International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.2 (2025) pp. 1921-1926
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Development of Intrusion detection system for VANET using Machine Learning

Anjal Bhasme[1]*, Abhay Kasetwar[2], Rahul Pethe[3]

[1]Research Scholar (MTech) Department of Electronics and Telecommunication Engineering S B Jain Institute of Technology Management and Research Nagpur
* **Corresponding Author Email:** kanishkskyler1718@gmail.com - **ORCID:** 0000-0002-5800-8764

[2]Department of Electronics mad Telecommunication Engineering S B Jain Institute of Technology Management and Research Nagpur
Email: email@email.edu.tr - **ORCID:** 0000-0002-5800-8764

[3]S B Jain Institute of Technology Management and Research Nagpur, Department of Electronics and Telecommunication Engineering,
Email: email@email.edu.tr - **ORCID:** 0000-0002-5800-8764

Article Info:

DOI: 10.22399/ijcesen.1502
Received : 07 January 2025
Accepted : 20 March 2025

Keywords :

VANETs,
Intelligent Transportation Systems,
Intrusion Detection System (IDS),
Fuzzy Logic-based Clustering,
Cluster Head (CH) Selection,
Cooperative Communication.

Abstract:

With the proliferation of vehicular technology, modern vehicles are fortified with ever more electronic maneuvers. This advancement ratifies the evolution of Intelligent Transportation Systems (ITS)to provide services like shared travel, smart driving, on-the-go Internet, etc. As a traditional application of ITS, a Vehicular Ad hoc Network (VANET) enables smart communication between vehicle nodes and network infrastructures to provide various expedient services such as road safety, data sharing, traffic management, parking assistance, entertainment, route recommendation, mobile payment, and even cloud applications. The high-speed mobile nodes (vehicles) in VANET perform very differently from other wireless communication networks and have a set of distinct features such as frequent link disconnection, highly dynamic topology, limited coverage area, and heterogeneous system architecture that may affect the performance and service quality of the VANET significantly. With this motivation, this work attempts to develop distributed cooperative cluster-based IDS to identify potential cyberattacks in VANET effectively. Firstly, this work develops a stable and reliable clustering method named Fuzzy Logic-based Clustering (FLC) to create a collaborative and reliable communication environment. A new fuzzy logic-based CH node selection algorithm is also developed based on node degree, average velocity difference, and relative velocity of the vehicle to create a more robust clustering structure with minimum cost in VANET.

1. Introduction

Combining ad hoc networks with WLANs, a new area of study known as vehicular ad hoc networks (VANETs) is just getting off the ground. Keep the Vehicle Units (VU) close to the road segments so they can wirelessly communicate with other cars or Roadside Units (RSUs) in the area. Users in VU are able to get the services they seek via internet connectivity. Enhanced mobility of the VU often causes topology changes in the network to be dynamic. So, the link isn't always steady. But the vehicle's interference and transmission range further limit its capabilities. The packet transmission between the source and destination vehicles uses more routes within their driving range when the source unit is further away from the target vehicle. In contrast, if there isn't already a vehicle in its communication range, the vehicle carrying the message will often communicate it as soon as the next vehicle comes into range. But, when packets are sent in this manner over the network, the transmission latency grows. Delays may be plainly avoided by choosing route segments with high car densities. Typically, this is considered while routing protocols. With the advent of wireless communication, VANET ad hoc network infrastructures are seeing rapid expansion. Reducing traffic congestion and improving traffic flow are three current uses of VANETs that aim to increase road safety. Onboard units (OBUs) and roadside units (RSUs) provide appropriate

communication between vehicles in Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V) communications. Additionally, we will go over the Trust Authority (TA), OBUs, and RSUs, which are the three parts of VANETs. Wireless Access in Vehicle Environment (WAVE) is the standard wireless protocol for VANETs that allows cars and RSUs to communicate with one another. Using up-to-date traffic and vehicle information, WAVE communication guarantees passenger safety, while the WAVE architecture explains the exchange of security messages. The application enhances traffic flow and efficiency while guaranteeing pedestrian and motorist safety. Among the several types of VANETs, you'll find operational beacon units (OBUs), tracking anchor units (TAs), and remote sensor units (RSUs). The RSUs facilitate communication between devices and allow the OBUs to attach on vehicle units (VUs) to gather fuel, position, and speed data. The information is then sent to the adjacent cars using the wireless network. Node A, B, and C in the RSU network all have direct cable connections to TA. Furthermore, TA is in charge of keeping VANET authentication up to date.

1.1 Communication Methods in VANETs

In order to alleviate traffic congestion, the Intelligent Transportation System (ITS) employs a number of networking approaches, such as MANETs and VANETs, with a constant emphasis on safe transport and road safety communications. When it comes to intelligent transportation systems (ITS), vehicle-to-everything (V2X) communications are crucial for enhancing traffic management experiences by providing trustworthy and real-time data on things like collision warnings, traffic congestion warnings, emergency situations, road bottlenecks, and other transportation services. For the sake of communication, VANETs are separated into three models. As seen in Figure 1, this encompasses the following types of communication: vehicle-to-roadside (V2R), vehicle-to-infrastructure (V2I), and vehicle-to-vehicle (V2V).1. With vehicle-to-vehicle (V2V) communication, which makes use of on-board units (OBUs), direct vehicular communication may be set up independently of permanent infrastructure. The vehicle-to-infrastructure (V2I) connection enables data and information collection applications by allowing vehicles to interact with roadside infrastructure via equipped Road Side Units (RSUs). The hybrid communication method integrates both vehicle-to-vehicle and vehicle-to-infrastructure communication. In this setup, a car may establish a link to the Internet or other distant vehicles via a single hop or several hops.

With very low latency and a high transmission rate, the transmission medium is ideal for vehicle-to-vehicle communication. V2V communication may provide a VU with data like as traffic conditions, emergency braking, and collision detection. The data may be sent to both automobiles and network infrastructures using V2I. In order to share data with other networks, the vehicle connected to RSUs in this domain. In addition, its infrastructure communications need a constant bandwidth to render it attack-proof.

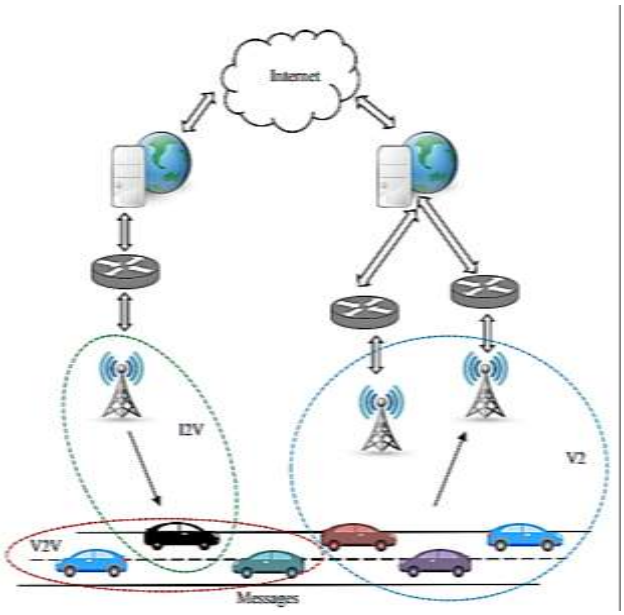

Figure 1. *VANET Architecture*

C-V2X technology was launched recently; a single platform that supports V2X communications. It is a unique connectivity platform. C-V2X is a strong communication technology that is developed within the framework of the third-generation partnership project (3GPP). It connects each car and enhances traffic efficiency by enabling Cooperative Intelligent Transport Systems (C-ITS)

3GPP released its first V2X communications support in 2016 and the standards include Long-term Evolution (LTE). Due to their high data rate, high coverage, and penetration rate, LTE has robust advantages in V2I communication [1]. However, the limited services and centralized structure to support V2V communication means LTE tends to face many challenges.

1.2 Critical Challenges In Routing

While there are a number of routing protocols that may be used to provide unique logical addresses to cars, none of them guarantee that no two vehicles will have the same address. A variety of issues arise

with VANETs, including those related to configuration, demography, vehicle count, mobility patterns, arbitrary vehicle entry and departure, and road dimensions that fall short of transmission coverage.

The routing algorithm's primary function is to identify and preserve the best path for data packet transmission via intermediary nodes. Since VANETs employ the unique routing protocols of MANETs, their operation is intricate due to the ever-changing nature of mobile nodes. For topology-based routing systems to work, each node must have its own distinct address. It necessitates a system to allocate distinct IP addresses; yet, these methods do not ensure that no two networks have the same set of addresses. Network topology, mobility model, traffic volume, quick changes, and road width are some of the unique VANET challenges that make typical routing protocols inadequate and MANET algorithms unsuitable. When it comes to building ad hoc intrinsic networks, the majority of routing protocols use one of two methods: either a routing table-driven approach or a source-on-demand routing mechanism. One of the ways in which nodes in a network are linked to one another is via proactive routing protocols like table-driven routing. Thanks to these protocols, every node in the network may consistently and clearly display its topology in its periodic updates. A proactive routing protocol's advantage is that it reduces available bandwidth via the use of idle data pathways rather than relying on low-latency real-time destination routes.

2. Literature Review

A software-powered, AI-based network controller is suggested for VANET as a centralized routing system with mobility prediction. Specifically, the SDN controller can execute an accurate mobility prediction with the use of sophisticated artificial neural network technology. With the use of the mobility prediction, the RSUs and BSs may determine the average latency of the vehicle request and the odds of successful transmission. The estimation is predicated on a stochastic model of urban traffic that, upon arrival of the vehicle, adheres to the uniform Poisson process. The software-defined network controller gathers data from the RSU and BS networks, which are like switches. Using data from all over the network, the SDN controller determines the best routes for the switches to take. Even if the source vehicle and the destination truck are in the same switch coverage region, the RSUs and the BS will make their own routing decisions to reduce the total amount of time vehicles spend in service. The research team came up with a protocol for parking VU relay routing that includes the following steps: updating the application relay list, assessing the strength of the communication connection, selecting the applicant relay list, and the regular Hello Packet Exchange Mechanism.

In order to maintain a stable connection to RSUs and minimize buffered packet loss due to lengthy paths. Abbas et al. (2018) used a greedy V2V cellular-based connection selection method to simulate decreased latency, which is an analytical solution to the issue [2].

Cyberattacks can be broadly classified into two types, according to their characteristics: (i) inter-node attacks, which aim to interfere with the connection between nodes or between nodes and network infrastructures; and (ii) intra-node attacks, which disrupt the communication maneuvers within a vehicle. The inter-node threat is similar to the intra-node danger in that it may cause more extensive damage to the network. One effective method of reducing inter-node risks is to install an intrusion detection system (IDS) that can detect unusual vehicles. The effectiveness of the intrusion detection system (IDS) in distributed cooperative VANET operations is controlled by the reliability of the cooperative team and the extent to which the nodes cooperate with one another. The assailants are well-aware of this fact, therefore they use malicious tactics to undermine the crew's detecting abilities and assault the main players in the cooperative team. The malicious cars will spread inaccurate road information, disrupt link connection, steal existing data, etc., via an assault.

In a spoofing attack, a malicious node pretends to be a CH in order to illicitly inject false traffic information, impair network connection, or steal sensitive data. Figure 2 (a) Sybil attack depicts a malicious node A posing as a cluster head in order to trick other nodes into sending data to it. The most fundamental kind of deceitful assault is the Sybil, also known as an identity spoofing attack, in which criminals take over passing automobiles and pretend to be someone else. Intruders use these aliases to launch further assaults, fooling victims into thinking the vehicle is in other locations, all in an effort to steal private information. An attacker may easily cause chaos in the network by inserting false information using this approach. A Sybil attacker is a malicious node that impersonates other cars, while a Sybil node is a node whose identity has been compromised, as seen in Figure 2(b). When an invader imagines a cluster of automobiles on a certain route while other, legitimate-looking cars spread false information about a traffic congestion, this is an example of a Sybil cyberattack. multiple denial-of-service attacks: The

goal of a denial-of-service (DoS) attack is to make the targeted node respond excessively slowly to other nodes by flooding it with false warnings about traffic jams or accidents. As shown in Figure 2 (c), nodes C and D are rendered helpless in the face of an assault because malicious nodes A and B persistently relay false information to them. x Deceptive data breach: The perpetrator of this treacherous hack may produce congestion on the network or send out erroneous signals to other nodes in an effort to gain an edge for themselves. An enemy may, for instance, notify other drivers of a "Heavy traffic jam" so that it can travel more easily. Figure 2 (d) shows a possible outcome of this kind of assault, in which two intruders (A and C) work together to disseminate false information in order to divert the attention of other nodes (D) and let intruder E.

3. Problem Statement

Various routing protocols have been created for various reasons up to this point. In order to choose its routing route, certain protocols detect vehicle density. The fact that such detection occurs is the issue. Following the discovery of density information, the data is shared with other vehicles, resulting in enhanced control over overhead. When the density of cars is constantly changing, convergent takes much longer. This degrades the efficiency of the routing protocol and causes erroneous data to be shown in real time. Because the routing protocol includes a per-hop computation, it has been shown that cars that only get information from their next or subsequent road segment result in an optimal local issue. For these reasons, VANET route selection may benefit from machine learning models. Using machine learning, RSUs can better block traffic and vehicle movements. It is possible to determine the danger posed by cars within its communication range. The package will only be sent down shorter or more suitable routes if this is done correctly. The machine learning model uses the vehicle's historical data and its present status to make condition predictions in real time. The most effective routing protocol may be determined with the use of such a prediction. When it comes to wireless sensor networks, chartered and multiple chartered security threats often disproportionately impact VANETs. A number of malicious devices may be overloading the message, forging it, or blocking it altogether, all of which would expose the attacker's customer information. This raises privacy exposure problems, and the only way VANETs can guarantee security and privacy is via strong authentication. Nevertheless, authentication methods in VANETs are often susceptible to a variety of security threats due to the scattered and mobile structure of the networks. In addition, these procedures are designed to protect sensitive information even when routing metrics are not used. Since the user's Quality of Services (QoS) is complex and varied, the security mechanism regrettably does not provide the measurements. Consequently, in order to safeguard the communication both before and after transmission, an improved authentication technique is required. When a malicious node receives a route request message, it may launch a black-hole attack by directing certain communications while dropping others. Because of this, the rate of data loss spikes suddenly. Figure 2 (e) shows an attack scenario where a node accident occurred in front of the malicious node A. Nodes B and C have sent the collision notice to A, but A chooses not to direct it, which might cause a traffic jam. In a gray-hole attack, more than two malicious nodes work together to convey data across a private transmission channel, shortening the trip and making it easier to intercept, send, discard, or change messages along the way. Figure 2 (f) shows a gray-hole assault in action. Nodes A, B, C, D, and E are tricked into taking the crowded route instead of the smooth one by the malicious nodes, who gather and transmit information on the collision's trajectory. The ever-increasing frequency of cyberattacks in VANETs and the constant expansion of attack scale have led to a crucial requirement for timely, secure, and reliable vehicular communications. The four types of assaults that are the subject of this study are denial-of-service, spoofing, gray-hole, and black-hole.

4. Intrusion Detection System for VANET

In most traditional digital communication networks, an intrusion detection system serves as a fundamental and essential component for managing security concerns. For intrusion detection systems (IDS) models to work, high-quality, reliable computer resources are essential, as is the ability to accurately and instantly detect a wide variety of sophisticated cyberattacks. Implementation location influences IDS enactment; typically, nodes, CHs, or RSUs undergo IDS implementation (. Distributed, centralized, and hybrid are the three main categories into which the current IDS systems fall. Using distributed intrusion detection systems, individual nodes or RSUs in VANETs keep an eye out for any dangers in their immediate vicinity. Because of their wide variety of applications, high effectiveness and low-cost constructions, VANETs become a major research motivation of governments, car manufacturers and academic

institutions, and attract more and more interests of them. However, the successful deployment of VANETs consists of a number of important components, a key one of which is how to establish adaptive and efficient routing paths from sources to destinations in the complex and dense urban scenarios. The benefits of VANETs will be limited without the available solution of this routing problem. The aim of this study is to monitor the behavior of the road segment, analyze and forecast the transmission capacities and availability of the vehicles using the Deep Reinforced Learning (DRL) model. This method allows RSU to maintain traffic information on DRL-used roads to enhance network capacity performance. Furthermore, the DRL forecasts the time to transmit based on the VU location. This is done by RSU to find the neighboring vehicle to transport the packages in real time

5. Overview of Proposed Intrusion Detection Framework

Nodes in vehicular communication may work together to improve intrusion detection by exchanging information and learning from each other's mistakes, as stated before. This work proposes a cluster-based intrusion detection system (IDS) paradigm with a distributed cooperative design. The detection accuracy is enhanced by data acquired from several nodes, allowing for improved predictions and judgments. On the other side, minimizing processing and communication overhead while gathering, analyzing, and interpreting the massive amounts of data generated is a major challenge. Another issue is efficiently managing the network resources while meeting the needs of an application. These concerns are addressed by our suggested strategy. The suggested paradigm takes use of cloud computing's limitless network resources and high-performance edge computing's extensive service offerings. In order to provide safe communication between cluster nodes and to cater to the specific demands of VANET applications, the suggested IDS design relies on a three-tiered bottom-up methodology. Without compromising the network's dependability or timeliness, this design aims to identify different types of harmful assaults. Similar works have been done and reported in the literature [3-16].

4. Conclusions

The rapid growth of VANETs and their critical role in Intelligent Transportation Systems necessitate robust security mechanisms to protect against cyber threats. This study successfully developed an

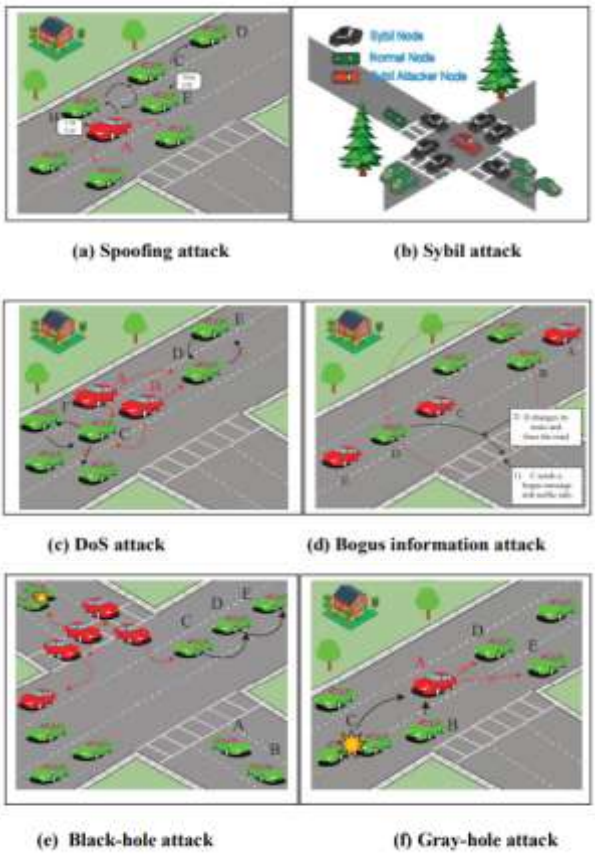

Figure 2. *Various attack scenarios in VANET*

intrusion detection system leveraging machine learning techniques to enhance the security and reliability of VANET communications. By analyzing network traffic and detecting anomalies, the proposed IDS effectively identifies and mitigates potential attacks such as Denial of Service (DoS), Sybil, and black hole attacks. Despite these achievements, the study highlights areas for future research. Incorporating federated learning could enhance the IDS's adaptability and privacy-preserving capabilities. Additionally, further evaluation in diverse and large-scale VANET scenarios will help refine the system's robustness against emerging threats. this work demonstrates the potential of machine learning-based IDS solutions to secure VANETs, contributing to safer and more reliable vehicular communication systems. With continued advancements, such systems will play a pivotal role in realizing secure intelligent transportation systems.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could

have appeared to influence the work reported in this paper

- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.

- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1]Chen, Y., Fan, M., (2014) A Novel Mobility-Based Clustering Algorithm for VANETs, *Sensors & Transducers*, 176(8);189-195.

[2] Alabbas, H & Huszák, A (2020) A New Clustering Algorithm for Live Road Surveillance on Highways based on DBSCAN and Fuzzy Logic, *International Journal of Advanced Computer Science and Applications*, 11(8);580–587.

[3]Abdel-Halim, IT, Fahmy, HMA, Din, AMB (2019), Mobility predictionbased efficient clustering scheme for connected and automated vehicles in VANETs', *Comput. Netw.*, 150;217–233.

[4] Ahmad, A, Adnane, A & Franqueira, V (2017), A systematic approach for cyber security in vehicular networks, *J. Comput. Commun*., 4;38-62.

[5] Alghamdi, SA (2020), Novel path similarity aware clustering and safety message dissemination via mobile gateway selection in cellular 5Gbased V2X and D2D communication for urban environment, *Ad Hoc Networks*, 103;102150.

[6] Aloqaily, M, Otoum, S, Al Ridhawi, I, &Jararweh, Y (2019), An intrusion detection system for connected vehicles in smart cities, *Ad Hoc Netw.*, 90;101842.

[7] Alsarhan, A, Kilani, Y, Al-Dubai, A, Zomaya, AY & Hussain, A, (2020), Novel Fuzzy and Game Theory Based Clustering and Decision Making for VANETs, *IEEE Transactions on Vehicular Technology*, 69(2);1568-1581.

[8] Arif, M, Wang, G, Bhuiyan, MZA, Wang, T & Chen, J (2019), A survey on security attacks in VANETs: communication, applications and challenges, *Vehicul. Commun.* 19;100179.

[9] Arkian, HR, Atani, RE, Diyanat, A & Pourkhalili, A (2015), A clusterbased vehicular cloud architecture with learning-based resource management, *J Supercomput*, vol. 71(4);1401–1426.

[10] Azam, F, Kumar, S & Priyadarshi, N (2021), A novel road side unit assisted hash chain based approach for authentication in vehicular Ad-hoc network, *Global Transitions Proceedings*, 2(2);163-168.

[11] Azees, M, Deborah, LJ & Vijayakumar, P (2016), Comprehensive survey on security services in vehicular ad-hoc networks, *IET Intelligent Transport Systems*, 10(6);379–388.

[12] Bhatti, DMS, Rehman, Y, Rajput, PS, Ahmed, S, Kumar, P & Kumar, D (2021), Machine learning based cluster formation in vehicular communication, *Telecommunication Systems: Modelling, Analysis, Design and Management*, 78(1);39–47.

[13]Olola, T. M., & Olatunde, T. I. (2025). Artificial Intelligence in Financial and Supply Chain Optimization: Predictive Analytics for Business Growth and Market Stability in The USA. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.18

[14] M. Shanthalakshmi, & R.S. Ponmagal. (2025). An Intelligent Intrusion Detection System for VANETs Using Adaptive Fusion Models. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.935

[15]Ibeh, C. V., & Adegbola, A. (2025). AI and Machine Learning for Sustainable Energy: Predictive Modelling, Optimization and Socioeconomic Impact In The USA. International Journal of Applied Sciences and Radiation Research , 2(1). https://doi.org/10.22399/ijasrar.19

[16]M. Shanthalakshmi, & R.S. Ponmagal. (2025). Optimizing Secure Communication in Intelligent Transportation Networks with Certificate-less Authorization in VANETs. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.934