International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Two-Phase Authentication Mechanism for Enhancing Security in Internet of Vehicles (IoV)

Ram Niwash Nitharwal (M. Tech.), Dr. Rohit Sharma

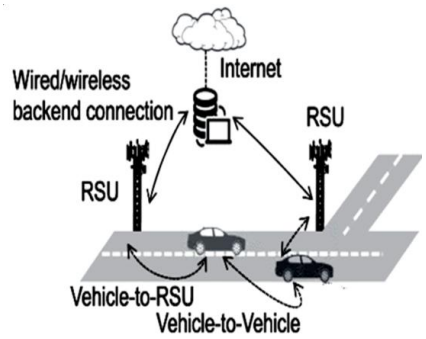
Submitted: 07/09/2024 **Revised:** 25/10/2024 **Accepted:** 05/11/2024

Abstract: The vehicular ad hoc network is the decentralized form of network in which malicious user can join the network which can trigger a variety of active and passive attacks. The denial of service is an active type of intrusion that is triggered by the malicious nodes present in the network. This research work introduces a new two-phase methodology for authentication and certificate distribution. In first phase, the vehicles nodes will be successfully authenticated using mutual authentication procedure. In the second phase the Vehicle-to-Vehicle Authentication method is implemented which will distribute certificate among the vehicles. NS2 is applied to stimulate proposed technique and certain metrics are considered to compute the results.

Keywords: *Internet-of-Vehicles, VANET, Authentication Mechanism, security.*

I. Introduction

The Internet of Vehicles (IoV) is an extension of the Internet of Things (IoT) that creates a comprehensive network connecting vehicles, infrastructure, pedestrians, and service platforms through advanced wireless communication technologies. By enabling real-time data exchange and collaboration among vehicles and their environment, IoV enhances driving safety, supports autonomous driving, and optimizes traffic management. This interconnected ecosystem is foundational to next-generation intelligent transportation systems, offering improved efficiency, convenience, and new business opportunities in the automotive sector. The Internet of Vehicles (IoV) has emerged as a critical component of smart transportation systems, enabling vehicles to communicate with each other and with infrastructure through Vehicular Ad Hoc Networks (VANETs). As an extension of Mobile Ad-hoc Networks (MANETs).



Department of Computer Science & Engineering Vivekananda Global University, Jaipur, Rajasthan (303012), India
Email Address: ramniwash143@gmail.com, rohit.sharma@vgu.ac.in

A. 5G-Enabled Vehicular Networks:

The advent of 5G technology has significantly enhanced the capabilities of IoV systems. The 5G-enabled vehicular network model includes several key components:

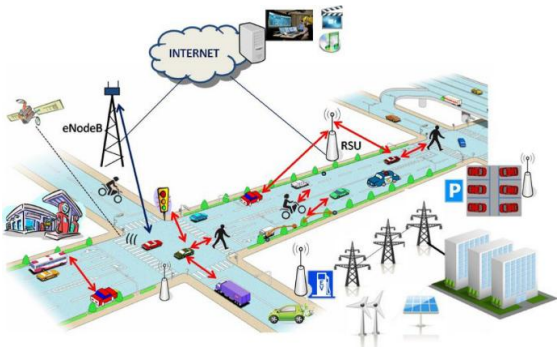
- Trusted Authority (TA): Manages vehicle registration and reputation scores.
- Global Reputation Centre (GRC): Stores reputation data for vehicles across different locations.
- 5G Base Stations (5G-BS): Facilitate high-speed data transmission between vehicles and the TA.
- Vehicles: Equipped with On-Board Units (OBUs) for secure communication.

B. Network Architecture of IoV:

The IoV architecture comprises several key communication paradigms:

- Vehicle-to-Infrastructure (V2I): Enables bidirectional wireless data exchange between vehicles and road infrastructure components like traffic lights and road signs.

- Vehicle-to-Vehicle (V2V): Allows real-time data transmission between vehicles using dedicated short-range communication (DSRC) frequencies.
- Vehicle-to-Pedestrian (V2P): Facilitates communication between vehicles and pedestrians or other vulnerable road users.
- Vehicle-to-Everything (V2X): Encompasses all forms of vehicular communication, integrating V2I, V2V, V2P, and other specialized modes.



C. IoV Architecture:

A typical IoV architecture is composed of three levels.

- Perception Layer: This layer contains all of the car's sensors, which gather ambient data and identify relevant events such as driving patterns, vehicle circumstances, and environmental variables. All of the following are included: radio frequency identification (RFID), satellite location perception, road environment perception, vehicle position perception, and car and object perception.
- Network Layer: This is the communication layer that permits access to GSM, 5G, WiMax, WLAN, and Bluetooth networks. It supports wireless communication modes such as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Sensor (V2S).
- Application Layer: This layer contains statistical tools, storage support, and processing infrastructure. It is responsible for storing, evaluating, processing, and making choices on a variety of risk situations, such as traffic congestion or inclement weather. This emblem represents intelligent applications, traffic safety, efficiency, and multimedia-based entertainment.

D. Application of IoV:

- Safe Driving: Collision detection, performance alerts, and automated hazard warnings via sensors and connected roads.
- Convenience Service: Remote vehicle access (locking/recovery), traffic/parking data for efficient transport management.
- Traffic & Crash Response: Real-time accident alerts with location data for faster emergency response and congestion management.
- In-Vehicle Infotainment (IVI): Entertainment (movies, games), navigation, voice-controlled IoT integration (smart home control while driving).

E. Challenges and Issues in IoV:

- Intelligent Routing: High mobility and dynamic VANET topologies demand predictive path planning for autonomous vehicles to ensure safe, efficient routes.
- Sensor & AI Integration: Requires robust data fusion from diverse sensors and rigorous real-world AI testing for reliable autonomous decisions.
- Real-Time Data Processing: Balances parallel/sequential methods to handle concurrent data collection, analytics, and processing.
- Standardization & Reliability: Device/platform diversity complicates communication (V2V) and data accuracy, risking safety without unified protocols.
- Security/Mobility: Cyber threats and high-speed connectivity demands necessitate secure, stable networks despite rapid topology changes.
- Interoperability of n/w architecture: Information sharing is a major problem when dealing with systems with varying features, as it may affect even system performance due to the heterogeneity of the de- vices and their massive data generation.

F. Security Requirements of Vehicular Networks:

The necessary security standards are listed below.

- Anonymity: In addition to the authority and 5GC, no other group or user may be informed of the vehicle's genuine identify. The participating vehicles in the connection should employ fictitious identities to make sure that the attacker cannot determine the real identity of the vehicle from the data transmitted.
- Message authentication and integrity: The integrity and validity of the data transmitted during vehicle communication should be ensured. By authenticating the sender, the recipient can be sure that what they have received is genuine and complete and not a message that has been altered or faked.

- Traceability: The authorities can rapidly track down the true identify of a hostile vehicle that spreads misleading information and announce that identity to the outer world.
- Unlinkability: Through transmission data that has been intercepted, the adversary is unable to connect various messages from the same vehicle.
- Common attack resistance: It can withstand frequent attacks on the Internet of Vehicles, including replay, man-in-the-middle, and modification attacks.

G. Attacks on Authentication:

- Masquerading Attack: Duplicate node IDs cause system confusion and malfunction.
- Sybil Attack: Malicious nodes use multiple fake identities to disrupt services and expose private data.
- Replay Attack: Message flooding wastes bandwidth, drops priority messages, and degrades performance.
- Wormhole Attack: Malicious nodes distort routing paths, absorb data, and disrupt network cohesion.
- GPS Deception: Fake location/speed data risks safety apps, navigation, and financial systems.

II. Authentication Mechanism in IoV

- Lightweight: Uses low-power cryptography (e.g., chaotic mapping) for secure group communication.
- Batch Verification: Validates multiple signatures simultaneously to reduce computational delays in dense traffic.
- Privacy-Preserving: Protects driver data (e.g., identity, location) during vehicle/RSU interactions.
- Dual Authentication: Implements multi-factor authentication (e.g., 2FA) to enhance security against compromised credentials.
- Hash-Based: Converts credentials to ciphertext (SHA, MD5) to prevent exposure during authentication.

III. Literature Survey

This section discusses the different type of authentication mechanism considerations associated with both VANETs and IoV. Since the IoV originated on VANETs, the attack spectrum may exhibit high overlap. Automobiles in VANETs may broadcast critical data on a variety of critical events, such as road conditions, traffic congestion, and accident notifications, to enable efficient and widespread traffic management. Cars may acquire information about traffic congestion or collisions from surrounding vehicles or the environment.

In such a critical circumstance, the existence of hostile and misbehaving nodes propagating forged and incorrect data over the network may have catastrophic effects, jeopardising the safety, security, and privacy of prospective users. Due to the fact that VANETs evolved from MANETs, their limitations are mostly inherited from MANETs' ad hoc design, which is often targeted from a restricted range due to the fact that automobiles are not constantly connected to the Internet. The most popular forms of attacks against VANETs are attacks on their authentication of the Vehicle.

A. Problem Statement:

When mobile networks reach the 5G era, they get a number of unmatched benefits such as 5G communications will expand the possibilities of what mobile networks can do, and extend upon what services they can deliver, by providing faster communication speeds, low latency and increased security.

5G will provide the foundational infrastructure for building smart IoV Environment, which will push vehicle network performance and capability requirements to their extremes. Thus, the introduction of 5G network technology to the Internet of Vehicles (IoV) may facilitate the development of more intelligent vehicular networks and the efficient transfer of vehicular information.

However, when 5G networks and vehicle networks are combined, secure and reliable authentication is required, with minimal processing overhead. In order to complement the present system, a safe and efficient lightweight authentication mechanism for vehicle groups is to be developed. Currently authentication Mechanism, utilizes an extended chaotic map, and the Chinese remainder theorem, which are used to distribute group keys.

Keeping in mind the above issues, the chaotic map is the complex algorithm which consume large amount of vehicles resources. The Authentication is done by using the RSUs for registration process, CA and TA for certificate distribution and authentication process, due to which the certificate generation process is also low to authenticate the vehicle in the network. The authentication scheme is required which consume least resources from the network

and also provide facility for the secure certificate distribution in the network.

B. Comparative study on Different Authentication Protocol:

S.No.	Title	Year	Authentication				
			Light weight	Batch Verification	Hash-Based	Dual Authentication	Privacy Preserving
1	[ZLX+18]	2018	✓	X	✓	X	X
2	[VAC+17]	2017	X	X	X	X	✓
3	[VAKD15]	2015	X	X	X	✓	X
4	[CE18]	2018	X	✓	X	X	X
5	[LWC17]	2017	X	X	X	✓	X
6	[BHC+18]	2018	✓	X	X	X	✓
7	[BBRA15]	2015	X	✓	X	X	X
8	[LG17]	2017	X	X	X	✓	X
9	[XFP+18]	2018	X	X	✓	X	X
10	[GTRR18]	2018	X	✓	X	X	X
11	[SJJ18]	2018	✓	X	X	X	X
12	[WDK+17]	2017	✓	X	X	X	X
13	[JZW16a]	2016	X	✓	X	X	X
14	[CWHZ18]	2018	X	X	✓	X	X
15	[HZXH15]	2015	X	X	X	X	✓
16	[IOV+18]	2017	X	X	✓	X	✓
17	[VD18]	2018	✓	X	X	X	X
18	[ZWSDF15]	2015	X	X	X	X	✓
19	[RMY16]	2016	X	X	X	X	✓
20	[JZW16b]	2016	X	✓	X	X	X

C. Objective of the Research:

To develop a lightweight and secure authentication mechanism for IoV that addresses the vulnerabilities of VANET-based systems, ensures message integrity, protects user privacy, and reduces computational overhead, making it suitable for resource-constrained vehicular environments.

D. Solution:

Integrate the strengths of existing protocols into a hybrid authentication scheme:

- Lightweight Key Exchange: Employ an Elliptic Curve Cryptography (ECC)-based key exchange protocol combined with a Physically Unclonable Function (PUF) for secure key generation and storage in vehicle OBUs and RSUs.
- Privacy-Preserving Pseudonyms: Utilize a Bloom filter-based pseudonym changing mechanism managed by RSUs to provide anonymity and unlinkability for vehicles. The pseudonym changes occur within predefined time windows and are based on vehicle speed and location to minimize traceability.
- Batch Verification with Hashing: Implement a hash-based message authentication code (HMAC) for lightweight message integrity

checks. Integrate this with a batch verification process at the RSU to handle multiple authentication requests efficiently.

- Trust Authority Revocation: Use a decentralized certificate revocation system, where RSUs maintain localized revocation lists for vehicles in their vicinity. Incorporate a reputation system where vehicles monitor and report malicious behaviour to the RSUs, enabling dynamic revocation.
- Sybil Attack Mitigation: Introduce a proof-of-work or proof-of-location mechanism combined with neighbour verification.

IV. Research Methodology

Chaos based cryptography is a security method in current cryptography field. The mathematicians and physicists have developed the Chaos theory which is related to the behaviours of nonlinear dynamic systems. Deterministic, nonlinear, irregular, long term prediction and sensitivity to initial situations are different expected attributes of this theory. These attributes are considered by the security research community for adopting the chaos theory in the modern cryptography. But this theory has some limitations which are also defined. Block ciphers are a kind of encryption algorithms which are utilized for processing one block of plaintext once. Most of the computing equipment makes the implementation of block ciphers as a symmetric encryption cipher. A block cipher is a kind of extensively used modern symmetric cipher. Unlike a stream cipher, the block cipher can be operated on a chuck of data at a time. On the other hand, the operations are carried out through a stream cipher on a single bit of plaintext once. The chaos based encryption will be further improved to reduce complexity for encryption. The security certificates in the network will be distributed through Vehicle-to-Vehicle Authentication. This network focuses on assigning a same position to every user in the network and maintaining the similar Vehicle to Vehicle Authentication replica. Thus, till the development of an effective capacity for confounding the masses, the facts stored in the Vehicle-to-Vehicle Authentication cannot be changed. AT present, Vehicle to Vehicle Authentication becomes popular as its security and reliability level is higher.

The methodology to implement IOV authentication in NS2 simulation using Vehicle to Vehicle Authentication technology and certificates is as follows:

i. **Define the requirements**: The first stage is to specify the simulation's requirements, which include the network architecture, the Vehicle to Vehicle Authentication frame- work to be used, the type of certificates to be generated, and the IOV authentication technique to be implemented.
ii. **Install the necessary software:** Once the prerequisites have been specified, install the appropriate software, which includes NS2, the Vehicle to Vehicle Authentication frame- work, and any required libraries or APIs.
iii. **Create the Vehicle to Vehicle Authentication network:** The next stage is to build the Vehicle to Vehicle Authentication network and configure it to meet the needs of the simulation. This includes establishing the nodes, designing the consensus process, and developing the appropriate smart contracts.
iv. **Create certificates for network nodes:** Create certificates for all network nodes. These certificates must be issued by a trustworthy certificate authority and include necessary details such as the node's public key, name, and IP address.
v. **Modify the NS2 code**: Use the certificates created in step 4 to incorporate the IOV authentication method in the NS2 code. This may include inserting code snippets into important NS2 code, such as the routing protocol or packet forwarding logic.
vi. **Test the simulation:** Once the implementation is complete, test the simulation to check that it is functioning properly. This involves running the simulation with various scenarios and analysing the outcomes.
vii. **Analysing the findings**: Finally, examine the simulation results to assess the efficiency of the IOV authentication method. This may include comparing the findings to those obtained using alternative authentication systems or testing the system's performance under various situations.

Proposed Architecture:

A. The proposed architecture of model is suggested as in the first stage start the deployment network for the internet of vehicle simulation in which deploy the network with finite number of vehicle nodes in it.

B. In the next stage create a path or establish a path from source to destination with reactive routing protocol as of the routing protocol which is AODV routing protocol for this simulation.

C. Next stage, deploy the Road side units flood beacon frames in the network to get easily

connected between the vehicles and vehicles can easily communicate with other through RSUs(Road Side Units).

D. The next process is vehicle registration process in which every new vehicle who came in the network first need to register itself to the network to start communicating to other vehicle nodes which is already present in the network.

E. In the registration phase a certificate is given to every vehicle who registered in the network in this stage the certificate is distributed of every vehicle in the network along with certificate id of each and every node present in the network.

F. The next stage is vehicle authentication process in which vehicle nodes get themselves authenticated by Vehicle to Vehicle Authentication technology. Every vehicle node stores the information of previous as well as next node such as certificate of the vehicle nodes. Authenticate the vehicle in the network by V2V (vehicle to vehicle) using Vehicle to Vehicle Authentication technology by certificate distribution process if the certificate the vehicle node did not match the authentication process of the need will not complete then the process of authentication will go the process of operation mode in which promiscuous operation mode is being start against that node, if the detection is verified then the vehicle node authentication process is again start otherwise that node is isolated from network and will not able to communicate with others nodes which is present in the network.

G. In the last stage if the vehicle node is authenticated successful then the vehicle node will start communicating with other vehicle nodes present in the network until and unless that vehicle node certificate changes or the node will left that particular area of network.

V. Results & Discussion

Tool: NS2 is an open-source simulation tool running on Unix-like operating systems. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired, wireless and satellite networks. It has many advantages that make it a useful tool, such as support for multiple protocols and the capability of graphically detailing network traffic. Additionally, NS-2 supports several algorithms in routing and queuing. LAN routing and broadcasts are part of routing algorithms. Queuing algorithm includes fair queuing, deficit round robin and FIFO. NS-2 started as a variant of the REAL network simulator in 1989. REAL is a network simulator originally intended for studying the dynamic behaviour of flow and congestion control schemes in packet-switched data networks.

The network simulator (NS), which is a discrete event simulator for networks, is a simulated program developed by VINT (Virtual Internetwork Test-bed) project group. It supports simulations of TCP and UDP, some of MAC layer protocols, various routing and multicast protocols over both wired and wireless network etc. Depending on user's requirement the simulation is stored in trace files, which can be fed as input for analysis by different component:

- A NAM trace file (.nam) is used for the ns animator to produce the simulated environment.
- A trace file (.tr) is used to generate the graphical results with the help of a component called gnuplot.

Number of Nodes	36
Antenna type	Omi-directional
Queue type	Priority queue
Standard	802.11
Routing Protocol	AODV
Queue size	50

Table 5.1: Simulation Parameters

- As illustrated in fig5.2, the vehicular adhoc network is deployed with fixed number of road side sensor and fixed number of vehicles which are moves freely on the road. At the network deployment process the vehicles registered themselves in the network. And this process provides themselves a identification number to every vehicle in the network which is unique for every vehicle through Road Side Unit.

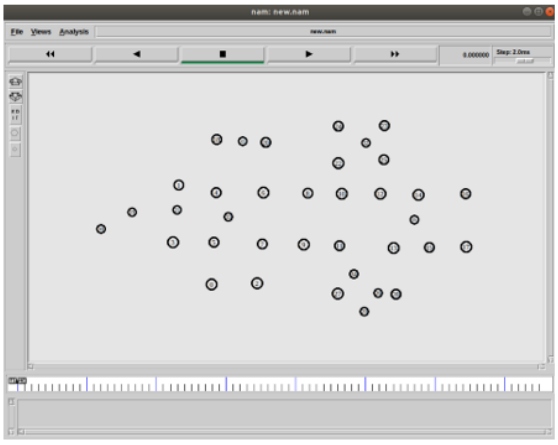


Figure 5.2: Network Deployment

• As shown in fig5.3, to move freely on the roads each vehicles had identification number which it gets at the time of registration. After the registration process the vehicles get authenticate themselves with the help of Vehicle to Vehicle Authentication technology. In the figure the vehicle 30 gets a registration identification number1. which is try to communicate with the vehicle 33 whose identification number is 4. Vehicle 21 whose root node which contains the details of both the vehicles e.g. vehicle 30 and vehicle 33. after checking the details of both the vehicles the root node generates the certificate for both vehicle which is unique to start the communication between the vehicle 30 and 33 in the network.

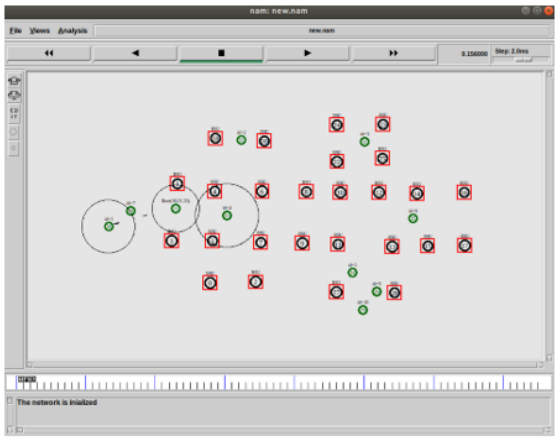


Figure 5.3: Vehicle to Vehicle Authentication

• As shown in fig5.4 , after successfully complete the process of generation of certificates of both vehicles through Vehicle to Vehicle Authentication the vehicles are now authenticated successfully to each other and start communicating with each other e.g. sending packets to each other in back-and-forth direction.

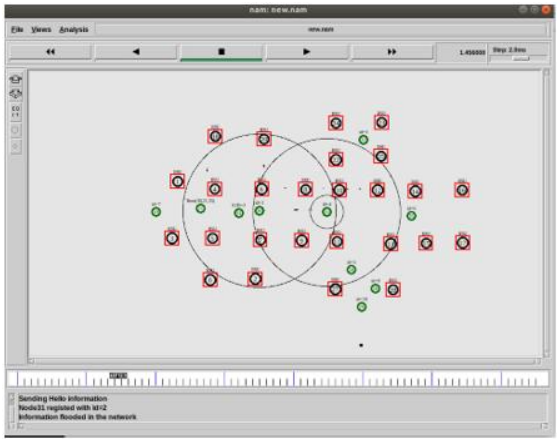


Figure 5.4: Communication Starts

• As illustrated in fig5.5, the cars are communicating with each other like the car with identification number of 1 is communicating with car with registration number of 4, The new car is entering in the network and sending registration request to register itself to the network with identification number 2.

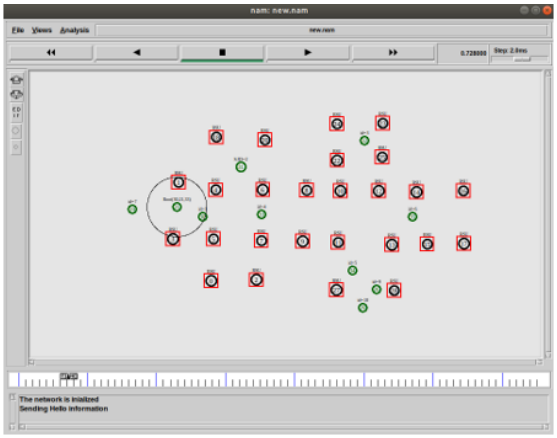


Figure 5.5: Registration process of new car

• As shown in fig5.6, the car which is entering in the network, and it need to register with the road side unit to get its registration number. The new car get its registration identify of 2.

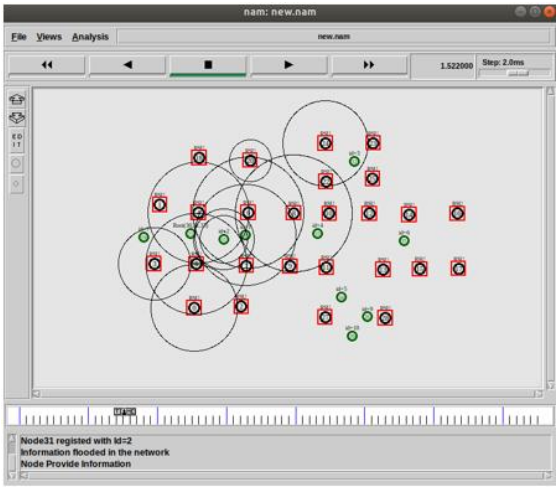


Figure 5.6: Allocation of new identification

• As illustrated in the fig5.7, the car with identification number of 1 is communication with the car of registration number of 4, The malicious node changes its identification from identification number of 2 to identification 4.

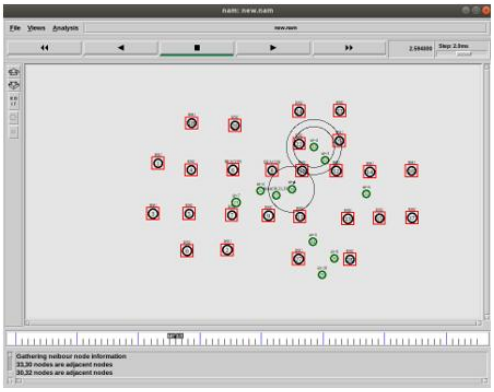


Figure 5.7: Changes identification Number

• As shown in fig5.8, The malicious node change its identification from 2 to 4. The malicious nodes had less distance from the legitimate node. The vehicle with identification number 1 try to start sending data to malicious nodes and Sybil attack had been triggered in the network.

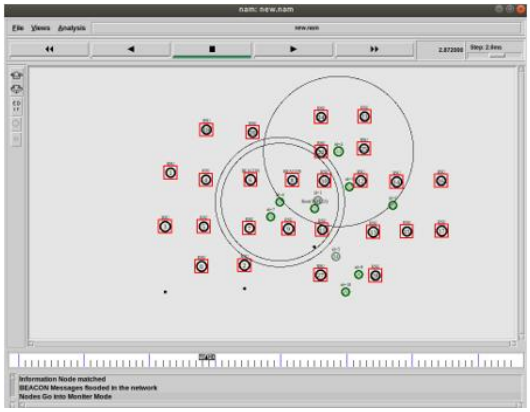


Figure 5.8: Attack triggered.

• As shown in the fig5.9, the malicious node changes its identification number and register with the identification number 4. The two legitimate cars are communicating with each other like car 30 and car 33. The road side units calculate distance of each node. As in the network two cars of id 4 trying to communicate with same car id 1, but the distance of are different. It means that some malicious nodes can exists in the network. So, the certificate to malicious node didn't generated by root node.

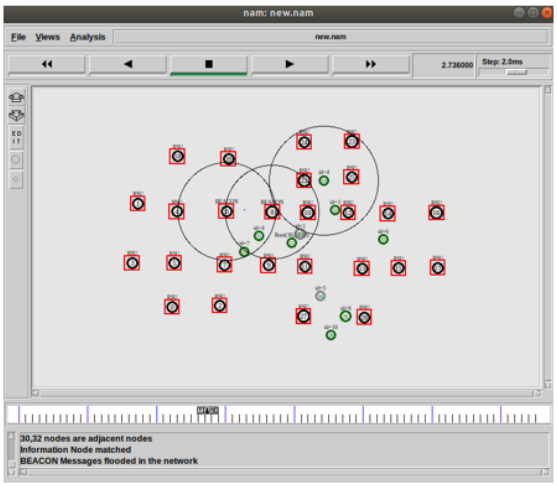


Figure 5.9: Getting distance information

• As illustrated in the fig5.10, the neighbours of car with identification no 4, is different. To detect the malicious cars from the network, the road side units define intrusion in the network.

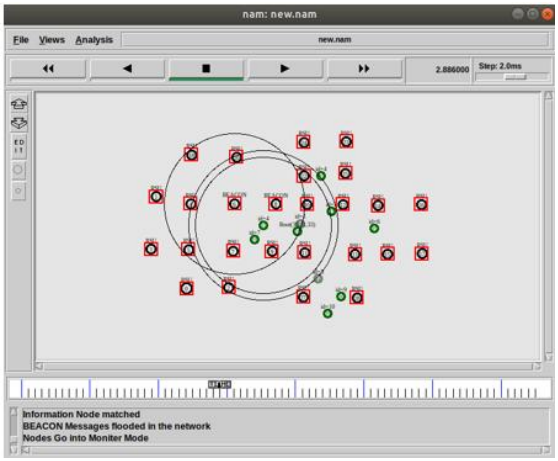


Figure 5.10: Changing to promiscuous mode

• As shown in fig5.11, when the intrusion possibility get defined in the network then the promiscuous mode detect malicious node from the network.

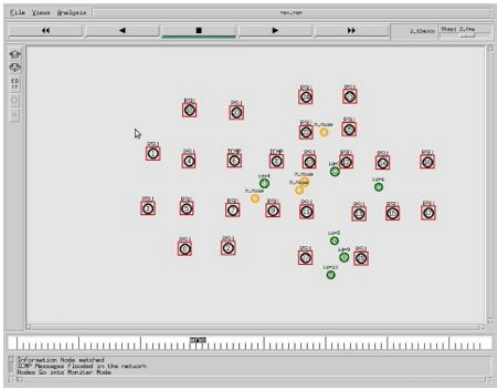


Figure 5.11: Network go to promiscuous mode

• As shown in fig5.12, when the intrusion possibility gets defined in the network then the promiscuous mode detects malicious node from the network. The malicious node get marked as malicious from the network.

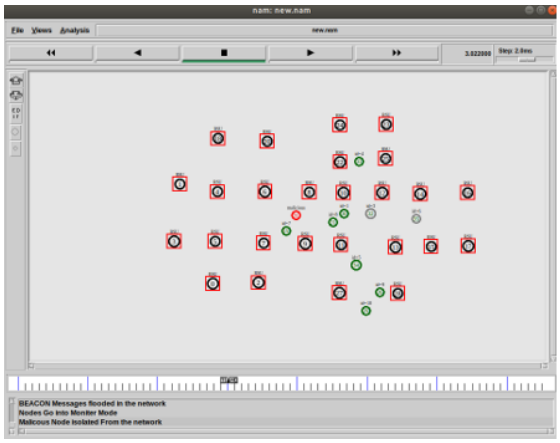


Figure 5.12: Malicious Node Get Identified

• As shown in fig5.13, again malicious node trying to get new identification number by send the request to RSUs(Rode side units) but malicious node get failed to get new identification number as it gets identified as malicious node by the network.

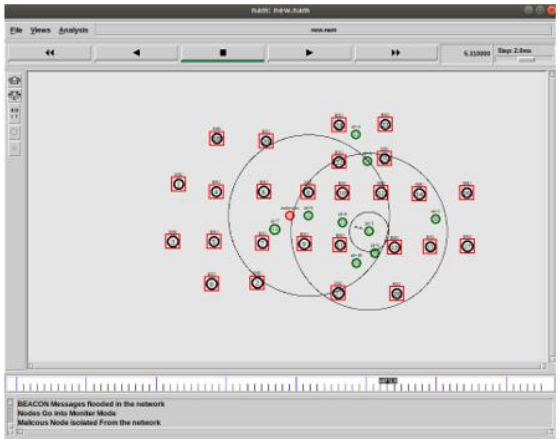


Figure 5.13: Malicious vehicle try to get new identification number

• As shown in fig5.14, after not getting the new identification number, As the node identified as a malicious node, the malicious node gets isolated from the network so the malicious node would not harm the network and other nodes which are present in the network.

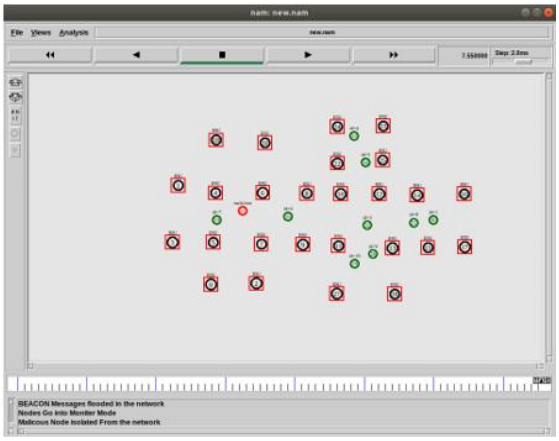


Figure 5.14: Malicious Vehicle isolated from network.

• As shown in fig5.15, at authentication process the certificates gets generated through Vehicle-to-Vehicle Authentication and every node have a unique ID to identify the nodes in the network and provide a Certificate ID to each and every node in the network with mapping of unique ID. This will help to identify if any malicious nodes enter in the network.

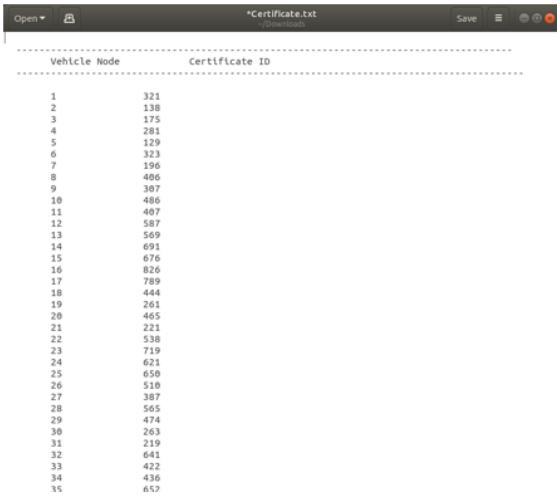


Figure 5.15: Certificate Distribution

• As shown in fig5.16, the delay in communication is compared between proposed and existing scheme. The delay in communication of proposed technique is less due to use of Vehicle to Vehicle Authentication method as compared to existing scheme.

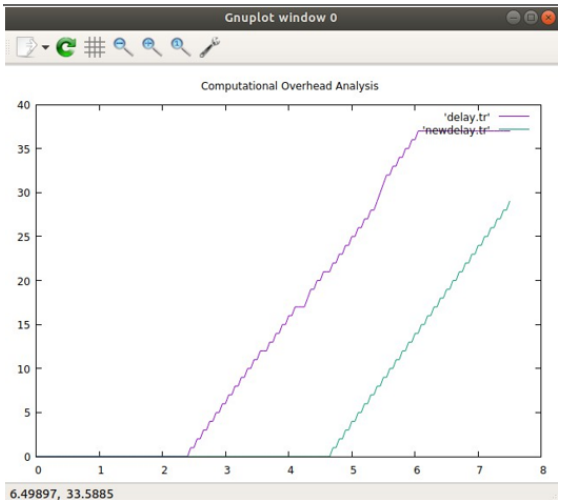


Figure 5.16: Delay in communication

• As shown in fig5.17, the communication overhead is compared between proposed and existing scheme. The communication overhead of proposed technique is less due to use of Vehicle to Vehicle Authentication method as compared to existing scheme.

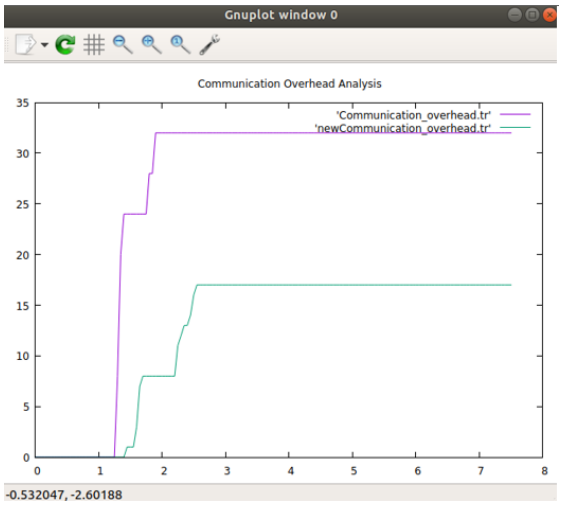


Figure 5.17: Communication Overhead

• As shown in fig5.18, the computational overhead is compared between proposed and existing scheme. The communication overhead of proposed technique is less due to use of Vehicle to Vehicle Authentication method as compared to existing scheme.

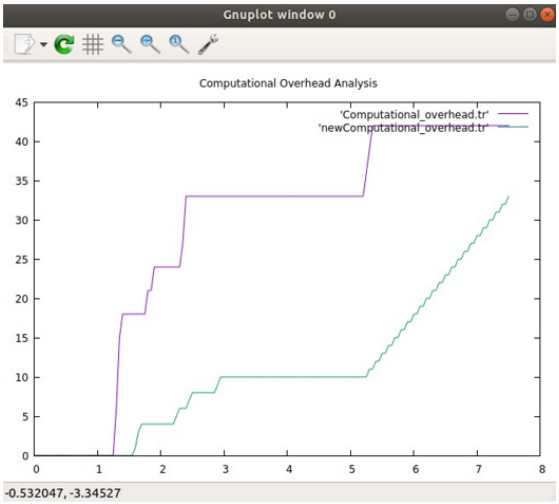


Figure 5.18: Computational Overhead

• As shown in fig5.19 throughput of proposed technique is compared with existing technique. The certificate is distributed in the network through the Vehicle to Vehicle Authentication method. When the network get secure throughput of the network is increased as compared with existing technique.

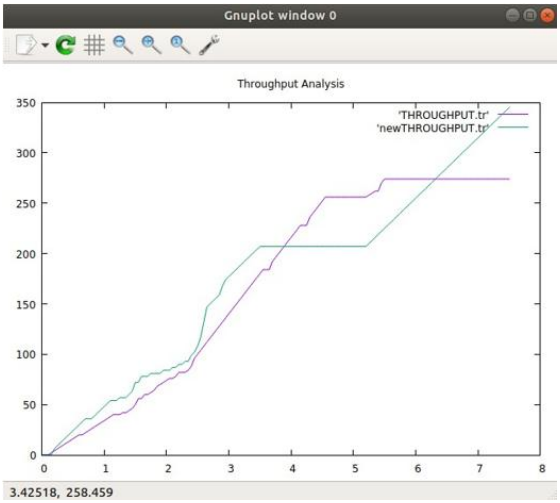


Figure 5.19: Throughput Analysis

• As shown in fig5.20 the packet-loss of the proposed technique is less as compared to existing scheme. The packet-loss of proposed technique is low as compared to existing technique due to use of Vehicle-to-Vehicle Authentication technique in the network.

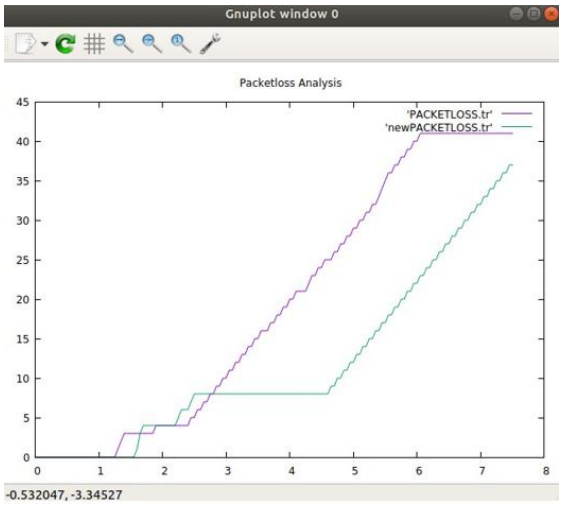


Figure 5.20: Packet loss Analysis

VI. Conclusion & Future Work

The vehicular ad hoc network is the self-configuring network that facilitates the malicious nodes for entering or departing in the network according to their requirement. This unique property makes the malicious free for entering the network and the node becomes capable of triggering intrusion in network.

To mitigate this problem we have implemented this work which is based on the secure authentication and certificate distribution in the network. The vehicular nodes when successfully authenticated then the authentication certificate will be distributed with other nodes using Vehicle to Vehicle Authentication. This directly leads to increase in security of VANET. The proposed methodology is implemented in network simulator version 2. The results of the proposed model show that throughput is improved up to 25.92 percent, packet loss is reduced to 9.75 percent, delay is reduced to 21.62 percent, communication overhead is reduced to 47 percent, computational overhead is reduced to 19.04 percent as compared to the existing authentication technique in VANET.

Future research in this area could focus on:

- Integrating machine learning algorithms for more adaptive and intelligent authentication processes.
- Exploring the impact of 5G and future 6G technologies on IoV authentication mechanisms.
- Developing standardized protocols for cross-platform and cross-manufacturer authentication in IoV ecosystems.

As IoV technology continues to evolve, robust authentication mechanisms will play a crucial role in ensuring the safety, security, and reliability of smart transportation systems.

References:

[1] S. K. Datta, R. P. F. Da Costa, J. Härri and C. Bonnet, "Integrating connected vehicles in Internet of Things ecosystems: Challenges and solutions," 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Coimbra, Portugal, 2016, pp. 1-6, doi: 10.1109/WoWMoM.2016.7523574

[2] S. K. Datta, J. Haerri, C. Bonnet and R. Ferreira Da Costa, "Vehicles as Connected Resources: Opportunities and Challenges for the Future," in IEEE Vehicular Technology Magazine, vol. 12, no. 2, pp. 26-35, June 2017, doi: 10.1109/MVT.2017.2670859.

[3] K. Bian, G. Zhang and L. Song, "Security in Use Cases of Vehicle-to-Everything Communications," 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, ON, Canada, 2017, pp. 1-5, doi: 10.1109/VTCFall.2017.8288208

[4] M. Hasan, S. Mohan, T. Shimizu and H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," in IEEE Transactions on Intelligent Vehicles, vol. 5, no. 4, pp. 693-713, Dec. 2020, doi: 10.1109/TIV.2020.2987430.

[5] J. Huang, D. Fang, Y. Qian and R. Q. Hu, "Recent Advances and Challenges in Security and Privacy for V2X Communications," in IEEE Open Journal of Vehicular Technology, vol. 1, pp. 244-266, 2020, doi: 10.1109/OJVT.2020.2999885.

[6] Talpur and M. Gurusamy, "Machine Learning for Security in Vehicular Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 346-379, Firstquarter 2022, doi: 10.1109/COMST.2021.3129079.

[7] S. Khan, F. Luo, Z. Zhang, M. A. Rahim, M. Ahmad and K. Wu, "Survey on Issues and Recent Advances in Vehicular Public-Key Infrastructure (VPKI)," in IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1574-1601, thirdquarter 2022, doi: 10.1109/COMST.2022.3178081.

[8] P. Moya Osorio et al., "Towards 6G-Enabled Internet of Vehicles: Security and Privacy," in IEEE Open Journal of the Communications

Society, vol. 3, pp. 82-105, 2022, doi: 10.1109/OJCOMS.2022.3143098.

[9] X. Shen, R. Fantacci and S. Chen, "Internet of Vehicles [Scanning the Issue]," in Proceedings of the IEEE, vol. 108, no. 2, pp. 242-245, Feb. 2020, doi: 10.1109/JPROC.2020.2964107.

[10] O. Kaiwartya et al., "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," in IEEE Access, vol. 4, pp. 5356-5373, 2016, doi: 10.1109/ACCESS.2016.2603219.

[11] L. Li, Y. Li and R. Hou, "A Novel Mobile Edge Computing-Based Architecture for Future Cellular Vehicular Networks," 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 2017, pp. 1-6, doi: 10.1109/WCNC.2017.7925830.

1.