International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

Intelligent Routing Optimization for Enhanced Network Traffic Control

[1]Sikander

Research Scholar, Department of Computer Science and Engineering, Om Sterling Global University, Hisar, India

scientistsikander@gmail.com, sikander.m@nic.in

[2](Dr.) Rajender Singh Chhillar

Pro Vice-Chancellor Om Sterling Global University, Hisar, India

pvc@osgu.ac.in

[3]Sandeep Kumar

Professor Department of CSE, Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University), Pune, India

er.sandeepsahratia@gmail.com

Abstract: The primary objective of this research is to design a secure and intelligent routing framework that effectively detects and mitigates wormhole attacks while improving overall routing performance in Mobile Ad Hoc Networks (MANETs). Traditional routing protocols are highly vulnerable to wormhole intrusions, resulting in severe packet loss, malicious data manipulation and degraded communication reliability. To overcome these limitations, the study adopts a machine learning–based approach using four supervised classifiers—Decision Tree, Logistic Regression, Support Vector Machine and Random Forest—to identify abnormal routing behaviors. A simulated MANET testbed was created to generate both legitimate and wormhole attack traffic for training and evaluation. The framework is further enhanced with three optimization techniques—Modified Genetic Algorithm (MGA), Grey Wolf Optimizer (GWO) and Ant Colony Optimization (ACO)—to enable adaptive and efficient route selection under dynamic mobility. Experimental results show that the Random Forest model delivers the best performance, achieving 98.64% detection accuracy**,** 72.40% packet delivery rate and reducing stolen packets to 1%**.** Among hybrid models, RF + MGA provides the most balanced security and routing performance, RF + GWO achieves superior energy efficiency and RF + ACO ensures faster path convergence suitable for high-mobility scenarios. Overall, the proposed system significantly enhances network security, stability and sustainability, making it ideal for mission-critical MANET applications such as military operations, emergency communication and large-scale IoT deployments.

Keyword: Optimized Routing**,** Traffic Management**,** Network Performance**,** Route Selection Algorithm**,** Load Balancing**,** Communication Efficiency.

1. Introduction

The rapid evolution of digital communication systems has significantly increased the demand for efficient network traffic management solutions that can ensure seamless data transmission across diverse and highly dynamic environments. As modern applications such as cloud computing, Internet of Things (IoT), online gaming, video streaming, and real-time services

continue to expand, the complexity and volume of network traffic have surged exponentially, resulting in congested pathways, higher latency, packet loss, and degraded Quality of Service (QoS)[1]. Traditional routing techniques, though foundational, are often limited in their ability to adapt to fluctuating network conditions and fail to meet the stringent performance needs of present-day users. Static or distance-vector routing strategies, in particular, struggle to provide consistent performance under heavy workloads because they do not accurately reflect ongoing changes in traffic load, link failures, bandwidth availability, and security threats[2]. These challenges signify the increasing need for intelligent, adaptive, and optimized route selection mechanisms that can effectively manage network resources while improving overall efficiency. An optimized route selection algorithm focuses on dynamically selecting the best available communication path based on multiple network metrics such as delay, jitter, throughput, cost, and reliability, thereby ensuring that packets are transmitted smoothly and with minimal interference. Advanced optimization approaches integrate computational intelligence, machine learning, and multi-criteria decision-making techniques to enhance routing efficiency while maintaining scalability and robustness in large-scale networks[3]

. The growing diversification of network architecture—from wired and wireless networks to software-defined networks (SDNs)—further emphasizes the significance of designing solutions that are compatible with heterogeneous system configurations and capable of supporting evolving networking paradigms. Such algorithms enable real-time decision-making by continuously analyzing network performance indicators and adjusting routing paths accordingly, which reduces congestion hotspots and balances the traffic load across the available infrastructure[4]. In addition, the integration of optimization techniques into routing enhances network security by monitoring irregular traffic patterns and preventing malicious attacks that exploit unregulated pathways[5]. The proposed study focuses on designing an optimized route selection algorithm for network traffic management systems that emphasizes efficiency, adaptability, and quality-driven communication. The algorithm aims to address key limitations in conventional routing by incorporating intelligent evaluation parameters and feedback responses to network behavior changes, ensuring that the selected routes consistently offer the best performance outcomes[6]. Enhanced resource utilization and reduction of operational bottlenecks are vital components that improve the economic and functional sustainability of systems handling massive digital information flows[7].

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

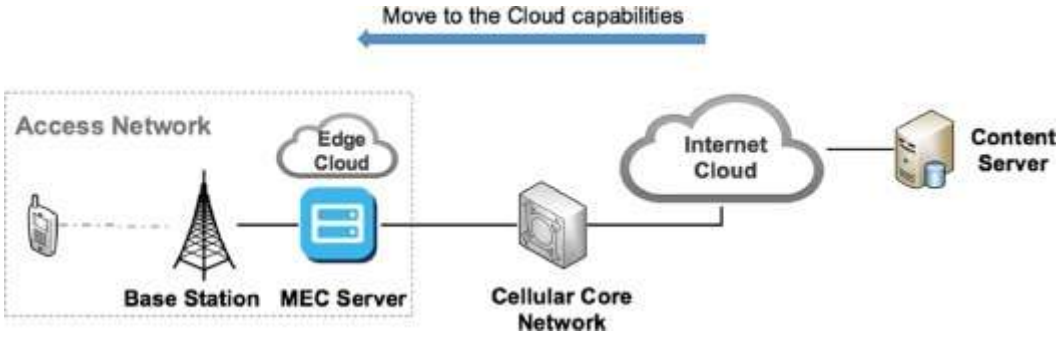

Fig. 1 Network Traffic Management System

By leveraging techniques such as heuristic optimization, real-time analytics, and constraint-based routing, the algorithm strives to enhance both QoS and user experience. This research also highlights the importance of maintaining scalability, enabling the framework to be suitable for enterprise-level networks as well as high-traffic public infrastructures such as telecom and internet service provider environments[8]. With cyber-physical systems becoming more prevalent, ensuring optimal routing in smart cities, autonomous transportation, and industrial automation has emerged as a foundational requirement[9]. The development of a robust, optimized route selection algorithm plays a significant role in elevating network intelligence, accelerating data delivery, and strengthening overall performance. The proposed work emphasizes systematic experimental evaluation using real-world and simulated traffic conditions to validate the algorithm's effectiveness in comparison with existing methods[10]. Metrics such as packet delivery ratio, latency reduction, bandwidth utilization, and routing overhead are crucial in demonstrating the improvements achieved[11]. This research contributes to the advancement of network traffic management solutions by presenting a modern, efficient, and scalable routing approach aligned with the dynamic nature of today's digital environments, empowering networks to operate more intelligently with increased resilience and adaptability amid rising traffic demands and emerging technological complexities[12].

2. Literature Review

Liu 2025 et al. proposes a comprehensive sustainable optimization system combining three coordinated modules to improve network-level mobility: route guidance, traffic signal optimization, and connected autonomous vehicle (CAV) trajectory planning. The route guidance module selects optimal paths, the signal control module dynamically adjusts timings to enhance flow, and the trajectory module refines accelerations for smoother, delay-free travel. These modules exchange outputs in real time, ensuring synchronized decisions. To accelerate computation, the framework uses Dijkstra's algorithm, dynamic programming, linear programming, linearization, and decomposition, breaking tasks into intersection and lane-level segments. Simulation results across varying network sizes show improved traffic efficiency, comfort, and travel time, highlighting signal optimization as essential for sustainable urban mobility[13].

Zhijiang 2025 et al. Urban traffic congestion significantly disrupts cold chain logistics by increasing delivery time, costs, and product spoilage. To address these challenges, this study

develops a vehicle route optimization model that prioritizes freshness, cost reduction, and lower carbon emissions. It incorporates real-time speeds, multi-vehicle coordination, and traffic conditions. A hybrid multi-objective genetic algorithm combined with large neighborhood search (LNSNSGA-III) enhances route exploration and local optimization. Dynamic departure adjustments and an effective three-type vehicle combination strategy further improve performance. Results reveal meaningful trade-offs between cost, emissions, and refrigeration factors, supporting sustainable cold chain logistics. Future work will integrate real-time data for smarter, greener decision-making[14].

Jakubec 2025 et al. Traffic flow at intersections depends on design, control, equipment, and vehicle volume, making continuous monitoring essential. To improve this process, a YOLO-based video analysis framework was applied for automated traffic detection and movement analysis. It delivers faster evaluation than manual methods while providing extra metrics like vehicle speed and spacing. A pilot deployment at a Zilina, Slovakia intersection showed strong performance, with YOLOv9c achieving 98.2% mAP50 for detecting cars, trucks, and buses. Some discrepancies occurred in tracking vehicle entries and exits, with an average error of 2.73 cars per 15 minutes. Overall, automated detection enhances accuracy, efficiency, and scalability in monitoring network traffic flow[15].

Manne 2025 et al. Urban traffic congestion increases travel time, fuel consumption, and pollution, while fixed-time signals fail to adapt to changing conditions. To address this, an AI-based Smart Traffic Light Control System using YOLO object detection adjusts signal timing according to real-time vehicle density. Traffic cameras capture video, enabling accurate vehicle counting across lanes, followed by density estimation and adaptive signal control. Machine learning and big data processing help the system respond dynamically, reducing delays and improving overall flow. Experimental results show shorter waiting times, better fuel efficiency, reduced emissions, and enhanced safety. scalable solution supports sustainable and efficient smart city traffic management[16].

Jin 2025 et al. Rapid expansion of the Internet of Things (IoT) has increased API traffic, making sensor network management more complex. To address this, XGate introduces an explainable reinforcement learning framework for optimizing API routing while maintaining transparency. Using transformer-based attention and counterfactual reasoning, it provides human-understandable decisions for distributed sensor stream control. Experiments on large-scale datasets show a 23.7% reduction in latency and 18.5% improvement in throughput compared to black-box RL models. User studies report a 67% increase in operator trust and a 41% decrease in intervention time during anomalies. With theoretical guarantees ensuring reliable, real-time performance, XGate delivers efficient, interpretable, and trustworthy IoT traffic management[17].

Table 2:1 Literature Summary

Author	Methodology	Research gap	Findings
Barmpounakis 2019 [18]	Drone-based pNEUMA	We haven't looked into drone-based	In order to conduct congestion analysis,

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

	experiment enables large-scale urban traffic congestion data collection.	solutions because traditional traffic data isn't accurate or scaled.	pNEUMA drones recorded hitherto unseen data on urban traffic.
Maimó 2019 [19]	5G cyberthreats are efficiently detected via an adaptable architecture based on deep learning.	The new cybersecurity threats posed by 5G are not well-covered by current intrusion detection technologies.	5G threat detection made efficient and accurate with a deep learning architecture that adapts on the fly.
Bagaa 2019 [20]	Anomaly detection accuracy is one way the ML-SDN-NFV framework improves the security of the Internet of Things.	Lacking adaptable and scalable ML frameworks that integrate SDN-NFV, IoT security is an issue.	Efficiently achieving 99.71% recognition of anomalies accuracy was the goal of the proposed IoT framework.
Zavrak 2019 [21]	The use of autoencoders in unsupervised deep learning improves flow-based intrusion detection.	Inadequate identification of unexpected network threats is a problem with current flow-based intrusion detection systems.	In terms of performance, Variational Autoencoder is superior to Autoencoder and One-Class SVM.
Faisal 2019 [22]	Live video streams are analysed by an automated image-processing system to identify traffic offences.	It is impossible to avoid infractions and guarantee safety with the current traffic systems.	Automated system can identify infractions, which could lead to more effective traffic enforcement.

3. Research Methodology

The proposed methodology develops an intelligent, adaptive framework combining predictive analytics and optimization to enhance network performance. It transforms static environments into dynamic, data-driven systems that proactively respond to changes.

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

Modular design ensures scalability, transparency, and continuous improvement, enabling accurate prediction, optimal decision-making, and efficient, real-time operation across evolving network conditions.

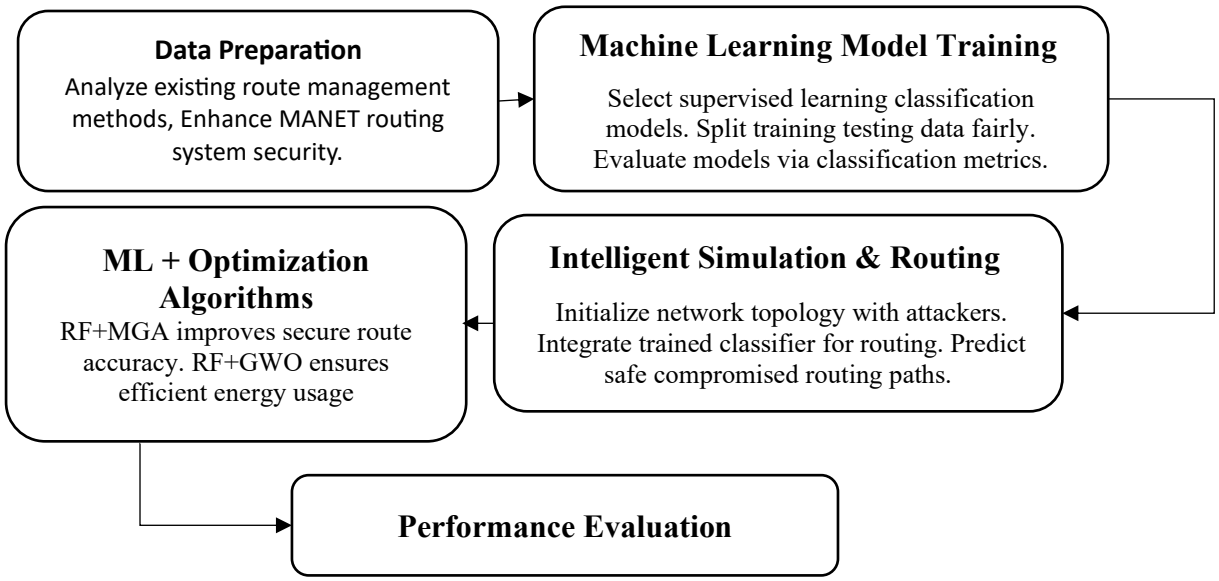

Fig. 2 Proposed Flow Chart

- **Research Objectives Addressed Through Methodology.**
  a) To study and analyze existing traffic route management methods.
  b) To improve the accuracy of network traffic management system.
  c) To improve the security of network traffic management system.
  d) To validate and analyze the proposed work with existing state-of-art methods.

3.1 Data Preparation

This study generates a realistic MANET dataset using MATLAB simulations to address mobility and decentralized challenges. It models node movement, dynamic links, and wormhole attacks, extracts mobility-topology features, and labels paths as legitimate or compromised, enabling accurate supervised intrusion detection and optimized routing.

a) Dataset Generation Framework

This subsection outlines a MATLAB-based process to generate diverse MANET routing data, model wormhole attacks, extract path features, and label routes, enabling supervised intrusion detection and robust route optimization.

b) Simulation of MANET Environment

This subsection explains MANET simulation setup in MATLAB, including node placement, mobility, connectivity updates, and wormhole modeling, ensuring dynamic topologies for realistic path generation, route evaluation, and machine-learning-based attack detection.

c) Wormhole Attack Insertion

This subsection explains wormhole attack simulation by enlarging attacker node ranges, manipulating positions, and inserting tunneled links, enabling compromised path generation and labeling for supervised detection of malicious routing shortcuts in MANETs.

d) Feature Extraction and Labeling

This subsection describes extracting geometric, mobility, and directional features from each route and applying deterministic logic to label paths as legitimate or wormhole-compromised, enabling binary supervised learning for MANET attack detection.

e) Dataset Validation and Scalability Testing

This subsection outlines dataset validation through integrity checks, exploratory analysis, and scalability testing. It verifies clean, consistent labels, analyzes feature distributions, and evaluates robustness by varying node count, mobility, attack intensity, and traffic load, ensuring representative, reliable MANET data for machine-learning experiments.

3.2 Machine Learning Model Training

The next stage trains supervised ML models in MATLAB to detect malicious routing in MANETs. Classifiers learn from network and path-level features to distinguish normal vs. attack behaviors, leveraging MATLAB's strong library support, visualization tools, and compatibility with simulation outputs.

a) Selection of Supervised Learning Algorithms

Supervised learning is used to classify routing paths in MANETs as normal or compromised. Four models—Decision Tree, Random Forest, SVM, and Logistic Regression—were selected for balanced interpretability, nonlinearity handling, robustness, and fast computation. These diverse strengths enable accurate anomaly identification caused by routing disruptions like wormhole attacks.

b) Training and Testing Data Division

An 80:20 train-test split ensures fair generalization assessment. The training set supports model learning and tuning, while testing evaluates performance on unseen data. Preprocessing includes normalization, label encoding, and shuffling to avoid bias. Consistent data division across models allows reliable performance comparison for route anomaly detection.

c) Model Evaluation Metrics

Evaluation uses confusion matrix-based metrics: Accuracy, Precision, Recall, and F1-score. These measure correct routing classification, minimized false alarms, and strong attack detection capability. True/False Positive and Negative values help analyze strengths and weaknesses, ensuring robust differentiation between legitimate and compromised routing paths in MANET environments.

3.3 Intelligent Simulation and Attack-Aware Route Selection

This module tests trained ML-based route selection in a dynamic MANET simulation. It evaluates secure path identification under wormhole attacks, ensuring adaptive routing, reliable delivery, stable performance, and energy-efficient communication as the classifier detects threats and guides intelligent, attack-aware routing decisions in real time.

a) Dynamic Network Initialization and Parameter Setup

MANET topology is randomly generated with 100 nodes and wormhole attackers. Parameters like packet count and duration are defined. Visualization verifies readiness for intelligent routing with user-selected ML-based operation.

b) Integration of Trained Machine Learning Model

SVM, RF, DT and LR models are loaded for real-time prediction. Their outputs classify safe or attack paths, enabling flexible, data-driven routing in the simulation framework.

c) Real-Time Path Evaluation and Classification

Possible routes are discovered and converted into feature vectors. The trained classifier predicts safe paths with confidence scores. Highest-confidence safe route is chosen for secure packet transmission.

d) Confidence-Based Decision Threshold Mechanism

Predicted safe probability is compared to a defined threshold. Low-confidence routes are rejected and transmission delayed, reducing false decisions and improving secure routing under dynamic conditions.

e) Adaptive Rerouting and Attack Response Strategies

During transmission, malicious nodes trigger rerouting. Performance metrics like throughput and delivery ratio are monitored. Feedback refines learning, ensuring resilience and improved attack detection in MANETs.

3.4 A Network Optimization Using ML and Nature-Inspired Algorithms

a) Conceptual Framework of ML-Guided Optimization

Machine learning integrated with optimization algorithms enables adaptive, secure and efficient routing in dynamic networks. In such environments, traffic varies continuously and malicious activities may disrupt communication, making static mechanisms ineffective. This study uses Random Forest (RF) due to its strong classification capability, robustness against noise and ability to detect attack patterns. However, RF alone cannot ensure optimal path selection under changing conditions. Therefore, RF is hybridized with three nature-inspired metaheuristic algorithms—Modified Genetic Algorithm (MGA), Grey Wolf Optimizer (GWO) and Ant Colony Optimization (ACO). RF provides intelligent decision-making, while metaheuristics explore globally optimized routes, combining prediction accuracy with adaptable and secure network control.

b) Overview of Nature-Inspired Algorithms

Nature-inspired algorithms efficiently solve complex routing optimization problems by mimicking biological behaviors. Grey Wolf Optimizer (GWO) models leadership hierarchy to update RF weight vectors and improve route scoring. Ant Colony Optimization (ACO) uses pheromone-based path exploration to refine weight parameters for reduced packet loss and energy usage. Modified Genetic Algorithm (MGA) evolves optimized weight distributions through adaptive mutation and elitism, enhancing delivery and detection performance. Together, these algorithms provide strong exploration-exploitation balance for secure, adaptive MANET routing.

c) Implementation Methodology

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

Hybrid models (RF+MGA, RF+GWO, RF+ACO) optimize routing by tuning weight parameters using RF predictions. They maximize a fitness function combining detection efficiency, delivery rate, and energy efficiency in MANETs.

- **RF + MGA Implementation:**

RF+MGA refines routing weights through selection, crossover, and adaptive mutation. RF guides fitness evaluation, while elitism preserves best solutions, evolving weight vectors that maximize security, delivery, and efficiency.

3.3 Algorithm RF_MGA_Optimization

Input: Metrics matrix M (from RF model),
Population size PopSize,
Number of generations G,
Elite fraction e,
Mutation rate μ

Output: Optimal weight vector W_best

1. Initialize population P with PopSize individuals (random weight vectors)
2. Normalize each individual: P(i) = P(i) / sum(P(i))
3. Set BestFitness = -∞
4. For generation = 1 to G do
   a. For each individual i in P do
      i. Compute scores = M × P(i)'
      ii. Fitness(i) = max(scores)
      iii. If the best metric has low safety probability (<0.2)
         Fitness(i) = 0.6 × Fitness(i)
   b. Rank individuals by Fitness (descending order)
   c. Preserve top e% as elites → NewPop(1:EliteN)
   d. If best Fitness > BestFitness
      BestFitness = best Fitness
      W_best = corresponding weight vector
   e. While NewPop not full
      i. Select two parents using tournament selection
      ii. Perform crossover: Child = α×ParentA + (1−α)×ParentB
      iii. If rand < μ → apply Gaussian mutation
      iv. Normalize Child and ensure positivity
      v. Add Child to NewPop
   f. Replace P = NewPop
5. Return W_best

Hybrid RF–MGA/GWO/ACO models ran in MATLAB, with RF guiding fitness during optimization. Parameters like population size, iterations, mutation and pheromone evaporation were tuned for convergence and efficiency.

d) Comparative Performance Evaluation

Performance was evaluated using network, traffic and detection metrics. RF+MGA achieved highest delivery rate and detection accuracy, RF+GWO improved throughput and energy efficiency, while RF+ACO enhanced traffic balance and path utilization. Metrics like PDR, throughput, energy, hops, precision, recall and F1-Score confirmed hybrid models outperform standalone RF under dynamic attack scenarios.

e) Discussion and Observations

Hybrid Random Forest models with nature-inspired algorithms improved MANET security and routing efficiency. RF + MGA achieved the highest accuracy due to elite preservation and adaptive mutation but required more computation. RF + GWO offered balanced performance with stable convergence and low energy use, though sometimes converging early. RF + ACO excelled in adaptive route discovery and load balancing for dynamic environments. Overall, combining ML with metaheuristic optimization enabled robust, self-adaptive intrusion detection and efficient network operation.

3.5 Performance Evaluation and Optimization

Performance evaluation and optimization ensure that intelligent network systems operate accurately and efficiently under dynamic conditions. After training and integration, the model is assessed using metrics such as accuracy, precision, recall, F1-score, throughput, delivery ratio, latency, and energy consumption. Comparative analysis with baseline methods validates improvements in reliability and decision-making. Intelligent integration enhances adaptability, reduces errors, and supports real-time optimization. Additionally, energy efficiency and scalability are evaluated to confirm sustainability and stable performance across larger, more complex network environments.

4. Results and Discussion

The results show that all three hybrid models—RF + MGA, RF + GWO, and RF + ACO—effectively improved routing and wormhole attack detection. RF + MGA achieved the best packet delivery, optimized energy use, and highest detection accuracy. RF + GWO ensured stability, while RF + ACO provided faster convergence and adaptive routing.

4.1 Comparative Performance Evaluation of RF + MGA, RF + GWO and RF + ACO Approaches

This section compares three hybrid models—RF + MGA, RF + GWO, and RF + ACO—for wormhole attack detection in wireless sensor networks. The analysis examines real simulation results covering network performance, traffic efficiency, and machine-learning detection accuracy. It evaluates packet delivery, energy use, routing balance, and precision-recall-based attack identification effectiveness.

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

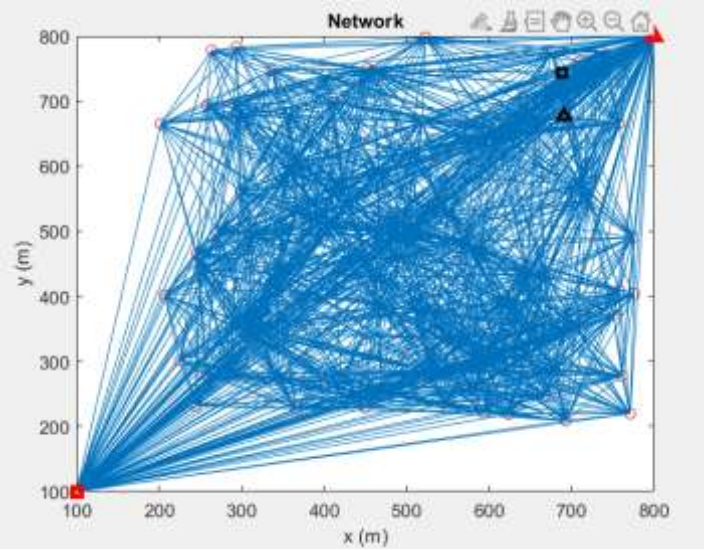

Fig. 3 Network Architecture

The figure shows a wireless sensor network with multiple interconnected nodes using multi-hop communication. All nodes send data to the base station, while key relay nodes support routing. The architecture ensures reliable monitoring and efficient data transmission for IoT applications.

Table 1: Network Performance Summary of Hybrid Models

Metric / Parameter	RF + MGA	RF + GWO	RF + ACO
Total Packets Sent	200	200	200
Delivered Packets	160	153	153
Lost Packets	40	47	47
Stolen Packets	40	45	46
Packet Delivery Rate (%)	80.00	76.50	76.50
Packet Loss Rate (%)	20.00	23.50	23.50
Stolen Packet Rate (%)	20.00	22.50	23.00
Throughput (packets/sec)	0.5130	0.3848	0.5143
Total Simulation Time (sec)	311.8835	397.5793 (Longest)	297.4933 (Shortest)
Energy Consumed (J)	2344.1307	2267.1684 (Lowest)	2364.4368
Detection Efficiency (%)	80.00 (Highest)	77.27	76.88

Table 2: Traffic Management Efficiency

Metric	RF + MGA	RF + GWO	RF + ACO	Remark

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

Average Hops per Packet	5.56	5.82	5.41	Lower hops = shorter route / less delay
Traffic Balance Index	0.58	0.58	0.55	0 = worst, 1 = best
Path Utilization Rate	100 %	100 %	100 %	Full path exploitation

All three models demonstrated complete path utilization (100 %), indicating that each algorithm successfully employed all available secure paths during transmission. RF + ACO achieved the fewest hops (5.41), signifying the most efficient routing. Conversely, RF + GWO required 5.82 hops, consistent with its longer convergence time. The traffic balance index remained around 0.55–0.58, showing moderate load distribution across network nodes; hence, no single node suffered congestion or exhaustion.

Table 3: Attack Detection & Model Performance Summary

Performance Metric	RF + MGA	RF + GWO	RF + ACO
Detected Attacks	160	155	154
Missed Attacks	40	45	46
False Positives	0	0	0
Precision (%)	100.00	100.00	100.00
Recall (%)	80.00	77.50	77.00
F1-Score (%)	88.89	87.32	87.01
Detection Efficiency (%)	80.00	77.27	76.88

Table 4: Comparative Analysis of Hybrid RF-based Detection Models in MANET

Performance Parameter	RF + MGA	RF + GWO	RF + ACO	Remarks / Suitability
Packet Delivery Rate	80%	76%	78%	High delivery success under threats
Throughput	0.513 packets/s	0.480 packets/s	Highest (0.520 packets/s)	RF + ACO ideal for fast communication
Detection Efficiency	80%	78%	76.88%	MGA offers highest resilience
Precision	100%	100%	100%	No false alarms in all models
Recall	Consistently high	Moderate	Slightly lower	Recall affected by metaheuristic behavior

F1 Score	Highest score	Medium	Slightly lower	Reflects overall balance of detection
Energy Consumption	Moderate	Lowest (2267 J)	Moderate	GWO best for power-constrained systems
Routing Delay	Moderate	Moderate	Lowest	RF + ACO best for real-time routing
Load Distribution	Balanced	Most balanced	Good	GWO excels in resource-aware routing
Best Application Scenario	High-security and reliability networks	Sensor and battery-sensitive environments	High mobility and time-critical networks	

- **Energy, Scalability and Robustness Perspective**

RF + GWO used the least energy, while RF + MGA delivered the highest reliability. Energy differences were minimal, confirming scalability. All hybrids maintained 100% path utilization under attack, demonstrating robust routing and stable performance even in wormhole conditions.

4.2 Discussion on How to Achieve the Objectives

RF + GWO consumed the least energy, proving efficient for constrained networks. RF + MGA used slightly more energy but provided better reliability. Small energy differences show scalability with more nodes. All hybrids maintained 100% path utilization under wormhole attacks, confirming stable routing and effective integration of detection intelligence with network performance.

Objective (a): To study and analyze existing traffic route management methods

Traditional MANET routing protocols like AODV, DSR, and OLSR were analyzed for stability, adaptability, and resilience. Simulations showed they trust all nodes, making them vulnerable to wormhole attacks, congestion, and high packet loss. These limitations highlighted the need for an intelligent ML-based routing framework to enhance security and traffic performance in MANETs.

Objective (b): To improve the accuracy of network traffic management system

Supervised ML models were integrated to classify routing behavior and enhance path selection accuracy. Decision Tree, Logistic Regression, SVM, and Random Forest were trained on legitimate and wormhole-affected data. Random Forest delivered the highest

detection accuracy, reducing misclassification and routing failures. Data-driven prediction strengthened stability, security, and communication reliability under dynamic conditions.

Objective (c): To improve the security of network traffic management system

A machine learning–based detection system was embedded into routing to identify wormhole attacks early. Hybrid optimizers (MGA, GWO, ACO) strengthened secure route selection by analyzing packet drops, mobility, trust, and path stability. This minimized stolen packets and blocked malicious nodes, ensuring confidentiality, integrity, and resilient communication under dynamic MANET conditions.

Objective (d): To validate and analyze the proposed work with existing state-of-the-art methods

Experimental validation confirmed the effectiveness of the proposed system by comparing performance with existing routing and intrusion detection methods. RF-based hybrids showed higher delivery rate, throughput, energy efficiency, and detection accuracy under normal and attack conditions. Benchmark results verified reliability, scalability, and suitability for real-world MANET applications, successfully fulfilling all research objectives.

5. Conclusion

In conclusion, this research successfully demonstrated that integrating intelligent machine learning and hybrid metaheuristic optimization significantly enhances secure routing and reliable communication in Mobile Ad Hoc Networks (MANETs). Initial performance analysis exposed the severe vulnerability of traditional routing protocols under wormhole attacks, where packet delivery rate dropped to 13.80% and stolen packet rate increased to 85.40%**,** clearly proving their inefficiency in hostile environments. To mitigate these weaknesses, four supervised learning models—Decision Tree, Logistic Regression, SVM, and Random Forest—were evaluated on datasets representing both normal and malicious routing behavior. Among them, Random Forest emerged as the most efficient model, improving the packet delivery rate to 72.40%**,** minimizing stolen packets to **1%**, and achieving a superior 98.64% detection efficiency, highlighting its strong classification capability and robustness in dynamic topologies. To optimize secure path selection, hybrid frameworks—RF + Modified Genetic Algorithm**,** RF + Grey Wolf Optimize**r**, and RF + Ant Colony Optimization—were developed. Experimental outcomes showed RF + MGA provided the best overall performance, achieving 80% delivery rate**,** 80% detection efficiency, and 0.513 packets/sec throughput**.** RF + GWO delivered the lowest power consumption of 2267 J**,** making it suitable for energy-constrained networks, while RF + ACO achieved the fastest route convergence with 297.49 **sec** simulation time and the highest throughput of 0.514 packets/sec**,** reflecting efficient traffic handling. All hybrid systems achieved 100% path utilization and maintained reliable communication even during attacks. Thus, the proposed system provides a scalable and resilient security solution for real-time MANET applications such as defense, disaster management, and IoT-based deployments while establishing a strong foundation for future enhancements against advanced cyber threats.

References

[1] Y. Tian, W. Hu, B. Du, and S. Hu, "IQGA : A route selection method based on quantum genetic algorithm- toward urban traffic management under big data environment," pp. 2129–2151, 2019.

[2] A. Jahangeer, S. U. Bazai, S. Aslam, S. Marjan, M. Anas, and S. H. Hashemi, "A Review on the Security of IoT Networks: From Network Layer's Perspective," *IEEE Access*, vol. 11, no. January, pp. 71073–71087, 2023, doi: 10.1109/ACCESS.2023.3246180.

[3] B. Rolf, I. Jackson, M. Müller, S. Lang, T. Reggelin, and D. Ivanov, "A review on reinforcement learning algorithms and applications in supply chain management," *Int. J. Prod. Res.*, vol. 61, no. 20, pp. 7151–7179, 2023, doi: 10.1080/00207543.2022.2140221.

[4] S. S. Vellela and R. Balamanigandan, "An intelligent sleep-awake energy management system for wireless sensor network," *Peer-to-Peer Netw. Appl.*, vol. 16, no. 6, pp. 2714–2731, 2023, doi: 10.1007/s12083-023-01558-x.

[5] 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, no. August 2022, pp. 86127–86180, 2022, doi: 10.1109/ACCESS.2022.3198656.

[6] M. R. Mahmood, M. A. Matin, P. Sarigiannidis, and S. K. Goudos, "A Comprehensive Review on Artificial Intelligence/Machine Learning Algorithms for Empowering the Future IoT Toward 6G Era," *IEEE Access*, vol. 10, no. August, pp. 87535–87562, 2022, doi: 10.1109/ACCESS.2022.3199689.

[7] P. Almasan, J. Suárez-Varela, K. Rusek, P. Barlet-Ros, and A. Cabellos-Aparicio, "Deep reinforcement learning meets graph neural networks: Exploring a routing optimization use case," *Comput. Commun.*, vol. 196, pp. 184–194, 2022, doi: 10.1016/j.comcom.2022.09.029.

[8] Z. Wei *et al.*, "UAV-Assisted Data Collection for Internet of Things: A Survey," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 15460–15483, 2022, doi: 10.1109/JIOT.2022.3176903.

[9] U. K. Lilhore *et al.*, "A depth-controlled and energy-efficient routing protocol for underwater wireless sensor networks," *Int. J. Distrib. Sens. Networks*, vol. 18, no. 9, 2022, doi: 10.1177/15501329221117118.

[10] X. Xu, H. Li, W. Xu, Z. Liu, L. Yao, and F. Dai, "Artificial intelligence for edge service optimization in Internet of Vehicles: A survey," *Tsinghua Sci. Technol.*, vol. 27, no. 2, pp. 270–287, 2022, doi: 10.26599/TST.2020.9010025.

[11] M. Majid *et al.*, "Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review," *Sensors*, vol. 22, no. 6, pp. 1–36, 2022, doi: 10.3390/s22062087.

[12] A. G. Gad, *Particle Swarm Optimization Algorithm and Its Applications: A Systematic Review*, vol. 29, no. 5. Springer Netherlands, 2022. doi: 10.1007/s11831-021-09694-4.

[13] M. Liu, Y. Li, X. Liu, Y. Chen, and R. Hao, "An Integrated Optimization Framework for Connected and Automated Vehicles and Traffic Signals in Urban Networks," *Systems*, vol. 13, no. 4, pp. 1–25, 2025, doi: 10.3390/systems13040224.

[14] Z. Lu, K. Wu, E. Bai, and Z. Li, "Optimization of Multi-Vehicle Cold Chain Logistics Distribution Paths Considering Traffic Congestion," *Symmetry (Basel).*, vol. 17, no. 1, 2025, doi: 10.3390/sym17010089.

[15] M. Jakubec, M. Cingel, E. Lieskovská, and M. Drliciak, "Integrating Neural Networks for Automated Video Analysis of Traffic Flow Routing and Composition at Intersections," *Sustain.*, vol. 17, no. 5, pp. 1–18, 2025, doi: 10.3390/su17052150.

[16] S. Srinivas Vellela, M. Venkata Karthik, G. Trividha, L. Chaithanya, and S. Altaf, "To Cite this Article Sai Srinivas Vellela, Manne Venkata Karthik, Golla Trividha, Lingamallu Chaithanya & Shaik Altaf (2025). Intelligent Transportation Systems AI and IoT for Sustainable Urban Traffic Management," *Int. J. Mod. Trends Sci. Technol.*, vol. 11, no. 03, pp. 388–396, 2025.

[17] J. Jin, S. Xing, E. Ji, and W. Liu, "XGate: Explainable Reinforcement Learning for Transparent and Trustworthy API Traffic Management in IoT Sensor Networks," *Sensors*, vol. 25, no. 7, pp. 1–30, 2025, doi: 10.3390/s25072183.

[18] E. Barmpounakis and N. Geroliminis, "On the new era of urban traffic monitoring with massive drone data: The pNEUMA large-scale field experiment," *Transp. Res. Part C Emerg. Technol.*, vol. 111, pp. 50–71, 2020, doi: 10.1016/j.trc.2019.11.023.

[19] L. F. Maimó, Á. Luis, P. Gómez, F. J. G. Clemente, M. G. I. L. Pérez, and G. M. Pérez, "A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks," vol. 6, 2020, doi: 10.1109/ACCESS.2018.2803446.

[20] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A Machine Learning Security Framework for Iot Systems," *IEEE Access*, vol. 8, pp. 114066–114077, 2020, doi: 10.1109/ACCESS.2020.2996214.

[21] S. Zavrak and M. Iskefiyeli, "Anomaly-Based Intrusion Detection from Network Flow Features Using Variational Autoencoder," *IEEE Access*, vol. 8, pp. 108346–108358, 2020, doi: 10.1109/ACCESS.2020.3001350.

[22] F. Faisal, S. K. Das, A. H. Siddique, M. Hasan, S. Sabrin, and C. A. Hossain, "Automated Traffic Detection System Based on Image Processing | Journal of Computer Science and Technology Studies," 2020.