Vehicle Traffic Analysis

A PROJECT REPORT

Submitted by

Subhamay pal

Supervised by

Dr. SHARMISTHA ADHIKARI

in partial fulfilment for the award of the degree

of

M.Sc.

IN

IT (CYBER SECURITY)

Year : 2023-25

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY

Main Campus – Simhat, Haringhata, Nadia – 741249

BONAFIDE CERTIFICATE

This is to certify that this project report **"Vehicular Ad Hoc Networks**"is the bonafide work of Subhamay Pal who carried out the project work under my supervision.

Signature of the HoD	**Signature of the Supervisor**
Dr. Pabitra Pal	**Dr. Sharmistha Adhikari**
HEAD OF THE DEPARTMENT	**SUPERVISOR**
Assistant Professor, Dept of Emerging Technologies , HoD, Dept of Computer Applications, Maulana Abul Kalam Azad University of Technology, Haringhata, Nadia, West Bengal-741249	Assistant Professor, Dept of Cyber Security, Maulana Abul Kalam Azad University of Technology Haringhata, Nadia, West Bengal- 741249

SIGNATURE

External Examiner

TABLE OF CONTENTS

ABSTRACT:

In a vehicular ad hoc network (VANET), there are many vehicles that can communicate with each other (vehicle-to-vehicle, V2V) and with the existing infrastructure (or vehicle-to-infrastructure, V2I) via wireless communication technology. Through V2V and V2I learning networks, coordinated data transmission can occur in real-time, improving road safety and traffic efficiency, and supporting intelligent transportation systems (ITS) [8]. Dedicated short-range communications (DSRC), fifth generation (5G), and other wireless communication technologies are in use for vehicular ad hoc networks (VANETs), used for applications such as collision avoidance, traffic monitoring, autonomy, amongst others. However, challenges like high mobility, frequent changes of topology, security vulnerabilities, and scalability issues, are essential for deployment. In this paper, we investigate the architecture, major technologies, applications, challenges, and future research directions of VANETs as an integral part of future intelligent transportation systems.

Keywords:

Ubuntu 18.04 LTS, NS3 version-ns-3.29, Sumo version-Eclipse SUMO Version v1_5_0+1154-40cc386 Open street Map,

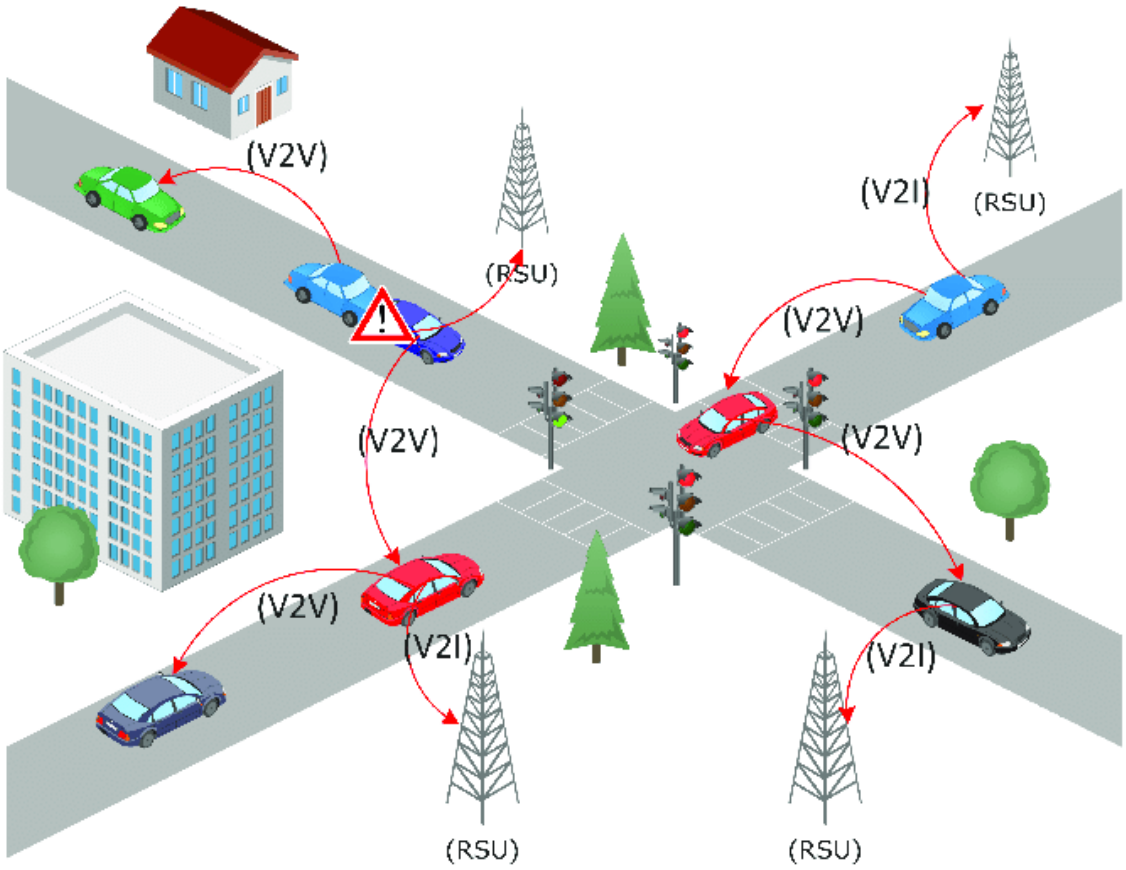
1. INTRODUCTION:

Vehicular Ad Hoc Network (VANET)is a type of Mobile Ad Hoc Network (MANET) that allows vehicle-to-vehicle and vehicular communication with roadside infrastructure. Aerial communication is an essential part of intelligent transportation systems (ITS), which is intended to improve road safety, traffic stream optimization, and infotainment services.

1.1 What is VANET?

The VANET is a more specialized type of mobile ad hoc networks (MANETs) that provides communications between vehicles and roadside, in other to address a vehicle communication. It allows vehicles to communicate with one another (V2V - Vehicle-to-Vehicle) and with road infrastructure (V2I - Vehicle-to-Infrastructure) for better road safety, traffic management, and driving efficacy.

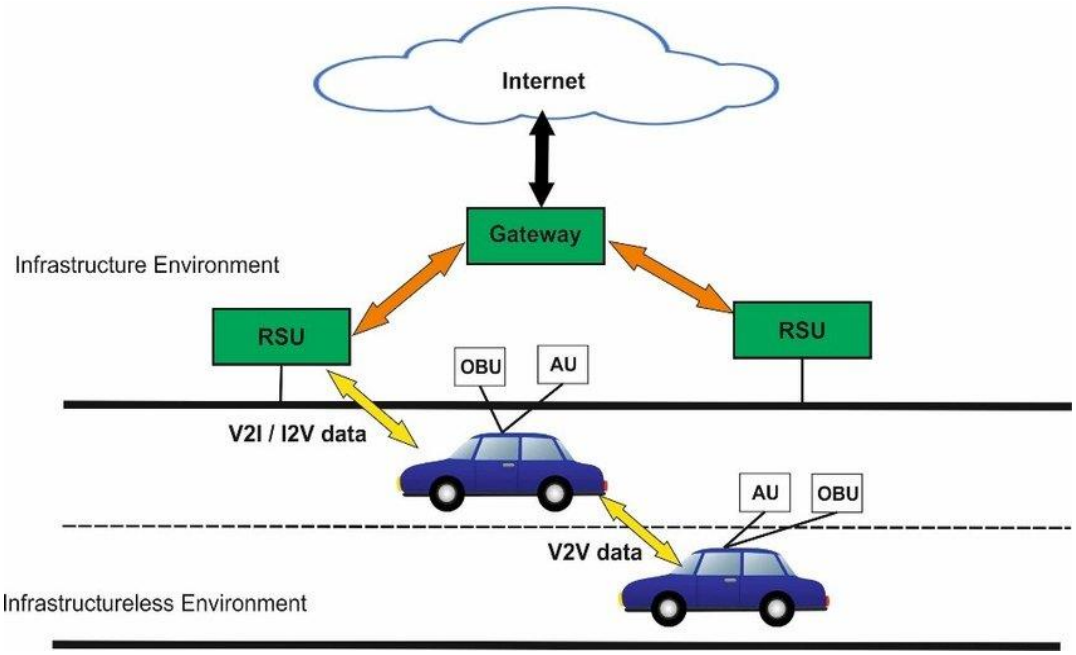
Basic Overview of VANET[21]



1.2 How VANET work?

In VANET (Vehicular Ad Hoc Network), it enables vehicles to connect and exchange information with one another and with roadside units through wireless communication technologies. This enables real-time data exchange to enhance safety, traffic management and driving efficiency VANET.

Work Process [22]



2. Components of VANET:

2.1 On-Board Unit (OBU):

- These small devices are fitted in vehicle for wireless communication.
- Based on DSRC (Dedicated Short-Range Communication), Wi-Fi or any 5G.

2.2 Roadside Unit (RSU):

- Permanent devices used at intersections, highways, or traffic signals.
- Serves as an intermediate layer between vehicles and traffic management systems.

2.3 Centralized Servers / Cloud:

- · Real-time traffic data storage and processing
- Aid to analytics, remote monitoring and making decisions

3. Working Mechanism of VANET:

3.1 Vehicle Sensing & Data Collection:

- Cars capture data on instantaneous speed, location, braking and road conditions.

3.2 Wireless Data Transmission

- V2V and V2I are used by vehicles to send and receive data.
- Communication using DSRC, Wi-Fi or 5G → fast and low-latency.

3.3 Data Processing & Decision Making

- Vehicles process the received data and respond to it (for example, slowing down if an accident is ahead).
- .RSUs and traffic management systems collect massive data for thorough city-wide traffic command.

3.4 Alert and Response

- Real-time alerts to the driver (traffic congestion, road accidents, emergency braking)
- This system enables autonomous cars to make automatic decisions based on the data received (e.g., rerouting).

.

4. VANET Communication Technologies:

Technology	Purpose
DSRC (Dedicated Short-Range Communication)	Low-latency, short-range communication (5.9 GHz).
5G / LTE-V2X	High-speed, long-range vehicle communication.
Wi-Fi	Used for infotainment and short-range vehicle connections.

5. Literature Review:

Year	Paper Name	Author Name	Summary	Limitations
2024	Security Control and Data Planes of SDN[1]	ABDINASIR HIRSI ABDLUKMAN AUDAHADEB SALH MOHAMMED A SALMAN AHMED	SDN enhances network management with flexibility and responsiveness but has a centralized control security risk	SDN centralized control and programmable data planes pose significant security challenges, making them targets for attacks.
2024	Security of Topology Discovery Service in SDN[2]	SANAZ SOLTANI ALI AMANLOU MOHAMMAD SHOJAFAR RAHIM TAFAZOLL	This paper provides a thorough survey to review and analyze existing threats against topology.	The Topology Discovery Service in SDNs is vulnerable to Topology Poisoning Attacks, risking network integrity and reliability.
2024	Exploring Security Dynamics in SDN Controller[3]	ARUSA KANWAL MOHAMMAD NIZAMUDDIN	SDN decouples control and data planes, enhancing security. This paper surveys SDN controllers, threats, and mitigation solutions	SDN's centralized control plane introduces significant security challenges across its layers, requiring robust solutions.
2024	Deep Reinforcement Learning-Based Technique for Enhancing Security and Performance in SDN-IoT Environments[4]	ZABEEHULLAH FAHIM ARIF NAUMAN ALI KHAN JAVED IQBAL	SDN enhances IoT network management with scalability and flexibility. The DQQS model improves routing, security, QoS, and QoE.	The DQQS model's reliance on specific activation functions and DL models limits its adaptability to diverse and evolving threats.
2023	A survey of the characteristics of SDN, NFV and information security in IoT and 5G networks [5]	Roger William Coêlho ElvioJoão Leonardo Luciana Andréia	This paper aims to elucidate some conceptions of what 5G technology is and the use of IoT in this network,	Mitigating vulnerabilities in the link layer of 5G transmission technology
2018	A Survey on Security-Aware Measurement in SDN[6]	Heng Zhang ZhipingCai Qiang Liu	we review the basic architecture of SDN and corresponding security challenges.	We focus on promoting a more balancing measurement method instead of evident shortage.

2019	A Completed Secure and Scalable Framework Using the Software-Defined Perimeter[7]	.AHMED SALLAM AHMED REFAEY ABDALLAH SHAMI1	In particular, it provides a completely scalable and managed security solution	Furthermore, it would reduce the Operating Expense (OPEX) and Capital Expense (CAPEX) of enterprises
2018	Services and Security Threats in SDN Based VANETs[8]	Hammed Shafer RanaAsifRehman Byung-Seo Kim	Te introduction of SDN in VANET has simplified the management of the overall behavior of the network.	SDN controller can control the security threats. Throughout this survey
, 2020	Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET [9]	OTHMAN S. AL-HEETY ZAHRILADHA ZAKARIA MAHAMOD ISMAIL	.This survey acts as a catalyst in raising the emergent robustness routing protocol, latency, connectivity and security issues of future SDN-VANET architectures	This survey is the first to address the strengths and weaknesses of VANET infrastructures
2020	SDN/NFV-Based Security Service Function Tree for Cloud[10]	JING-LUN LUO SHUN-ZHENG YU SI-JIE PENG	we build a SecSFT in an experiment cloud and test and validate its security services in detection and mitigation of network attacks.	we will evaluate SecSFT with more types of attacks and compare it with the existing attack detection schemes.
2024	Enhancing Multi-Operator Network Handovers With Blockchain-Enabled SDN Architecture[12]	Asuquo A. Okon Karam M. Sallman NishantJagannath	Integrating SDN and block chain improves 6G networks. Raft consensus mechanism reduces delays. Cell residence time impacts performance. Analytical models and simulations validate findings.	Evaluating energy efficiency, resource allocation, and AI-driven predictive mobility management in block chain-enabled SDN networks remains an open research challenge.
2023	A Comprehensive Analysis of Machine Learning- and Deep Learning-Based Solutions for DDoS Attack Detection in SDN[13]	ShashankSrivastava M. M. Gore1	SDN improves network management but faces DDoS vulnerabilities. Machine learning solutions detect attacks; SDN-specific datasets are needed.	Timely handling of DDoS attacks in SDN remains a significant challenge.

2023	Controller placement problem during SDN deployment in the ISP/Telco networks[14]	BinodSapkota. Babu R Dawadi. Shashidhar R Joshi.	SDN deployment in large-scale ISP/Telco networks faces challenges in controller placement and load balancing.	Current research on SDN controller placement focuses mainly on data centers, lacking effective solutions for large ISP/Telco networks
2024	SDN-Based VANET Routing[15]	NehadHameed Hussein Siaw Paw Koh Chong Tak Yaw	. This study reviews SDN-based VANET routing protocols, detailing mechanisms, strengths, and challenges for improved vehicular networks.	Limited practical implementation of SDN in VANETs hinders real-world evaluation and refinement of proposed routing protocols. .
2024.	Genetic Algorithm-Powered QoS-Aware Cross-Network Traffic Engineering in BlockchainEnabled SDN [16]	. MURAT KARAKUS	GATE-BC integrates Genetic Algorithms, SDN, and Blockchain for superior QoS-aware network traffic management.	Higher Path Setup Time (PST) due to GA's computational demands.
2024	Federated Learning for Privacy-Preserving Intrusion Detection in Software-Defined Networks [17]	MUBASHAR RAZA MUHAMMAD JASIM SAEED MUHAMMAD BILAL RIAZ MUHAMMAD AWAIS SATTAR	SDN revolutionizes networking but needs secure IDS. Federated learning improves IDS by preserving data privacy.	High accuracy in FL-based IDS requires meticulous model tuning and data processing, which is complex.
2024	Optimal Topology Management for Software-Defined Networks Minimizing Latency and Using Network Slicing[18]	Andre´s Viveros Pablo Adasme	The paper proposes models and algorithms for managing user connections in SDN, optimizing latency and resource efficiency.	. The quadratic models require significant CPU time as network complexity increases, favoring the heuristic algorithm.
2024	Analysis of the SNORT intrusion detection system using machine learning[19]	Ouafae El Aeraj CherkaouiLeghris	Cyber-attacks increasingly exploit vulnerabilities, impacting individuals and businesses. IDS like SNORT, enhanced with machine learning,	Machine learning models in SNORT may require extensive resources and fine-tuning for optimal performance.

			improve network security.	
2024.	Research on Detection and Mitigation Methods of Adaptive Flow Table Overflow Attacks in Software-Defined Networks[20]	YING ZENG YONG WANG YUMING LIU	.ALFO targets SDN's TCAM capacity with low-rate attacks. ALFO-Guard detects and mitigates these attacks effectively	ALFO-Guard's system overhead and real-world deployment remain challenges, with future work needed for optimization.
2024	Threat Taxonomy, Implications, and Open Challenges[21]	MOHAMED RAHOUT KAIQI XIONG YUFENG XIN	SDN enables dynamic, flexible network control via separation of control and data planes, improving management but introducing new security vulnerabilities	SDN faces security issues with increased smart device connections and traffic.

6. What are the security challenges:

Vehicular Ad Hoc Networks (VANETs) are highly dynamic networks that enable vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. However, they face several security challenges due to their open wireless communication environment,

5.1 Authentication and Access Control:

- Ensuring only legitimate vehicles and infrastructure nodes can participate in the network.
- Preventing unauthorized users from injecting malicious data.

5.2 Privacy and Anonymity:

- Protecting drivers' identities and location data from unauthorized tracking.
- Balancing privacy with law enforcement needs (e.g., identifying malicious vehicles).

5.3 Data Integrity and Trust

- Ensuring messages (e.g., accident alerts, traffic updates) are not altered during transmission.
- Edifying the trustworthiness of the sender before acting on the message.

5.4 Replay Attacks

- Protecting against attackers replaying old messages to create confusion or false warnings.

5.5 Man-in-the-Middle (MitM) Attacks

- Preventing attackers from intercepting and altering messages between communicating vehicles.

5.6 Malware and Rogue Nodes

- Detecting and mitigating malware-infected vehicles or compromised roadside units (RSUs).

7. Attacks:

7.1 Distributed Denial of Service (DDoS) Attacks:

Description: Overwhelm the VANET controller or network resources with excessive traffic.

Impact: Can cripple network operations, making the network unresponsive or slow.

7.2 Man-in- the-Middle Attack(MITM):

Description: Intercept and potentially alter communications between the VANET controller and network devices.

Impact: Allows attackers to eavesdrop on or modify network traffic

7.3 Controller Attack:

Description: Target the central SDN controller to exploit vulnerabilities and gain control over the network.

Impact: The controller can result in full network control.

8. Research Objective

- In this project our motivation is study in details the overall VANET architecture and routing in respect to the existing relevant security threats on VANET.
- To develop and improve secure routing mechanism unique state of the ECC technique.
- To simulate our proposed frame work in NS3.

9. Brief Study on ECC

ECC: A public key cryptography based on the algebraic structure of elliptic curves over finite fields.

9.1 **Introduction to ECC**

9.2 Benefits of ECC

9.3 Applications of ECC

- **Introduction to ECC:** Elliptic Curve Cryptography (ECC) is a form of public key cryptography, based on the algebraic structure of elliptic curves over finite fields. They convert commonly used data into a fraction of the original size. The internet also benefits from ECC for security purposes. ECC is used to secure digital communications and provides a relatively high level of security with smaller thin keys.
- **Benefits of ECC:**

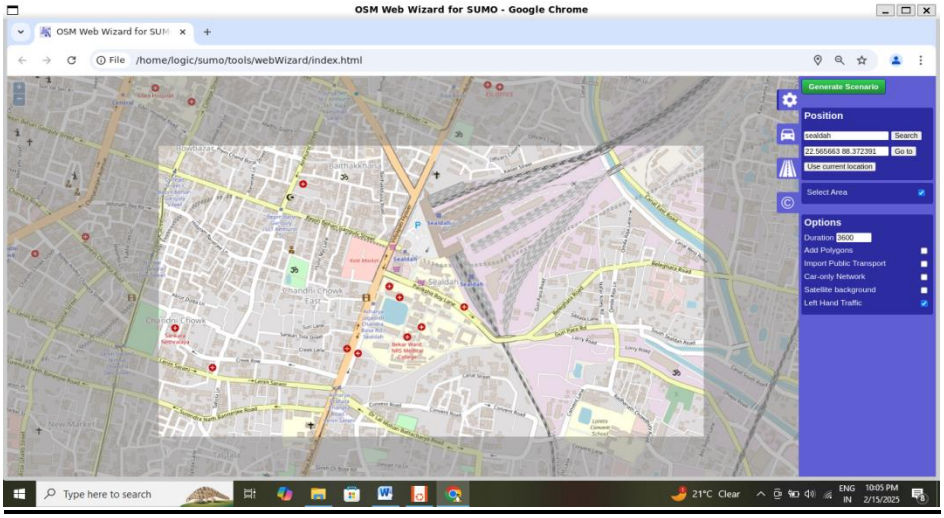
- **Strong Security:** ECC, at relatively smaller key sizes, offers a better level of security when Compared with other algorithms such as RSA. For instance, a 256-bit key in ECC has comparable security to a 3072-bit key in RSA
- **Efficiency:** Smaller key sizes result in faster computations, reduced storage requirements, and lower power consumption, making ECC suitable for mobile and IoT devices.

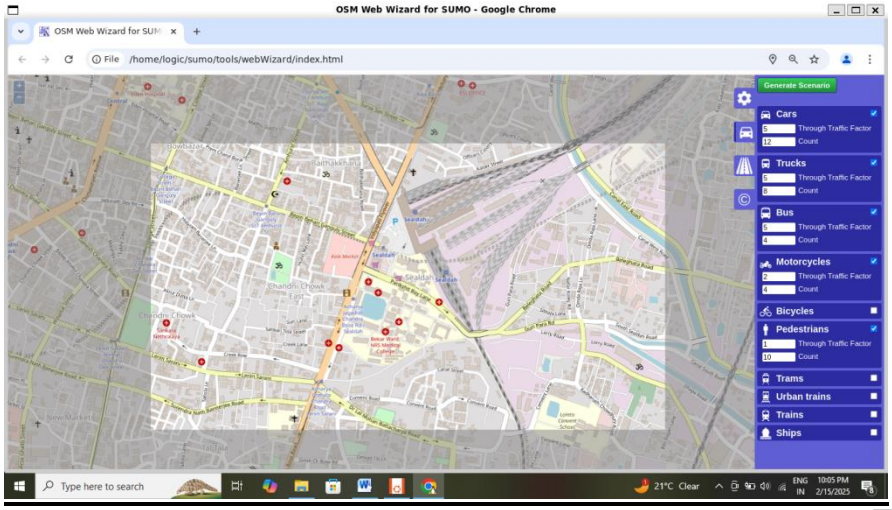
- **Applications of ECC**

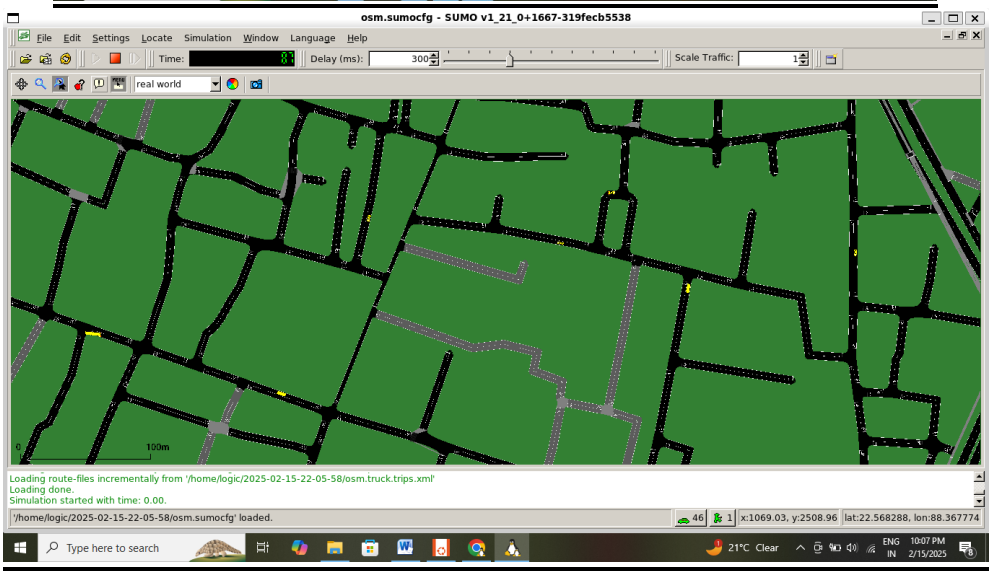
- **Digital Signatures**: ECC is used in ECDSA (Elliptic Curve Digital Signature Algorithm) to authenticate messages.
- **Diffie-Hellman Key Exchange:** ECC is used as ECDH (Elliptic Curve Diffie-Hellman) to securely exchange keys solution

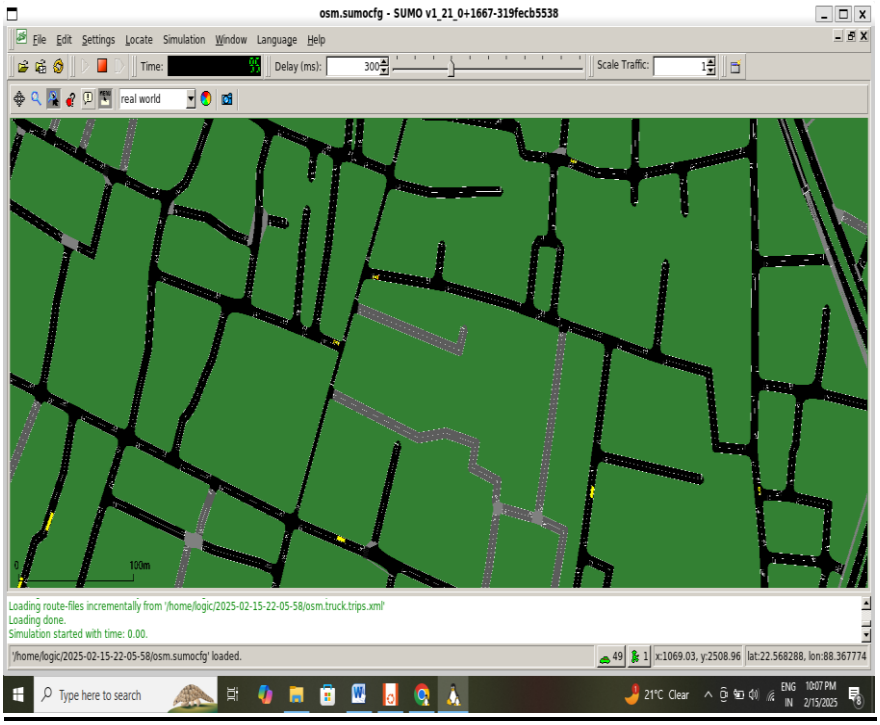
- **Encryption:** ECC-based schemes, like ECIES (Elliptic Curve Integrated Encryption Scheme), are used for encrypting data.

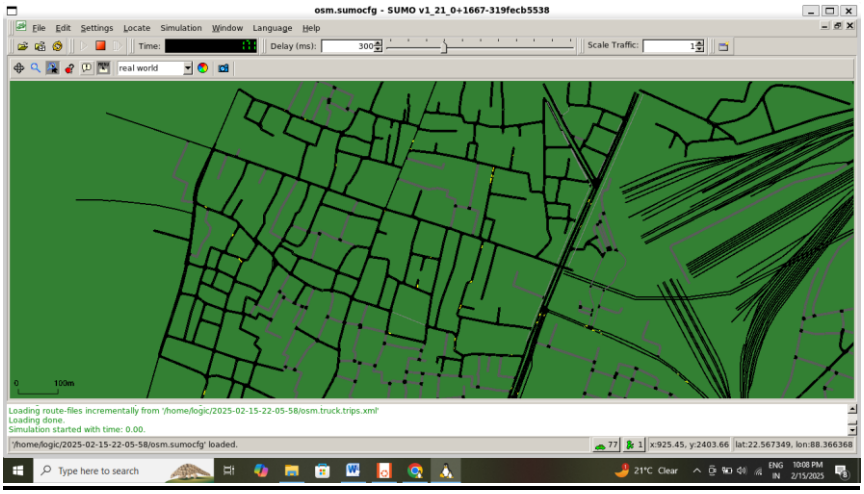
10.TESTING AND RESULTS:

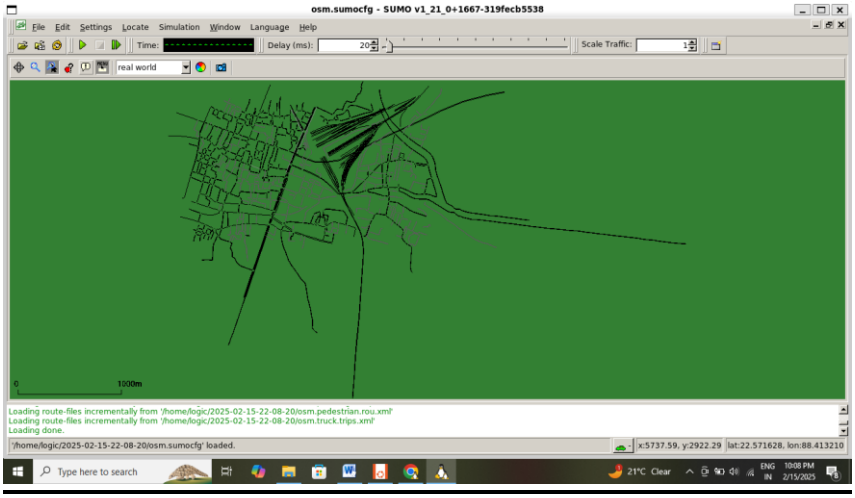







osm.sumocfg - SUMO v1_21_0+1667-319fecb5538
File Edit Settings Locate Simulation Window Language Help
Time:
Delay (ms):
300
Scale Traffic:
1
real world
0
100m
Loading route-files incrementally from '/home/logic/2025-02-15-22-05-58/osm.truck.trips.xml'
Loading done.
Simulation started with time: 0.00.
'/home/logic/2025-02-15-22-05-58/osm.sumocfg' loaded.
49
1
x:1069.03, y:2508.96
lat:22.568288, lon:88.367774
Type here to search
21°C Clear
ENG
IN
10:07 PM
2/15/2025


osm.sumocfg - SUMO v1_21_0+1667-319fecb5538
File Edit Settings Locate Simulation Window Language Help
Time:
Delay (ms): 300
Scale Traffic: 1
real world
0 100m
Loading route-files incrementally from '/home/logic/2025-02-15-22-05-58/osm.truck.trips.xml'
Loading done.
Simulation started with time: 0.00.
'/home/logic/2025-02-15-22-05-58/osm.sumocfg' loaded.
x:925.45, y:2403.66
lat:22.567349, lon:88.366368
Type here to search
21°C Clear
ENG IN
10:08 PM 2/15/2025


osm.sumocfg - SUMO v1_21_0+1667-319fecb5538
File Edit Settings Locate Simulation Window Language Help
Time:
Delay (ms): 20
Scale Traffic: 1
real world
0 1000m
Loading route-files incrementally from '/home/logic/2025-02-15-22-08-20/osm.pedestrian.rou.xml'
Loading route-files incrementally from '/home/logic/2025-02-15-22-08-20/osm.truck.trips.xml'
Loading done.
'/home/logic/2025-02-15-22-08-20/osm.sumocfg' loaded.
x:5737.59, y:2922.29
lat:22.571628, lon:88.413210
Type here to search
21°C Clear
ENG IN
10:08 PM 2/15/2025

11. CONCLUSION

Motor vehicle ad hoc networks (VANETs) play a key role in its developmental phase of road safety, traffic efficiency and development of intelligent transportation systems. Although due to their openness, portability and real-time embodied some security challenges such as authentication, privacy, data integrity, cyber-attack, and beyond, etc. To break these above limitations, secure techniques (cryptographic authentication, intrusion detection system, block chain, and machine learning based threat detection) are required to be implemented in the VANETs. Even though the community research on VANET security measures has become clear, special attention should be paid to identify the right trade-off regarding effectiveness, scalability, and privacy since it is necessary for efficient deployment. It is equally, to a great extent, necessary with the functionalities of intelligent and autonomous vehicular transportation system from helping to set up an adequate safe and efficient vehicular networks for VANET, in order to provide these functionalities of intelligent and autonomous vehicle transportation system.

12. Future work:-

Vehicular Ad Hoc Networks (VANETs) are a crucial component of Intelligent Transportation Systems (ITS), enabling vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. Future work in VANET research focuses on improving reliability, security, scalability, and efficiency. Here are some key areas for future development:

A. Security and Privacy Enhancements

- Developing stronger encryption and authentication mechanisms to prevent cyber-attacks.
- Implementing block chain-based security frameworks for secure data exchange. Edge and Cloud Computing for VANETs

B. Edge and Cloud Computing for VANETs

- Utilizing edge computing to reduce latency in vehicle communications.
- Enhancing cloud-VANET integration for improved data storage, processing, and real-time decision-making.

C. Advanced Routing and Network Management

- Designing robust routing algorithms for high-mobility environments.
- Implementing predictive analytics for better traffic flow optimization.

[1] Abdi, A. H., Audah, L., Salh, A., Alhartomi, M. A., Rasheed, H., Ahmed, S., &Tahir, A. (2024). Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI and MTD Approaches to Security Solutions. ***IEEE Access*****.**

[2] Soltani, S., Amanlou, A., Shojafar, M., &Tafazolli, R. (2024). Security of Topology Discovery Service in SDN: Vulnerabilities and Countermeasures. ***IEEE Open Journal of the Communications Society*****.**

[3] Kanwal, A., Nizamuddin, M., Iqbal, W., Aman, W., Abbas, Y., &Mussiraliyeva, S. (2024). Exploring Security Dynamics in SDN Controller Architectures: Threat Landscape and Implications. ***IEEE Access*****.**

[4] Arif, F., Khan, N. A., Iqbal, J., Karim, F. K., Innab, N., &Mostafa, S. M. (2024). DQQS: Deep Reinforcement Learning based Technique for Enhancing Security and Performance in SDN-IoT Environments. ***IEEE Access*****.**

[5] M. Dhawan, R. Poddar, K. Mahajan, and V. Mann, "SPHINX: detecting security attacks in sofware-defned networks," in Proceedings of the Network and Distributed System Security Symposium, 2015.

[6] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," Journal of Network and Computer Applications, vol. 37, no. 1, pp. 380–392, 2014.

[7]Yassine, S., Najib, N., &Abdellah, J. (2024). A review of SDN-enabled routing protocols for Named Data Networking. ***Engineering Reports*****,** ***6*****(5), e12884.**

[8] A. A. Okon, K. M. Sallam, M. FarhadHossain, N. Jagannath, A. Jamalipour and K. S. Munasinghe, "Enhancing Multi-Operator Network Handovers WithBlockchain-Enabled SDN Architectures," in ***IEEE Access*****,**

[9]Aslam, N., Srivastava, S., & Gore, M. M. (2024). A comprehensive analysis of machine learning- and deep learning-based solutions for DDoS attack detection in SDN. ***Arabian Journal for Science and Engineering*****,** ***49*****(3), 3533-3573.**

[10]Sapkota, B., Dawadi, B. R., & Joshi, S. R. (2024). Controller placement problem during SDN deployment in the ISP/Telco networks

[11] Hussein, N. H., Koh, S. P., Yaw, C. T., Tiong, S. K., Benedict, F., Yusaf, T., ... & Hong, T. C. (2024). SDN-based VANET routing.

[12]Karakus, M. (2024). GATE-BC: Genetic Algorithm-Powered QoS-Aware Cross-Network Traffic Engineering in Blockchain-Enabled SDN. ***IEEE Access*****.**

[13]Raza, M., Saeed, M. J., Riaz, M. B., &Sattar, M. A. (2024). Federated Learning for Privacy Preserving Intrusion Detection in Software Defined Networks. ***IEEE Access*****.**

[14]Viveros, A., Adasme, P., &DehghanFiroozabadi, A. (2024). Optimal Topology Management for Software-Defined Networks Minimizing Latency and Using Network Slicing.

[15] Machine learning models in SNORT may require extensive resources and fine-tuning for optimal performance.

[16]Zeng, Y., Wang, Y., & Liu, Y. (2024). Research on detection and mitigation methods of Adaptive Flow Table Overflow Attacks in Software-Defined Networks.

[17]Rahouti, M., Xiong, K., Xin, Y., Jagatheesaperumal, S. K., Ayyash, M., &Shaheed, M. (2022). SDN security review:

14. Appendix:

```
include "ns3/netanim-module.h"


    AnimationInterfaceanim("Vanetanim.xml"); //Add before Simulator::Run();
//Step 5: Add performance analysis code to vanet program
////////////////////////// Network Perfomance Calculation //////////////////////
uint32_tSentPackets = 0;
uint32_tReceivedPackets = 0;
uint32_tLostPackets = 0;
int j=0;
floatAvgThroughput = 0;
Time Jitter;
Time Delay;


Ptr<Ipv4FlowClassifier> classifier = DynamicCast<Ipv4FlowClassifier> (flowmon.GetClassifier ());
std::map<FlowId, FlowMonitor::FlowStats> stats = monitor->GetFlowStats ();


for (std::map<FlowId, FlowMonitor::FlowStats>::const_iteratoriter = stats.begin (); iter != stats.end (); ++iter)
  {
    Ipv4FlowClassifier::FiveTuple t = classifier->FindFlow (iter->first);


NS_LOG_UNCOND("----Flow ID:" <<iter->first);
NS_LOG_UNCOND("SrcAddr" <<t.sourceAddress<< "DstAddr "<<t.destinationAddress);
NS_LOG_UNCOND("Sent Packets=" <<iter->second.txPackets);
NS_LOG_UNCOND("Received Packets =" <<iter->second.rxPackets);
```

```
NS_LOG_UNCOND("Lost Packets =" <<iter->second.txPackets-iter->second.rxPackets);

NS_LOG_UNCOND("Packet delivery ratio =" <<iter->second.rxPackets*100/iter->second.txPackets<< "%");

NS_LOG_UNCOND("Packet loss ratio =" << (iter->second.txPackets-iter->second.rxPackets)*100/iter->second.txPackets << "%");

NS_LOG_UNCOND("Delay =" <<iter->second.delaySum);

NS_LOG_UNCOND("Jitter =" <<iter->second.jitterSum);

NS_LOG_UNCOND("Throughput =" <<iter->second.rxBytes * 8.0/(iter->second.timeLastRxPacket.GetSeconds()-iter->second.timeFirstTxPacket.GetSeconds())/1024<<"Kbps");


SentPackets = SentPackets+(iter->second.txPackets);

ReceivedPackets = ReceivedPackets + (iter->second.rxPackets);

LostPackets = LostPackets + (iter->second.txPackets-iter->second.rxPackets);

AvgThroughput = AvgThroughput + (iter->second.rxBytes * 8.0/(iter->second.timeLastRxPacket.GetSeconds()-iter->second.timeFirstTxPacket.GetSeconds())/1024);

Delay = Delay + (iter->second.delaySum);

Jitter = Jitter + (iter->second.jitterSum);


j = j + 1;


}


AvgThroughput = AvgThroughput/j;

NS_LOG_UNCOND("--------Total Results of the simulation----------"<<std::endl);

NS_LOG_UNCOND("Total sent packets  =" <<SentPackets);

NS_LOG_UNCOND("Total Received Packets =" <<ReceivedPackets);

NS_LOG_UNCOND("Total Lost Packets =" <<LostPackets);

NS_LOG_UNCOND("Packet Loss ratio =" << ((LostPackets*100)/SentPackets)<< "%");

NS_LOG_UNCOND("Packet delivery ratio =" << ((ReceivedPackets*100)/SentPackets)<< "%");

NS_LOG_UNCOND("Average Throughput =" <<AvgThroughput<< "Kbps");

NS_LOG_UNCOND("End to End Delay =" << Delay);
```

```
NS_LOG_UNCOND("End to End Jitter delay =" << Jitter);
NS_LOG_UNCOND("Total Flod id " << j);
monitor->SerializeToXmlFile("manet-routing.flowmon", true, true);
//step 6:configure scenario 2

else if (m_scenario == 2)
   {
     // Realistic vehicular trace Erode
     // "low density, 50 total vehicles"
m_traceFile = "/home/logu/sumo/tools/2020-05-04-17-03-02/vanetmobility.tcl";
m_logFile = "vanet.log";
m_mobility = 1;
m_nNodes = 50;
m_TotalSimTime = 300.01;
m_nodeSpeed = 0;
m_nodePause = 0;
m_CSVfileName = "vanet.csv";
m_CSVfileName = "vanet2.csv";
   }


//Step 7:Run the program

      $ ./waf --run "scratch/vanet-routing-compare --protocol=1 --scenario=2"

//Step 8: Open Netanim
      $ cd ns-allinone-3.29/netanim
      $ ./NetAnim
```