Neural Network-Based Intelligent Routing for Secure VANET Communication

Wisal Jereis Alrabadi
Faculty of Physical Education, Yarmouk University, 21163 Irbid, Jordan
wrabadi10@gmail.com

Keywords: Vehicular Ad-Hoc Networks (VANETs), Neural Network-Based Routing, Intelligent Transportation Systems (ITS), Machine Learning, Network Security and Attacks.

Abstract: Transportation Systems (ITS) enable seamless communication between vehicles and roadside infrastructure. This connectivity significantly enhances road safety, traffic efficiency, and overall driving enjoyment for users. However, router protocols in VANETs encounter substantial challenges due to the high mobility of vehicles and the rapid changes in network topologies. Traditional routing methods often suffer from delays and packet loss as a result of these dynamic conditions. To address these issues, we propose a novel algorithm that leverages machine learning techniques, specifically utilizing neural networks for intelligent routing in VANETs. This innovative approach dynamically optimizes routing decisions while also enhancing communication security. By effectively detecting and mitigating potential attacks, our algorithm improves routing efficiency, reduces communication delays, and strengthens data security. Simulation results indicate that our proposed system outperforms existing routing protocols, leading to improved network performance and a significant reduction in end-to-end delay, particularly in challenging scenarios such as black hole attacks.

1 INTRODUCTION

When vehicular ad-hoc networks (VANETs) are used in intelligent transportation systems (ITS), traffic can be managed better, and drivers are more comfortable by being able to communicate with one another and with roadside infrastructure. In an increasingly complex and scaled network, ensuring secure and efficient communication between vehicles becomes a more challenging task [1]. The key challenge facing VANETs is ensuring robust, adaptive, and secure routing mechanisms that can cope with the changing topologies, mobility, and communication conditions in vehicular environments.

A promising approach to addressing these challenges is to use neural networks-based intelligent routing. Neural networks can be used to optimize data transmission efficiency and security by using artificial intelligence and machine learning. In addition to improving the accuracy of route selection, minimizing communication delays, and enhancing the overall security of information exchange, these intelligent routing techniques can detect and mitigate potential threats in real time. Using a vehicle ad hoc network (VANET), vehicles can communicate with roadside units (RSUs) [2]. In Vehicle Area Networks (VANETs), traffic congestion is reduced, road safety is improved, and traffic efficiency is increased, as shown in Figure 1 [3], [4]. Vehicle-to-vehicle networks provide data communication, either with or without fixed infrastructure [5]. With this communication, a variety of safety and infotainment applications can be integrated into the vehicle to enhance the overall driving experience and contribute to smarter transportation systems [6], [7]. Because VANETs are wireless and mobile, they are highly susceptible to security threats [8]. There is the potential for catastrophic results from malicious activities, especially when it comes to the propagation of emergency messages and the management of traffic [9]. To ensure the success and wide adoption of VANETs, security must be addressed at the highest level [10]. It is vital to ensure the security of data communication and that messages are trusted and reliable in VANETs in order to operate efficiently and safely [11], [12]. A secure and intelligent routing scheme is crucial to addressing these challenges [4]. Traditionally designed routing protocols for MANETs often do not work well in VANETs due to

their high mobility and dynamic topology [13]. Smart systems need to be designed for VANET routing protocols, and the network environment is rapidly changing. Due to malicious nodes and potential attacks, innovative routing algorithms are required to ensure efficient and secure data transmission [14].

A neural network and machine learning technique can be used to improve routing in VANETs. In addition to optimizing network performance and mitigating security threats, NNs can enable smart routing decisions based on data-driven predictions and adaptive learning. With neural network-based routing protocols, optimal paths can be predicted, anomalies can be detected, and VANET communications can be enhanced in terms of overall security [15], [16].

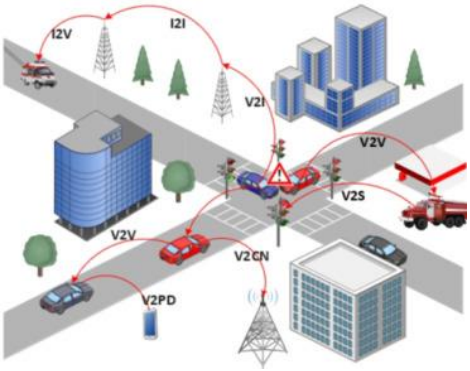

Figure 1: A VANET is composed of the following elements of communication.

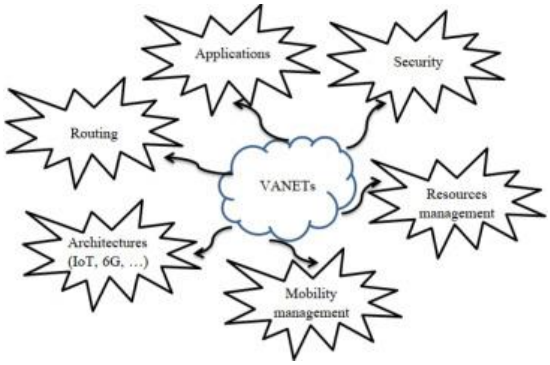

Figure 2: Topics for VANET research and issues.

A variety of VANET features, from entertainment features to driving assistance systems, have significantly improved automobile capabilities [17]. While these services are beneficial, they also present new challenges in terms of quality, security, and privacy. Since the 1990s, VANET research has encompassed a variety of topics, including application development, routing, security, and privacy. The challenges remain despite technological advances, especially with the advent of IoT, cloud computing, fog computing, edge computing, and 5G/6G technologies, as shown in Figure 2 [18], [19].

2 LITERATURE REVIEW

VANET is an integral part of Intelligent Transportation Systems (ITS), which improve traffic efficiency, safety, and convenience for drivers. As a result, routing protocols struggle to keep up with the rapid changes in topologies and highly mobile vehicles of VANETs. This dynamic environment often results in delays, packet losses, and security vulnerabilities with traditional routing protocols. As VANET communications have become more secure, machine learning (ML) techniques, especially neural networks (NNs), have become increasingly important for developing smart and adaptive routing solutions [20].

2.1 Intelligent Routing Protocols in VANETs Machine Learning-Based Routing

VANET routing protocols have benefited from machine learning (ML) due to their ability to learn network behaviour on its own and in an adaptive manner [21]. This learning-based approach can address many challenges in VANETs, including mobility and dynamic topologies [22]. The use of machine learning algorithms can improve routing protocols' performance and security by making intelligent decisions based on real-time network conditions. Optimization of routing decisions can be achieved using reinforcement learning (RL). Using deep reinforcement learning, an author proposed a roadside unit (RSU) model that can maintain traffic information and predict vehicle movements to find feasible routes [23].

Further studies investigate using Q-learning and fuzzy logic to route VANETs hierarchically. The QFHR protocol consists of three phases: identifying traffic conditions, routing at intersections and routing at roads. In comparison with other routing protocols, QFHR improved packet delivery rate and reduced delay.

2.2 ANN-Based Routing

It has become increasingly evident that Artificial Neural Networks (ANNs) are powerful tools for

predicting routing in VANETs, enabling protocols to adapt to changing network characteristics. In accordance with the author [3], MPANN is a Multimetric predictive routing protocol for VANETs in urban environments. With the protocol, the best route to the destination is predicted by a neural network, increasing delivery probability and reducing delivery times. According to MPANN simulations, losses at different densities of vehicles are less than 20%, while delays are less than 0.4 ms.

To combine clustering algorithms with artificial neural networks, the author has developed an enhanced routing protocol [24] capable of detecting malicious nodes and establishing clusters. Through a modified version of the ad hoc on-demand distance vector protocol (AODV), it is possible to detect black hole attacks 98.97% accurately using an ANN classification model.

In this study, a neural network is used to provide a dynamic routing and switching scheme (NARSS) for Software-Defined Vehicular Networks (SDVNs) using artificial neural networks [25]. In simulations, NARSS is shown to outperform traditional protocols in terms of packet delivery ratios and end-to-end delays based on a neural network generating a scheme-switching model.

2.3 Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol

The AODV protocol is used in VANETs for reactive routing. In his study of AODV in VANETs, the author [26] used SUMO, MOVE, and NS2 simulators to examine how it was implemented in those networks. AODV uses request-response mechanisms to establish routes only when they are needed. Based on a comparison of AODV's results with those of other studies, the authors evaluate packet drop rate, throughput, average end delay, jitter, and routing workload. AODV protocol was modified and incorporated into the intelligent cluster-based routing protocol. Modified AODV is used to discover routes on demand, select routes optimally and reduce packet transmission delays through enhanced request and reply protocols [27]. Other approaches, such as multicast routing protocols designed for delay-tolerant vehicular environments, have also been explored to enhance data dissemination [34/28].

3 METHODOLOGY

In VANETs, nodes move, and their topology often changes, which makes them more difficult to distinguish from Mobile Ad Hoc Networks (MANETs) [28/29]. Moreover, VANETs are independently developed and have a short lifespan. Mobile nodes (cars) primarily use VANETs, but roadside units (RSUs) also operate on VANETs [29/30]. It is possible for nodes that want to interact with another node that is not immediately within range to do so by forwarding their target to neighbouring nodes. There are a number of routing protocols to choose from, but we focus on the AODV protocol, which is among the most common and important protocols used today. VANETs and other IoT devices are becoming increasingly vulnerable to security breaches as intra-vehicular communication becomes increasingly important to applications [31], [32], [33]. Using our solution to simulate attacks and demonstrate their effectiveness can help us improve prevention methods. By analyzing these simulations, we show that our countermeasure detects and prevents Black Hole attacks accurately and effectively. As a result of our approach, network performance was boosted proportionally in instances of Black Hole attacks.

3.1 Data Rescaling Techniques

Due to the different sizes of the input variables, rescaling the data is essential before applying the statistical methods cited above. Analyzing data this way might result in biased results. It is thus necessary to transform or rescale input data in a way that no single attribute dominates another [34]. This can be accomplished by transforming the original data into a standard range, such as [−1, 1] or [0, 1].

The original data must be transformed so that it falls within a smaller or standard range.

Using $V\_1, V\_2, \ldots, V\_n$ as an example V, we have n observations for this numeric variable

3.2 Z-Score Normalization

As a result, the data are rescaled to yield zero mean and unit variance [34]. To transform [27] into $v_i' i$we follow the steps below:

$$v_i' = \frac{v_i - \mu}{\sigma}. \quad (1)$$

Among the variables, $V, i = 1, \ldots\ldots\ldots\ldots\ldots\ldots, n,\ \mu,$ and σ reflect the means and standard deviations of the original values.

3.3 Min-Max Normalization

To map each value $v_i' i$ of v_i to a value within the series [0, 1], this new value is computed as tracks:

$$v_i' = \frac{v_i - \min V}{\max V - \min V} \quad . \tag{2}$$

In this case, $v_i'i$ reflects its original value, $V, i = 1, \ldots\ldots\ldots, n$, $\min V$ and $\max V$ is its maximum value.

A variable's minimum value becomes 0, and its maximum value becomes 1. If = min V; then $v_i'i = 0$. If = max V; then $v_i'i = 0$.

3.4 Normalization by Decimal Scaling

In this method, variable maximum values are determined by moving their decimal points. When variables have logarithmic variations, the approach is suitable [34].

Using the given data, instances v_i are rescaled into $v_i'i$. As follows:

$$v_i' = \frac{v_i}{10^j} \quad . \tag{3}$$

Anywhere: $j = \log\_10\ Max(v\_i)$. A comparison of three different techniques was conducted using original research data [34].

3.5 Network Simulator 2 (NS-2)

To evaluate the performance of the proposed neural network–based routing scheme, we conducted experiments using Network Simulator 2 (NS-2). NS-2 provides a discrete-event simulation environment widely used for testing ad-hoc and vehicular networks due to its flexibility and support for wireless protocols.

In our setup, the mobility of vehicles was generated using traffic simulation tools (SUMO/MOVE), which were then integrated into NS-2. The simulation included vehicles (mobile nodes) and roadside units (RSUs), representing a realistic VANET environment. Each vehicle was equipped with wireless communication capability, and nodes were allowed to dynamically join or leave the network depending on their movement patterns.

The proposed routing model was implemented as an extension of AODV, where neural network–based decision-making was applied to detect malicious behavior (e.g., black hole attacks) and to select optimal routes. During simulation, packet headers and routing tables were updated dynamically to reflect real-time changes in topology.

For performance analysis, we measured:

- Packet delivery ratio (PDR) – the proportion of successfully delivered packets.
- End-to-end delay – the average time taken for a packet to reach its destination.
- Throughput – the overall amount of data successfully transmitted across the network.
- Energy consumption – estimated for both vehicle nodes and RSUs during communication.
- Attack detection accuracy – evaluated using confusion matrix–based metrics (Accuracy, Precision, Recall, F1-score).

These metrics allowed us to assess not only the efficiency of the routing protocol but also its ability to resist malicious nodes. By comparing results with baseline protocols (AODV, DSR, and trust-based schemes), we demonstrated that the proposed solution achieves higher delivery ratios, lower delays, and better resilience under attack scenarios.

3.6 Performance Evaluation

To evaluate the proposed neural network–based routing scheme in VANETs, we used both network-level metrics (alive and dead nodes, energy efficiency) and machine learning–based classification metrics (accuracy, precision, recall, F1 score).

3.6.1 Number of Dead Nodes

Since VANET nodes are mobile vehicles equipped with communication modules, their availability directly influences routing performance. In our simulations, we observed the number of alive nodes (vehicles that remained active and able to forward packets) and dead nodes (vehicles that could no longer participate due to depleted communication resources or disconnection). A higher number of alive nodes indicates better network sustainability and routing efficiency.

3.6.2 Energy Consumption

Even though vehicles have more energy resources than traditional sensor nodes, efficient energy usage is still important for VANET devices, especially roadside units (RSUs) and relay vehicles. We modeled energy dissipation during data transmission and reception. The total energy consumed by a vehicle node $E_{total}(i)$ is represented as the sum of residual energy and the energy harvested or supplied:

$$E_{total}(i) = E_{res}(i) + E_{harvest}(i). \tag{4}$$

Here, $E_{res}(i)$ - represents the remaining energy of the node after communication activities, while $E_{harvest}(i)$ - accounts for energy replenishment (for example, from vehicle batteries or hybrid systems).

The required transmitter power was estimated as:

$$TP=SNR/\alpha,$$

where SNR is the signal-to-noise ratio and α is the channel attenuation factor.

3.7 Model Performance Evaluation

Model performance was comprehensively evaluated using classification metrics derived from the confusion matrix framework. The confusion matrix is a tabular representation that summarizes the predictions of a classification model, making it easy to identify misclassified instances and calculate performance measures. For a classification task with multiple classes, four fundamental outcomes are recorded for each class:

- true positive (TP) represents correctly classified positive instances,
- false positive (FP) represents negative instances incorrectly classified as positive,
- false negative (FN) represents positive instances incorrectly classified as negative,
- true negative (TN) represents correctly classified negative instances.

Based on these four classification outcomes, four key performance metrics were calculated according to the formulas presented in [35].

Accuracy reflects the overall correctness of the model's predictions across all instances, providing a general measure of classification performance. Precision indicates the relationship between correctly predicted positive instances and all instances flagged as positive by the model, measuring the reliability of positive predictions. Recall, also known as the true positive rate, measures the proportion of actual positive instances that were successfully identified by the model, indicating the model's ability to capture all positive cases. The F1-score represents a harmonic mean of precision and recall, providing a balanced single metric that accounts for both false positives and false negatives, making it particularly useful when the class distribution is imbalanced.

For the attack detection task in this study, accuracy reflects the overall correctness of intrusion detection. Precision indicates how many nodes flagged as malicious were truly malicious, reducing false alarms. Recall measures the proportion of actual malicious nodes that were successfully detected by the model. The F1-score balances precision and recall, providing a reliable single metric for evaluating overall attack detection performance.

4 RESULTS AND DISCUSSION

With the help of the BHT dataset, a comprehensive set of outcomes was developed to provide analytical and predictive capabilities for evaluating the proposed system's performance. A significant improvement in the system's predictive capabilities has resulted from our training efforts, enabling us to compare its performance across different datasets in a meaningful way. A clear illustration of the model's accuracy can be found in Figure 3.

Using the proposed BHT dataset, Figure 4 shows the model's loss. A graph showing the system's loss across the specified dataset is shown below. Based on these metrics, iterative training and testing can be conducted on the proposed model. Figure 4 illustrates the model's loss graphically.

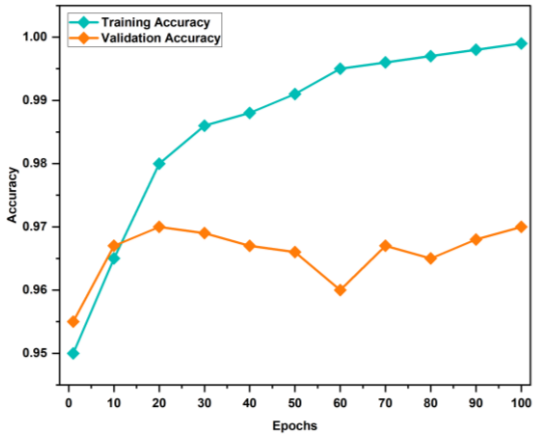

Figure 3: A model for BHT with high accuracy.

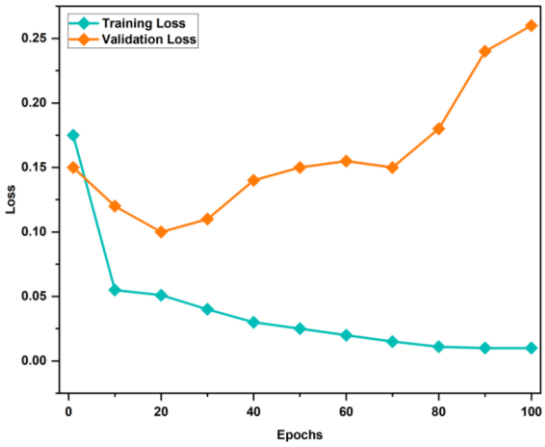

Figure 4: An analysis of the BHT dataset's model loss.

According to Figure 5, existing techniques are compared to the minimum number of under-attack scenarios that can occur. Compared to existing techniques, these occurrences occur less frequently, suggesting less impact on network routing performance. Data transfer efficiency in a VANET environment is reflected by this metric, which is important during routing. Based on the end-to-end delay comparison shown in Figure 5, our proposed approach is faster than existing approaches.

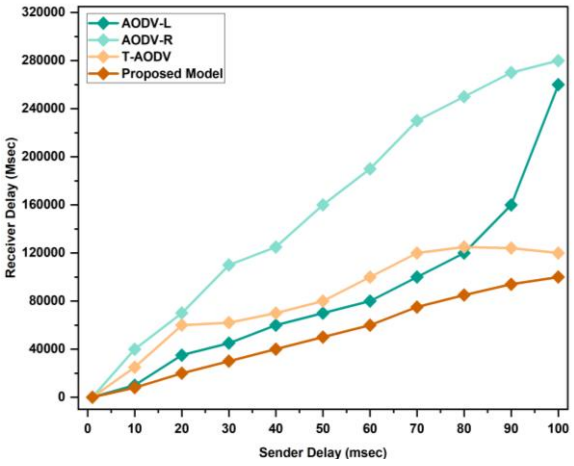

Figure 5: Packets to be delivered from end to end.

There are several established routing strategies compared in Figure 6, including I-AODV (improved ad hoc on-demand distance vector routing), L-AODV (load-balancing ad hoc on-demand distance vector routing), R-AODV (reliable ad hoc on-demand distance vector routing), and T-AODV (trust-based ad hoc on-demand distance vector routing). Figure 7 compares the hop counts obtained using the proposed method.

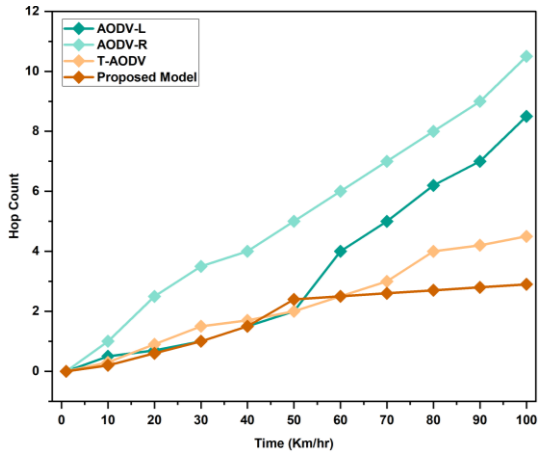

Figure 6: Number of hops in the network.

Figure 8 illustrates how these two concepts relate to a black hole attack scenario. A comparison was conducted with established protocols such as TRFHP (reverse-path forwarding) and DSDV (destination-sequenced distance vector routing). Results demonstrate that the proposed technique is superior to current techniques for network throughput, routing, and performance improvement during black hole attacks.

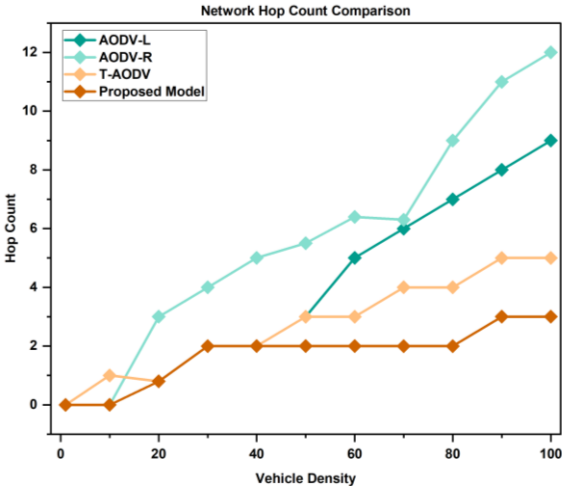

Figure 7: Comparison of hop counts.

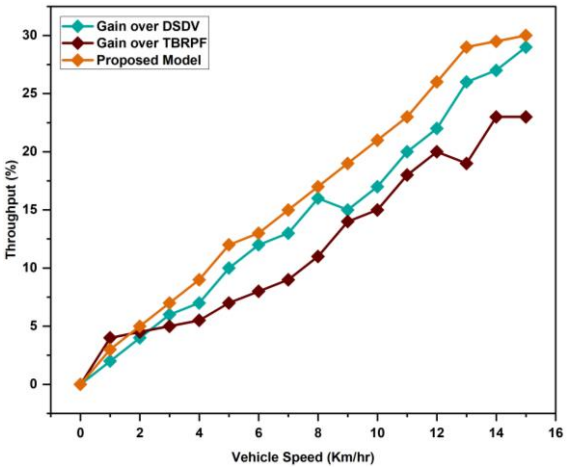

Figure 8: Comparing the throughput of the proposed technique versus vehicle speeds.

As shown in Figure 9, the average delay initially increased and then stabilized. RPCC improves point coverage and connectivity by improving point coverage. It ensured that lower-level cluster leaders would not be eligible for future elections through a hierarchical structure. The CCMP mode in DSR enabled packet encryption and authentication in

MANET's routing and link layers in order to prevent black hole attacks. Latencies on the network have decreased significantly, enhancing cooperative performance, as shown in the Figure 9.

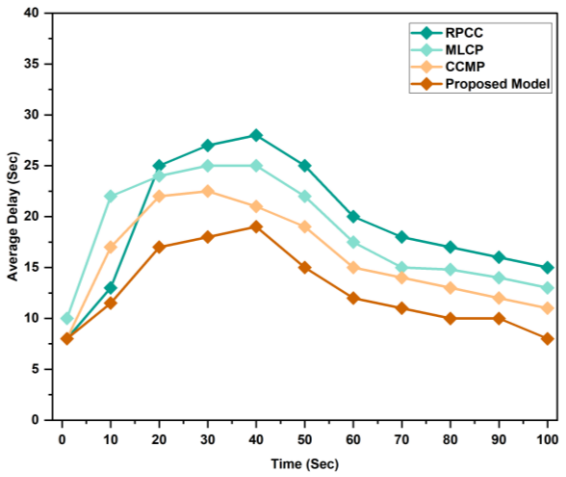

Figure 9: Comparison between MLCP, RPSS, and CCMP in terms of average delay.

5 CONCLUSIONS

VANETs face several challenges, including the need to deal with dynamic network conditions and to ensure communication security, which the proposed neural network-based intelligent routing protocol aims to solve. It optimizes routing decisions, improves overall performance, and adapts to changing traffic patterns and network topologies by using machine learning. Simulated results indicate that the proposed routing protocol reduces delays and increases throughput compared to traditional routing protocols. Through machine learning, the proposed system optimizes routing decisions, significantly enhances network performance, and effectively adapts to changing traffic patterns and environmental conditions. Even though this approach has demonstrated strong performance, further practical research is necessary to understand scaling complexities, seamless integration with emerging 5G networks and IoT-based communication systems, and improve resilience under real-world vehicular conditions. Neural network-based routing in VANETs presents promising opportunities to reduce accidents, manage congestion efficiently, and ensure reliable, secure communication between vehicles.

REFERENCES

[1] P. Rani and R. Sharma, "Intelligent transportation system for internet of vehicles based vehicular networks for smart cities," Comput. Electr. Eng., vol. 105, p. 108543, 2023, [Online]. Available: https://doi.org/10.1016/j.compeleceng.2022.108543.

[2] P. Sathya Narayanan and C. S. Joice, "Vehicle-to-Vehicle (V2V) Communication using Routing Protocols: A Review," in 2019 International Conference on Smart Structures and Systems (ICSSS), Chennai, India: IEEE, Mar. 2019, pp. 1-10, [Online]. Available: https://doi.org/10.1109/ICSSS.2019.8882828.

[3] S. K., A. R. Deshmukh, and S. S. Dorle, "A Survey of Routing Protocols for Vehicular Ad-hoc Networks," Int. J. Comput. Appl., vol. 139, no. 13, pp. 34-37, Apr. 2016, [Online]. Available: https://doi.org/10.5120/ijca2016909541.

[4] L. L. Cardenas, A. M. Mezher, P. A. Barbecho Bautista, J. P. Astudillo Leon, and M. A. Igartua, "A Multimetric Predictive ANN-Based Routing Protocol for Vehicular Ad Hoc Networks," IEEE Access, vol. 9, pp. 86037-86053, 2021, [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3088474.

[5] K. N. Qureshi, F. Bashir, and A. H. Abdullah, "Provision of Security in Vehicular Ad Hoc Networks through an Intelligent Secure Routing Scheme," in 2017 International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan: IEEE, Dec. 2017, pp. 200-205, [Online]. Available: https://doi.org/10.1109/FIT.2017.00043.

[6] N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong, and K. H. Chong, "A Comprehensive Survey on Vehicular Networking: Communications, Applications, Challenges, and Upcoming Research Directions," IEEE Access, vol. 10, pp. 86127-86180, 2022, [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3198656.

[7] P. Rani and R. Sharma, "Intelligent Transportation System Performance Analysis of Indoor and Outdoor Internet of Vehicle (IoV) Applications Towards 5G," Tsinghua Sci. Technol., vol. 29, no. 6, pp. 1785-1795, Dec. 2024, [Online]. Available: https://doi.org/10.26599/TST.2023.9010119.

[8] T. Alladi, A. Agrawal, B. Gera, V. Chamola, B. Sikdar, and M. Guizani, "Deep Neural Networks for Securing IoT Enabled Vehicular Ad-Hoc Networks," in ICC 2021 - IEEE International Conference on Communications, Montreal, QC, Canada: IEEE, Jun. 2021, pp. 1-6, [Online]. Available: https://doi.org/10.1109/ICC42927.2021.9500823.

[9] A. Malik, M. Z. Khan, M. Faisal, F. Khan, and J.-T. Seo, "An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs," Sensors, vol. 22, no. 5, p. 1897, Feb. 2022, [Online]. Available: https://doi.org/10.3390/s22051897.

[10] Y. Qian and N. Moayeri, "Design of Secure and Application-Oriented VANETs," in VTC Spring 2008 - IEEE Vehicular Technology Conference, Marina Bay, Singapore: IEEE, May 2008, pp. 2794-2799, [Online]. Available: https://doi.org/10.1109/VETECS.2008.610.

[11] G. Kumar, R. Saha, M. K. Rai, and T.-H. Kim, "Multidimensional Security Provision for Secure Communication in Vehicular Ad Hoc Networks Using Hierarchical Structure and End-to-End Authentication," IEEE Access, vol. 6, pp. 46558-46567, 2018, [Online]. Available: https://doi.org/10.1109/ACCESS.2018.2866759.

[12] S. A. Soleymani et al., "A Secure Trust Model Based on Fuzzy Logic in Vehicular Ad Hoc Networks With Fog Computing," IEEE Access, vol. 5, pp. 15619-15629, 2017, [Online]. Available: https://doi.org/10.1109/ACCESS.2017.2733225.

[13] P. Rani and M. H. Falaah, "Real-Time Congestion Control and Load Optimization in Cloud-MANETs Using Predictive Algorithms," NJF Intell. Eng. J., vol. 1, no. 1, pp. 66-76, 2024.

[14] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, "Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles," IEEE Access, vol. 8, pp. 199618-199628, 2020, [Online]. Available: https://doi.org/10.1109/ACCESS.2020.3034327.

[15] B. Karthiga, D. Durairaj, N. Nawaz, T. K. Venkatasamy, G. Ramasamy, and A. Hariharasudan, "Intelligent Intrusion Detection System for VANET Using Machine Learning and Deep Learning Approaches," Wirel. Commun. Mob. Comput., vol. 2022, pp. 1-13, Oct. 2022, [Online]. Available: https://doi.org/10.1155/2022/5069104.

[16] P. Rani and R. Sharma, "An experimental study of IEEE 802.11 n devices for vehicular networks with various propagation loss models," in International Conference on Signal Processing and Integrated Networks, Springer, 2022, pp. 125-135.

[17] S. Zeadally, M. A. Javed, and E. B. Hamida, "Vehicular Communications for ITS: Standardization and Challenges," IEEE Commun. Stand. Mag., vol. 4, no. 1, pp. 11-17, Mar. 2020, [Online]. Available: https://doi.org/10.1109/MCOMSTD.001.1900044.

[18] A. Rahim, P. K. Malik, and V. A. Sankar Ponnapalli, "State of the Art: A Review on Vehicular Communications, Impact of 5G, Fractal Antennas for Future Communication," in Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019), vol. 121, P. K. Singh, W. Pawłowski, S. Tanwar, N. Kumar, J. J. P. C. Rodrigues, and M. S. Obaidat, Eds., in Lecture Notes in Networks and Systems, vol. 121, Singapore: Springer Singapore, 2020, pp. 3-15, [Online]. Available: https://doi.org/10.1007/978-981-15-3369-3_1.

[19] S. Yin, H. Li, A. A. Laghari, T. R. Gadekallu, G. A. Sampedro, and A. Almadhor, "An Anomaly Detection Model Based on Deep Auto-Encoder and Capsule Graph Convolution via Sparrow Search Algorithm in 6G Internet of Everything," IEEE Internet Things J., vol. 11, no. 18, pp. 29402-29411, Sep. 2024, [Online]. Available: https://doi.org/10.1109/JIOT.2024.3353337.

[20] P. Rani and R. Sharma, "IMFOCA-IOV: Intelligent Moth Flame Optimization based Clustering Algorithm for Internet of Vehicle," in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, 2023, pp. 1-6.

[21] A. M. Rahmani et al., "A Q-Learning and Fuzzy Logic-Based Hierarchical Routing Scheme in the Intelligent Transportation System for Smart Cities," Mathematics, vol. 10, no. 22, p. 4192, Nov. 2022, [Online]. Available: https://doi.org/10.3390/math10224192.

[22] M. N. Allawi, A. N. Hussain, M. K. Wali, and D.A. Pereira, "High Impedance Fault Detection in Distribution Feeder Based on Spectrum Analysis and ANN with Non-Linear Load", JT, vol. 6, no. 2, pp. 36-47, Jun. 2024.

[23] M. Saravanan and P. Ganeshkumar, "Routing using reinforcement learning in vehicular ad hoc networks," Comput. Intell., vol. 36, no. 2, pp. 682-697, May 2020, [Online]. Available: https://doi.org/10.1111/coin.12261.

[24] M. Ul Hassan et al., "ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV," Sensors, vol. 24, no. 3, p. 818, Jan. 2024, [Online]. Available: https://doi.org/10.3390/s24030818.

[25] Najwa Mohammed Jawad and Nahideh Derakhshanfard, "Assigning Optimal Multi-Objective Model in Cognitive Radio Networks", EETJ, vol. 2, no. 1, pp. 33-41, Jan. 2025.

[26] A. N. Upadhyaya and J. S. Shah, "AODV ROUTING PROTOCOL IMPLEMENTATION IN VANET," Int. J. Adv. Res. Eng. Technol., vol. 10, no. 2, Jun. 2019, [Online]. Available: https://doi.org/10.34218/IJARET.10.2.2019.055.

[27] N. Hussain, P. Rani, N. Kumar, and M. G. Chaudhary, "A deep comprehensive research architecture, characteristics, challenges, issues, and benefits of routing protocol for vehicular ad-hoc networks," Int. J. Distrib. Syst. Technol. IJDST, vol. 13, no. 8, pp. 1-23, 2022.

[28] A. Palma, P. R. Pereira, P. R. Pereira, and A. Casaca, "Multicast routing protocol for Vehicular Delay-Tolerant Networks," in 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain: IEEE, Oct. 2012, pp. 753-760, [Online]. Available: https://doi.org/10.1109/WiMOB.2012.6379160.

[29] X. Liu, "An Optimal-Distance-Based Transmission Strategy for Lifetime Maximization of Wireless Sensor Networks," IEEE Sens. J., vol. 15, no. 6, pp. 3484-3491, Jun. 2015, [Online]. Available: https://doi.org/10.1109/JSEN.2014.2372340.

[30] D. Chou and M. Jiang, "A Survey on Data-driven Network Intrusion Detection," ACM Comput. Surv., vol. 54, no. 9, pp. 1-36, Dec. 2022, [Online]. Available: https://doi.org/10.1145/3472753.

[31] A. Adeel et al., "A multi-attack resilient, lightweight IoT authentication scheme," Trans. Emerg. Telecommun. Technol., vol. 33, no. 3, p. e3676, Mar. 2022, [Online]. Available: https://doi.org/10.1002/ett.3676.

[32] P. Rani, U. C. Garjola, and H. Abbas, "A Predictive IoT and Cloud Framework for Smart Healthcare Monitoring Using Integrated Deep Learning Model," NJF Intell. Eng. J., vol. 1, no. 1, pp. 53-65, 2024.

[33] A. Khurshid, A. N. Khan, F. G. Khan, M. Ali, J. Shuja, and A. U. R. Khan, "Secure-CamFlow: A device-oriented security model to assist information flow control systems in cloud environments for IoTs," Concurr. Comput. Pract. Exp., vol. 31, no. 8, p. e4729, Apr. 2019, [Online]. Available: https://doi.org/10.1002/cpe.4729.

[34] D. Singh and B. Singh, "Investigating the impact of data normalization on classification performance," Appl. Soft Comput., vol. 97, p. 105524, Dec. 2020, [Online]. Available: https://doi.org/10.1016/j.asoc.2019.105524.

[35] D. M. W. Powers, “Evaluation: From precision, recall and F-measure to ROC, informedness, markedness and correlation,” J. Mach. Learn. Technol., vol. 2, pp. 37–63, 2011, doi: 10.9735/2229-3981.