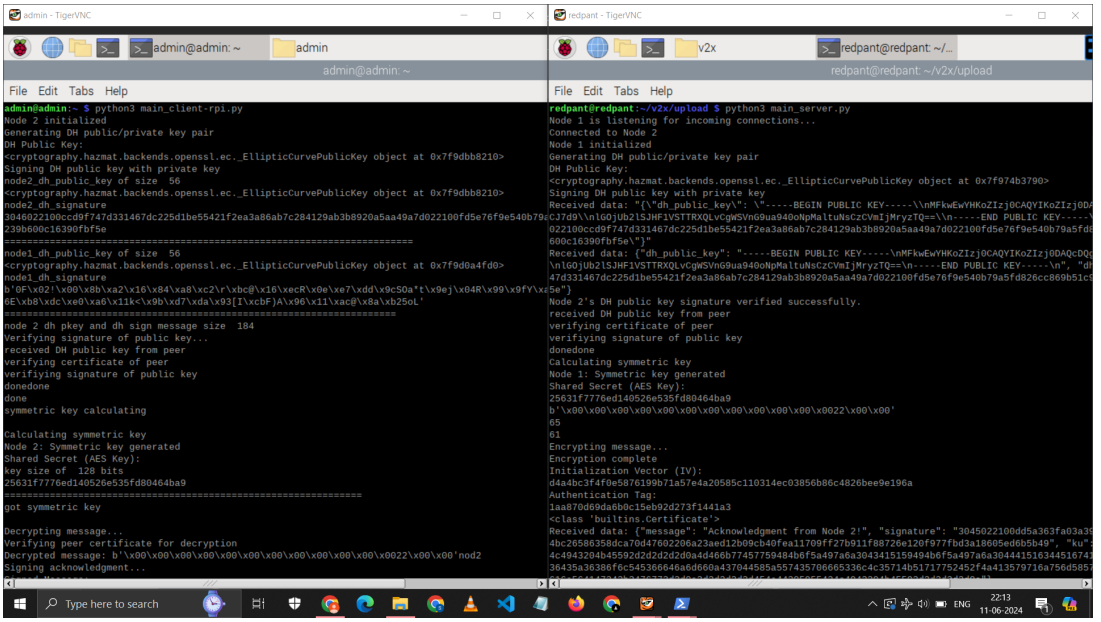

Figure 5.1: server and client sharing symmetric key

Figure 5.1 illustrates how to successfully establish trust by exchanging certificates and DH keys, verifying signatures, and computing the 128-bit symmetric key. The client is located on the left side of the window, while the server is located on the right side. We have not yet optimized the system. As we can see above, sharing the certificate at the outset will result in a smaller message size rather than sending it with the message every time. The upcoming chapter covers this section.

The whole encrypted packet's structure is seen in image 5.2. This does in fact contain an encrypted certificate, IV, message, and tag. This translates to 712 bytes. Figure 5.4 illustrates the peak memory utilization, which is 4.3 Mb.

As seen in figure 5.3, this arrangement took 0.0716 seconds to create the symmetric key immediately following the socket connection. However, in this instance, the speed will be constrained

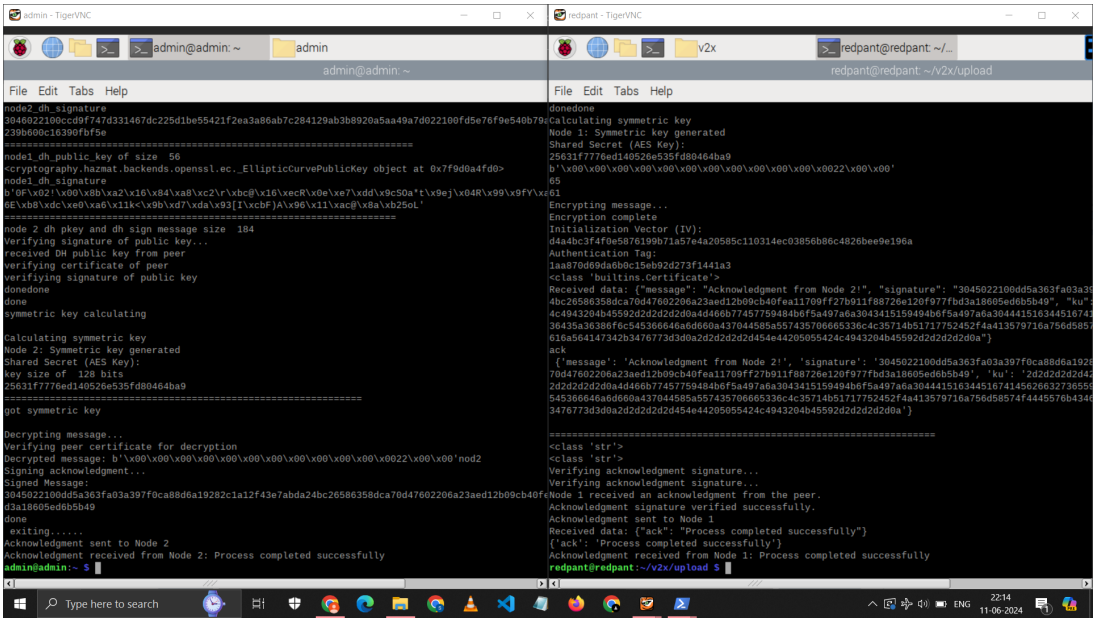

Figure 5.2: communicating with encryption after symmetric key calculation

by baudrate because we are utilizing an esp8266 as a socket and the raspberry is interacting with it via USB serial connection. However, in practical situations, rapid results may be obtained with the aid of strong connection. It implies that real-time applications are possible with this.

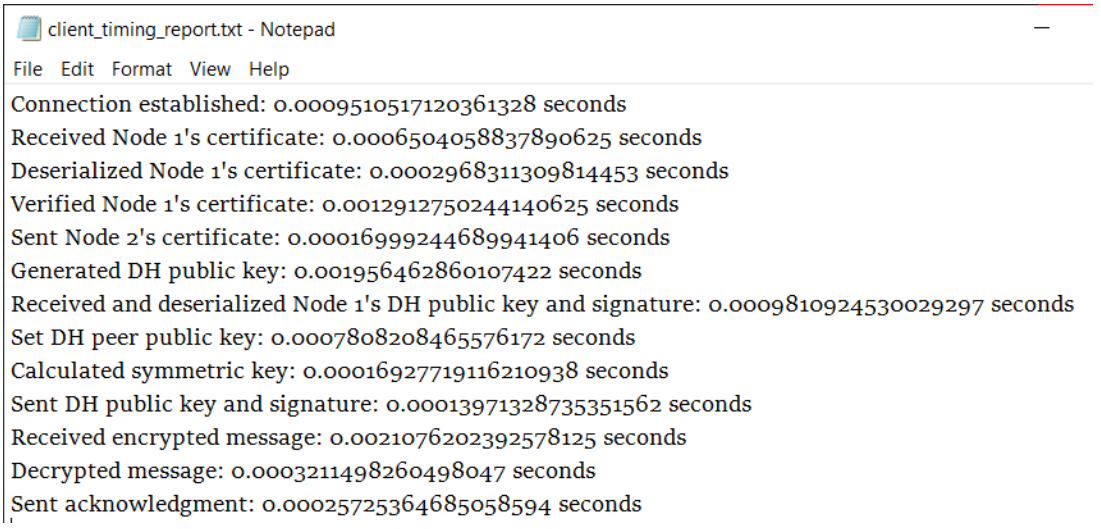

Figure 5.4: time profiling

5.1 optimization

As we previously said, we have decided to optimize the method, especially the initializations.

In our project, the certificate is sent with each encrypted communication at each stage of transmission in order to confirm the signature. In that instance, the packet requires a total of

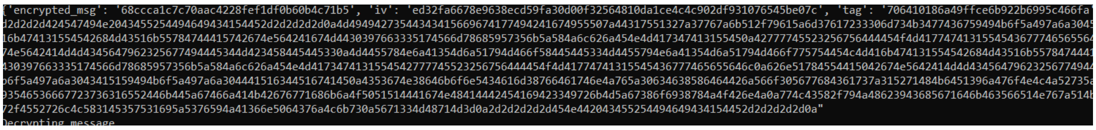

Figure 5.5: packet before optimization

712 bytes of RAM. The certificate (648 bytes) that we transmit with the message makes up the majority of its size. The longer it takes to reach the recipient, the larger the packet size.

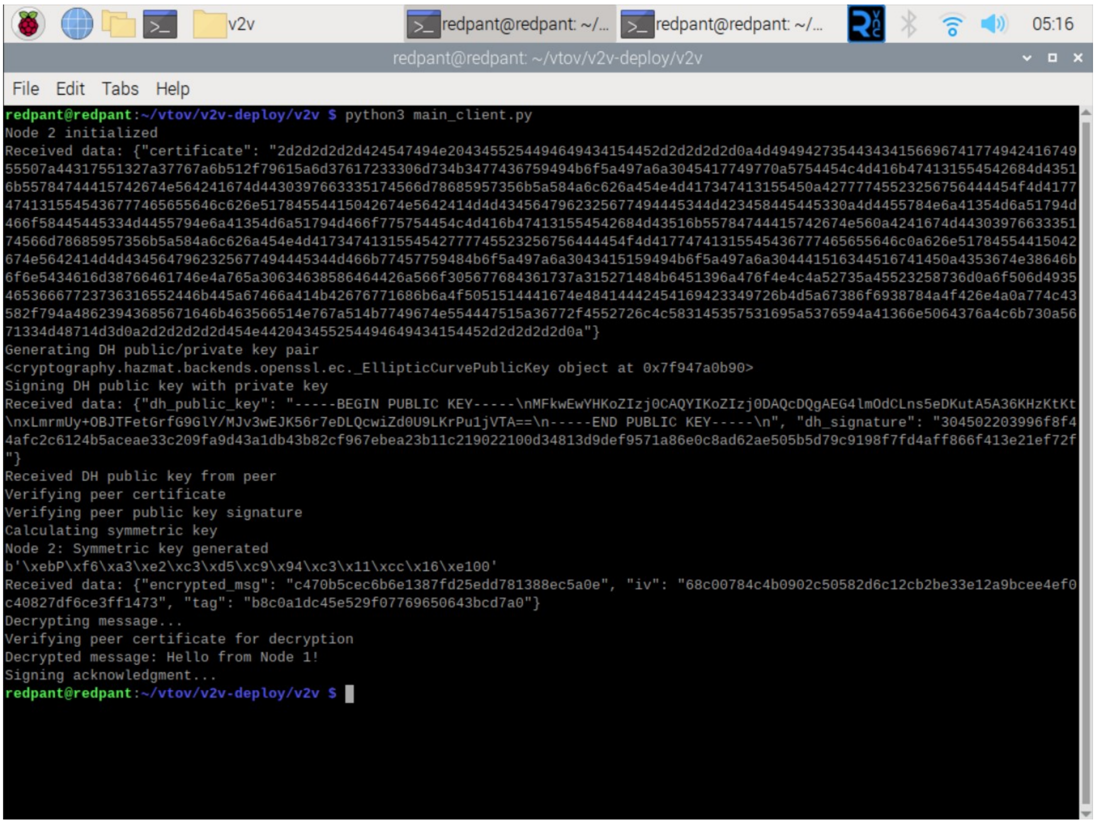

Figure 5.6: after optimization

In order to minimize packet size, we just exchange the certificate at the outset of trust formation in order to obtain the peer's public keys, eliminating the need to repeatedly communicate the same public keys. When we implement certification revocation procedures and use various keys for signatures on different messages to increase security, this optimization might need to be reviewed in the future. Following this optimization, 64 bytes were the size of the packet.

Chapter 6

Alignment with SDG

To ensure that everyone has access to safe, affordable, accessible, and sustainable transport systems, a secure Vehicle-to-Everything (V2X) data transmission system must be developed. This is in line with Sustainable Development Goal (SDG) 11.2 for transportation. Through the use of cutting-edge cryptographic algorithms, this system will guarantee the authenticity and integrity of messages sent between infrastructure and vehicles. The system will guard against tampering and unwanted access by utilizing strong authentication procedures, digital signatures, encryption, and cryptographic hash functions. By doing this, the safety and dependability of vehicular data will be preserved, which is essential for lowering the likelihood of accidents and improving road safety. Furthermore, the safe functioning of autonomous cars, stakeholder and user trust, and the uptake of V2X technologies will all be facilitated by the secure V2X system. In the end, this project will fulfill SDG 11.2 by helping to build safer and more resilient urban and rural transportation infrastructure.

Figure 6.1: SDG 11.2

6.1 Targets and Indicators

With certain goals and indicators, the creation of a secure V2X data communication system in line with SDG 11.2 can be monitored. By 2030, the main goal is to have a dependable and secure V2X communication infrastructure in place, guaranteeing that all messages sent back and forth between vehicles and the infrastructure are verified and shielded from manipulation. The frequency of traffic accidents caused by malicious interference or communication breakdowns, the proportion of vehicles having secure V2X systems, and the rate at which transportation authorities are implementing V2X technology are important metrics to track development. Survey-based measures of user trust in the V2X system, the average time to identify and react to tampering attempts, and the latency of V2X connections are further signs.In order to achieve SDG 11.2's goals of improving road safety, enabling the safe operation of autonomous vehicles, and assisting in the development of a resilient and sustainable transportation infrastructure, these targets and indicators will be helpful in evaluating the efficacy of the secure V2X communication system.

Chapter 7

Conclusions and future scope

7.1 Conclusion

The MPU6050 sensors were successfully integrated for accurate environmental data gathering, and enhanced security mechanisms specifically designed for V2X (Vehicle-to-Everything) connections were put in place. The system ensured safe and secured communication channels by using X.509 certificates for mutual authentication between nodes. In order to improve data confidentiality and integrity in V2X communications, secure symmetric key negotiation was made easier via the Diffie-Hellman key exchange. To protect sensitive data sent across the network, AES-GCM encryption was used, providing strong defense against manipulation and eavesdropping. Critical insights into resource consumption were obtained by memory profiling using 'psutil, paving the way for effective memory management and optimization techniques. Accurate measurement and monitoring of acceleration and gyroscope data, which are essential for real-time environmental sensing in V2X applications, were made possible by the integration of MPU6050 sensors. This project is an excellent example of how strict security procedures and sensor integration may work together.

7.2 Future scope

Developing a secure vehicle-to-everything (V2X) data transmission system is crucial for the development of intelligent transportation systems (ITS). By leveraging cryptographic techniques, such a system ensures the integrity and authenticity of messages exchanged between media and infrastructure, thereby preventing access and tampering. illegal. This secure communication framework not only maintains the reliability and security of vehicle data but also paves the way for various future innovations. The future scope of this issue statement includes the integration of advanced machine learning algorithms for anomaly detection and predictive maintenance, ensuring real-time data analysis for traffic management. better access and incorporate quantum-resistant encryption methods to protect against emerging quantum-driven threats. information technology. . Additionally, the system can be expanded to support seamless communication with autonomous vehicles and smart city infrastructure, thereby improving the efficiency and safety of urban mobility solutions. town. As V2X technology matures, this secure communications infrastructure will be the foundation to support innovations such as vehicle platooning, collaborative driving and enhanced environmental sensing, transforming the transportation landscape. modern pine.

Chapter 8

References

[1]. Yu, Huafeng, and Chung-Wei Lin. "Security concerns for automotive communication and software architecture." 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2016.

[2]. Singh, Madhusudan, and Shiho Kim. "Security analysis of intelligent vehicles: Challenges and scope." 2017 International SoC Design Conference (ISOCC). IEEE, 2017.

[3]. Jungk, Bernhard. "Automotive security state of the art and future challenges." 2016 International Symposium on Integrated Circuits (ISIC). IEEE, 2016.

[4]. Yeg, Authenticated Variable Yeg. "Astudy of Authentication Encryption Algorithms (POET, Deoxys, AEZ, MORUS, ACORN, AEGIS, AES-GCM) For Automotive Security."

[5]. Siddiqui, Ali Shuja, et al. "Poster: Hardware based security enhanced framework for automotives." 2016 IEEE Vehicular Networking Conference (VNC). IEEE, 2016.

[6]. Vershinin, Yu A., and Yao Zhan. "Vehicle to vehicle communication: dedicated short range communication and safety awareness." 2020 Systems of Signals Generating and Processing in the Field of on Board Communications. IEEE, 2020.

[7]. Andreica, Tudor, and Bogdan Groza. "Secure v2v communication with identity-based cryptography from license plate recognition." 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS). IEEE, 2019.