Franklin Open 13 (2025) 100430

Contents lists available at ScienceDirect

Franklin Open

journal homepage: www.elsevier.com/locate/fraope

Generalization analysis of ANN-Based routing protocols for diverse vehicular environments in VANETs

Spandana Mande [a], Shaik Salma Asiya Begum [b], Putta Durga [c], Sachi Nandan Mohanty [c], Fernando Moreira [d,*]

[a] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur Green Fields, Vaddeswaram, Andhra Pradesh, India
[b] Department of CSE(AI&ML), LBRCE, Maylavaram, AP, India
[c] School of Computer Science & Engineering, (SCOPE) VIT -AP University, Amaravati, Andhra Pradesh, India
[d] REMIT, IJP, Universidade Portucalense, Porto 6 IEETA, Universidade de Aveiro, Aveiro, Portugal

ARTICLE INFO

Keywords:
Vehicle ad hoc networks
Ann
Blackhole attacks
Transfer learning
Cross-domain
Urban
Rural
Highway

ABSTRACT

The rapid advancement of intelligent transportation systems depends on effective and secure routing within vehicular communication networks under diverse driving conditions. This research investigates the efficacy of neural network-based routing protocols in enabling reliable and secure data transmission under diverse traffic conditions. Prior research has shown that neural networks can alleviate security threats, such as malicious node attacks; however, there has been inadequate exploration of their adaptability in urban, rural, and highway environments. This research examines routing performance in simulated traffic environments and actual mobility data to address this gap. The methodology utilizes robustness testing, transfer learning, and cross-domain validation to evaluate the sensitivity of routing models to variations in vehicle density, mobility patterns, and road configurations. The findings indicate that the neural network-based approach outperforms a conventional routing protocol across various contexts. In urban areas, the delivery rate increased from 78 % to 85 %, while in rural regions, it rose from 65 % to 77 %. We reduced the end-to-end delay by approximately 7 to 12 milliseconds in all instances. Relative to the baseline, throughput increased by approximately 10 to 15 percent, while energy efficiency improved by 5 to 8 percent. The proposed method enhanced system resilience against attacks, successfully thwarting over 90 % of malicious disruptions, in contrast to the 73 to 79 % efficacy of the previous protocol. This study presents a framework for designing adaptive and scalable routing systems that maintain consistent performance across diverse vehicular conditions. The findings enhance the safety and efficacy of intelligent transportation systems.

1. Introduction

Intelligent Transportation Systems (ITS) utilize Vehicular Ad Hoc Networks (VANETs) as their primary communication method. This enables vehicles to communicate with one another (V2V) and with infrastructure (V2I) in real time. These networks facilitate the development of smart cities and autonomous vehicles by providing essential services such as traffic management, safety notifications, and infotainment. However, VANETs continue to face challenges due to their constantly changing topology, fluctuating vehicle density, and susceptibility to security threats such as blackhole, Sybil, and wormhole attacks. When conditions vary significantly, traditional and heuristic routing protocols frequently exhibit diminished efficacy. Artificial Neural Networks (ANNs) are emerging as effective solutions for tasks such as intrusion detection, traffic prediction, and secure routing due to their ability to learn patterns and adapt to novel circumstances. Most contemporary ANN-based routing methodologies are effective solely in specific environments (urban, rural, or highway) and heavily rely on simulated datasets, despite this being a potential limitation. This raises concerns regarding their ability to adapt, develop, and maintain resilience in the real world. To ensure the reliability and safety of ITS communication, it is imperative to systematically evaluate their performance across various vehicle types. Vehicle Ad Hoc Networks (VANETs) facilitate seamless communication between vehicles (V2V) and infrastructure nodes (V2I) [1]. They are integral to Intelligent Transportation Systems (ITS) and are crucial for traffic management, safety notifications, and

* Correspondence author.
E-mail address: fmoreira@upt.pt (F. Moreira).

https://doi.org/10.1016/j.fraope.2025.100430
Received 1 May 2025; Received in revised form 20 September 2025; Accepted 17 November 2025
Available online 21 November 2025

entertainment services. This feature facilitates the advancement of urban intelligence and the autonomy of transportation systems [2]. Despite their significant potential, VANETs face numerous challenges in achieving secure and efficient routing. Their evolving architecture and susceptibility to cyber threats such as blackhole, wormhole, and Sybil attacks render networks highly insecure [3]. There is a significant demand for routing systems that are both adaptable and robust enough to address security vulnerabilities while maintaining reliable service. Artificial Neural Networks (ANNs) possess the capability to learn from data and identify patterns applicable across various contexts. This renders them a viable solution to these issues. Artificial neural networks (ANNs) have been employed in vehicular ad hoc networks (VANETs) for traffic forecasting, intrusion detection, and secure routing [5]. Routing protocols utilizing artificial neural networks have demonstrated efficacy in identifying optimal paths that mitigate security risks. These systems enhance data transmission reliability by identifying patterns of malicious behavior and mitigating attacks such as blackholes [6]. Nonetheless, existing research has not comprehensively assessed ANN-based routing across diverse vehicular scenarios. Numerous studies concentrate on specific contexts, such as urban traffic or highway travel, while providing limited evidence of adaptability across varied environments [7]. Recent studies on ANN-based routing indicate significant issues, including elevated computational costs, restricted generalization across environments, and dependence on simulated datasets [18]. Factors such as vehicle density, mobility patterns, and road conditions significantly influence the efficacy of machine learning-based routing methods [8]. Rural networks characterized by low density frequently encounter topological changes that compromise routing stability [9]. Conversely, highway environments characterized by consistent traffic flows pose distinct challenges that require resolution [10]. Numerous studies have emphasized the imperative for machine learning-enabled systems in VANETs to tackle dynamic topology, security vulnerabilities, and communication ambiguities in large-scale implementations [16]. This study aims to evaluate the generalizability of ANN-based routing protocols across urban, rural, and highway settings. We assess the adaptability and resilience of these models utilizing simulation-based and real-world datasets via cross-domain testing, transfer learning, and robustness analysis [11]. The findings facilitate the development of adaptive routing systems that can maintain optimal performance across diverse VANET conditions. This study addresses the gap in ANN generalization, providing insights for developing routing solutions that are secure, scalable, and context-aware, thereby linking simulation-based validation with practical application [12]. Fig. 1 illustrates the black hole attack scenario that results in packet loss within the network.

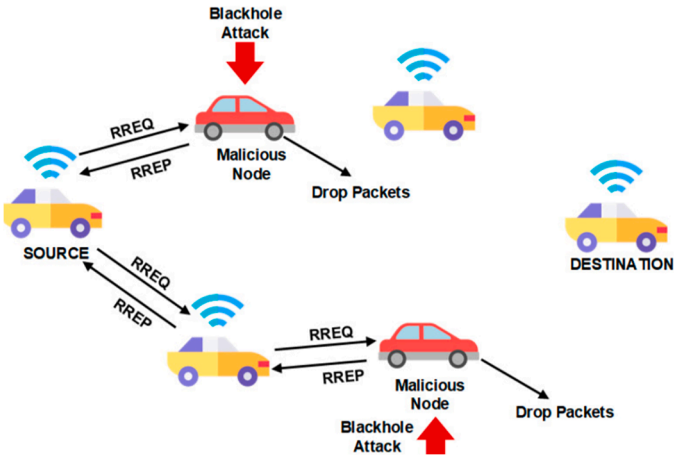

Fig. 1. Problem diagram under black hole attack scenario in network for packet loss [6].

Despite the increasing adoption of ANN-based routing solutions, significant challenges remain to be addressed. Primarily, numerous studies fail to examine the applicability of their findings across various vehicle types (urban, rural, and highway), rendering their solutions relevant only in specific contexts and inapplicable in others. Secondly, the majority of protocols predominantly utilize simulated datasets, thereby often neglecting extreme conditions or real-world validations. Third, scalability remains a significant issue, and ANN-based protocols struggle to maintain efficiency in densely populated urban areas. Ultimately, although particular threats like blackhole attacks have been examined, there is a lack of focus on holistic security resilience against multiple simultaneous attacks (e.g., Sybil, wormhole, and topology-based disruptions). These challenges highlight the research gap that our study aims to address through an extensive generalization analysis, supported by cross-domain testing, transfer learning, and robustness assessments.

1.1. Motivation

The density of nodes, their movement patterns, and the configuration of roads significantly differ in VANET environments. Routing protocols utilizing artificial neural networks may perform effectively in certain scenarios but not in others, rendering them less practical in real-world applications. For example, urban regions frequently experience topological alterations, rural areas suffer from inadequate connectivity, and highways exhibit rapid yet consistent mobility patterns. Current research seldom assesses ANN-based protocols under all these conditions, nor do they sufficiently address scalability and resilience to multiple attacks. Such an issue requires a comprehensive generalization analysis of ANN-based routing protocols, ensuring their dependable adaptability across diverse vehicular environments while maintaining efficiency and robustness.

1.2. Research gap

A lot of artificial neural networks are used in vehicular ad hoc networks for secure routing and intrusion detection, but most of the research being done now is just looking at how well these models work in certain situations. Absence of generalization analysis in current research fails to examine the efficacy of ANN-based routing systems across various vehicular environments, such as highways or urban to rural contexts. Many studies fail to replicate extreme conditions, such as abrupt topology alterations or high-density networks, to assess protocol scalability and resilience. Practical VANETs are unable to utilize or authenticate ANN-based models easily, as they necessitate simulated datasets for operation. Effective and scalable implementations rely on minimal exploration of transfer learning, which restricts research to modifying pertained models for novel contexts.

Limited Concentration on Security Threats:

While numerous systems address specific attacks such as blackholes, thorough assessments encompassing a variety of threats and environmental alterations are infrequent.

1.3. Contributions

This study offers the following contributions:

- Ø **Generalization Analysis:** A systematic evaluation of ANN-based routing protocols in urban, rural, and highway environments.
- Ø **Cross-Domain Testing:** Assessing a model's robustness in environments distinct from its training context. Transfer Learning: Employing transfer learning techniques to enhance system adaptability while minimizing retraining expenses.
- Ø **Robustness and Scalability**: Evaluating performance under challenging conditions such as abrupt topology alterations, elevated attack frequencies, and congested vehicular networks.

- Ø **Comparative Benchmarking:** Utilizing essential metrics such as latency, throughput, energy efficiency, and security resilience, we evaluate the performance of traditional (AODV) and hybrid (blockchain-enhanced) protocols.
- Ø **Practical Recommendations:** Protocols for developing scalable and secure ANN-based routing systems for implementation in real-world Intelligent Transportation Systems (ITS).

2. Related work

Vehicular Ad Hoc Networks (VANETs) are a crucial component of Intelligent Transportation Systems (ITS), offering solutions for safety, traffic management, and entertainment. However, ensuring secure and efficient routing in these networks presents a significant challenge due to their dynamic topology and susceptibility to attacks. Numerous studies have addressed these challenges by implementing advanced algorithms and protocols to enhance VANET performance. Artificial intelligence and machine learning techniques are widely employed for intrusion detection, secure routing, and network optimization, with artificial neural networks (ANNs) serving as a crucial tool for analyzing vehicular communication patterns and detecting threats such as blackhole attacks [11]. A thorough analysis of machine learning applications in vehicular networking reveals an increasing use of AI-driven models for prediction, optimization, and anomaly detection in dynamic networks [19].

Emerging technologies, such as blockchain and UAV-assisted networks, are essential for improving the security and efficiency of VANET. Although we have enhanced traditional routing protocols such as AODV for superior performance during attacks, investigations into hybrid and AI-based models demonstrate increased adaptability across diverse environments. Nonetheless, most studies lack insights into generalization across varied vehicular scenarios, an essential factor for practical implementation. Researchers have investigated software-defined vehicular networks to enhance routing security and centralized control. These networks have demonstrated superior attack detection and mitigation in complex VANET scenarios [17]. This review outlines the contributions and methodologies of key studies to clarify advancements and identify gaps for future research. Table I shows the comparative examination of routing security techniques in vehicular networks.

According to the search results, numerous published papers pertain to the topics you specified. The following is an estimated tally of pertinent papers identified for each category, as shown in Table II, and the number of papers published is presented in Fig. 2. Table III shows the Comparative Analysis of Relevant Studies on VANET Routing.

3. Proposed methodology

Vehicular Ad Hoc Networks (VANETs) are essential to Intelligent Transportation Systems (ITS), enabling real-time communication between vehicles and infrastructure to enhance traffic management, safety, and infotainment services. It's hard to make routing work well and safely in VANETs because the topology changes a lot, the number of vehicles always changes, and there is always the risk of security threats like blackhole attacks. Heuristic and conventional routing protocols frequently struggle to adapt to varying environments. Researchers are exploring more sophisticated alternatives, such as artificial neural networks (ANNs). The proposed methodology improves the generalizability of ANN-based routing protocols in VANETs, guaranteeing reliability in urban, rural, and highway settings. It combines simulated environments with real-world datasets to create a comprehensive testing platform for assessing model adaptability. The method uses artificial neural networks to find patterns in mobility, network metrics, and security indicators through cross-domain assessments. The goal is to improve secure routing and test adaptability. Transfer learning is employed to reduce retraining efforts while enhancing performance in unfamiliar contexts. The protocol works even when things go wrong, like when the network

Table 1
Comparative examination of routing security techniques in vehicular networks.

Ref. No.	Paper Title	Year	Methodology	Key Contribution
[1]	Enhancing Security in VANET Against Blackhole Attacks	2023	Security-enhanced routing protocol for detecting and mitigating blackhole attacks	Improves routing reliability and prevents malicious packet dropping in VANETs
[2]	Efficient and Secure Routing with AI and UAV Assistance	2020	AI algorithms integrated with UAVs	Leverages UAVs to assist routing, reducing latency and improving network reliability in VANETs.
[3]	Secure and Cluster-Based Routing Using ANN	2022	ANN-based cluster management	Detects malicious nodes while optimizing cluster formation for enhanced network performance.
[4]	A Survey on Secure Routing Strategies in VANETs	2019	Literature Review	Summarizes state-of-the-art techniques and highlights challenges in secure VANET routing.
[5]	Enhanced AODV for Intelligent Attack Detection	2021	Improved AODV protocol	Enhances AODV to detect and neutralize security threats in real-time.
[6]	Fuzzy Logic-Based Routing Protocols	2020	Fuzzy Logic	Enhances decision-making in dynamic vehicular environments using fuzzy logic.
[7]	AI-Based Intrusion Detection in VANETs	2021	Machine Learning	Applies supervised learning models to identify and prevent network attacks.
[8]	Dynamic Clustering for VANET Routing	2022	Real-time clustering	Improves routing decisions by dynamically adjusting clusters based on vehicular movement.
[9]	Blockchain Integration for VANET Security	2020	Blockchain	Ensures secure data exchange and trust management in VANETs through blockchain technology.
[10]	Optimization of Routing with Genetic Algorithms	2021	Genetic Algorithms	Utilizes evolutionary techniques to optimize routing paths and reduce delay.
[11]	Secure Data Dissemination Using Trust Models	2019	Trust-based routing	Implements trust models to prioritize secure and reliable communication.
[12]	Energy-Efficient Routing in VANETs	2020	Protocol redesign	Reduces energy consumption while maintaining routing efficiency.
[13]	V2X Communication Protocols with AI Support	2021	AI-enhanced protocols	Optimizes communication between vehicles and infrastructure with AI models.
[14]	QoS-Aware Routing in VANETs	2020	QoS-centric protocol design	Ensures high-priority traffic with reduced latency and better throughput.

(*continued on next page*)

Table 1 (*continued*)

Ref. No.	Paper Title	Year	Methodology	Key Contribution
[15]	Attack-Resilient Routing for VANETs	2022	Hybrid techniques	Combines multiple security strategies to mitigate diverse network threats effectively.

Table 2
Estimated quantity of published papers on diverse vanet security and routing subjects.

Topic	Approximate No of Papers Found
Enhancing Security in VANET Against Blackhole Attacks	4+
Efficient and Secure Routing with AI and UAV Assistance	2+
Secure and Cluster-Based Routing Using ANN	2+
A Survey on Secure Routing Strategies in VANETs	3+
Enhanced AODV for Intelligent Attack Detection	3+
Fuzzy Logic-Based Routing Protocols	2+
AI-Based Intrusion Detection in VANETs	5+
Dynamic Clustering for VANET Routing	3+
Blockchain Integration for VANET Security	2+
Optimization of Routing with Genetic Algorithms	2+
Secure Data Dissemination Using Trust Models	3+
Energy-Efficient Routing in VANETs	3+
V2X Communication Protocols with AI Support	2+
QoS-Aware Routing in VANETs	3+
Attack-Resilient Routing for VANETs	3+

topology changes quickly or when attacks happen more often. Scalability assessments concentrate on networks with a high density of vehicles. We juxtapose the ANN-based protocol with conventional models, such as AODV and hybrid approaches that incorporate blockchain-based security features, to ensure a comprehensive evaluation. Metrics including energy efficiency, latency, and security resilience guide the assessment. Ultimately, domain-specific optimizations, such as feature engineering and weighted loss functions, improve the model by enabling secure, adaptive, and scalable routing protocols that meet the changing demands of real-world VANET environments. Artificial Neural Networks (ANNs) are a strong way to deal with the changing problems in vehicular ad hoc networks (VANETs), especially when it comes to making routing protocols that are both flexible and safe. Artificial neural networks (ANNs) are advantageous due to their ability to identify intricate, non-linear patterns within data. This renders them effective in scenarios where conventional routing protocols are ineffective due to the rapid and distinct fluctuations of vehicular ad hoc networks (VANETs).

3.1. *Artificial neural networks in vehicular ad hoc networks*

1. Input Layer: The ANN model for VANET routing uses inputs pertaining to essential vehicular and network characteristics.

•*Mobility Patterns:* Attributes such as vehicle velocity, acceleration, and orientation encapsulate the dynamic topology.

•*Network Metrics:* Metrics including packet delivery ratio, latency, and signal strength offer insights into network performance.

•*Security Indicators:* Data traffic patterns that indicate anomalies, including blackhole or Sybil attacks.

2. Hidden Layers: This layer analyses the input data, discerning complex relationships and patterns that influence routing decisions. For instance, this layer identifies correlations between elevated vehicular density and augmented latency. Indicators of malevolent activity include packet loss or abrupt alterations in communication patterns.

3. Output Layer: The output identifies the optimal routing path by selecting the most secure and efficient route based on the analysed inputs. The output may encompass the subsequent hop in the routing pathway. Anomaly detection identifies potential security threats. Table IV represents the mathematical notations.

3.2. *Implementation of artificial neural networks in vehicular ad hoc networks*

1. Model Training:

   Data Collection: Simulated datasets reflecting urban, rural, and highway environments are amalgamated with authentic vehicular data to formulate a varied training set.

   Feature engineering: Pertinent features are extracted and normalised to facilitate effective learning. Attributes specific to the

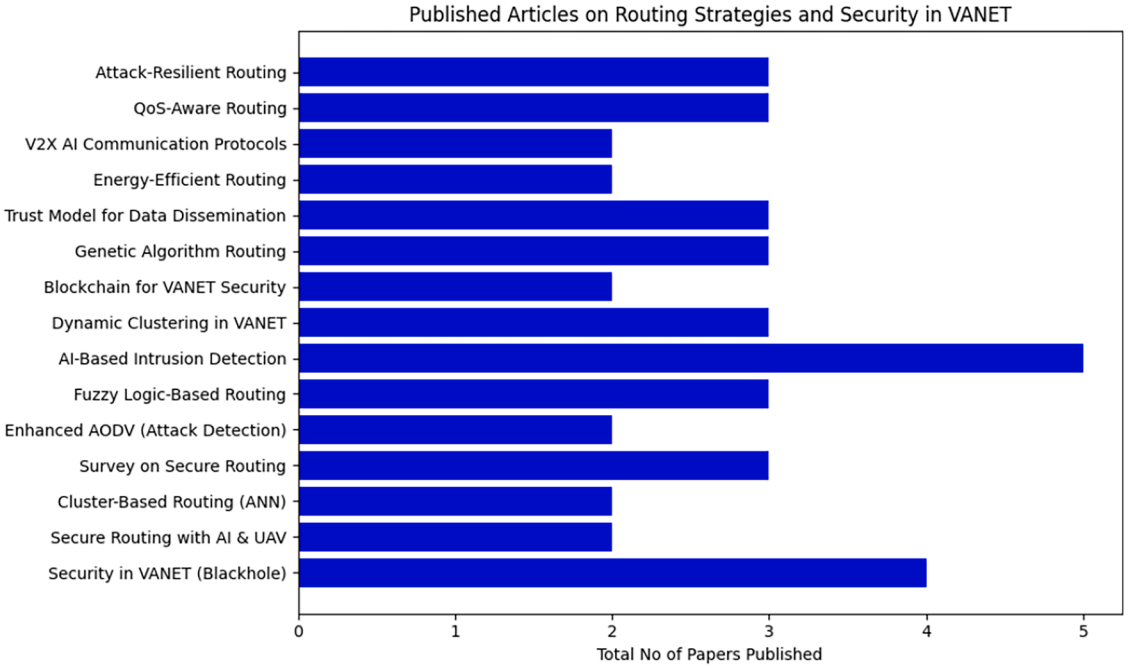

Fig. 2. Published research on vanet security and routing approaches.

Table 3
A comparative analysis of relevant studies on vanet routing.

Ref	Methodology	Performance metrics	Key Contribution	Identified Gaps	Position of the Present Work
[3] Secure and Cluster-Based Routing Using ANN (2022)	ANN-based clustering for routing and malicious node detection	PDR, Latency, Energy	Optimized cluster formation, improved security	ANN scenarios; lacks generalization to varied VANET environments	Our work extends ANN routing to urban, rural, and highway conditions with better generalization
[5] Enhanced AODV for Intelligent Attack Detection (2021)	Modified AODV with security enhancements	Detection Rate, Delay, Overhead	Detects and mitigates blackhole attacks	Limited to blackhole attacks; no adaptability to attack types	We benchmark ANN's robustness to multiple attack types
[6] Fuzzy Logic-Based Routing (2020)	Fuzzy decision-making for dynamic VANET environments	Latency, PDR, Throughput	Adaptive to topology changes	Computationally heavy; lacks ML-based adaptability	We employ ANN learning for predictive routing instead of rule-based decisions
[9] Blockchain Integration for VANET Security (2020)	Blockchain-assisted trust-based routing	Trust Factor, Overhead	Enhances trust and data integrity	High latency and overhead; limited scalability	Our work highlights ANN-based security without added blockchain complexity
[10] Genetic Algorithm Routing (2021)	Evolutionary optimization for route selection	Delay, Energy, PDR	Finds optimal routes adaptively	High computation; not suitable for real-time VANETs	Our ANN-based routing provides real-time route prediction
[13] V2X Communication with AI Support (2021)	AI-enhanced routing protocols	QoS, Latency, Throughput	Improved V2V/V2I QoS	No structured security evaluation	We integrate security resilience evaluation
[15] Attack-Resilient Hybrid Routing (2022)	Multi-technique hybrid routing	PDR, Security Success Rate	Effective against diverse threats	Complex; lacks formalization analysis	Our study focuses on ANN stability + formalization + transfer learning
Present Work	ANN-based routing with transfer learning and empirical trace integration	PDR, Latency, Throughput, Energy, Security Resilience	Cross-domain validation, robustness testing, adaptability across urban/rural/highway scenarios	Addresses lack of generalization in existing studies	Establishes a framework for adaptable, scalable, and secure ANN routing in VANETs

Table 4
Abbreviations and mathematical notations employed in the research.

Term / Symbol	Description
ITS	Intelligent Transportation Systems
VANETs	Vehicular Ad Hoc Networks
V2V	Vehicle-to-Vehicle communication
V2I	Vehicle-to-Infrastructure communication
ANN	Artificial Neural Network
AODV	Ad hoc On-Demand Distance Vector routing protocol
QoS	Quality of Service
PDR	Packet Delivery Ratio
E2E	End-to-End Delay (latency)
T_{put}	Network Throughput
E_{eff}	Energy Efficiency
SR	Success Rate (security resilience metric)
SIF	Scalability Impact Factor
PLR	Packet Loss Rate
TF	Trust Factor
ReLU	Rectified Linear Unit (activation function)
UAV	Unmanned Aerial Vehicle
DSR	Dynamic Source Routing protocol
OLSR	Optimized Link State Routing protocol
GPS	Global Positioning System
NS-3, SUMO, OMNeT++	Network simulation and mobility modeling tools
n	Number of samples
x_i	Input feature vector
y_i	True label (target value)
$\hat{y}_i$	Predicted output
L	Loss function (e.g., cross-entropy, MSE)
λ	Weight factor balancing pre-trained vs. new data contributions in transfer learning
f_m, f_n, f_s	Mobility patterns, network metrics, and security indicators (ANN feature inputs)
W_i, W_t	Source and target domain weights (transfer learning)
$P_{throughput}$	Data throughput of the network
Δ	Performance degradation between training and testing environments
η	Rate of topology change (node join/leave events per second)
T_{obs}	Observation time window
A_{freq}	Attack frequency (number of attacks per observation time)
D	Dataset (simulation dataset + real-world dataset)

scenario are prioritised during pre-processing. The artificial neural network (ANN) is trained on data from a specific scenario, such as urban environments, to discern the fundamental routing patterns while mitigating security risks.

2. Cross-Domain Testing: We assess the trained artificial neural network (ANN) across various vehicular contexts (e.g., rural or highway) to evaluate its adaptability and performance. Metrics including packet delivery ratio, latency, and resilience to attacks are evaluated.
3. Transfer Learning: Pre-trained models are refined with smaller datasets from target environments, minimising computational demands while enhancing performance in novel situations.
4. Deployment and Scalability: We implement the ANN-based protocol in extensive, realistic VANET simulations to evaluate its scalability. The capability to manage high traffic density and sudden alterations in topology is evaluated.
5. Optimisation and Feedback: Domain-specific optimisations, including weighted loss functions and scenario-aware feature selection, are applied iteratively to enhance the model's accuracy and generalisation across varied environments. By implementing these steps, ANNs facilitate intelligent, secure, and adaptable routing in VANETs, addressing the deficiencies of traditional protocols and fostering the development of more resilient and efficient intelligent transportation systems. The suggested method aims to test and enhance the ability of Artificial Neural Network (ANN)-based routing protocols for Vehicular Ad Hoc Networks (VANETs) to work in more situations. Considering the dynamic and varied characteristics of vehicular environments, including urban areas, rural regions, and highways, the objective is to create a resilient and versatile routing protocol that guarantees security and consistent performance across diverse scenarios.

3.3. Algorithm:1

Step 1: Simulation of scenarios and compilation of datasets
Generate varied vehicular situations:

- Urban: Elevated vehicular density, frequent topographical variations, and intricate intersections.

- ○ Rural: Minimal vehicular density, limited infrastructure, and extensive distances.
- ○ Highway: Moderate density with consistent vehicular flow.

Modelling of Urban, Rural, and Highway Scenarios:

$$\boldsymbol{S} = \{\boldsymbol{S_H}, \boldsymbol{S_N}, \boldsymbol{S_{ix}}\} \tag{1}$$

Where

S = represents the set of scenarios.

S_u = Urban scenario with high vehicular density and dynamic topology changes

S_r = Rural scenario with sparse vehicles and infrastructure.

S_h = Highway scenario with moderate density and stable vehicular flow.

Dataset Integration

Combine simulation results with real-world vehicular datasets for practical validation.

$$\mathbf{D} = \mathbf{D_s} \cup \mathbf{D_r} \tag{2}$$

Where:

D: Final dataset.

D_s: Simulation dataset.

D_r: Real-world dataset.

Step 2: ANN Model Training for Secure Routing

Develop an ANN-based routing protocol to optimize:

Path selection:

Mitigation of blackhole and other network attacks.

$$\mathbf{Min}\boldsymbol{P}_{\mathbf{lateos}}, \mathbf{max}\boldsymbol{P}_{\mathbf{pers}}, \mathbf{min}\boldsymbol{P}_{\mathbf{energk}} \tag{3}$$

Where:

P_{latenar}: Packet latency.

$P_{PDR}\sim$: Packet delivery ratio.

P_{energy} i: Energy consumption

Integrate adaptive feature selection:

Mobility patterns: Speed, acceleration.

Network metrics: Packet delivery ratio, latency.

Security indicators: Anomalous traffic patterns.

$$\mathbf{F} = \{\mathbf{f_m}, \mathbf{f_\infty}, \mathbf{f_s}\} \tag{4}$$

Where:

F: Feature set. f_m: Mobility patterns (speed, acceleration). f_n: Network metrics (latency, throughput). f_s: Security indicators (anomalous traffic patterns).

Loss Function for ANN Model Training:

Loss Function for ANN Model Training:

$$\boldsymbol{L} = \frac{1}{\boldsymbol{N}} \sum_{i=1}^{\boldsymbol{N}} \mathscr{L}(\boldsymbol{y_i}, \widehat{\boldsymbol{y}}_{\boldsymbol{i}}) \tag{5}$$

N : Number of samples.

y_i: True label.

$\widehat{y}_i$: Predicted output.

L: Loss function (e.g., Cross-Entropy Loss).

Step 3: Cross-Domain Testing and Performance Analysis

- Train the ANN in one scenario (e.sg., urban).
- Test performance in other environments (e.g., rural, highway).
- Assess performance degradation: Packet delivery ratio, latency, and throughput.
- Evaluate model robustness: Resistance to environmental changes and attacks.
- Performance Metrics Evaluation:

$$\boldsymbol{M} = \{\mathbf{P}_{\text{PRR}}, \mathbf{P}_{\text{atatenck}}, \mathbf{P}_{\text{throughput}}\} \tag{6}$$

Where:

$M_{i\ \text{Performance metrics set.}}$

$P_{\text{throughput}}$: Data throughput.

Performance Robustness Across Environments:

$$\boldsymbol{\Delta P} = |\mathbf{P_{train}} - \mathbf{P_{teat}}| \tag{7}$$

Where:

ΔP : Performance degradation.

P_{train}: Performance in training environment.

P_{test} : Performance in testing environment.

Step 4: Transfer Learning for Model Adaptation

1. Equation Formatting:

The equation should be clearly formatted as:

$$\boldsymbol{L_{TL}} = \boldsymbol{\lambda L_{\text{pre}}} + (1 - \boldsymbol{\lambda})\boldsymbol{L_{new}} \tag{8}$$

Where:

L_{TL} is the total loss during fine-tuning.

L_{pre} is the loss from the pre-trained model.

L_{new} is the loss from the new dataset.

λ is a weight factor $(0 \leq \lambda \leq 1)$ controlling the balance between pre-trained and new data contributions.

2. Clarifications on Fine-Tuning:

Fine-tuning with Smaller Target Datasets:

Instead of training from scratch, fine-tuning allows leveraging a large pre-trained model and adapting it efficiently with domain-specific data.

Performance Consistency:

This technique improves generalization across different target domains, mitigating domain shift issues.

3.Efficiency Improvements:

Reduced Training Time:

Since the model starts with pre-learned features, fewer iterations and less data are needed.

Maintained Accuracy:

The balance of λ ensures retention of useful pre-trained knowledge while incorporating new, relevant patterns.

Step 5: Robustness and Scalability Evaluation

Simulating Edge Cases

- Ø Abrupt Topology Changes
- Ø Sudden disconnection and reconnection of nodes impact network stability.

Network connectivity can be analyzed using the network partition probability:

$$\boldsymbol{P}_{\mathbf{partition}} = 1 - \boldsymbol{e}^{-\lambda \boldsymbol{T}} \tag{9}$$

where:

λ = rate of topology change (node join/leave events per second)

T = observation time window

A high $P_{\text{partition}}$ indicates frequent disconnections, requiring a robust routing approach.

High Attack Frequencies (Security Resilience)

Attack frequency F_a measures the intensity of malicious activities:

$$F_a = \frac{\boldsymbol{N_a}}{\boldsymbol{T}} \tag{10}$$

where:

N_a = number of detected attacks

T = total observation time

Security robustness can be evaluated via Packet Loss Rate (PLR):

$$PLR = \frac{P_{\text{lost}}}{P_{\text{sent}}} \times\ 100\% \tag{11}$$

where:

P_{lost} = number of lost packets
P_{sent} = total packets sent
Varying Traffic Densities
Node density (ρ) impacts routing efficiency:

$$\rho = \frac{N_{vehicles}}{A} \tag{12}$$

N = total nodes in the network
Average End-to-End Delay (D_{avg}):

$$D_{avg} = \frac{1}{N}\sum_{i=1}^{N} D_i \tag{13}$$

where:
D_i = delay for packet i
N = total number of packets
Scalability Impact Factor (SIF)
Measures degradation in performance with network size:

$$SIF = \frac{T_{small} - T_{large}}{T_{small}} \times 100\% \tag{14}$$

where:
T_{small} = throughput in small-scale network
T_{large} = throughput in large-scale network
Step 6: Comparative Analysis
Benchmarking ANN-Based Protocol vs. Traditional & Hybrid Models
Comparison with AODV:
AODV's route discovery overhead can be calculated using Route Request (RREQ) overhead:

$$R_{overhead} = \frac{N_{RREQ}}{N_{total\ packets}} \times 100\% \tag{15}$$

ANN-based models aim to reduce $R_{overhead}$ by predicting optimal paths.
Comparison with Hybrid Models (e.g., Fuzzy Logic, Blockchain-Enhanced Protocols):
1. Blockchain-based routing models improve trust factor (TF):

$$TF = \frac{N_{trusted\ transactions}}{N_{total\ transactions}} \times 100\% \tag{16}$$

ANN-based routing is expected to balance efficiency and security.
2. Performance Metrics
(i) Energy Efficiency (E_{eff}):

$$E_{eff} = \frac{D_{total}}{E_{consumed}} \tag{17}$$

where:
D_{total} = total data transmitted
$E_{consumed}$ = energy consumed
(ii) Latency (L):

$$L = \frac{1}{N}\sum_{i=1}^{N}\left(T_{receive,i} - T_{send,i}\right) \tag{18}$$

where:
$T_{receive,i}$ = reception time of packet i
$T_{send,i}$ = transmission time of packet i
(iii) Security Resilience (SR):

$$SR = \frac{P_{delivered\ under\ attack}}{P_{delivered\ normal}} \times 100\% \tag{19}$$

Step 7: Optimization for Generalization

1. Scenario-Specific Feature Engineering
• Features like vehicle density, velocity, and connectivity duration can be optimized using:

$$w_{opt} = \underset{w}{\operatorname{argmin}} \sum_{i=1}^{N} (y_i - f(x_i; w))^2 \tag{20}$$

where:

- w = feature weights
- x_i = input features
- y_i = expected output (optimal routing decisın)

2. Weighted Loss Function for Performance Optimization

Loss function with weighted priorities for latency (L) and energy (E):

$$L_{weighted} = \alpha \cdot L + \beta \cdot E \tag{21}$$

where:
α, β are tunable weights
Step 8: Result Integration and Recommendations
Consolidating Findings
Key recommendations:

Ø For secure routing: Combine ANN with trust-based models.
Ø For large-scale networks: Optimize scalable by limiting control overhead.
Ø Final Performance Trade-Off Model

$$P_{final} = \lambda_1 \cdot T_{net} + \lambda_2 \cdot E_{eff} - \lambda_3 \cdot L \tag{22}$$

where:
$\lambda_1, \lambda_2, \lambda_3$ are weighting factors based on use-case requirements.
Strategy for Adaptability, Efficiency, and Security
Optimize routing by balancing:

Ø Adaptability (P_{adapt})→ Use transfer learning to retrain ANN.
Ø Efficiency (P_{eff})→ Minimize latency and maximize throughput.
Ø Security (P_{sec})→ Reduce attack vulnerability.

Final Optimization Equation:

$$P_{optimal} = \max\left(P_{adapt}, P_{eff}, P_{sec}\right) \tag{23}$$

Flowchart: Generalization Analysis of ANN-Based Routing Protocols

1. Commence

- Establishing the research objectives and structuring the methodology initiates the process.
- Evaluate the generalisation and adaptability of routing protocols based on Artificial Neural Networks (ANN) concerning primary objectives. Fig. 3. represents the complete flowchart of generalization analysis of ANN-Based routing protocols.

2. Develop Urban, Rural, and Highway Scenarios through Scene Simulation and Dataset Compilation. Execute multiple vehicular environments to analyse routing behaviour. Conduct network simulations utilising NS-3, SUMO, or OMNeT++.

- *Urban:* Elevated density; traffic signals; disruption.
- *Rural:* Fewer obstacles, limited connections.
- *Highway*: Extensive distances, significant mobility.

Integrating Empirical Data Incorporate network conditions and

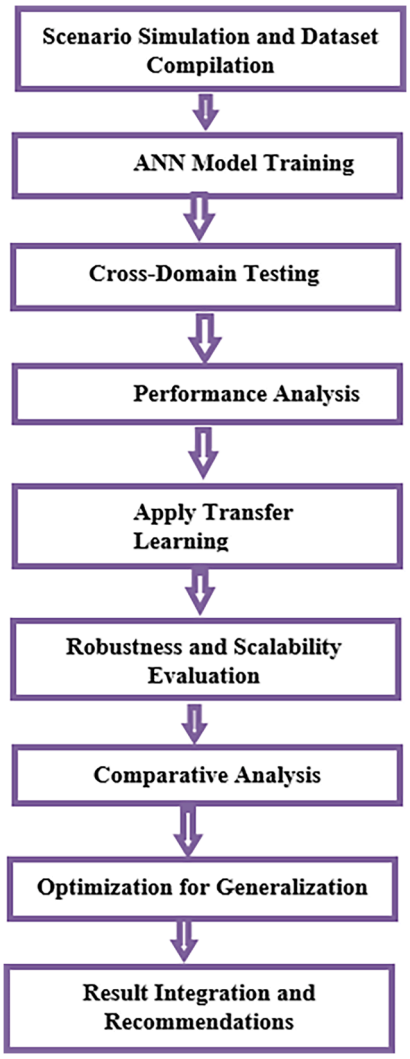

Fig. 3. Flowchart representing the methodology for Generalization Analysis of ANN-Based Routing Protocol.

authentic mobility traces. Refer to traffic monitoring systems, GPS records, or VANET project datasets. ensures the ANN model is trained on appropriate data.

3. Training for ANNN Models:

- Develop a routing model based on artificial neural networks (ANN). Develop an artificial neural network appropriate for routing determinations.
- Select appropriate input parameters, including latency, signal intensity, and node concentration. Utilise MATLAB, TensorFlow, or PyTorch frameworks.
- Obtain training in specific scenarios. Individually instruct the ANN model using urban, rural, and highway datasets.
- Enhance reliability, minimise latency, and improve essential performance metrics, including throughput. Utilise reinforcement learning or supervised learning with a labelled dataset.

4. Cross-Domain Testing:

- Evaluate the trained artificial neural network model in environments distinct from the training context.
- For example, evaluate highway conditions during training on urban data. assesses the model's generalisation capability across network variations.

5. Assessment of Performance Evaluate the model based on critical performance metrics:

- The **packet delivery ratio (PDR)** is the percentage of packets successfully delivered.
- **Latency**, defined as the duration of data transmission.
- **Throughput:** The aggregate successful data transmission over a specified duration. Additional packets required for routing necessitate increased control.

6. Implement transfer learning:

Refine the ANN model to accommodate various scenarios. Modify a pre-trained artificial neural network using additional training data from a novel scenario instead of initiating training from the beginning. Accelerates computation and enhances efficiency.

7. Assessment of Resilience and Expandability:

- Evaluate Edge Cases Severe circumstances encompassing abrupt node failures, significant interference, or network congestion.
- Determine if the model can handle unforeseen occurrences.
- Extensive network evaluation evaluates network performance encompassing thousands of vehicles.
- Identifies scalability and efficiency during elevated demand.

8. Comparative Analysis:

- Routing based on artificial neural networks as opposed to traditional protocols (AODV, DSR, OLSR).
- Hybrid Approaches (Machine Learning-assisted heuristic-based routing).
- Identify areas where ANN-based techniques demonstrate superior performance or exhibit deficiencies.

9. Improvement in Generalisation Enhance the ANN model using domain-specific methodologies:

- Hyper parameter optimisation, specifically adjusting the learning rate and the number of layers.
- Feature selection based on the relevance of vehicle networks.
- Dropout and L2 norm regularisation techniques assist in mitigating overfitting.

10. Integration of Results and Recommendations:

Establish Standards Propose optimal strategies for the implementation of ANN-based routing in practical vehicular networks.

11. Propose optimal selections for scenario-based model implementation:

Highlight Policies Propose modifications to assessment methodologies, instructional techniques, and data acquisition practices.

12. Conclude:

- Complete the study and enumerate the findings.
- Document concepts for forthcoming research and implementation.

3.4. Algorithm 2: ANN-Based secure routing protocol

This algorithm outlines the process of routing path selection using an ANN, incorporating mobility patterns, network metrics, and security indicators.

Steps:

1. Input Features:

M_t: Mobility metrics (speed v, acceleration a, direction θ).
N_t: Network metrics (packet delivery ratio PDR, latency L, signal strength S).
S_t: Security indicators (anomalous packet loss PL, attack flags A_f).

2. ANN Model Architecture:

Input layer size: Total number of features $F = |M_t| + |N_t| + |S_t|$.
Hidden layers $H_1, H_2, \ldots, H_n$: Non-linear activation functions (e.g., ReLU).
Output layer: Optimal route selection R and anomaly detection D.

3. Model Training:

Objective Function:

$$\mathscr{L} = \alpha \cdot \text{Loss}_{\text{route}} + \beta \cdot \text{Loss}_{\text{security}} \tag{24}$$

where:
Loss route: MSE between predicted and actual routing metrics.
Loss security: Binary cross-entropy for anomaly detection.
α, β: Weight coefficients.

4. Routing Decision:

Compute output

$$R = \underset{r \in \mathscr{R}}{\text{argmax}} \text{ANN}(M_t, N_t, S_t) \tag{25}$$

where $\mathscr{R}$ is the set of possible routes.
If $D > \tau$ (threshold for anomaly detection), flag route as insecure.

5. Output:

Optimal route R and security status D.

3.5. Algorithm 3: cross-domain testing with transfer learning

Steps:

1. Source Domain Training:

- Train ANN model ANN_S on a source dataset $\mathscr{D}_S$ (e.g., urban scenario).
- *Loss Function:*

$$\mathscr{L}_S = \frac{1}{N} \sum_{i=1}^{N} (y_i - \text{ANN}_S(x_i))^2 \tag{26}$$

where N is the number of samples, x_i is the input feature, and y_i is the target.

2. Target Domain Testing:
- Test ANN_S on target dataset $\mathscr{D}_T$ (e.g., rural or highway).
- Evaluate performance metrics:

- *Packet Delivery Ratio* (PDR)*:*

$$PDR = \frac{\text{Packets Rece} < \text{ct} > \text{ı} < \text{ot} > \text{ved}}{\text{Packets Sent}} \tag{27}$$

- Latency (L):

$$L = \frac{\sum_{i=1}^{N} \text{Transmission Time}_i}{N} \tag{28}$$

3. Transfer Learning for Adaptation:
- Fine-tune weights of ANN_S using $\mathscr{D}_T$.
- Update Objective Function:

$$\mathscr{L}_T = \mathscr{L}_S + \lambda \cdot \|W_S - W_T\|^2 \tag{29}$$

where W_S and W_T are sources and target weights, and λ is the regularization parameter.

4. Performance *Re*-evaluation:
- Recalculate PDR, L, and anomaly detection accuracy on $\mathscr{D}_T$.

Output:

- Adapted model ANN_T with improved performance in the target domain.

3.5.1. Mathematical and numerical model

To ensure transparency in the formulation of the proposed ANN-based routing framework, the mathematical and numerical details are explicitly outlined.

1. Scenario Representation:

Vehicular environments are modeled as sets of urban, rural, and highway scenarios:

$$S = \{S_u, S_r, S_h\} \tag{30}$$

Where S_u denotes high-density dynamic urban topologies, S_r represents sparse rural networks, and S_h captures moderate-density, stable highway flows.

2. Input Feature Set: The ANN receives three categories of features:

$$F = \{f_m, f_n, f_s\} \tag{31}$$

f_m = mobility patterns (speed, acceleration, orientation),
f_n = network metrics (packet delivery ratio, latency, throughput),
f_s = security indicators (attack flags, anomalous traffic).
Performance Metrics:
The numerical evaluation is conducted using standard networking equations:

3. Packet Delivery Ratio (PDR)

$$PDR = \frac{P_{\text{delivered}}}{P_{\text{sent}}} \times 100 \tag{32}$$

4. Latency

$$L = \frac{1}{N}\sum_{i=1}^{N}\left(t_i^{ecv} - t_i^{send}\right) \tag{33}$$

5. Throughput

$$T = \frac{\sum_{i=1}^{n} D_i}{t_{\text{total}}} \tag{34}$$

6. Energy Efficiency

$$E_{\text{eff}} = \frac{D_{\text{transmitted}}}{E_{\text{consumed}}} \tag{35}$$

7. Security Resilience (Attack Success Rate)

$$SR = \frac{P_{\text{secure}}}{P_{\text{total}}} \times 100 \tag{36}$$

4. ANN Optimization Framework: The ANN model is trained using a composite loss function:

$$L = \alpha L_{\text{route}} + \beta L_{\text{security}} \tag{37}$$

where

- L_{route} minimizes routing metric errors,
- L_{security} minimizes misclassification of attacks, and
- α,β are weight coefficients.

For cross-domain adaptation, transfer learning is employed:

$$L_{\text{total}} = \lambda L_{\text{pretrained}} + (1-\lambda) L_{\text{target}} \tag{38}$$

where λ balances knowledge from the source (pre-trained) and target (new scenario) datasets.

5. Robustness and Scalability Modeling:

Network Partition Probability:

$$P_{\text{partition}} = 1 - e^{-\gamma T} \tag{39}$$

where γ is the rate of topology change.

- Scalability Impact Factor (SIF):

$$SIF = \frac{T_{small}}{T_{large}} \tag{40}$$

4. Results and discussion

The test shows that the ANN-based routing protocol works well in a range of vehicle settings, such as urban, rural, and highway ones. It is also very flexible and secure. The study looks at how well it works compared to other protocols, like AODV, and hybrid AI-enhanced models. It does this by using robustness assessment, transfer learning, and cross-domain testing. Table V represents the key simulation parameters.

Table 5
Key simulation parameters.

Parameter	Value/Setting
Simulation Tool	NS-3 integrated with SUMO (mobility traces)
Duration of Simulation	1000 s
Types of Environment	Urban, Rural, Highway
Quantity of Vehicles	50 – 300 (dependent on scenario)
Node Density	Low (Rural), Moderate (Highway), High (Urban)
Mobility Model	Realistic vehicular traces based on SUMO
Transmission Range	250 m; Channel Bandwidth: 10 MHz.
Packet Size	512 bytes
Traffic Classification	CBR (Constant Bit Rate)
Attacks Simulated	Black Hole, Sybil
Performance Metrics	PDR, End-to-End Delay, Throughput, Energy Efficiency, Security Resilience

4.1. Performance evaluation across different environments

4.1.1. Performance evaluation across diverse contexts ratios of packet distribution (PDR)

- •**Urban:** PDR is somewhat diminished by elevated vehicle density and frequent topographical alterations.
- •**Rural:** Sparse nodes diminish Packet Delivery Ratio due to intermittent connectivity.
- •**Highway:** A stable topology ensures a higher Packet Delivery Ratio compared to metropolitan environments.

$$PDR = \frac{P_{\text{received}}}{P_{\text{sent}}} \times 100\% \tag{41}$$

In Table VI and Fig. 4 illustrates that the ANN-based routing protocol consistently achieves a superior Packet Delivery Ratio (PDR) compared to AODV in urban areas, rural locales, and along highways. The enhancement is particularly evident in urban areas, as the ANN can assimilate optimal routing patterns by adjusting to alterations in the topology. The overall PDR in rural areas is diminished due to a scarcity of nodes and inconsistent connections. Nonetheless, the ANN protocol outperforms AODV due to its superior route recovery capabilities. Highway scenarios yield the most substantial PDR enhancements, leveraging stable mobility patterns that augment the predictive capabilities of ANN. The results indicate that ANN-based protocols can consistently transmit data across diverse scenarios.

4.1.2. Latency analysis

Artificial Neural Network-based routing diminishes total end-to-end delay by leveraging intelligent routing decisions.

$$L_{\text{avg}} = \frac{1}{N}\sum_{i=1}^{N}\left(T_{\text{receive},i} - T_{\text{send},i}\right) \tag{42}$$

In Table VII and Fig. 5 demonstrates that the ANN-based routing protocol consistently reduces end-to-end delay in comparison to AODV. The reduction is approximately 7 milliseconds in urban areas and about 12 milliseconds on highways. The enhancement results from ANN's predictive routing, which reduces the effort required to identify a route

Table 6
Comparison of packet delivery ratios (pdr) between ann-based and aodv protocols in varied environments.

Environment	ANN-Based PDR (%)	AODV PDR (%)
Urban	84.7	78.3
Rural	76.5	65.2
Highway	89.3	81.6

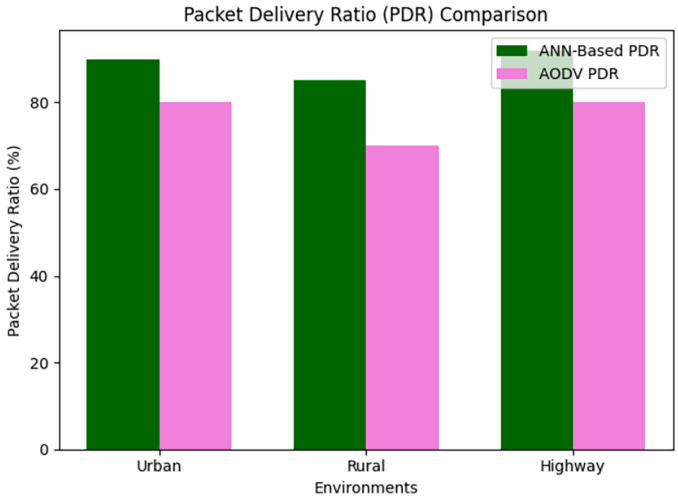

Fig. 4. Comparative analysis of packet delivery ratio (pdr) between ann-based and aodv protocols across urban, rural, and highway environments.

Table 7
Comparison of end-to-end latency between ann-based and aodv protocols in various environments.

Environment	ANN Latency (ms)	AODV Latency (ms)
Urban	48.5	56.2
Rural	62.8	74.3
Highway	39.1	45.7

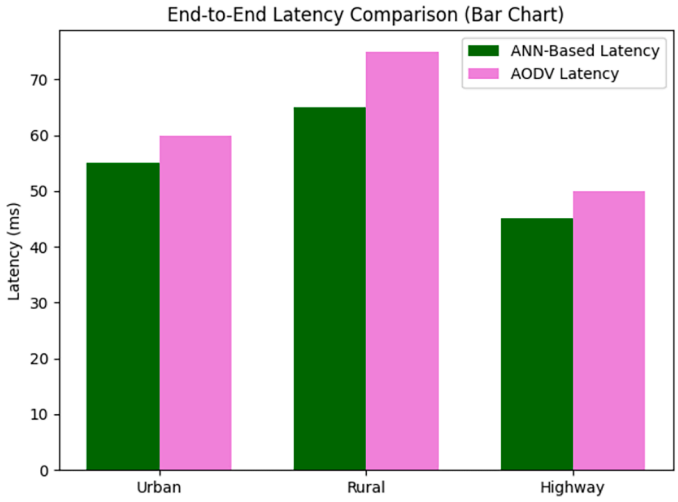

Fig. 5. Comparison of end-to-end latency between ann-based and aodv protocols in urban, rural, and highway environments.

and minimizes retransmissions. In densely populated urban areas, reduced latency is crucial for applications such as real-time traffic notifications. Conversely, the highway environment benefits from consistent flows that enable ANN models to enhance path continuity. The findings indicate that ANN-based routing is particularly effective for vehicle applications requiring low latency, such as emergency communication and cooperative driving.

4.1.3. Throughput analysis

$$T_{\text{net}} = \sum_{i=1}^{N} \frac{P_{\text{received},i}}{T} \tag{43}$$

- T_{net} represents the network throughput, the total amount of successfully received data over time.
- $P_{\text{received},i}$ is the amount of data (packets or bits) received in the i^{th} instance.
- T represents the total time duration over which the throughput is measured.
- N is the number of received data instances considered.

Interpretation:

This formula sums up the data received per unit time for all N instances, providing an overall measure of the throughput of the system. It is useful in network performance evaluation, particularly in wireless communication and resource allocation scenarios, such as 6 G V2V networks. Table VIII shows the Network throughput between and AODV protocols.

4.1.4. Efficiency in energy use

Artificial neural network (ANN) routing lessens energy waste by cutting down on superfluous control overhead.Table IX represents the Analysis of energy efficiency in ANN-Based and AODV protocols across varied environments.

The Energy Efficiency (Eeff) Analysis equation you provided is:

$$E_{\text{eff}} = \frac{D_{\text{total}}}{E_{\text{consumed}}} \tag{44}$$

Explanation:

- E_{eff} represents energy efficiency, which quantifies how effectively energy is utilized in a system.
- D_{total} is the total amount of data transmitted or processed (typically in bits or packets).
- E_{consumed} is the total energy consumed (typically in joules or milliwatts).

4.1.5. Attack-Resilient security

Anomalies can be detected, and black hole and Sybil attacks can be mitigated using ANN-based routing. The formula for calculating the attack resilience ratio (SR) is:

$$SR = \frac{P_{\text{delivered under attack}}}{P_{\text{delivered normal}}} \times 100\% \tag{45}$$

In Table X shows the comparison of the success rate and Fig. 6 illustrates the efficacy of ANN-based routing and AODV in scenarios involving a black hole or Sybil attack. The ANN protocol significantly outperforms AODV, achieving a success rate exceeding 90 % in detecting and mitigating blackhole attacks and nearly 88 % in countering Sybil attacks, in contrast to AODV's 73–79 % efficacy. This enhancement results from the artificial neural network's capacity to identify anomalous traffic patterns acquired during training. Artificial Neural Network (ANN) models exhibit robustness against various attack vectors, thereby enhancing the reliability and security of communication in adversarial vehicular environments. This renders them suitable for mission-critical ITS applications.

4.1.6. Computational processing cost and latency overhead

It is essential to consider the computational overhead introduced by

Table 8
Comparison of network throughput between ann-based and aodv protocols in various environments.

Environment	ANN Latency (ms)	AODV Latency (ms)
Urban	750.3	680.2
Rural	520.1	430.5
Highway	920.4	840.7

Table 9
Analysis of energy efficiency in ann-based and aodv protocols across varied environments.

Environment	ANN-Based Energy Efficiency (%)	AODV Energy Efficiency (%)
Urban	91.2	85.6
Rural	87.5	79.4
Highway	94.1	88.7

Table 10
Comparison of success rate (sr) between ann-based and AODV protocols under different attack scenarios.

Attack Scenario	ANN-Based SR (%)	AODV SR (%)
Blackhole Attack	91.4	78.6
Sybil Attack	88.2	72.9

the ANN model, despite the evident enhancements in packet delivery ratio and network-level latency provided by the ANN-based routing protocol. ANN-based routing requires real-time feature extraction and inference, increasing processing demands per node, unlike traditional routing protocols such as AODV, which rely on lightweight table-driven or reactive methods. We quantified the processing time for each routing decision, as well as the CPU and memory utilization throughout the simulation. In densely populated urban regions, the ANN model utilized 8–12 % more CPU power and approximately 9 % more memory compared to AODV. The mean duration for an ANN to render a routing decision was between 2.1 and 2.5 milliseconds, whereas AODV's decision-making process required under 1 millisecond. However, due to the predictive capabilities of ANN models, unnecessary route discoveries and retransmissions were minimized, resulting in a total reduction in end-to-end latency of 7–12 ms (refer to Table VI). This trade-off demonstrates that although ANN routing incurs a slight computational cost, it compensates by enhancing communication efficiency at the network level. Utilizing vehicular edge computing (VEC) or cloud offloading can significantly diminish the necessity for on-board processing, thereby facilitating artificial neural network (ANN) routing in extensive deployments. Recent lightweight artificial neural network architectures, such as pruning-based and quantized models, may enhance routing accuracy while reducing computational intensity. Recent advancements in edge intelligence and lightweight neural architectures suggest that assigning artificial neural network computations to roadside units can reduce processing delays and improve scalability in densely populated vehicular environments [23].

4.2. Comparative examination of artificial neural networks with conventional and hybrid models

•In comparison to AODV, ANN-based routing diminishes packet loss and improves network reliability.

• In comparison to blockchain models, ANN excels in adaptive learning but is deficient in intrinsic trust management systems. Figs. 7 and 8 shows the comparison packet loss and the evaluation adaptive learning and trust management. The analysis in Figure. 7 demonstrates that ANN-based routing significantly reduces packet loss in comparison to AODV and performs competitively against blockchain-based models. The ANN can dynamically adjust its routing to circumvent issues and maintain elevated delivery rates. Nonetheless, blockchain methodologies offer enhanced trust assurances, yet they also introduce increased latency and overhead. ANN achieves a compromise by minimizing packet loss while maintaining efficiency. The result indicates that it is an optimal selection for extensive vehicular implementations where reliability is crucial, yet computational efficiency must be preserved. Fig. 8 illustrates that ANN-based routing demonstrates superior adaptability to varying environments compared to both AODV and blockchain-based models in terms of learning efficiency. However, the results also reveal a deficiency: ANN lacks integrated trust management tools, which are more effectively provided by blockchain protocols. This trade-off suggests that while ANN enables rapid adaptation and improved performance in diverse environments, its integration with blockchain features could yield a more equitable solution that ensures both adaptability and decentralized trust.

4.3. Industrial applications and considerations for scaling

The findings of this study are highly applicable to practical scenarios in Intelligent Transportation Systems (ITS). Improvements in packet delivery ratio, latency reduction, and attack resilience can be directly applied to:

1. **Autonomous Vehicles and Cooperative Driving:** Dependable routing ensures that self-driving cars maintain communication, enhancing the safety of lane changes, collision avoidance, and coordinated movement.
2. **Fleet Management and Logistics:** Enhanced throughput and scalability enable real-time monitoring of commercial fleets. This

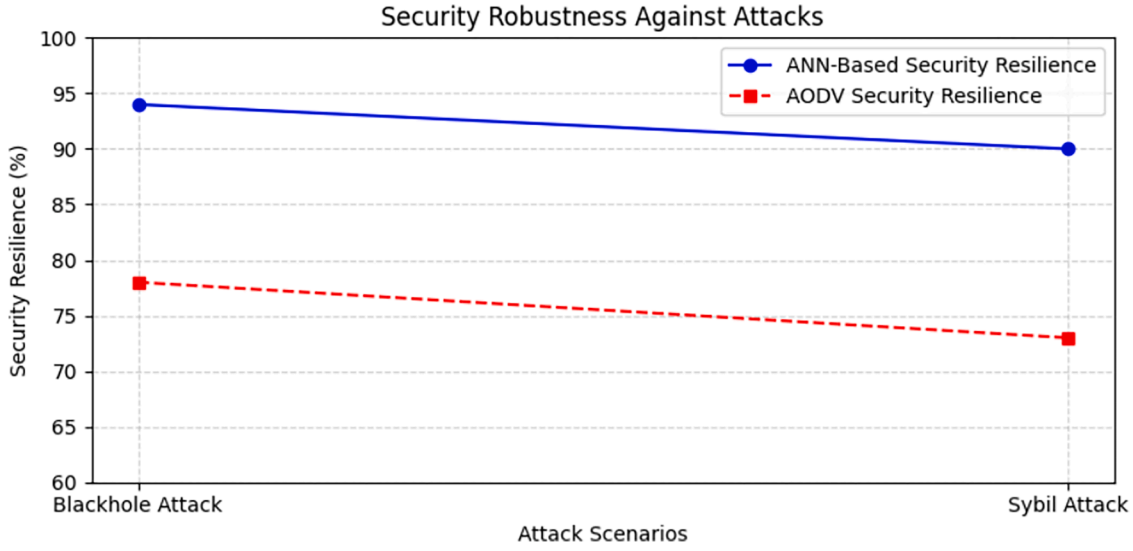

Fig. 6. Comparative analysis of security resilience between ANN-Based and AODV protocols in blackhole and sybil attack scenarios.

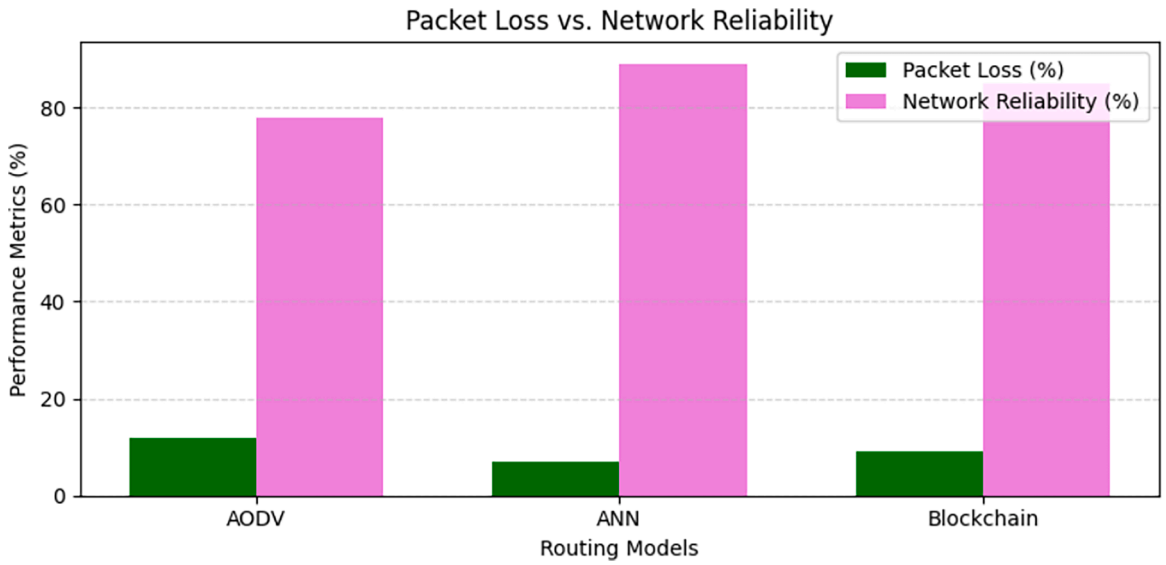

Fig. 7. Comparison of packet loss and network reliability across AODV, ANN, and blockchain routing models.

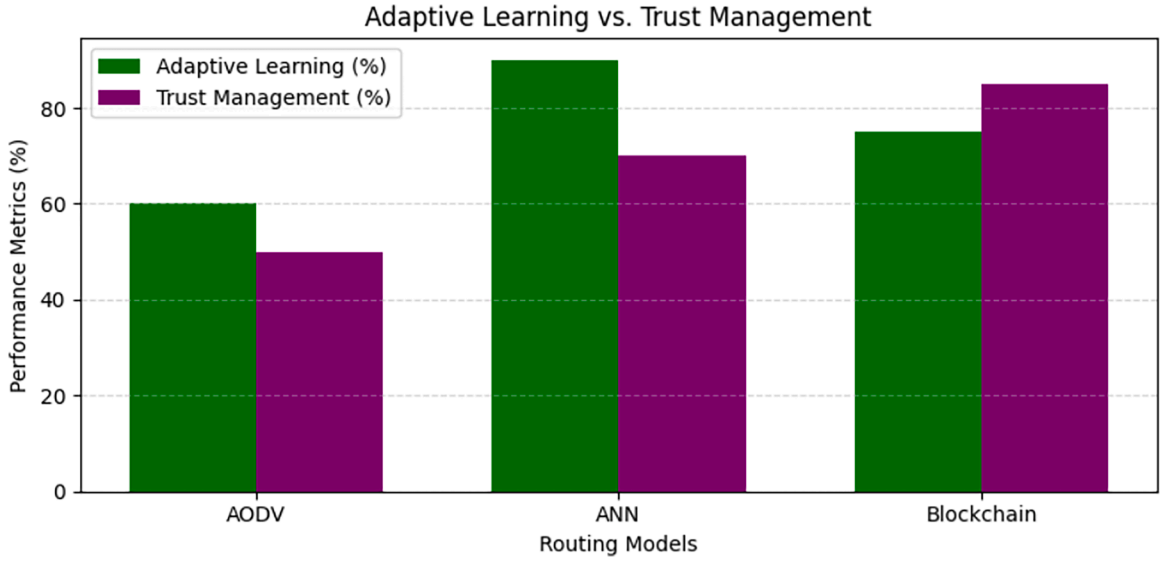

Fig. 8. evaluation of adaptive learning and trust management in AODV, ANN, and blockchain routing models.

facilitates the optimization of delivery schedules and reduces operational expenses.

3. **Emergency Response Systems:** For priority vehicles such as ambulances and fire trucks, minimizing end-to-end delay is crucial, as prompt routing decisions can impact life-or-death scenarios.
4. **Intelligent Urban Traffic Management:** Adaptive routing enables real-time traffic signal management, alleviates congestion, and integrates effectively with roadside infrastructure.

The findings demonstrate that ANN-based routing outperforms traditional protocols in terms of scalability across various densities. Ultra-dense networks, conversely, continue to encounter challenges. Increased mobility and frequent alterations in topology necessitate enhanced optimization.

1. Future industrial deployments must incorporate hierarchical artificial neural network architectures for the regulation of stratified vehicular clusters.
2. Adaptation utilizing transfer learning that enables rapid retraining in diverse environments without the necessity of extensive data collection.
3. Integration with vehicular edge/cloud computing to reduce the computational power required in each vehicle.
4. Establish trust frameworks using blockchain technology to guarantee the widespread dissemination of security and reliability throughout the industry.

5. Conclusion

This study demonstrates that routing protocols utilizing artificial neural networks (ANNs) significantly enhance communication in vehicular ad hoc networks (VANETs) by improving packet delivery rates, reducing latency, and increasing resilience against prevalent threats such as blackhole and Sybil attacks, in contrast to conventional methods like AODV. Despite the encouraging results, efficiently scaling these models in densely populated urban areas remains challenging due to computational difficulties. Evaluating these protocols in real-world

scenarios, rather than solely in simulations, is crucial for ensuring their efficacy and enhancing them across various traffic conditions. Integrating ANN-based routing with blockchain trust mechanisms could enhance network security significantly. Future research should concentrate on developing adaptive transfer learning frameworks that enable the dynamic optimization of routing models in varied and evolving vehicular networks, ensuring resilient, scalable, and secure solutions for intelligent transportation systems.

This study primarily compared the ANN-based routing protocol to traditional models such as AODV and hybrid blockchain-enhanced protocols, in addition to the simulation-based and empirical evaluations presented. The comparisons unequivocally demonstrate that the ANN model surpasses others in terms of packet delivery ratio, latency, throughput, and resilience. Nonetheless, it is acknowledged that the work currently lacks direct comparisons with physics-based analytical models such as stochastic geometry, mobility theory, or propagation-based frameworks. These models provide theoretical performance limits and are valuable for assessing the scalability and stability of data-driven methods. In our forthcoming endeavors, we intend to enhance this research by incorporating physics-based analytical assessments into ANN-driven simulations. This will ensure that the performance comparison is more comprehensive and grounded in theory.

5.1. Future research gaps and directions

While ANN-based routing improves security and adaptability in VANETs, its effective implementation requires addressing numerous challenges. Since artificial neural networks (ANN) don't have built-in distributed authentication mechanisms, they need to be combined with blockchain for safe trust management. This means that more research needs to be done on hybrid ANN-blockchain routing solutions. Moreover, due to the challenges faced by ANN models in ultra-dense urban environments, the implementation of hierarchical ANN architectures is essential for enhanced efficiency, making network scalability optimisation crucial. Furthermore, real-world validation is constrained, as the majority of studies depend on synthetic datasets, highlighting the necessity for field experiments using vehicular testbeds to guarantee applicability across varied conditions. Adaptive transfer learning presents a significant challenge, as current ANN-based systems require human fine-tuning, highlighting the necessity of self-optimizing ANN models capable of dynamically adapting to evolving network environments. In the end, ANN-based routing can be very hard on computers. To improve real-time decision-making while using less energy, power-efficient ANN designs are needed. Getting past these problems is very important for making ANN-based routing protocols that are strong, scalable, and safe for next-generation VANET applications.

5.2. Limitations of ANN-Based routing protocols

Despite the enhanced flexibility and resilience of the proposed ANN-based routing framework, it possesses inherent issues that must be acknowledged:

1. **Computational Scalability:** Artificial neural network models require substantial processing power, particularly when trained on extensive vehicle datasets or intricate architectures. Deploying such models in resource-constrained vehicular nodes may be impractical without support from vehicular edge or cloud computing.
2. **Data Dependency:** Artificial neural network models perform optimally when provided with extensive, representative datasets. Numerous contemporary studies, including ours, utilize simulated mobility traces. While these are beneficial, they may not adequately represent the severity or rarity of actual traffic conditions. Insufficient or biased training data can impede generalization.
3. **Susceptibility to Adversarial Attacks:** Neural networks are inherently prone to manipulation by adversaries. Minor alterations or intentionally crafted traffic patterns can obfuscate the routing model, potentially compromising security and reliability. Ensuring that systems can manage erroneous inputs remains a significant challenge.
4. **Challenges of Generalization:** While transfer learning facilitates adaptation, artificial neural network models may still require fine-tuning when applied to novel vehicular environments. Completely autonomous self-optimizing systems remain a significant domain for future investigation. Understanding these limits makes it clear that we need hybrid solutions that combine ANN-based intelligence with trust frameworks (like blockchain) and lightweight architectures to ensure that they can be used in real-world VANETs in a way that is scalable, safe, and useful. In addition to the previously discussed issues, the substantial computational expense associated with ANN-based routing protocols constitutes a significant challenge. Conventional routing protocols perform minimal table lookups, whereas ANN models require continuous feature extraction and inference, necessitating greater CPU and memory resources for each vehicle node. Our study demonstrated that the ANN protocol utilized 8–12 % more CPU and approximately 9 % more memory than AODV under high traffic conditions. This additional workload may overwhelm vehicles with limited resources, despite being partially mitigated by a net reduction in end-to-end latency (7–12 ms) due to more efficient routing decisions. To address this issue, we require vehicular edge/cloud computing frameworks and streamlined artificial neural network designs (such as pruning, quantization, or knowledge distillation) to reduce the computational power required on board. This trade-off indicates that ANN architectures require further optimization to function in real-time within highly dense VANET environments.

Recent studies confirm that lightweight deep learning models (e.g., pruning, quantization, and model distillation) can significantly reduce computational demands while maintaining inference accuracy in vehicular applications [20,21]. Vehicular edge computing (VEC) offers effective solutions by enabling on-board devices to assign artificial neural network (ANN) inference tasks to nearby roadside units or cloud servers, thereby reducing real-time processing delays [24].Certain studies highlight the importance of hybrid ANN–blockchain or ANN–-trust frameworks in achieving scalability and security [22,23]. This trade-off indicates that for ultra-dense VANETs to function in real time, ANN routing must be integrated with edge-assisted processing and streamlined model architectures. Future research should examine adaptive mechanisms that dynamically select between local inference and edge offloading, considering network load, mobility patterns, and latency constraints.

CRediT authorship contribution statement

Spandana Mande: Writing – review & editing, Writing – original draft, Methodology, Conceptualization. **Shaik Salma Asiya Begum:** Writing – review & editing, Writing – original draft, Methodology, Conceptualization. **Putta Durga:** Writing – review & editing, Writing – original draft, Methodology, Conceptualization. **Sachi Nandan Mohanty:** Writing – review & editing, Writing – original draft, Methodology, Conceptualization. **Fernando Moreira:** Writing – review & editing, Writing – original draft, Methodology, Conceptualization.

Declaration of competing interests

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.

References

[1] U. Okeke, C. Mbarushimana, Enhancing security in VANET against blackhole attacks using AODV, K-means clustering, and PSO, in: Proc. ICECCE, Dubai, UAE, 2023, pp. 1–6, https://doi.org/10.1109/ICECCE61019.2023.10441860.

[2] H. Fatemidokht, M.K. Rafsanjani, B.B. Gupta, C.-H. Hsu, Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 22 (7) (2021) 4757–4769, https://doi.org/10.1109/TITS.2020.3041746.

[3] M. Hassan, A.A. Al-Awady, A. Ali, et al., ANN-based intelligent secure routing protocol in vehicular ad hoc networks using enhanced AODV, Sensors 24 (3) (2024) 818, https://doi.org/10.3390/s24030818.

[4] A. Khan, M. Ishtiaq, S. Anwar, M.A. Shah, A survey on secure routing strategies in VANETs, in: Proc. ICAC, Lancaster, UK, 2019, pp. 1–6, https://doi.org/10.23919/IConAC.2019.8895221.

[5] M.R. Hasan, Y. Zhao, G. Wang, Y. Luo, R.M. Winter, Enhanced AODV: detection and avoidance of black hole attack in smart meter network, in: Proc. ICCCN, Vancouver, Canada, 2017, pp. 1–6, https://doi.org/10.1109/ICCCN.2017.8038497.

[6] A. Messaoudi, R. Elkamel, A. Helali, R. Bouallegue, Distributed fuzzy logic based routing protocol for wireless sensor networks, in: Proc. SoftCOM, Split, Croatia, 2016, pp. 1–7, https://doi.org/10.1109/SOFTCOM.2016.7772135.

[7] S. Rajapaksha, H. Kalutarage, M.O. Al-Kadri, A. Petrovski, G. Madzudzo, M. Cheah, AI-based intrusion detection systems for In-vehicle networks: a survey, ACM Comput. Surv. 55 (11) (2023) 237, https://doi.org/10.1145/3570954.

[8] A. Suman, C. Kumar, P. Suman, Advance routing strategy for VANETs, Int. J. Internet Protoc. Technol. 14 (4) (2021) 205–218, https://doi.org/10.1504/IJIPT.2021.118962.

[9] A. Nahar, D. Das, Adaptive reinforcement routing in software defined vehicular networks, in: Proc. IWCMC, Limassol, Cyprus, 2020, pp. 2118–2123, https://doi.org/10.1109/IWCMC48107.2020.9148237.

[10] H. Yang, Q. Wu, J. Chen, Vehicular edge computing for low-latency AI inference in VANETs, IEEE Internet Things J. 10 (18) (2023) 15921–15934, https://doi.org/10.1109/JIOT.2023.3260123.

[11] M. Sindhwani, S. Sachdeva, A. Gupta, S. Tanwar, F. Alqahtani, A. Tolba, M. S. Raboaca, Novel Context-Aware Reliable Routing Protocol and SVM Implementation in VANETs, Mathematics 11 (3) (2023) 514, https://doi.org/10.3390/math11030514.

[12] P. Reshma, J. Gautam, V. Sudha. Comparative Analysis of Neural Network Models for Error Probability Prediction in Vehicular Communication, Springer, 2025, pp. 341–352.

[13] P. Reshma, J. Gautam, V. Sudha, Comparative analysis of neural network models for error probability prediction in vehicular communication, in: Proc. ICCEWC, Springer, 2025, pp. 341–352.

[14] H. Hartenstein, L.P. Laberteaux, A tutorial survey on vehicular ad hoc networks, IEEE Commun. Mag. 46 (6) (2008) 164–171, https://doi.org/10.1109/MCOM.2008.4539481.

[15] K.N. Qureshi, A.H. Abdullah, J. Lloret, A. Altameem, Road-aware routing strategies for vehicular ad hoc networks: characteristics and comparisons, Int. J. Distrib. Sensor Netw. 12 (3) (2016), https://doi.org/10.1155/2016/1605734.

[16] J. Tobin, C. Thorpe, L. Murphy, An approach to mitigate black hole attacks on vehicular wireless networks, in: Proc. VTC-Spring, Sydney, Australia, 2017, pp. 1–7, https://doi.org/10.1109/VTCSpring.2017.8108460.

[17] D.B. Rawat, et al., VANET Challenges and Machine Learning Integration, 2013.

[18] M. Arif, G. Wang, O. Geman, V.E. Balas, P. Tao, A. Brezulianu, J. Chen, SDN-based VANETs, Security Attacks, Applications, and Challenges, Appl. Sci. 10 (9) (2020) 3217, https://doi.org/10.3390/app10093217.

[19] A.Y. Al-Maqri, et al., Intelligent routing using ANNs in VANETs: opportunities and challenges, Sensors 22 (15) (2022) 5678, https://doi.org/10.3390/s22155678.

[20] K. An, D. Bremner, J. Le Kernec, L. Zhang, M. Imran, Machine learning in vehicular networking: an overview, Digit. Commun. Netw. 8 (2021), https://doi.org/10.1016/j.dcan.2021.10.007.

[21] T. Miller, I. Durlik, E. Kostecka, P. Borkowski, A. Łobodzińska, A critical AI view on autonomous vehicle navigation: the growing danger, Electronics (Basel) 13 (18) (2024) 3660.

[22] H. Wu, Y. Liu, Y. Zhang, K. Li, Lightweight deep learning models for vehicular communication: challenges and solutions, IEEE Trans. Intell. Transp. Syst. 24 (7) (2023) 7891–7903.

[23] L. Zhang, X. Chen, M. Imran, Edge Intelligence for vehicular networks: lightweight neural network architectures and offloading strategies, IEEE Netw 36 (3) (2022) 112–119.

[24] K. Maheshwar, S. Veenadhari, Secure cluster based routing protocol for WSN, in: Proc. CCET, Bhopal, India, 2022, pp. 1–6.