SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

# Adaptive Machine Learning in Roadside Units for Blackhole-Resistant Secure Routing in VANETs: RSML

Kashifa Khan[1*], Devdas Saraswat[2]

[1,2] Computer Science & Engineering, LNCT University Bhopal (M.P.).
E-mail: kashifa.khan23@gmail.com

**Abstract**

Vehicle traffic on roads is the major problem in the whole world. Vehicles are moving on the roads but are not aware of the vehicle's density in a particular area. The role of attacker presence in the network makes it more complicated to recognize the traffic-free route. In a Vehicular Ad hoc Network (VANET), all the vehicles are transferring traffic status information to other vehicles to ignore traffic congestion. The route formation process in vehicular communication is critical, as a malicious node may divert the path or disrupt the network for personal advantage during this phase. Consequently, it is imperative to choose a suitable routing method that guarantees secure communication. This research proposed an RSML approach for securing the traffic information dropping from the blackhole attack in VANET. This proposed approach facilitates the quickest communication route but requires enhancement through a security mechanism capable of detecting and preventing the VANET from blackhole attacks. A vehicle acquires the communication channel from the roadside unit (RSU) when attempting to communicate with another vehicle. Machine learning (ML) is an algorithmic framework designed to analyse extensive traffic information to discern patterns and facilitate decision-making or forecasting. The RSML method uses machine learning to effectively detect and mitigate black hole threats in vehicle ad hoc networks. The machine learning concept is incorporated with the AODV routing protocol to ascertain dependable paths and provide secure communication. This RSU functions as a centralized controller system, which offers real-time roadside information, manages any congestion, and gathers data from every vehicle within its range for security purposes. The RSML approach shows better data receiving and throughput as compared to the previous T-AODV and ANN-AODV approaches.

**Keywords:** Blackhole Attacker, Machine Learning, Routing, RSML, Security.

## 1. Introduction

Traditional security solution in vehicular ad hoc network apply the cryptographic techniques such as digital signature, encryption and authentication protocols [2][3]. These mechanisms ensure data integrity and authentication but insufficient to detect routing or internal attacks where malicious node shows itself valid credential but actual behavior dishonestly. In addition, rule-based intrusion detection systems (IDS) [4] typically depends on predefined threshold and defined static rules which may fail to adapt highly movable network and context aware network. Therefore it's necessary to develop intelligent and adaptive security mechanism which capable to learn from evolving network condition of vehicular ad hoc network.

Machine learning (ML) has emerging and promising approach to address complex security challenges in dynamic ad hoc network [5] machine learning technique can able to analyze network behavior pattern, malicious node detection and classify unwanted activity in real time. In the vehicular ad hoc network, machine learning technique capable to detect routing misbehavior including blackhole, grayhole and sybil attack. However, many existing approach suffer from centralized processing, higher computational overhead, delayed attack detection or limited adaptability to rapid changing traffic patterns [6]. Furthermore, the advantages of machine learning based routing prediction extend beyond individual model choice, instead it ensemble methods which combine the multiple models to perform exceptional enhancing prediction accuracy and security [7]. The hybrid model integrate machine learning model with traditional routing algorithm provides balanced solution that benefits from the adaptability of machine learning and stability to conventional routing methods. The dynamic nature of VANET communication necessity which can adapt to changing conditions and machine learning for appropriate route prediction, context aware decision making and safer and more efficient transportation system [8].

In this article proposed RSML framework operates in multiple phases. Firstly road side unit collect routing related feature from vehicles such as route request frequency, patterns of sequence number, packet forwarding ratio, delay

and data drop rates. These information fetch to machine learning model to classify and capable to distinguishing between normal and malicious routing. In the second phase, detect suspicious behavior by RSUs using cross validation of route information through neighbour RSUs and legitimate vehicles. Third phase, malicious attack confirmation and isolation from routing process through dynamic trust, finally secure route decision selection which select secure and stable route to forward data packet source to destination vehicle. The multi layered RSML approach ensures both detection accuracy and rapid mitigation [21-22].

The article is organized into five modules. The first module presents an introduction to vehicular ad hoc networks (VANETs), including their characteristics, applications and operational challenges. This section also discusses the limitations of VANETs, their vulnerability to various security attacks and highlights the importance of machine learning methodologies for enhancing network security. Section II reviews both traditional and recent security schemes designed to protect VANETs from different types of attacks. This section provides a comprehensive analysis of existing approaches, which helps establish the research gap and define the objective for developing an adaptive machine learning security framework. The third module provides a detailed description of the proposed RSML (Adaptive machine learning in road side units) framework for detecting and mitigation blackhole attack in VANETs. This section explains the machine learning model, trust computation mechanism, secure routing strategy, algorithm steps and the overall system architecture.

Module IV presents the performance evaluation of the proposed RSML mechanism. The results are analyzed using various network factors and comparative study is conducted between the proposed RSML framework and existing routing protocols to demonstrate its effectiveness. Finally, module V concludes the study by summarizing the key finding and discussing future research directions for enhancing the RSML-based secure touting mechanism.

## 2. Literature Survey

Amin A., et al. [1] design intelligent secure routing protocol using ANN-based technique for vehicular ad hoc network. In this article they address issues regarding malicious activity which lead to packet drops due to their security activities. Their proposed ANN-based security approach encompasses the task of forecasting and identifying optimal path and effectively adopt with modified version of the AODV routing protocols. This complex protocol utilizes forward and backward control packets in route discovery and incorporates objective function to precisely identify the ideal path for data transmission.

G. Soni et al. [9] presents an Intrusion Detection and Prevention System (IDPS) designed to secure vehicle-to-RSU (V–RSU) communications against malicious activities, including blackhole and wormhole attacks, in VANET environments. The proposed IPS mechanism is deployed at the Roadside Unit (RSU) level, where it monitors vehicular behavior to identify abnormal or adversarial patterns. A swarm optimization–based algorithm is employed to enhance detection accuracy and efficiently recognize malicious vehicles, thereby strengthening network security and communication reliability.

S. Mande, et al. [10] was analyze the behavior of AN –based routing protocol for diverse vehicular communication. This study examines the effectiveness of neural network-based routing protocols in achieving reliable and secure data transmission across heterogeneous traffic environments. Although prior investigation have demonstrated the potential of neural networks to mitigate security threats such as malicious or compromised node attacks, limited attention has been given to their adaptability under varying mobility scenarios which includes urban, rural and highway conditions. To bridge this gap, they evaluate routing performance using both simulation traffic model and real-world mobility datasets.

G. Soni et al. [11] introduces a security framework termed SHLPLN (Security against Hatchetman Attacks in Low-Power and Lossy Networks) to counter a specialized flooding-based adversary known as the Hatchetman attacker. The proposed approach aims to detect and mitigate such energy-depletion attacks, ensuring sustainable and reliable network operation.

E. Farsimadan, et al. [12] has been detail survey about security challenges in vehicle to-things (V2X) communication for VANETs. The survey provides a systematic and comprehensive overview of emerging research directions in V2X communication security, with particular emphasis on identifying and analyzing the critical security challenges and corresponding solutions. It evaluates existing security mechanism design to mitigate the risk and classify current solution as per to the underlying security strategies employed.

Komaram, K, et al. [13] highlight the traditional rule based and standalone machine learning approaches to address critical challenges in vehicular ad hoc networks (VANETs), namely reliable and real-time tracking roadside units (RSUs) under dynamic and large scale traffic condition. There proposed Bayesian deep neural network (BDNN) model is employed for adaptive feature extraction confidence and uncertainty conditions.

Qi and Zhang [14] proposed a distributed machine learning-based intrusion detection system for VANETs that ensures the security and privacy through a federated learning framework. The approach archives high detection accuracy which is around 97% with reduced communication overhead, making it suitable for dynamic vehicular environments.

Goapalasamy and Muthaiya [15] Proposed the H-MAntentSVM, which is hybrid approach combining Antnet routing with SVM-based blackhole detection in MANETs. The method improves energy-efficient routing while accurately

identifying malicious nodes. The system achieves 92% detection accuracy along with significant gains in throughput and packet delivery ratio.

Singh et al. [16] Propose a reinforcement learning-based routing protocol for MANETs that enhances energy efficiency, security and adaptability in zone-based network structures. The proposed approach dynamically selects optimal routes by learning from network conditions, improving resilience against attacks and reducing energy consumption. The results show improved packet delivery and network stability.

Srinivasan [17] presents a cross-layer defense mechanism to detect and mitigate blackhole as well as wormhole attacks in wireless ad hoc networks by integrating information from multiple protocol layers. The approach enhances detection accuracy and improves routing reliability by correlating network behaviour across layers.

Ilango et al. [18] Propose a blockchain based secure framework for VANETs that integrates adaptive echo state networks with dual trapdoor homomorphic encryption to ensure authentication and privacy-preserving data sharing. The approach enhances data integrity and secure communication by combining machine learning-based authentication with advanced encryption techniques. Results indicate improved security and reliability compared to existing models.

Baihan et al. [19] Propose a novel quantum federated learning-based framework for VANET security that combines quantum computing with federated learning to detect DoS attacks while preserving data privacy. The model uses lightweight distributed training, quantum key distribution for secure communication and explainable AI techniques, achieving very high detection accuracy around 99%.

Gayathri et al. [20] propose a machine learning-enhanced framework (HDL-LF) for detecting and mitigating DDoS attacks in VANETs using deep learning and federated learning. The model leverages CNNs to capture traffic patterns and enable distributed, privacy-preserving training across vehicles and RSUs, improve scalability and reducing communication overhead. Experimental results show high detection accuracy, reduced false positive and improved latency, making it effective for secure VANET infrastructure.

## 3. Proposed RSML Methodology

In VANETs, the proposed RSML (adaptable Machine Learning in Roadside Units for Blackhole-Resistant Secure Routing in VANETs) architecture aims to achieve secure, reliable and adaptable routing under blackhole assaults. In traditional routing of VANETs, cars rely on nearby nodes for route discovery and packet forwarding. This makes the network susceptible to rogue vehicles that masquerade as valid next-hop nodes but purposefully drop the incoming packets. To solve this challenge, RSML proposes the Roadside Units (RSUs) as intelligent security and learning entities to observe the vehicle routing and forwarding behavior in real time. The RSU collects routing observations from the vehicles within its communication range and extracts behavioral parameters including packet delivery ratio, packet loss, forwarding rate, routing reaction time, hop count, delay and route consistency. The behavioral feature vector of vehicle vi is denoted as

$X_i = [PDR_i, DR_i, FR_i, RT_i, HC_i, DL_i, RC_i]$……(1)

where $PDR_i$is packet delivery ratio, $DR_i$is packet drop rate, $FR_i$ is forwarding rate, $RT_i$ is routing response time, $HC_i$is hop count, $DL_i$is communication delay, and $RC_i$ is routing consistency.

Behavioral analysis at RSU is performed using the RSML framework to discover anomalous routing features. We believe that the discrepancy between the routing advertisement of a blackhole node and its real forwarding behavior is a crucial security indication, because a blackhole node usually responds quickly to route requests and advertises an attractive route but does not forward packets. Therefore, a first suspicion value for the vehicle vi can be computed as

$Si = w_1(1 - PDR_i) + w_2 DR_i + w_3(1 - FR_i) + w_4 RT_i + w_5(1 - RC_i)$……(2)

where w1……..w5 are feature weights with $\sum w_i = 1$The larger $S_i$, the more likely the behavior is anomalous. Rather of depending on a set threshold alone, RSML offers these features to an adaptive machine-learning classifier that executes on the RSU. The training data set can be described as:

$D = \{(X_i, Y_i)\}i = 1$ to n……(3)

where Yi=0 is normal behavior and Yi=1 is blackhole behavior. The trained model estimates the probability of malicious activity as

$P_i = P(Y_i = 1 \mid X_i)$.----------(4)

A vehicle is suspicious when (Pi $\geq \tau$, where $\tau$ is the detection threshold.

To deal with the very dynamic nature of VANETs, RSML changes its learning model continually with newly observed routing behavior. The procedure of adaptive learning can be expressed as

$\theta_{t+1} = \theta_t + \eta\Delta\theta_t$,……(5)

where $\theta_t$ are the current model parameters, ¥(¥eta¥) is the learning rate, and $\Delta\theta_t$ is the model update calculated from the new observations. The observed behavior is then integrated into a dynamic trust management framework. The trust value of vehicle vi is computed by machine-learning confidence, packet delivery, forwarding behavior and routing consistency as

$T_i = \alpha T_i^{ML} + \beta T_i^{PDR} + \gamma T_i^{FWD} + \delta T_i^{CON}$,.....(6)

Where α + β + γ + δ=1, and $T_i^{ML} = 1 - P_i$
The estimated trust value is then included in secure route selection. RSML computes a multi-constraint routing cost for each candidate route Rk as
$C(R_k) = w_h H_k + w_d D_k + w_l L_k + w_t(1 - T_k) + w_o O_k$,.....(7)
where Hk, Dk, Lk, Tk, and Ok denote the hop count, delay, packet loss, route trust, and routing overhead, respectively. The safe path is selected among the paths that do not include detected blackhole nodes:
$R_{secure} = \{R_k \in R \mid R_k \cap B = \emptyset\}$,.....(8)
To maintain the trust history of a vehicle when it travels across RSU coverage areas. Therefore, the suggested framework provides a continuous monitor-learn-detect-trust-route-update process. Its performance can be assessed by PDR, throughput, end-to-end delay, packet loss, routing overhead, detection rate, accuracy, precision, recall, F1-score, and false-positive rate. The detection rate and the false-positive rate are computed as

$DR = \frac{TP}{TP+FN} X100$.....(9)
And
$FPR = \frac{FP}{FP+TN} X100$.....(10)
To summarize, RSML incorporates adaptive machine learning, RSU-assisted monitoring, dynamic trust management, blackhole isolation, and multi-constraint secure routing to enhance the reliability and security of VANET communication in dynamic vehicular settings.

## 4. Result Discussion

To evaluate network performance under diverse operational scenarios, simulations are conducted using network simulator-2 (NS-2). This section details the simulation configuration parameters and presents a comprehensive comparative performance analysis of the proposed system. The evaluation is carried out using standard network performance metrics, including packet delivery ratio (PDR), throughput, routing overhead and end-to=end delay. The results are systematically analyzed and compared with existing approaches to validate the effectiveness, reliability and robustness of the proposed RSML framework.

### 4.1 Network Simulation Parameters

The following simulation parameters are mentioned in table 1. These parameters are used to simulate the regular T-AODV, ANN-AODV, and RSML schemes. These parameters are used to simulate the above approaches. On the basis of dynamic VANET topology, these simulation parameters are chosen after careful consideration. The performance of T-AODV, ANN-AODV, and RSML was evaluated in situations with a density of 25, 50, 100, and 150 vehicles, respectively.
Table 1: Simulation Parameters

| Parameter | Value |
|---|---|
| Simulator Tool | NS-2.31 |
| Network Type | VANET |
| MAC Protocol | IEEE 802.11 |
| Routing Protocol | AODV |
| Attack Type | Black Attack |
| Number of Attacker | 1 to- 5 |
| Security Type | T-AODV, ANN-AODV, RSML |
| Network Size (m3) | 1200 X 1200 m2 |
| Mobility Model | Random Way Point |
| Number of Vehicles | 25, 50, 100, 150 |
| Number of RSS's | 4 |
| Speed of Vehicles (m/s) | Random |
| Communication Ranges (m) | 550m2 |
| Simulation Time (s) | 300 |

The rest of all the parameters that are accessible through table 1. These parameters are essential for assessing the efficiency and dependability of any routing security under different traffic scenarios. By analysing the findings, we can ascertain which method produces the optimal performance for packet delivery ratio, end-to-end delay, and overall network throughput.

4.2 Percentage of Data Receives

The percentage of packets received in the presence of an attacker is the important criterion for measuring the packet-receiving percentage performance in the network. In the figure 1 shows the performance of the proposed RSML approach shows the 5% average improvement in PDR performance as compared to Blackhole, T-AODV, and ANN-AODV.

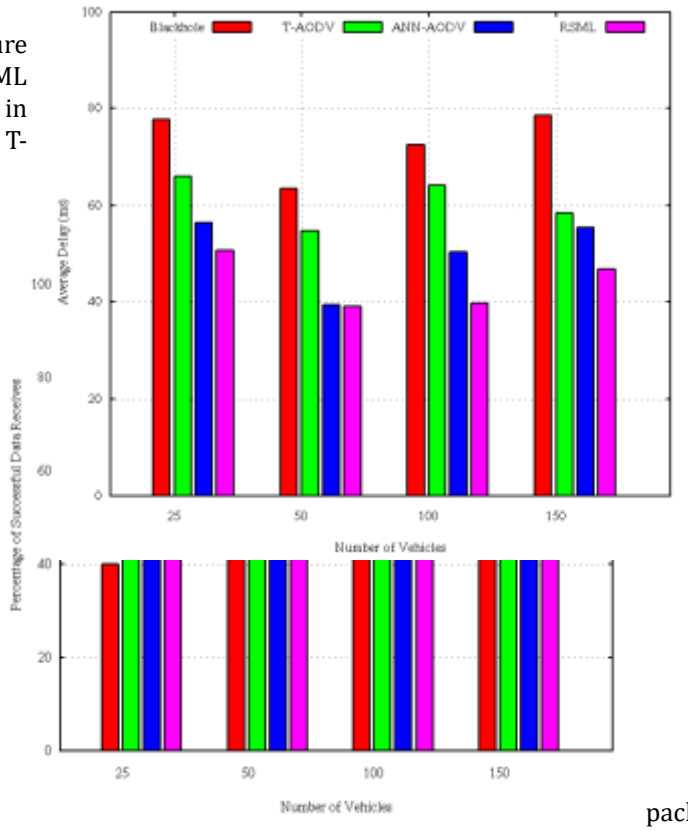


**Fig 1: Percentage of Data Receive Analysis**

The proper receiving of packets is required for better network performance. Achieving a higher packet delivery ratio enhances the reliability of data transmission and contributes to overall user satisfaction. The performance of the proposed security scheme shows reliable communication between vehicles.

**Table 2: Data Receiving Percentage Analysis**

| Percentage of Data Receives | | | | |
|---|---|---|---|---|
| Number of Nodes | Blackhole | T-AODV | ANN-AODV | RSML |
| 25 | 39.99 | 44.29 | 70.86 | 79.14 |
| 50 | 45.9 | 52.87 | 64.16 | 79.68 |
| 100 | 50.94 | 60.41 | 77.71 | 82.84 |
| 150 | 49.21 | 59.45 | 75.44 | 82.85 |

4.5 Average Network Delay Analysis

The average delay measures the average extra time required to send the traffic information to the destination in VANET. Blackhole attacker presence in the network always degrades the routing performance. These types of attackers directly attack the traffic information packets. If packets are dropped by the attacker, it means the chances of packet retransmission are enhanced. The retransmission packets are sent multiple times in the network, which enhances the delay in data receiving at the destination. Figure 3 shows the performance of the Blackhole attacker, T-AODV, ANN-AODV, and the novel RSML scheme in vehicular communication. The delay performance of the proposed RSML is the lowest as compared to all approaches in all vehicle density scenarios. The average time delay in traffic information interchange of RSML is the lowest as compared to all approaches in all vehicle density scenarios in VANET. The novel approach detects and prevents the network from attackers and provides secure data delivery with less delay.

**Fig 3: Delay Performance Analysis**

Delay performance analysis measures the extra time required in the network for data received at the destination. Delay analysis of the Blackhole attacker scenario, T-AODV, ANN-AODV, and the proposed RSML is mentioned in table 3. The performance of all the approaches is evaluated in different vehicle density scenarios in VANET. The proposed RSML demonstrates the lowest overhead performance. The average delay is about 9ms less as compared to the previous ANN-AODV approach. The low delay shows less dropping and strong link establishment for traffic information forwarding in network.

**Table 3: Average Delay Performance Analysis**

| Average Network Delay (ms) | | | | |
|---|---|---|---|---|
| Number of Nodes | Blackhole | T-AODV | ANN-AODV | RSML |
| 25 | 77.81 | 66.02 | 56.45 | 50.71 |
| 50 | 63.37 | 54.67 | 39.5 | 39.11 |
| 100 | 72.48 | 64.08 | 50.34 | 39.82 |
| 150 | 78.65 | 58.43 | 55.43 | 46.8 |

## 5. Conclusion and Future Work

Vehicle ad hoc networks (VANETs) are a type of mobile ad hoc network (MANET) that use moving cars and fixed roadside equipment to create dynamic networks for two-way communication. VANETs have many problems because vehicles can move freely on the roads in the network. These problems include high bandwidth consumption; vehicles are waiting for the responses and properly received traffic information from the other vehicles. In the routing, blackhole attackers aim to disrupt the normal routing's functioning. Attackers always generate the high sequence number to take part in the routing procedure. The source vehicle doesn't check the adversarial route and quickly starts sending data. The blackhole node then intercepts this data. It throws away data packets instead of sending them to the right person when it gets them. The process of establishing a route is not simple in vehicular communication because a malicious vehicle could disrupt the network during this period for its own benefit. Therefore, choosing a routing technique that ensures secure communication is crucial. The novel RSML system uses ad hoc on-demand distance vector (AODV) routing, which speeds up communication but needs to be made safer by adding a security feature that can find and protect the VANET from blackhole attacks. RSML uses machine learning techniques built into roadside units (RSUs) to protect the transportation network. The data collecting module explains work on the RSU monitoring system. Vehicles continuously send traffic information and receive updates on the traffic status on the roads. The malicious vehicle or blackhole attacker's role is to drop the traffic information or not forward it to the other vehicles. To detect the attacker, RSUs are observing the behaviour of malicious vehicles and maintaining the record of data receiving, forwarding, and response during connection establishment. The proposed RSML approach is showing 5% improvement in packet receiving percentage as compared to the Blackhole, T-AODV, and ANN-AODV approaches in all vehicle density scenarios. The higher packet receiving percentage means reliable route establishment and less packets dropping in network. The delay also show the better performance as compared to Blackhole, T-AODV, and ANN-AODV approaches.

Vehicular communication and traffic control systems are the requirements of modern traffic scenarios. If the vehicles are aware of upcoming traffic, then decide on a route change or route diversion. Add a location-aware system to the network in the future to track the whereabouts of cars travelling the same path. Location-aware systems are also helpful for identifying the location of the particular vehicles on the roads in an emergency. It can

also detect the attacker's location to disable its presence in the network.

## References


1. Ul Hassan, M.; Al-Awady, (2024), ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV. Sensors, 24, 818.
2. A. Malik, (2025), Comprehensive taxonomy and critical analysis of mitigation approaches for black-hole and gray-hole security attacks in AODV-based VANETs, Comput. Electr. Eng., vol. 122, 109950.
3. Soni, G., Chandravanshi, K. (2022). A Novel Privacy-Preserving and Denser Traffic Management System in 6G-VANET Routing Against Black Hole Attack. Sustainable Communication Networks and Application. vol 93. Springer.
4. C. Balakumar and S. Vydehi, (2025), Multi-Dimensional Trust based Data Dissemination mechanism for eliminating blackhole attack in VANET, J. Intell. Syst. Internet Things.
5. Edris Khezri and Hiwa Hassanzadeh, (2025), Security Challenges in Internet of Vehicles (IoV) for ITS: A Survey,Vol-30, issue 4, pp. 1700-1723.
6. T. N. Canh, X. HoangVan, (2024), Machine Learning-Based Malicious Vehicle Detection for Security Threats and Attacks in Vehicle Ad-hoc Network (VANET) Communications" arXiv:2401.08135, 2024.
7. K. Chandravanshi, G. Soni, J. Ahmed, C. Gautam and K. Khan, (2024), Machine Learning Technique for Mobility and Signal Strength-Based Route Selection in MANET, 2024 First International Conference on Software, Systems and Information Technology (SSITCON), Tumkur, India, pp. 1-7
8. Fatemidokht, H.; Marjan, K.R. (2020), QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks. J. Syst. Softw. 2020, 165, 110561.
9. Soni, G., Chandravanshi, K., Jhariya, M.K., Rajput, A. (2022). An IPS Approach to Secure V-RSU Communication from Blackhole and Wormhole Attacks in VANET. In: Sarma, H.K.D., Balas, V.E., Bhuyan, B., Dutta, N. (eds) Contemporary Issues in Communication, Cloud and Big Data Analytics. Lecture Notes in Networks and Systems, vol 281. Springer, Singapore.
10. Spandana Mande, Shaik Salma Asiya Begum, Putta Durga, Sachi Nandan Mohanty, Fernando Moreira, (2025), Generalization analysis of ANN-Based routing protocols for diverse vehicular environments in VANETs, Franklin Open, Volume 13, 2025.
11. Gaurav Soni, Kamlesh Chandravanshi, Arun Singh Kaurav, Aradhana Saxena, Durgesh Nandan, Anurag Mahajan, (2024), Behavioural Analysis of Hatchetman Attacker for Detection & Prevention in Low Power and Lossy IoT Network, Instrumentation, Mesures, Métrologies, 2024, Vol 23, Issue 5, p391
12. E. Farsimadan, L. Moradi and F. Palmieri, (2025), A Review on Security Challenges in V2X Communications Technology for VANETs, in IEEE Access, vol. 13, pp. 31069-31094, 2025
13. Komaram, K., Karyemsetty, N, (2026), A hybrid machine learning approach for scalable and uncertainty-aware RSU-based tracking and performance optimization in VANETs. J. Wirel. Commun. Netw. 2026, 76.
14. B. Qi and G. Zhang, (2026), Security and Private Collaboration IDS for VANET: Utilizing Distributed Machine Learning to Detect Network Attacks, Transactions on Emerging Telecommunications Technologies 37, no. 6 (2026): e70442,
15. Kalaiselvi Gopalasamy, Kavitha Govindarajan Muthaiya, (2025), Optimizing packet routing and security in MANETs with the H-MAntnetSVM algorithm for energy efficiency and blackhole detection, Sustainable Computing: Informatics and Systems, Volume 46.
16. Singh, S.B., Rizvi, M., Saxena, K., (2026), An adaptive, energy-efficient and secure routing protocol for zone-related mobile Ad-hoc networks using reinforcement learning. Sci Rep 16, 3002.
17. Srinivasan, J., (2025), Innovative cross-layer defense mechanisms for blackhole and wormhole attacks in wireless ad-hoc networks. Sci Rep 15, 14747.
18. Ilango, P., Sivarajan, N., Rajakumar, M.P, (2026), Blockchain-enabled secure authentication and privacy-preserving information sharing in VANETs using adaptive echo state networks and dual trapdoor homomorphic encryption. Sci Rep.
19. A. Baihan, Z. Ullah, A. Irshad, M. Shafiq, J.-G. Choi, and M. Amoon, (2026), Quantum Federated Learning for DoS Attack Detection and Privacy Preserving of VANET: A Novel Hybrid Machine Learning Approach, Transactions on Emerging Telecommunications Technologies 37, no. 3 (2026): e70375.
20. T. Gayathri, S. Uma Maheswari, S. P. A. Sathya, T. S. Murthy, and P. Patro, (2025), Machine Learning-Enhanced DDoS Attack Detection and Mitigation in VANET Infrastructure, Transactions on Emerging Telecommunications Technologies 36, no. 10.
21. Gupta, P., & Singh, B. (2024). Tool Chatter Diagnosis using EMD and LMD Techniques: A Comparative Study. EVERGREEN – Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, 11(2), 1216–1226.
22. Gupta, P., Singh, B., & Shrivastava, Y. (2023). Theoretical and Experimental Prediction of Optimal Process Variables for Enhanced Metal Removal Rate during Turning on CNC Lathe. EVERGREEN – Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, 10(2).