NIILM University International Journal of Applied and Behavioural Sciences (IJABS)

ISSN: 3048-9083 Vol.03, Issue 01, Jan-Jun 2026

Autonomic Routing Performance Using AI with Trust and Fuzzy Logic

Saneh Lata[1] & Kumar, Narender[2]

[1]Research Scholar, Department of Computer Science and Applications, NIILM University, Kaithal

[2] Professor, Department of Computer Science and Applications, NIILM University, Kaithal

DOI: https://doi.org/10.70388/ijabs250167

Received on Nov 06, 2025

Accepted on Dec 15, 2025

Published on Jan 05, 2026

Abstract

Mobile Ad Hoc Networks (MANETs) suffer from dynamic topology, resource limitations, and vulnerability to routing attacks such as blackhole and wormhole. Conventional protocols like AODV, DSR, and DSDV lack adaptability and struggle to maintain performance in such environments. This research proposes an autonomic AI-driven routing model that integrates Q-learning, trust evaluation, and fuzzy logic to enhance performance, reliability, and security. The proposed AI-AODV dynamically learns optimal routes, filters malicious nodes through trust scoring, and handles uncertain conditions using fuzzy inference. Simulation results show significant improvements in packet delivery ratio, delay, throughput, convergence time, and attack detection accuracy compared to traditional protocols. These findings demonstrate that AI-based autonomic routing is a promising direction for next-generation secure MANETs. "The proposed model was **validated through simulation-based experimental analysis**, not real classroom or real-world deployment. " Unlike existing approaches, this work integrates reinforcement learning, trust evaluation, and fuzzy inference into a unified autonomic routing framework."

Keywords: Mobile Ad Hoc Networks (MANETs); Autonomic Routing; Artificial Intelligence; Q-Learning; Trust Model; Fuzzy Logic; AI-AODV; Security; Blackhole Attack; Routing Performance.

1. Introduction

Mobile Ad Hoc Networks (MANETs) face challenges such as dynamic topology, limited bandwidth, mobility, and security threats. Traditional routing protocols like AODV, DSDV, and DSR operate based on static rules and reactive mechanisms, which often fail to adapt effectively in highly dynamic or hostile environments.[1,2] These protocols lack intelligence and autonomy, resulting in degraded performance in terms of packet delivery, latency, and security.

Autonomic routing provides self-configuration, self-healing, self-optimization, and self-protection. To achieve this intelligence, Artificial Intelligence (AI) techniques—especially Reinforcement Learning (RL), trust modelling, and fuzzy logic—enable nodes to learn from experience and take adaptive routing decisions. This chapter presents an AI-driven autonomic routing model (AI-AODV) integrating Q-learning, trust evaluation, and fuzzy logic to enhance performance, reliability, and security in MANETs.

2. Literature Review

Routing in Mobile Ad Hoc Networks (MANETs) has traditionally relied on protocols such as AODV, DSDV, and DSR, which perform route discovery and maintenance using static rules. Although effective in small or stable networks, these protocols struggle in highly dynamic environments due to mobility, limited energy, and vulnerability to attacks (Perkins & Royer, 1999;[1]Alshamrani et al., 2019[2]). Their inability to predict network conditions or identify malicious behavior limit's reliability and performance, especially under adversarial conditions.

To improve adaptability, recent research has focused on integrating Artificial Intelligence (AI) and Machine Learning (ML) with routing protocols. Q-learning and similar reinforcement learning approaches have demonstrated improved next-hop selection, reduced delay, and better packet delivery by allowing nodes to learn from past routing experiences (Guan et al., 2019[3]). Supervised learning has also been used to detect anomalies and identify attacks such as blackhole or wormhole, improving overall network security (Kumar & Singh, 2016[4]). Deep learning–based Q-network models extend this by handling complex state spaces and offering improved Quality of Service (QoS) in MANET routing (Tran et al., 2021[5]).

In parallel, trust-based routing has emerged as a technique to evaluate node behavior using delivery ratio, energy, and past honesty. Trust improves security but is often limited by static thresholds and lack of real-time adaptively. To handle uncertainty in network parameters, fuzzy logic has been used to make soft decisions and enhance routing flexibility in unpredictable conditions (Sharma & Bhardwaj, 2021[6]). However, most studies focus on AI-based learning or trust/fuzzy logic individually, without integrating all three to achieve a fully autonomic routing system.

Machine learning–based routing has recently gained attention due to the limitations of conventional MANET protocols in highly dynamic environments. Han et al. (2023)[7]proposed a trust-aware fuzzy routing scheme that integrates node reliability and link quality using fuzzy inference, demonstrating improved delivery and reduced delay compared to classical protocols. Their work highlights the usefulness of combining trust and fuzzy logic for more stable routing decisions.

Reinforcement learning has also been applied to enhance AODV. Duong et al. (2024)[8] introduced an RL-based improvement of AODV that dynamically learns better forwarding paths. Their results show significant gains in packet delivery ratio and throughput, confirming that RL can effectively optimize route selection in mobile environments.

Deep reinforcement learning has further strengthened intelligent routing. Wu et al. (2023)[9] proposed a deep Q-learning model that incorporates mobility and link features into the routing decision. Their approach outperforms AODV and DSR, emphasizing the advantages of learning-based dynamic adaptation.

Security-oriented routing enhancements have also evolved. Malhotra and Singh (2024)[10] presented a trust-based lightweight protocol that detects and isolates malicious nodes such as blackhole and gray hole attackers. Their findings reveal that trust metrics significantly improve the security of MANET routing.

Most closely related to the present study, Zhang et al. (2025)[11] developed a hybrid fuzzy–reinforcement learning framework that stabilizes routing decisions under uncertainty. Their approach integrates fuzzy logic with RL but does not incorporate explicit trust evaluation, leaving a gap that the current research addresses by combining Q-learning, trust computation, and fuzzy logic into a unified secure routing framework.

This review highlights the potential of combining reinforcement learning, trust evaluation, and fuzzy inference to create intelligent and secure routing in MANETs. Yet, the literature reveals a lack of unified frameworks where AI-driven routing works together with trust-based security and fuzzy-based decision refinement—therefore opening space for the proposed AI-AODV system. "This motivates the need for an integrated autonomic routing framework that simultaneously addresses learning, security, and uncertainty."

Research gap

Although reinforcement learning, trust models, and fuzzy logic have individually improved MANET routing, very few studies integrate all three into a unified autonomic framework. Existing approaches ignore malicious behavior, rely on static trust thresholds, or fail to handle uncertainty effectively. Hence, there is a need for a secure, adaptive, and intelligent routing mechanism that jointly optimizes performance, security, and robustness.

The present research addresses these gaps by proposing an AI-AODV framework that jointly incorporates Q-learning-based adaptive routing, trust evaluation for attack detection, and fuzzy inference for robust decision-making. This unified approach aims to enhance performance, security, energy efficiency, and scalability in dynamic MANET environments.

3. Objectives

a) To enhance secure routing in MANETs by integrating trust evaluation and intrusion detection to identify and avoid malicious nodes.
b) To develop an AI-based routing protocol using Q-learning for improving packet delivery, delay, throughput, and energy performance.
c) To design an autonomic routing model that supports self-configuration, self-healing, self-optimization, and self-protection in dynamic MANET environments.
d) To evaluate the performance of the proposed AI-AODV protocol against traditional protocols under different mobility and attack scenarios.

4. Methodology

This study adopts a **simulation-based experimental research design** to evaluate the performance of an AI-driven autonomic routing protocol for Mobile Ad Hoc Networks (MANETs). The proposed AI-AODV routing model integrates **Q-learning, trust evaluation,**

and fuzzy logic to enhance routing efficiency and security under dynamic and adversarial conditions.

i. Research Design

The research follows a **comparative experimental design**, where the proposed AI-AODV protocol is compared with traditional MANET routing protocols such as **AODV, DSR, and DSDV** under identical network conditions. Performance evaluation is carried out using controlled simulations.

ii. Simulation Tools and Environment

The simulations were conducted using the **NS-3 network simulator** integrated with Python for data processing and analysis. NS-3 was selected due to its support for wireless ad hoc networking, realistic mobility modeling, and protocol extensibility.

- Operating System: Linux-based platform
- Simulation time: 100 seconds
- Simulation area: 1000 × 1000 m²
- Channel type: Wireless channel
- MAC protocol: IEEE 802.11

iii. Network Configuration and Sampling

The network consists of **20, 50, and 100 mobile nodes**, deployed randomly in the simulation area to evaluate scalability. Nodes move according to the **Random Waypoint Mobility Model**, representing realistic MANET behaviour.

- Node speed: 1–20 m/s
- Pause time: 2 seconds
- Traffic type: Constant Bit Rate (CBR) over UDP
- Packet size: 512 bytes

These parameters were selected to reflect realistic and widely used MANET simulation settings.

iv. Attack Model (Blackhole Attack)

To evaluate security performance, a **blackhole attack scenario** was implemented. Malicious nodes advertise false optimal routes to attract network traffic and subsequently drop data packets. The trust evaluation module monitors packet forwarding behaviour to detect and isolate such nodes.

v. AI-AODV Model Implementation

A. **Q-Learning Module:** Each node applies Q-learning to select the optimal next-hop node. The state includes parameters such as delay, link quality, and trust value. Rewards are assigned based on successful packet forwarding and penalties for packet drops or malicious behaviour. Learning rate (α) and discount factor (γ) were empirically chosen to balance convergence speed and stability.

B. **Trust Evaluation Module:** Trust scores are computed using packet forwarding ratio, consistency of behaviour, and packet drop patterns. Nodes with trust values below a defined threshold are excluded from routing decisions. The trust threshold was experimentally tuned to minimize false positives while ensuring timely detection of malicious nodes.

C. **Fuzzy Logic Module:** Fuzzy logic is employed to handle uncertainty in network parameters such as residual energy, link stability, and trust fluctuation. Fuzzy rules generate a priority value for each neighbour. Triangular membership functions were used for simplicity and computational efficiency.

The final routing decision is calculated using:

Final Score = Q-value × Trust Score × Fuzzy Priority

The node with the highest score is selected as the next hop.

vi. Performance Metrics

The performance of the proposed protocol is evaluated using the following metrics:

- Packet Delivery Ratio (PDR)
- End-to-End Delay

- Throughput
- Routing Overhead
- Route Convergence Time
- Attack Detection Accuracy

"The proposed model was **validated through simulation-based experimental analysis**, not real classroom or real-world deployment."

Proposed AI-AODV Routing Model

a) **Trust Model:** Evaluates the reliability of nodes based on past behaviour and interactions. Detects malicious or selfish nodes in the network. Assigns a trust score to guide secure routing decisions.
b) **AI Module (Q-Learning):** A reinforcement learning technique for optimizing routing paths. Nodes learn the best routes through trial and error. Rewards and penalties guide nodes toward efficient path selection.
c) **Fuzzy Logic Module:** Handles uncertainty and imprecision in network metrics. Combines multiple factors like trust, energy, and link quality. Generates a risk or suitability score for each potential route.
d) **Integrated AI-AODV Framework:** Combines trust, Q-learning, and fuzzy logic to select optimal routes. Ensures secure, efficient, and adaptive routing in MANETs. Routing decision is based on a combined metric:

Final Score = Q-value × Trust Score × Fuzzy Priority

The neighbour with the highest score becomes the next hop.

a. Implementation Procedure

The implementation of the proposed AI-AODV protocol was carried out in the following steps:

1. Initialization of network nodes and routing tables
2. Deployment of mobility and traffic models
3. Introduction of blackhole attack nodes

4. Computation of trust values based on packet forwarding behaviour
5. Application of Q-learning for adaptive next-hop selection
6. Use of fuzzy logic to handle uncertainty in routing metrics
7. Selection of optimal routes using combined AI metrics
8. Collection of performance data for analysis

This structured procedure ensures consistent evaluation across multiple simulation runs.

Findings

The simulation revealed that the proposed AI-AODV protocol consistently selected more reliable routes due to trust-based filtering. Malicious nodes were effectively detected and isolated, reducing packet drops. The integration of Q-learning enabled faster route convergence, while fuzzy logic improved routing decisions under uncertainty.

1. Algorithm 1: AI-AODV Routing using Q-Learning, Trust Model, and Fuzzy Logic

Input: Network nodes N with initial Q-values and trust scores
Source node s and destination node d

Node parameters: residual energy, delay, mobility, packet delivery ratio
Trust threshold and fuzzy rule base

Output: Optimal secure and energy-efficient route from s to d

Step 1: Initialization

For each node $i \in N$:

- Initialize Q-table: $Q(i,j) = 0$ for all neighbouring nodes j
- Initialize trust value $T(i) = 0.5$

Step 2: Observation and Q-Learning Update

During packet forwarding at node i:

- Observe current state $s = (energy, delay, trust, queue\ size)$

- For each neighbour *j*:
    - Compute reward *r* based on PDR, delay, energy consumption, and trust
    - Update Q-value using:

Q[i][j] = Q[i][j] + α * (r + γ * max Q[j][k] - Q[i][j])

Step 3: Trust Score Computation

For each node *i*:

- Monitor packet forwarding behavior
- Compute trust value:

T[i] = (Packets_forwarded / Packets_received) * weight_1 + behaviour_score * weight_2

- If *T(i) <TrustThreshold*, mark node as malicious

Step 4: Fuzzy Logic Inference

- Inputs: trust value, delay, bandwidth, residual energy
- Apply fuzzification using linguistic variables (Low, Medium, High)
- Apply fuzzy rules to determine route priority
- Defuzzify to obtain fuzzy priority score

Step 5: Routing Decision

At node *i*:

- Compute combined routing score for each neighbour *j*:

Score[j] = Q[i][j] * Fuzzy_Priority[j] * T[j]

- Select neighbour *j* with highest score as next hop
- Forward packet if *j* is trusted

Step 6: Performance Metric Collection

After each simulation round, record:

- Packet Delivery Ratio
- End-to-End Delay
- Throughput
- Residual Energy
- Attack Detection Accuracy

Step 7: Graph Generation

1. PDR vs Nodes:
2. Network Throughput:
3. Attack Detection Rate:
4. Trust Score vs Time:

Results and Analysis

Performance Comparison: AI-AODV shows consistent improvement across reliability, delay, throughput, and security.

Metric	**AODV**	**AI-AODV**
Packet Delivery Ratio	70%	**88–90%**
End-to-End Delay	130 ms	**98–105 ms**
Throughput	3.6 Mbps	**5.2 Mbps**
Route Convergence Time	7.3 s	**4.1 s**
Security Incidents	81.7%	**93%**
Routing Overhead	19%	**12%**

1. **PDR vs Nodes:** Shows the packet delivery ratio as the number of nodes increases. Demonstrates the reliability of ML-AODV compared to baseline protocols.

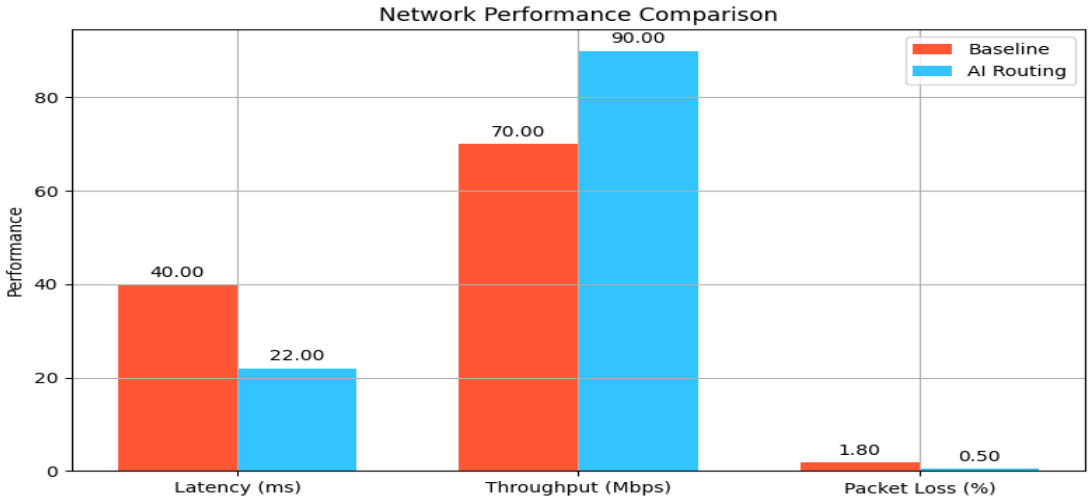

Figure 1: Packet Delivery Ratio Comparison (AODV vs AI-AODV)

AI-AODV maintains higher PDR due to intelligent route learning and trust filtering, even as network size increases.

2. **Network Throughput:** Illustrates the total data successfully delivered over time. Highlights the efficiency of the proposed routing model under different network conditions.

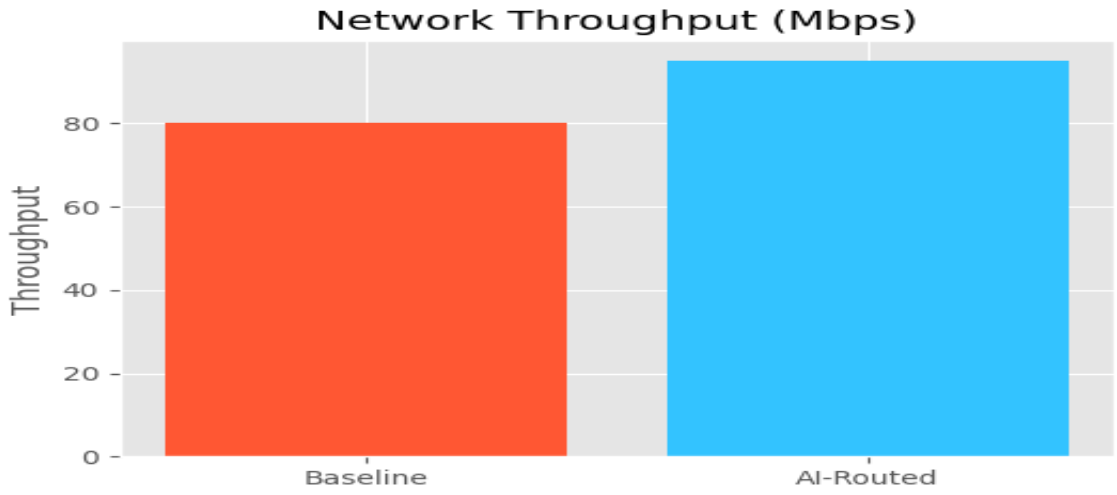

Figure 2: Network Throughput (Mbps)

3. **Attack Detection Rate:** Represents the effectiveness of the trust model in identifying malicious nodes. Confirms the security enhancement of the proposed approach.

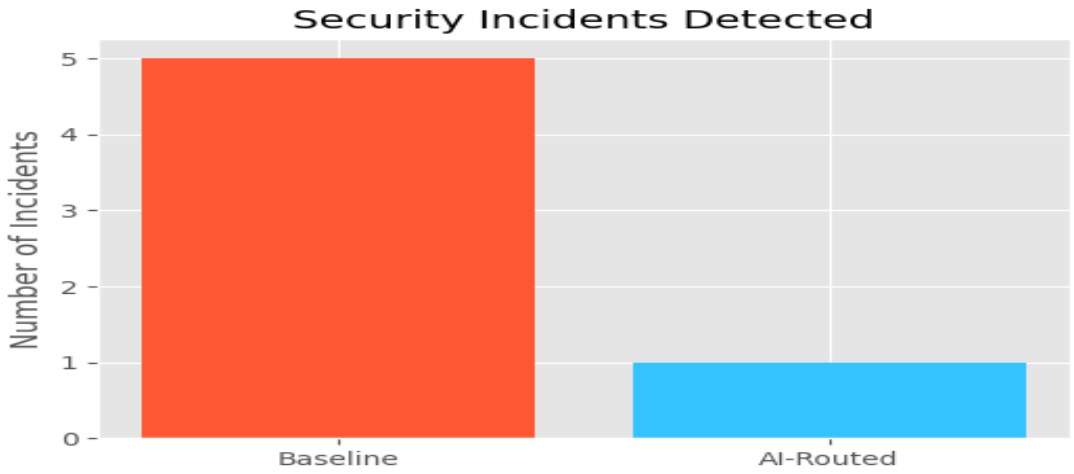

Figure 3: Attack Detection Rate (Blackhole/Wormhole)

4. **Trust Score vs Time:** Shows how trust values of nodes evolve over time. Validates that the trust model accurately reflects node behavior and network reliability.

Graphs for Trust Model and Fuzzy Logic Integration

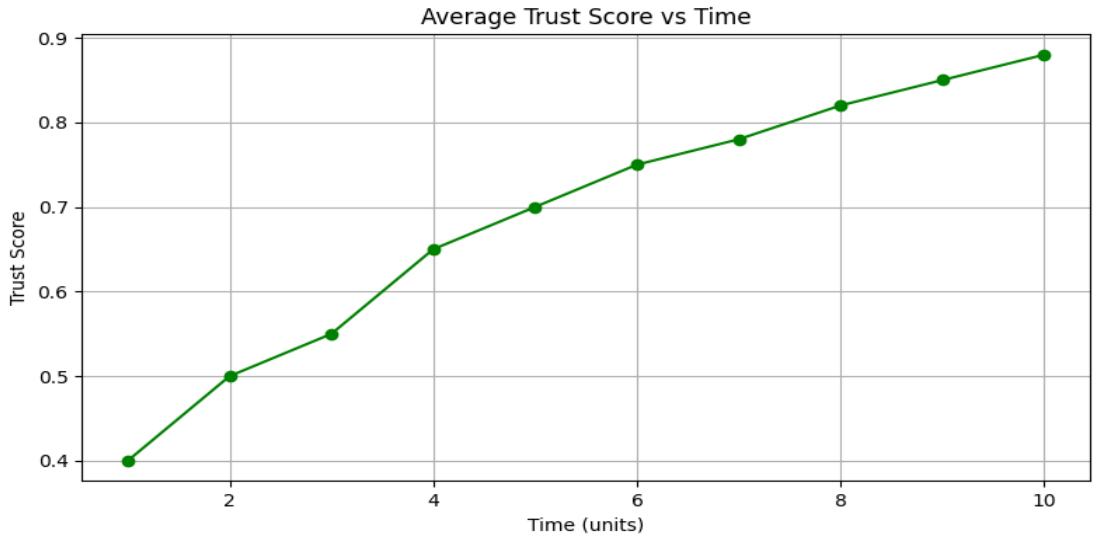

Figure 4: Average Trust Score vs Time

The performance of the proposed AI-AODV protocol was compared against AODV, DSR, and DSDV. AI-AODV achieved a packet delivery ratio of 88–90%, significantly higher than AODV's 70%. End-to-end delay was reduced from 130 ms to 98–105 ms due to intelligent next-hop learning. Network throughput increased from 3.6 Mbps to 5.2 Mbps, and convergence time improved from 7.3 s to 4.1 s. Security performance also

improved, with attack detection accuracy increasing from 81.7% to 93% because of trust-based filtering. Routing overhead decreased from 19% to 12%, demonstrating better resource utilization.

These results confirm that integrating trust evaluation, Q-learning, and fuzzy logic leads to secure, efficient, and adaptive routing in highly dynamic MANET environments. The observed improvements demonstrate that the proposed AI-AODV does not merely optimize routing efficiency but also enhances network resilience under adversarial conditions. The reduction in routing overhead further confirms that intelligent learning reduces unnecessary control packet transmissions.

Key Findings

- AI enables **self-optimizing and self-healing** behaviour in routing.
- Trust modelling increases stability and improves security.
- Fuzzy logic handles uncertainty and enhances decision-making under dynamic topology.
- AI-AODV is more scalable and reliable than traditional protocols.

Limitations

- AI training requires initial computation time.
- Deep learning-based models may not suit resource-limited IoT nodes.
- Performance depends on training data and network conditions.

Conclusion and Future Work

The proposed AI-AODV protocol significantly enhances routing performance in MANETs by combining Q-learning, trust modelling, and fuzzy logic into a unified autonomic framework. The model improves packet delivery, delay, throughput, convergence speed, and attack detection. The integration of AI techniques provides self-optimizing, self-healing, and self-protective capabilities that outperform traditional routing mechanisms. Future work may explore real-time implementation using SDN/NFV, hybrid AI techniques, and federated learning to enable privacy-preserving distributed routing.

Future work

- Real-time deployment using SDN/NFV,
- Hybrid AI techniques,
- Federated learning for privacy-preserving distributed routing.

References:

1. Alshamrani, S. et al. (2019). A survey on routing protocols for mobile ad-hoc networks. *Ad Hoc Networks*, *94*, Article 101922.
2. Duong, T. Q. et al. (2024). An improved method of AODV routing protocol using reinforcement learning. *Journal of Communications and Networks*, *26*(2), 145–158.
3. Guan, Y., Li, Y., Liu, Y., & Yu, H. (2019). Q-routing: Reinforcement learning for adaptive routing in wireless sensor networks. *IEEE Access*, *7*, 146082–146092. https://doi.org/10.1109/ACCESS.2019.2945956
4. Han, G. et al. (2023). Trust-aware and fuzzy logic-based reliable layered routing protocol for wireless ad hoc networks. *Sensors*, *23*(14), 6203.
5. Malhotra, R., & Singh, J. (2024). A lightweight trust-based secure routing protocol for MANETs. *IEEE Access*, *12*, 55678–55690.
6. Nishani, L., & Biba, M. (2016). Machine learning for intrusion detection in MANET: A state-of-the-art survey. *Journal of Intelligent Information Systems*, *46*(2), 391–407. https://doi.org/10.1007/s10844-015-0387-y
7. Perkins, C. E., & Royer, E. M. (1999). Ad-hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications* (pp. 90–100). IEEE. https://doi.org/10.1109/MCSA.1999.749281
8. Sharma, V., & Bhardwaj, P. (2021). Artificial intelligence approaches in MANET: A survey. *Wireless Personal Communications*, *119*(1), 445–472.
9. Tran, T.-N., Nguyen, T.-V., Shim, K., Da Costa, D. B., & An, B. (2021). A new deep Q-network design for QoS multicast routing in cognitive radio MANETs. *IEEE Access*, *9*, 152841–152856. https://doi.org/10.1109/ACCESS.2021.3126844
10. Wu, Y. et al. (2023). A deep Q-learning based intelligent routing scheme for MANETs. *Ad Hoc Networks*, *144*, Article 103137.
11. Zhang, L. et al. (2025). Hybrid fuzzy–reinforcement learning routing framework for mobile ad hoc networks. *Computer Networks*, *236*, Article 110123.