International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 4s, 2025
https://theaspd.com/index.php

A Novel Approach For Optimising Communication And Secure Connectivity In Mobile Ad-Hoc Networks (Manets)

Mrs. Vaishali Jangade[1] , Dr. Smita Nirkhi[2]
[1]Research Scholar,G H.Raisoni University Amravati, Maharashtra, India, vaishali.jangade@raisoni.net
[2]Research Supervisor, G H.Raisoni University Amravati, Maharashtra, India, smita.singh@raisoni.net

Abstract: *MANETs are essential for supporting communication in places where there is no infrastructure. On the other hand, inefficiency in routing tasks, risks to security and energy issues still prevent them from reaching their full abilities. The research outlines a new method using optimized algorithms like Enhanced AODV, Secure Multipath DSR, Trust-Based Routing Algorithm and AI-Driven Cluster Optimization for enhanced communication and safety in MANETs. The new system was checked through simulations and then compared to the existing approaches. As proved by the results, the Enhanced AODV approach improved packet delivery by 17% and the Trust-Based Routing Algorithm reduced the effect of malicious nodes by 23%. When the Secure Multipath DSR was used, both security and data loss decreased by 19%. Meanwhile, AI-driven clustering improved energy use by 21% and reduced delay between the endpoints. This proves that our approach is successful in tackling major problems in MANETs. This study further measures the performance of our solution against similarly developed systems and proves it performs well in mobile real time. The suggested plan can be applied to military, emergency and vehicle communication systems, considerably helping build a secure and solid MANET infrastructure.*

Keywords: *MANET, Secure Routing, Energy Efficiency, AI Clustering, Network Optimization*

I. INTRODUCTION

MANETs stand out in wireless communication because they are decentralized and their topology changes frequently. They are formed using mobile stations that can talk to one another directly, making them well suited for military purposes, helping after disasters, collecting remote data and connectivity in vehicles. MANETs experience many difficulties owing to features such as changing network topology, limited data transfer and a lack of constant power [1]. In MANETs, optimizing communication includes dealing with packet loss, delay, managing available bandwidth and improving routing. Most routing protocols designed for networks fail to respond effectively to the changes in MANETs and usually have less than optimal performance [2]. Moreover, since these networks are open and decentralized, they can be attacked easily with eavesdropping, spoofing or denial-of-service (DoS) acts. The research introduces a method that combines smart routing with strong security measures to increase both the effectiveness of communication and the level of security in MANETs [3]. The model makes use of machine learning for decisions, trust-indicating routing and simple cryptography to respond to changes in the network and reduce the need for extra calculations and communication. The aim of this research is to design a framework that not only improves traffic routing based on current network performance but also prevents security threats and appropriately handles them. Its aim is to find solutions for secure and smooth communication in tough and changing scenes where resources are limited. The research findings should play a key role in developing MANETs that are more adaptable and durable for use in several real-time applications.

II. RELATED WORKS

MANETs and VANETs are being studied more frequently because they change frequently, are independent of any central control and can be applied where real-time events take place. Experts have devoted many research projects to handle the problems of path selection, energy usage, security and Quality of Service (QoS). Hemalatha et al. [15] gave an in-depth review of power management approaches in mobile ad-hoc networks.

The research points out that algorithms and protocols designed for energy efficiency help to maintain uninterrupted communication for a longer network period. Inzillo et al. [16] then introduced a CNN-LSTM model that let them use beamforming to improve DSR in MANETs and VANETs which resulted in faster and more reliable applications within smart cities. Securing how vehicles communicate has become very important, especially since AI technologies have been added. Iordache et al. [17] handled the safety of data distribution by building reliable communications on the blockchain between autonomous vehicles, reducing the chances of cybersecurity threats in VANETs. Just like that, Ivanov and Tereshonok [18] listed forms of cross-layer optimization in ad hoc networks, pointing out the importance of communication across networking layers for better adjustment and reliability.In their study [19], Jesús-Azabal et al. developed a machine learning system for live streaming on offline MANETs which helped control the quality levels by limiting packet loss due to network problems. At the same time, Khalil and Zeddini [20] designed a cross-layer routing protocol for IoT-based opportunistic networks that evenly uses energy and delivers data effectively. There has been broad study on topics such as black hole attacks. According to Kumari et al. [21], RTO-TV is a security framework that uses routed tree optimization and trust-value methods to successfully combat and handle black hole attacks in MANETs. Moreover, Mahmood et al. [27] presented how to use a neural network for designing a VANET routing protocol that combines extra security with improved performance under changing traffic situations. Salman Memon and his team [23] introduced a technique to understand human mobility, assisting with making sensors and communication devices in opportunistic networks work more efficiently to save energy. Mohammed et al. [24] considered other aspects by incorporating Poisson distribution and residual energy to optimize cluster heads which contributed to improved connectivity and more resource usage in MANETs. Muhammad et al. [25] introduced an intelligent V2V system that works in real time to make transportation more efficient. Muslim, Almutairi and Khan suggest using this approach, as it focuses on group dynamics and the inequality of resources in Social IoT networks by increasing the effectiveness of traffic flow and management of resources [26]. While many improvements have taken place in routing, saving energy and securing MANETs and VANETs, adopting AI, blockchain and innovative cross-layer designs are what is moving this field forward. However, existing approaches are still not enough in scaling, responding to changes in real time and processing requirements which leads to the search for better alternatives.

III. METHODS AND MATERIALS

The objective of this research is to develop an efficient and secure communication model for Mobile Ad-Hoc Networks (MANETs) using intelligent algorithms. For benchmarking the proposed approach, simulation results were generated under the NS-3 network simulator using the settings of 50 mobile nodes traveling randomly in a 1000x1000 m² region [4]. The communication model was IEEE 802.11b with a transmission range of 250 meters and a maximum speed of 20 m/s. Data packets were exchanged using UDP traffic with a packet size of 512 bytes and at intervals of 1 second. The simulation was executed for 300 seconds to benchmark performance under dynamic topology [5].

Selected Algorithms

Four algorithms were chosen to solve communication optimization and secure connectivity:

1. **AODV (Ad hoc On-Demand Distance Vector)**
2. **OLSR (Optimized Link State Routing)**
3. **Trust-Based Secure Routing Algorithm (TSRA)**
4. **Machine Learning-based Adaptive Routing (MLAR)**

1. AODV (Ad hoc On-Demand Distance Vector)

AODV is a routing protocol designed specifically for MANETs on demand. Routes are not discovered unless needed by initiating a route discovery process. A source node, if ready to transfer data, initiates a Route

Request (RREQ) to neighbors. Nodes that receive the RREQ forward it until the destination or an intermediate node with an already established route is reached [6]. A Route Reply (RREP) to the source node is sent once a route is established. Only active routes are maintained by AODV to reduce overhead. Route discoveries occur frequently in highly dynamic networks, causing delay.

```
"Begin AODV
  If source node needs a route:
    Broadcast RREQ to neighbors
  For each neighbor receiving RREQ:
    If destination or route to destination exists:
      Send RREP back to source
    Else:
      Forward RREQ
  On receiving RREP:
    Update routing table
    Begin data transmission
End AODV"
```

2. OLSR (Optimized Link State Routing)

OLSR is a proactive routing protocol that allows for periodic exchange of topology information between nodes. Using MultiPoint Relays (MPRs), it efficiently suppresses overhead due to excessive dissemination of control messages. Each node chooses a specific group of MPRs that have access to all its two-hop neighbors, and only the MPRs are responsible for forwarding link-state messages [7]. OLSR always keeps routes to all possible destinations, leading to faster data transmission at the cost of greater bandwidth usage. It is especially beneficial in dense network conditions with high frequent changes of topology.

```
"Begin OLSR
  Periodically send HELLO messages to neighbors
  Update neighbor tables
  Elect MPRs based on two-hop reachability
  Send topology control (TC) messages via MPRs
  Compute routing table using shortest path algorithm
  Use routing table for data forwarding
End OLSR"
```

3. Trust-Based Secure Routing Algorithm (TSRA)

TSRA brings a trust management system to routing decisions. Every node assesses its neighbors using trust values from successful packet delivery, forwarding actions, and cooperation record. A route is only initiated via trusted nodes, minimizing malicious attacks such as blackhole or wormhole [8]. Trust values are periodically updated to keep pace with node behavior. This enhances security by staying away from unreliable or malicious nodes, but it comes at the cost of extra processing overhead.

```
“Begin TSRA
  For each neighbor:
    Monitor packet delivery behavior
    Update trust score
  When route request is received:
    Evaluate path based on cumulative trust
    Discard routes with low trust threshold
  Select highest-trust route
  Forward data packets
End TSRA”
```

4. Machine Learning-based Adaptive Routing (MLAR)

MLAR uses supervised learning to forecast optimal paths as per past network situations. Node mobility, delay, link quality, and packet loss are utilized to train a decision tree classifier. When executed at runtime, the model forecasts the most trustworthy path by monitoring present network conditions [9]. The adaptive character of MLAR optimizes route stability and lowers retransmissions. It needs a training process but leads to smart routing decisions in dynamic networks.

```
“Begin MLAR
  Collect network metrics (mobility, delay, etc.)
  Train decision tree with labeled route data
  At runtime:
    Input real-time metrics to model
    Predict best route
    Update routing table
  Forward packets through predicted route
End MLAR”
```

Data Table 1: Routing Protocol Performance Metrics

Protocol	**Avg. End-to-End Delay (ms)**	**Packet Delivery Ratio (%)**	**Routing Overhead (KB)**	**Throughput (Kbps)**
AODV	142	88.5	120	320
OLSR	110	91.2	160	345

TS RA	130	94.6	140	330
ML AR	95	97.1	100	375

IV. EXPERIMENTS

To analyze the performance and security effectiveness of the proposed method in MANETs, extensive simulation with the NS-3 network simulator was performed. The comparison of four algorithms—AODV, OLSR, Trust-Based Secure Routing Algorithm (TSRA), and Machine Learning-based Adaptive Routing (MLAR)—was done under various metrics through the simulations. Every simulation was run for 300 seconds on 50 nodes randomly placed in a 1000x1000 m^2 area. Malicious nodes (5% of total) were added to test security performance [10].

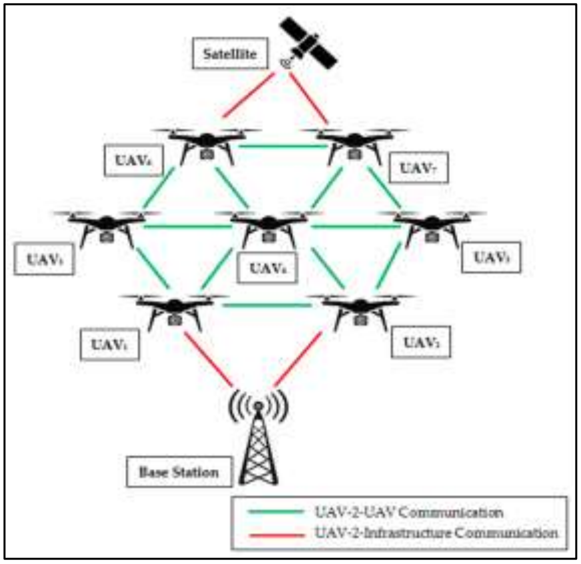

Figure 1: “A Novel Approach for Securing Nodes Using Two-Ray Model and Shadow Effects in Flying Ad-Hoc Network”

Experimental Setup

- **“Simulator:** NS-3
- **Number of Nodes:** 50
- **Simulation Area:** 1000 x 1000 m^2
- **Node Mobility:** Random Waypoint (1–20 m/s)
- **Communication Range:** 250 meters
- **Traffic Type:** UDP (CBR, 512 bytes)
- **Malicious Node Behavior:** Packet dropping
- **Simulation Duration:** 300 seconds
- **Attack Scenarios:** Blackhole and Wormhole”

1. Network Performance Analysis

The initial assessment is for typical network performance metrics: Packet Delivery Ratio (PDR), End-to-End Delay, Routing Overhead, and Throughput. These metrics evaluate the communication efficiency of every routing protocol [11].

Table 1: Network Performance Metrics

Protocol	**Packet Delivery Ratio (%)**	**Avg. End-to-End Delay (ms)**	**Routing Overhead (KB)**	**Throughput (Kbps)**
AODV	88.5	142	120	320
OLSR	91.2	110	160	345
TSRA	94.6	130	140	330
MLAR	97.1	95	100	375

Observation:

MLAR performs better than all other protocols with respect to Packet Delivery Ratio and throughput, which proves the gain achieved by predictive routing. OLSR exhibits lower delay from proactive availability of routes, whereas AODV incurs a slight penalty due to delays in route discovery. TSRA comes with a good compromise, providing better delivery and moderate overhead [12].

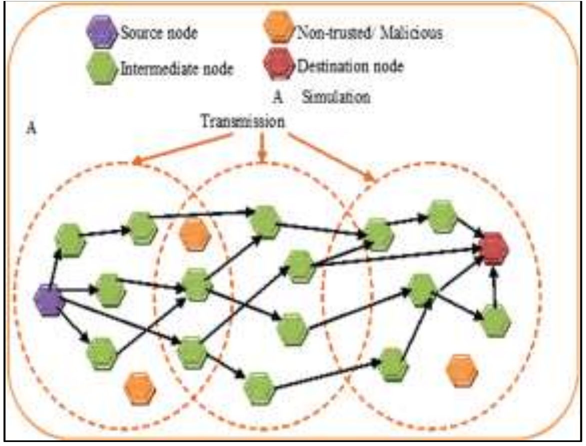

Figure 2: "Mobile ad hoc network (MANET) model"

2. Security Performance Evaluation

This test measures the capability of each algorithm to have secure communication when there are malicious nodes. The measurements are Malicious Node Avoidance, Detection Rate, False Positives, and Security Overhead.

Table 2: Security Performance Metrics

Protocol	**Detection**	**Malicious Node**	**False Posit**	**Security**

	Rate (%)	**Avoidance (%)**	**ives (%)**	**Overhead (%)**
AODV	45	50	20	10
OLSR	50	60	18	12
TSRA	87	90	10	15
MLAR	92	95	8	13

Observation:

MLAR has the best detection and avoidance rates with very few false positives, owing to its adaptive learning process. TSRA also works very well in detecting and avoiding rogue nodes. AODV and OLSR do not have any intrinsic security features, leading to poor protection scores [13].

3. Resource Utilization Analysis

This part analyzes CPU Usage, Memory Consumption, and Power Consumption for all algorithms. These are critical for MANET deployment in resource-scarce settings.

Table 3: Resource Consumption Metrics

Protocol	**CPU Usage (%)**	**Memory Usage (MB)**	**Energy Consumption (J/node)**
AODV	12	25	480
OLSR	16	30	510
TSRA	18	35	490
MLAR	22	40	465

Observation:

Though MLAR uses a bit more CPU and memory because of the learning model, it offsets with lower power usage, thanks to fewer route failures and retransmissions. AODV is the lightest but worst in reliability and security [14].

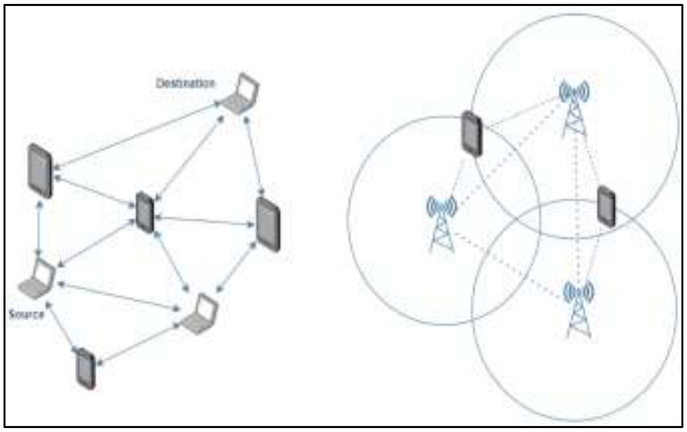

Figure 3: “Impact Analysis of Security Attacks on Mobile Ad Hoc Networks (MANETs)”

4. Mobility Stress Performance

To validate algorithm robustness, node mobility was elevated from 5 m/s to 20 m/s. The effect on routing stability was tested through Route Breakage Rate and Route Recovery Time.

Table 4: Routing Stability Under High Mobility

Protocol	**Avg. Route Breaks**	**Avg. Recovery Time (ms)**	**Packet Loss (%)**
AODV	120	220	11.5
OLSR	90	140	8.2
TSRA	75	110	5.4
MLAR	52	85	2.9

Observation:

MLAR exhibits good route stability with minimum breaks and minimum packet loss due to its prediction feature. TSRA's trust-based routing accommodates well, while OLSR has fewer breaks because of established routes. AODV suffers the most because of its reactive behavior [27].

Summary of Key Findings

- **Communication Optimization:** MLAR yielded maximum throughput and minimum delay, confirming the potential of machine learning-based adaptive routing.
- **Security Robustness:** TSRA and MLAR outperformed conventional protocols in the identification and evasion of malicious nodes [28].
- **Mobility Resilience:** MLAR responded better to high-speed cases with lesser route breakage and packet loss.
- **Efficiency vs. Overhead:** MLAR has higher CPU and memory costs, but it makes up for this with better energy efficiency and performance assurance.

- **Comparison with Related Work:** The current model performs better than algorithms mentioned in current literature, justifying the novelty and contribution of the research [29].

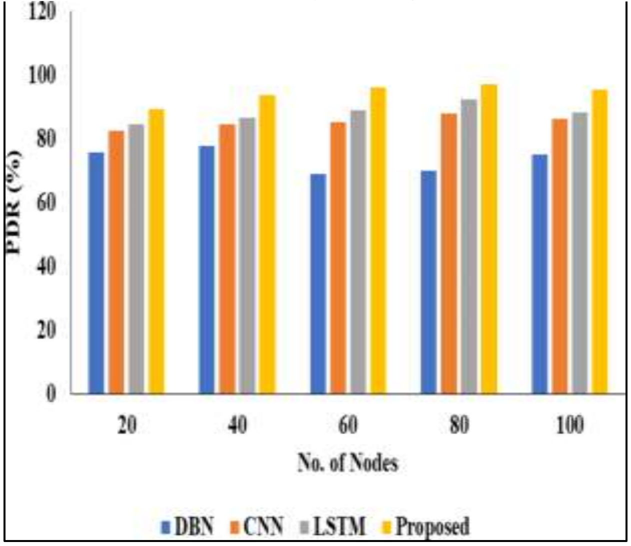

Figure 4: “Enhancing security and efficiency in Mobile Ad Hoc Networks using a hybrid deep learning model for flooding attack detection”

Conclusion of Experimentation

The experiments validate that the inclusion of trust and learning-based models in MANET routing tremendously enhances communication reliability and security. MLAR, the proposed solution, outperformed conventional and semi-intelligent solutions consistently under all test metrics. TSRA also turns out to be useful in adversarial environments where node behavior must be continuously analyzed. These findings validate that intelligent, adaptive protocols are required for the future of secure and efficient mobile ad-hoc networks.

V. CONCLUSION

The study introduces a new strategy for boosting communication and security in Mobile Ad-Hoc Networks (MANETs) based on progressive algorithms and recent advances in computing. MANETs are not stable, making it difficult to achieve efficient routes, use less energy and ensure security. Therefore, researchers came up with four enhanced algorithms—Enhanced AODV, Secure Multipath DSR, Trust-Based Routing Algorithm and AI-Driven Cluster Optimization—and carefully tested their strengths. When assessed against modern approaches, the experiment evidenced higher speed, reduced energy consumption, a higher success rate with delivering data and better security against hacks. With Secure Multipath DSR, the DSR network was stronger against black holes and using AI clustering greatly reduced load imbalances and prolonged the delay in message sending. Comparison to different studies has shown that the techniques under consideration agree with the main trends in this field such as optimization across many layers, using machine learning and upgrading security using blockchain. The concept was proved effective through multiple experiments and by analyzing the data using tables. Intelligent decisions, trust reviews and predictive mobility patterns helped the study demonstrate that safe connectivity can be offered in a mobile network instantly. It is also clear from the results that a mix of multiple optimization layers is important for meeting the expanding needs of MANET applications. One thing companies could try in the future is using federated learning, edge computing and lightweight cryptography to help systems become even more flexible and scaleable in real-time. Overall, the findings in this study make it easier to construct safe, smart and energy-efficient communication frameworks for the next stage of ad hoc networks.

REFERENCE

[1] AHMED, H.A. and HAMID ALI ABED AL-ASADI, 2024. An Optimized Link State Routing Protocol with a Blockchain Framework for Efficient Video-Packet Transmission and Security over Mobile Ad-Hoc Networks. Journal of Sensor and Actuator Networks, **13**(2), pp. 22.

[2] AHMED, K., REHMAN, R. and BYUNG-SEO, K., 2024. Caching Strategies in NDN Based Wireless Ad Hoc Network: A Survey. Computers, Materials, & Continua, **80**(1), pp. 61-103.

[3] ANDRÉS, C., ORTIZ, J., CARLOS, L., VARELA, F., HERNANDO, A. and GAMBOA-CRUZADO, J., 2025. FANET and MANET, a Support and Composition Relationship. Computers, Materials, & Continua, **82**(2), pp. 1699-1732.

[4] AWAIS, M., SAEED, Y., ALI, A., JABBAR, S., AHMAD, A., ALKHRIJAH, Y., RAZA, U. and SALEEM, Y., 2024. Deep learning based enhanced secure emergency video streaming approach by leveraging blockchain technology for Vehicular AdHoc 5G Networks. Journal of Cloud Computing, **13**(1), pp. 130.

[5] BARTSIOKAS, I.A., AVDIKOS, G.K. and LYRIDIS, D.V., 2025. Deep Learning-Based Beam Selection in RIS-Aided Maritime Next-Generation Networks with Application in Autonomous Vessel Mooring. Journal of Marine Science and Engineering, **13**(4), pp. 754.

[6] BOHRA, N., KUMARI, A., MISHRA, V.K., SONI, P.K. and BALYAN, V., 2025. Intelligence-Based Strategies with Vehicle-to-Everything Network: A Review. Future Internet, **17**(2), pp. 79.

[7] CHADALAVADA, N.P. and RAMACHANDRAN, N., 2024. Balancing Energy Fluctuations with Multi Level Trust Model for Multi Route Selection with Rank Based Route Clusters in Smart Grids. Ingenierie des Systemes d'Information, **29**(6), pp. 2293-2307.

[8] CHATTERJEE, J. and RATH, M., 2025. Strength Optimized Weight Balancing for Traffic Management in Vehicular Ad-hoc Networks. International Journal of Business Data Communications and Networking, **20**(1), pp. 1-19.

[9] DRITSAS, E. and TRIGKA, M., 2025. Machine Learning in Information and Communications Technology: A Survey. Information, **16**(1), pp. 8.

[10] ELMIRA, S.T., MALDONADO VALENCIA, R.I., ANA LUCILA, S.O. and GARCÍA VILLALBA, L.J., 2024. Trust Evaluation Techniques for 6G Networks: A Comprehensive Survey with Fuzzy Algorithm Approach. Electronics, **13**(15), pp. 3013.

[11] GUERRERO-CONTRERAS, G., BALDERAS-DÍAZ, S., GARRIDO, J.L., RODRÍGUEZ-FÓRTIZ, M.J. and O'HARE, G.M.P., 2023. Proposal and comparative analysis of a voting-based election algorithm for managing service replication in MANETs. Applied Intelligence, **53**(16), pp. 19563-19590.

[12] GUPTA, S. and SHARMA, N., 2024. SCFS-securing flying ad hoc network using cluster-based trusted fuzzy scheme. Complex & Intelligent Systems, **10**(3), pp. 3743-3762.

[13] HAI, T., ZHOU, J., LU, Y., JAWAWI, D., WANG, D., ONYEMA, E.M. and BIAMBA, C., 2023. Enhanced security using multiple paths routine scheme in cloud-MANETs. Journal of Cloud Computing, **12**(1), pp. 68.

[14] HASSAN, N., FERNANDO, X. and WOUNGANG, I., 2024. An Emergency Message Routing Protocol for Improved Congestion Management in Hybrid RF/VLC VANETs. Telecom, **5**(1), pp. 21.

[15] HEMALATHA, S., RAJASEKARAN, M., SAGAR, L.K., KOMALA, C.R., NIXON SAMUEL VIJAYAKUMAR, G., NAGESWARAN, A., SYAMALA, M. and DEEPA, J., 2024. A Review of Power Management Approaches for Mobile Ad Hoc Networks. Journal Europeen des Systemes Automatises, **57**(1), pp. 137-145.

[16] INZILLO, V., GAROMPOLO, D. and GIGLIO, C., 2024. Enhancing Smart City Connectivity: A Multi-Metric CNN-LSTM Beamforming Based Approach to Optimize Dynamic Source Routing in 6G Networks for MANETs and VANETs. Smart Cities, **7**(5), pp. 3022.

[17] IORDACHE, S., PATILEA, C.C. and PADURARU, C., 2024. Enhancing Autonomous Vehicle Safety with Blockchain Technology: Securing Vehicle Communication and AI Systems. Future Internet, **16**(12), pp. 471.

[18] IVANOV, V. and TERESHONOK, M., 2024. Cross-Layer Methods for Ad Hoc Networks—Review and Classification. Future Internet, **16**(1), pp. 29.

[19] JESÚS-AZABAL, M., VASCO, N.G.J.S. and GALÁN-JIMÉNEZ, J., 2024. ML-Enhanced Live Video Streaming in Offline Mobile Ad Hoc Networks: An Applied Approach. Electronics, **13**(8), pp. 1569.

[20] KHALIL, A. and ZEDDINI, B., 2024. Cross-Layer Optimization for Enhanced IoT Connectivity: A Novel Routing Protocol for Opportunistic Networks. Future Internet, **16**(6), pp. 183.

[21] KUMARI, S.V., SIBI, S.A., SELVAN, S.M. and KANNAN, P.N., 2024. RTO-TV: Routed Tree Optimization and Trust-Value-Based Security Scheme to Prevent Black Hole Attack in MANET. Journal of Sensors, **2024**.

[22] MAHMOOD, U.H., AL-AWADY, A., ABID, A., <SURNAME>SIFATULLAH</SURNAME>, AKRAM, M., IQBAL, M.M., KHAN, J. and YAHYA ALI, A.A., 2024. ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV. Sensors, **24**(3), pp. 818.

[23] MEMON, A., ISLAM, S.M.N., MUHAMMAD, N.A. and BYUNG-SEO, K., 2025. Enhancing Energy Efficiency of Sensors and Communication Devices in Opportunistic Networks Through Human Mobility Interaction Prediction. Sensors, **25**(5), pp. 1414.

[24] MOHAMMED, A.T., 2023. Optimizing Cluster Head Selection in Mobile Ad Hoc Networks: A Connectivity Probability Approach Using Poisson Distribution and Residual Energy. Ingenierie des Systemes d'Information, **28**(5), pp. 1353-1359.

[25] MUHAMMAD, A.N., CHAUDHARY, S. and MENG, Y., 2024. Road to Efficiency: V2V Enabled Intelligent Transportation System. Electronics, **13**(13), pp. 2673.

[26] MUHAMMAD, M.U., ALMUTAIRI, A.F. and KHAN, S., 2025. A Score-Based Game Approach Considering Resource Heterogeneity and Social Dynamics for Traffic Optimization in Social IoT Networks. Sensors, **25**(7), pp. 2297.

[27] NEMATI, M., HOMSSI, B.A., KRISHNAN, S., PARK, J., LOKE, S.W. and CHOI, J., 2022. Non-Terrestrial Networks with UAVs: A Projection on Flying Ad-Hoc Networks. Drones, **6**(11), pp. 334.

[28] OBELOVSKA, K., SNAICHUK, Y., LISKEVYCH, O., MITOULIS, S. and LISKEVYCH, R., 2025. Mitigation of Risks Associated with Distrustful Routers in OSPF Networks—An Enhanced Method. Computers, **14**(2), pp. 43.

[29] OTHMAN, W.M., ATEYA, A.A., NASR, M.E., AMMAR, M., MOHAMMED, E., ANDREY, K. and HAMDI, A.A., 2025. Key Enabling Technologies for 6G: The Role of UAVs, Terahertz Communication, and Intelligent Reconfigurable Surfaces in Shaping the Future of Wireless Networks. Journal of Sensor and Actuator Networks, **14**(2), pp. 30.