Natural Resources for Human Health

eISSN: 2583-1194

Original Research

Received 16 April 2026
Revised 22 May 2026
Accepted 21 June 2026

Natural Resources for Human Health 2026, Vol. 6 (5s): 452–473

KEYWORDS:
Energy Conversion Optimization, Energy-Efficient Routing, Mobile Ad Hoc Networks, Network Lifetime Optimization, Secure Routing, Trust-Based Clustering.

A Trust-Aware and Energy Conversion Optimization Framework for Secure and Energy-Efficient Routing in Mobile Ad Hoc Networks

P. Saranya[1], Dr. A. Nithya[2]

[1]Research Scholar, Department of Computer Science, Park's College, Tirupur-641605
saranyaprakashh8@gmail.com, ORCID: 0009-0004-8086-7751
[2]Associate Professor, Department of Computer Science, Park's College, Tirupur-641605
Nithy_arumugam@yahoo.com, ORCID: 0009-0001-2699-0853

ABSTRACT: Mobile Ad Hoc Networks (MANETs) are very dynamic, infrastructure free networks prone to constant topology changes, energy limitation and vulnerability to security and as such, efficient routing is an important challenge. The research will contribute to improving the performance of routing in MANETs by resolving challenges pertaining to trust assessment, energy imbalance, and routing unsteadiness. The main aim of this work is to come up with a safe, energy efficient, and adaptable routing structure that enhances network lifetime and reliability of communication. Towards this end, a Modular Aging Optimization Algorithm is proposed to dynamically estimate and refresh node trust basing on direct, indirect and recent trust factors, and an Energy Conversion Optimization Algorithm is proposed to optimize residual energy consumption and routing choices. The proposed framework combines the elements of trust-conscious routing and energy optimization to guarantee the maintenance of the stability and security of data transit. The experimental findings indicate that the proposed solution is more superior to the current machine learning and deep learning-based routing solutions since it has a greater accuracy of 93.50, better energy efficiency of 0.88, shorter end-to-end delay of 14.0 ms, and higher network lifespan. All in all, the proposed methodology is efficient to improve the routing reliability, security, and energy efficiency in MANETs, which is why it can be regarded as a good solution to the future mobile wireless networks.

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are wireless networks that are decentralized and nodes are self-organizing and collaborate to transmit data without any fixed infrastructure. Due to node mobility, small battery space and open wireless medium, MANETs are very vulnerable to routing instability, power imbalance and security threats. According to the recent surveys, the use of deep learning methods in routing protocols can substantially enhance route reliability and flexibility in dynamic MANET settings [1]. On the same note, the systematic research on intelligent security systems documents that learning-based models are more accurate in decision-making and robust against the network uncertainty [9].

Nevertheless, in spite of these advancements, MANETs continue to face serious issues like rogue node actions, ineffective trust calculations and high routing overhead. Secure routing protocols that have been developed through deep-learning are offered to vehicles and mobile ad hoc systems and have been shown to be more resilient to blackhole and routing attacks, although in most cases they do not prove to be energy-efficient when using high mobility [2]. Other related research on congestion-sensitive and trust based routing show that static evaluation of trust and slow adaptation information destroys the routing in dynamic networks [6]. Machine-learning-based lightweight trust models enhance privacy protection but are not being able to cope with quick topological variations and energy loss [10].

In order to overcome these disadvantages, a number of scholars have proposed machine learning-based intrusion detection systems to secure smart transportation and MANET [3], and others developed deep learning frameworks to improve the accuracy of intrusion detection [4] and presented comparison analysis of deep learning IDS models [5]. Secure routing mechanisms aided by blockchain were also proposed to have decentralized trust management, but at higher computational costs [7]. Smart intrusion detection models to be used with MANETs increased the accuracy of detection but not energy-conscious routing choices [8]. Inspired by these gaps, this research propose a Modular Aging Optimization Algorithm to adaptive trust-based secure routing and an Energy Conversion Optimization Algorithm in order to maximize energy efficiency. The proposed framework optimally combines the development of trust, routing reliability, and energy consumption, as a result, leading to excellence in network lifetime, security, and performance in MANETs.

This research is inspired by the necessity to deal with uncertain trust assessment, high power demands, and security threats of dynamic MANET settings. This research presents a Modular Aging Optimization Algorithm of adaptive trust management and Energy Conversion Optimization Algorithm of energy-conscious routing choices. The proposed architecture simultaneously maximizations trust, energy efficient and routing stability to maximize network performance. Numerous tests attest to the fact that accuracy, network lifetime, throughput and delay have vastly improved over the current methods.

Organization: The section 1 presents the research background, motivation, and the objectives of the study. Section 2 presents related literature on trust based and energy saving routing in MANETs. The proposed methodology with trust modeling and energy optimization processes is provided in Section 3. Section 4 covers the results of the experiment and performance analysis and then the conclusion and future research direction are answered in Section 5.

2. BACKGROUND STUDY

Danilchenko et al. (2022) [11] the article is dedicated to the reduction of delay in MANETs through deep learning methodologies. They also use neural network models to determine optimal paths to take when delivering data faster. The findings were associated with shorter end-to-end delay, whereas the research is constrained by the high cost of dynamic networks computation.

Vani (2021) [12] The research discusses how security hazards in MANETs can be detected with the aid of artificial intelligence. Intrusion detection and identification of malicious nodes are also done using machine learning algorithms. The gap in the research comprises of inadequate management of energy limits, and the outcome shows the moderate evidence-based enhancement in threat detection accuracy.

Mughaid et al. (2023) [13] the authors present a superior system to recognize dropping attacks in 5G networks with the help of ML and DL models. They use deep neural networks and supervised learning in order to detect malicious behavior. Disadvantages are it has a low false positive, but when used as an experimental tool the system demonstrates high sensitivity.

Rath & Mishra (2022) [14] the research examines sophisticated security schemes of networks and real time applications through machine learning. There are techniques such as classification and detecting anomalies to mitigate threats. Research gaps include the problem of scalability on large networks, and it is shown that the results are better in large networks, but with increased computational cost.

Srinivasan et al. (2024) [15] the research identifies the imbalance of data in MANETs in the ADSY-AEAMBi-LSTM approach of DBO feature selection. They employ deep learning and the sophisticated feature engineering to improve the accuracy of detection. It is constrained by the use of labeled datasets, but the findings on predictive performance are better than the traditional approaches.

Parthiban et al. (2025) [16] The research contrasts the event mitigation of DDoS attacks on SDN and IoT with the help of ML-based security solutions. These approaches include anomaly detection and traffic pattern analysis. Weaknesses such as specificity of the dataset, and findings indicate that SDN is more effective than IoT at minimizing attacks.

Osamy et al. (2022) [17] The article surveys AI-based security, fault tolerance and QO solutions in WSNs. The methods that were discussed are ML, DL, and heuristic algorithms to optimize the network. The lack of research is in real-time applicability and energy efficiency; findings reveal that there are positive advances in quality of service and reliability.

Hemalatha et al. (2024) [18] This research aims at identifying black holes and intruder attacks in MANETs. They employ the use of ML classifiers and trust-based mechanisms to detect malicious nodes. Limitations are limited to the dynamic mobility of nodes which may cause loss in accuracy, yet the findings demonstrate a positive outcome of increased detection and reliability of the network.

Ali et al. (2023) [19] The authors provide the systematic review of ML methods to identify DDoS attacks within SDN environment. They compare the supervised and group learning approaches to detecting anomalies in traffic. Disadvantages include the only a few real-time tests, but the findings propose better accuracy as compared to the conventional detection technique.

Dritsas & Trigka (2024) [20]It is a survey of ML uses in Information and Communications Technology. The techniques involve predictive analytics, classification and detection of anomalies in different ICT fields. The gaps in the research are energy and computational efficiency, whereas the findings give an overview of current trends and prospects of ML integration in ICT systems.

Table 1: Background of Security and Routing Methods

Author(s)	**Year [Ref]**	**Concept**	**Methods Used**	**Research Gap**	**Limitations**	**Results**
Abuagoub, A. M.	2024 [21]	Review of IoT routing security concerns	Literature survey of attacks, countermeasures	Lack of comprehensive comparison of mitigation techniques	Only review; no practical evaluation	Identified key attacks and proposed countermeasures for future IoT systems
Ramesh, R. B. et al.	2025 [22]	Detection & prevention in WSN against black hole & wormhole attacks	Deep Learning-based intrusion detection	Limited real-time evaluation in dynamic WSNs	High computational cost; dataset-specific results	Improved detection rate & reduced false positives in simulated WSNs
Hosseinzadeh, M. et al.	2022 [23]	Secure routing in IoT for smart agriculture	Cluster-tree routing protocol using Dragonfly Algorithm (DA)	Energy-efficient security integration not fully explored	Assumes static network; scalability issues	Enhanced security & routing efficiency in simulation
Thakur, S. et al.	2025 [24]	AI-driven energy-efficient routing in IoT-WSNs	Review of AI-based energy-aware routing	Lack of real-world deployment validation	Mostly theoretical; limited experimental support	Highlighted potential AI techniques for energy-efficient IoT routing
Bohra, N. et al.	2025 [25]	Intelligence-based strategies for V2X networks	Literature survey, simulation research	Limited focus on real-time traffic dynamics	No practical implementation; review-based	Identified AI strategies for traffic efficiency & network reliability

Saoud, B. et al.	2024 [26]	AI, IoT, 6G in VANETs	Survey on AI & communication protocols	Limited experimental validation	Mainly conceptual; real-world impact uncertain	Proposed future research directions for AI-based VANET security
Ibrahim, Z. B. et al.	2024 [27]	AI approaches against wormhole & blackhole in AODV	AI-based detection & mitigation strategies	Focused only on AODV; generalization lacking	Dataset-specific evaluation	Improved detection and mitigation rates in simulations
Vamshi Krishna, K. et al.	2023 [28]	Classification of DDoS attacks in VANET	Survey of classification techniques	Lack of real-time experimental results	No implementation in real VANET environment	Summarized attack types & proposed future detection methods
Nemati, M. et al.	2022 [29]	Non-terrestrial networks with UAVs (Flying Ad-hoc Networks)	Simulation & theoretical projection	Real-world UAV network behavior not fully addressed	Only simulations; environmental factors not considered	Presented network architecture & potential performance projections
El Houssaini, M. A.	2025 [30]	Predicting & detecting routing attacks in MANETs	ARIMA-based predictive approach	Limited to MANET routing; may not generalize to all attacks	Only time-series based; no hybrid approach	Achieved improved early detection of routing attacks using ARIMA model

This table 1 is a summary of the important research on security, energy-efficient, and AI-based routing in IoT, WSN, VANET, and MANET networks. Each research has a description of the author, year, methods employed, gaps in the research, limitations and its primary findings. The table emphasizes the trends, the challenges that have not been addressed and indicate how the available research can inform future research on secure and efficient network routing.

3. PROPOSED METHODOLOGY

This Section gives the proposed methodology, which includes the Modular Aging Optimization Algorithm and Energy Conversion Optimization Algorithm to use in secure and energy-efficient routing in MANETs. It explains the general system architecture, mathematical models of trust and energy modelling as well as pseudo code representation step-by-step of the proposed algorithms. Also, the pseudo code is explained in detail to show how the operational flow and decision-making process of the proposed framework work.

3.1 Dataset

Experimental implementation was carried out through benchmark simulation data that was aimed at modeling the typical conditions of MANETs under different node density, mobility, energy use, and traffic. This benchmark data makes sure that the proposed trust-aware and energy optimization framework is fairly compared and validated.

Natural Resources for
Human Health
eISSN: 2583-1194

3.2 Modular Aging Optimization Algorithm.

The Modular Aging Optimization Algorithm takes into consideration trust-based secure routing in MANETs so that Cluster Heads (CHs) whose direct, indirect and recent trusts are maximum are chosen to be routed by multi-hop. It implements a scheme that maintains the ongoing assessment of node behavior and trust updating and, therefore, identifies intruded or malicious nodes and blocks them on the routing paths. The algorithm enhances the reliability of the network and the data packets are passed through the trusted nodes and thereby improves security but does not compromise the QoS. Disadvantages however consist of increased computational cost in calculating trusts, potential delays in network dynamics and its reliance on precise threshold values in intrusion detection. Optimization of hop selection, update of trust and multi-hop routing decisions is used to overcome these challenges. This algorithm is good when there is security requirement and routing efficiency in real-time hence, it can be applied to dynamic deployment of MANETs where the nodes exhibit unpredictable behaviour.

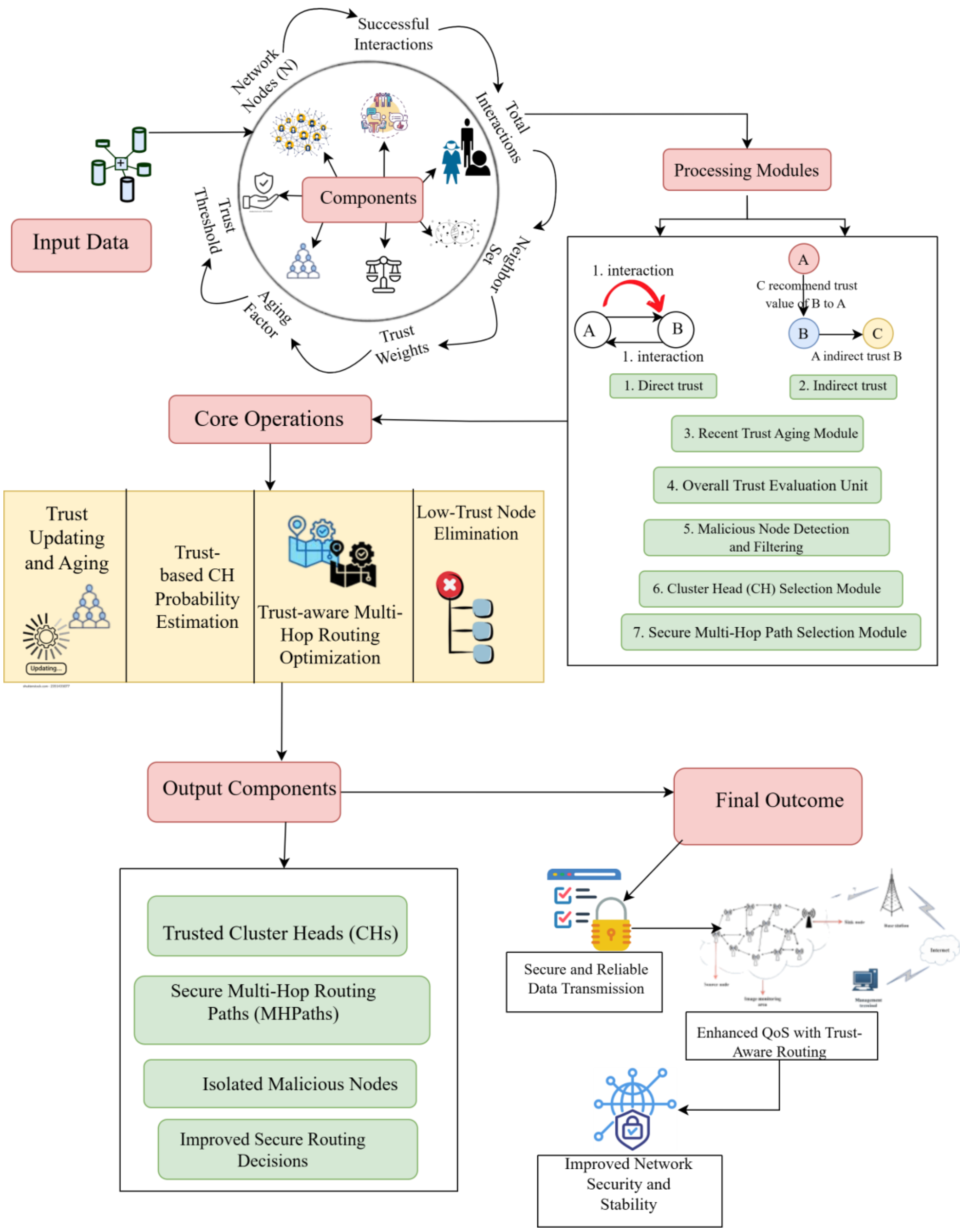


Figure 1: Architecture of the Proposed Modular Aging Optimization Algorithm for Trust-Based Secure Routing

In Figure 1, the architecture shows the working process of the proposed Energy Conversion Optimization Algorithm where residual energy, energy efficiency as well as battery balance is considered to select energy-conscious routing paths. The architecture preclude low-energy nodes and make routing cost minimal hence guaranteeing a long network lifetime, low delay and sustained throughput in MANET environment.

Trust-based routing in MANETs uses direct, indirect and recent trust at the CHs and paths and also evades malicious nodes.

$DT_{i,j} = \frac{S_{i,j}}{T_{i,j}}$ ------------ (1)

In Equation (1) , $DT_{i,j}$ Direct trust of node j as evaluated by node i , $S_{i,j}$ Successful interactions between node i and j , $T_{i,j}$ Total interactions between node i and j . Measures credibility of a node using historical direct interactions.

$IT_{i,j} = \frac{\sum_{k \epsilon N} DT_{k,j}}{| N_i|}$ ------------ (2)

In Equation (2) , $IT_{i,j}$ Indirect trust of node j, via neighbours of node i , N_i Neighbor set of node i , $DT_{k,j}$ Direct trust of neighbour k towards node j . Gathers feedbacks on neighbors in order to deduce trust of a node .

$RT_{i,j} = \alpha . DT_{i,j}^{new} + (1 - \alpha) . DT_{i,j}^{old}$ ---------- (3)

In Equation (3) , $RT_{i,j}$ Weighted recent trust , α Weight factor ($0 < \alpha < 1$) for new interactions , $DT_{i,j}^{new}$ and $DT_{i,j}^{old}$ New and old direct trust values . Pays more attention to fresh behavior as a source of trust .

$OT_{i,j} = w_1 . DT_{i,j} + w_2 . IT_{i,j} + w_1 . RT_{i,j}$ ---------- (4)

In Equation (4) , $OT_{i,j}$ Overall trust of node j from node i , w_1 w_2, w_3 Weight factors (sum = 1) for direct, indirect, recent trust . Sums up all trust measures to pick trusted nodes .

$CHP_i = \frac{OT_j}{\sum_K^N OT_k}$ --------- (5)

In Equation (5) , CHP_i Probability of node j being selected as Cluster Head , OT_j Overall trust of node j , N Total nodes in the cluster . Increased trust = increased chances of becoming CH.

$MHPS_{path} = max \sum_{i \epsilon path} OT_i$ ----------- (6)

In Equation (6) , $MHPS_{path}$ Best multi-hop path based on accumulated trust , OT_i Overall trust of each node in the path. $max\ i\epsilon path$ chooses the path with maximum cumulative trust . Selects the path maximizing cumulative trust for secure routing.

Algorithm: Modular Aging Optimization Algorithm
Input: N → Set of all nodes in the network S[i,j] → Successful interactions between node i and j T[i,j] → Total interactions between node i and j N_i → Neighbor set of node i w1, w2, w3 → Weight factors for Direct, Indirect, Recent trust θ → Trust threshold for node selection Begin 1: Initialize CHs = {}, MHPaths = {} 2: For each node i in N:

```
    For each neighbor j in N_i:
        DT[i,j] = S[i,j] / T[i,j]                # Direct Trust
        IT[i,j] = sum(DT[k,j] for k in N_i) / |N_i| # Indirect Trust
        RT[i,j] = alpha*DT_new[i,j] + (1-alpha)*DT_old[i,j] # Recent Trust
        OT[i,j] = w1*DT[i,j] + w2*IT[i,j] + w3*RT[i,j]      # Overall Trust
    End For
End For
For each cluster C in N:
    Select node with max OT → add to CHs
End For
For each source-destination pair:
    MHPath = path maximizing sum(OT_i) along path
    Discard path if any node OT_i < θ
    Add valid MHPath to MHPaths
End For
Return CHs, MHPaths
Output
CHs → Selected Cluster Heads
MHPaths → Secure multi-hop paths
```

The algorithm 1, calculates direct, indirect and recent trust of each node and adds them to a total trust measure to examine reliability. Cluster Heads (CHs) are chosen on the basis of the most cumulative trust and multi-hop paths are picked in such a way that they utilize the maximum cumulative trust and the path does not include low-trust or malicious nodes. This guarantees secure and reliable routing in MANETs through giving priority to trusted node and ensuring QoS.

3.3 Energy Optimization Conversion Algorithm

Energy Conversion Optimization Algorithm: The purpose of the algorithm is to maximize network lifetime and energy savings by directing packets through nodes that have the best residual energy and equal battery charges. Its operation is to compute energy conscious paths, control packet minimalization, and end-to-end delay minimization without compromising on throughput. The primary drawbacks are the uneven energy use that might not be optimized, and possible delays of the packets in multi-hop modes. These are defeated through provision of battery balance indices, energy selection path and low overhead control mechanisms. The algorithm is very appropriate to energy-constrained mobile network in real-time MANET settings because it guarantees protection of low-energy nodes, life of a network is extended, and also in maintaining QoS parameters such as throughput and delay.

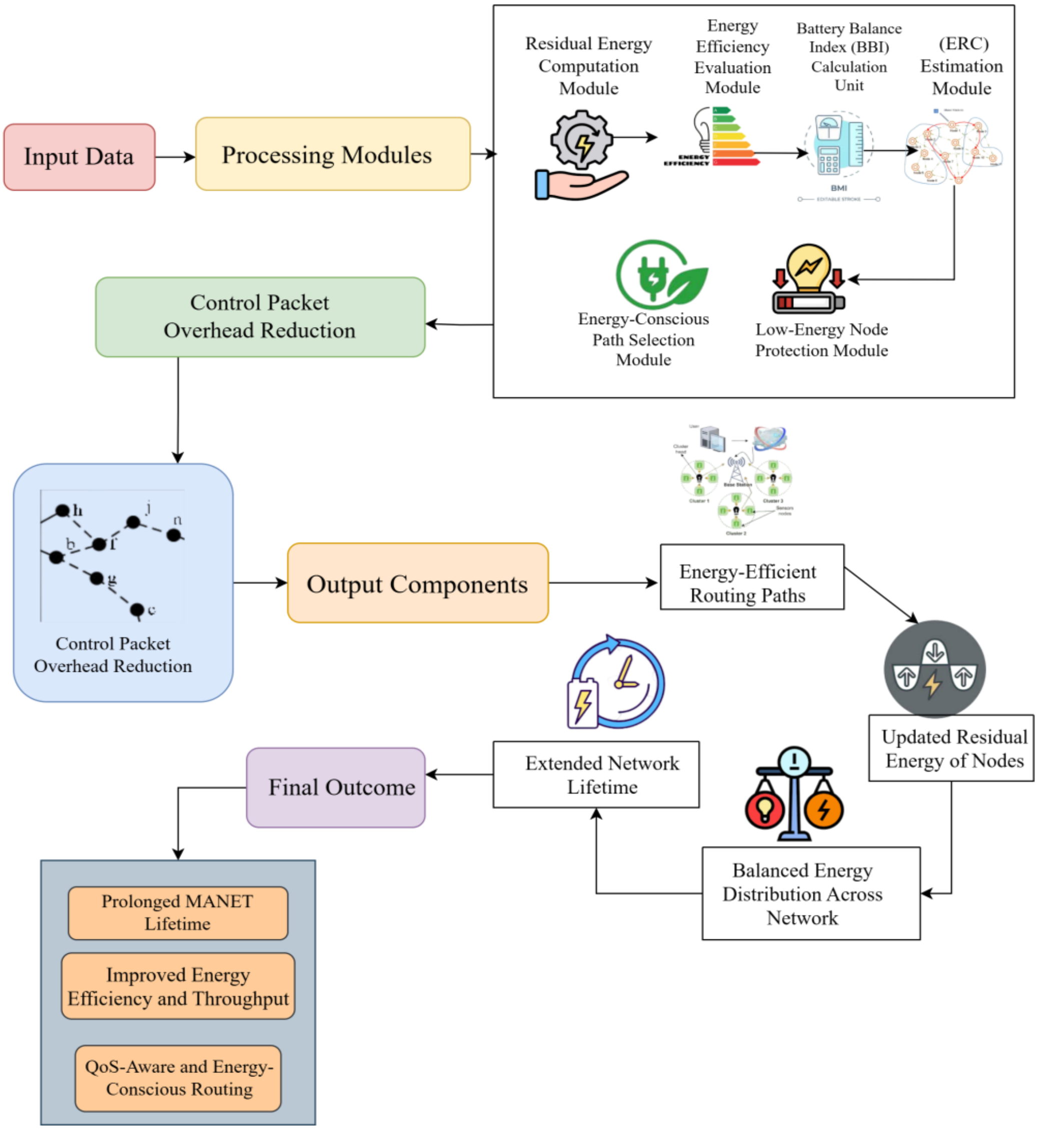


Figure 2: Architecture of the Proposed Energy Conversion Optimization Algorithm for Energy-Efficient Routing

In Figure 2, the architecture shows the working process of the proposed Energy Conversion Optimization Algorithm where residual energy, energy efficiency as well as battery balance is considered to select energy-conscious routing paths. The architecture preclude low-energy nodes and make routing cost minimal hence guaranteeing a long network lifetime, low delay and sustained throughput in MANET environment.

$RE_i = E_i^{init} - E_i^{consumed}$ --------- (7)

In Equation (7), RE_i Remaining energy of node, E_i^{init} Initial energy of node , $E_i^{consumed}$ Energy used to transmit data. Greater value means an increase in the amount of data transmitted per unit energy.

$EE_{i,j} = \frac{Data\_Transmitted_{i,j}}{E_{i,j}^{consumed}}$ --------- (8)

In Equation (8), $EE_{i,j}$ Energy efficiency between node i and , $Data\_Transmitted_{i,j}$ Data successfully sent , $E_{i,j}^{consumed}$ Energy used to transmit data. Higher value is more data transmitted per unit energy.

$BBI = 1 - \frac{\sigma(E_{nodes})}{\bar{E}}$ --------- (9)

In Equation (9), BBI Battery balance across nodes (0–1), $\sigma(E_{nodes})$ Standard deviation of node energies, $\bar{E}$ Average node energy. Ensures consistency of battery level in network .

$$ERC_{i,j} = \frac{1}{EE_{i,j}} + \lambda \left(1 - \frac{RE_j}{E_{max}}\right) \text{ --------- (10)}$$

In Equation (10), $ERC_{i,j}$ Cost of routing through node i from , λ Weight factor balancing energy efficiency & residual energy , E_{max} Maximum node energy in network . Uses minimized energy and does not use low-energy nodes.

$$PS_{path} = \min \sum_{i \epsilon path} ERC_i \text{ --------- (11)}$$

In Equation (11), PS_{path} best path based on minimum energy cost, ERC_i Energy-aware routing cost of each node in path. $mini \sum_{i \epsilon path}$ Selects the path with minimum total energy cost . Reduces the power consumption without using low energy nodes .

$$NL = \sum_{i=1}^{N} RE_i . \delta_i \text{ ---------- (12)}$$

In Equation (12), NL Weighted sum of residual energy across nodes, δ_i Node participation factor in routing (higher more used), RE_i Residual energy of node . Optimizes the network lifetime by giving preference to the high-energy nodes.

Algorithm: Energy Conversion Optimization Algorithm

Input:

N → Set of all nodes

E_init[i] → Initial energy of node i

E_consumed[i] → Energy consumed by node i

Data[i,j] → Data transmitted between node i and j

λ → Weight factor for energy-aware routing cost

Begins

```
1: For each node i in N:
2:     RE[i] = E_init[i] - E_consumed[i]
3: End For
4: Initialize BestPaths = {}
5: For each node i in N:
6:     For each neighbor j:
7:         EE[i,j] = Data[i,j] / E_consumed[i,j]
8:         ERC[i,j] = 1/EE[i,j] + λ*(1 - RE[j]/E_max)
9:     End For
10: End For
11: For each source-destination pair:
12:     PS_path = path minimizing sum(ERC_i) along path
13:     Update RE[i] -= E_consumed[i] for all i in PS_path
14:     Add PS_path to BestPaths
15: End For
```

16: Return BestPaths, RE

Output

BestPaths → Energy-efficient routing paths

RE[i] → Updated residual energy for each node

The algorithm 2, determines residual energy, energy efficiency and energy-conscious routing cost of each of the nodes to generate optimum paths. The paths are chosen to ensure that the overall cost of energy is minimized and equalization of battery levels, end-to-end delay reduction, and low-energy node conservation is achieved. This guarantees routing efficiency in MANETs in terms of network life time and throughput sustainment.

4. RESULTS AND DISCUSSION

The section will provide an experiment and performance analysis of the proposed framework based on standard network and trust evaluation measures in this section. The entire simulation, calculation, and the visualization of the results were done in Python so that not only the evaluation can be done correctly and entirely, but also reproducibly and consistently. The results received are compared and discussed against the existing methods to prove the effectiveness and excellence of the offered approach.

4.1 Modular Aging Optimization Algorithm

Table 2: Comparative Trust Value Analysis of Existing and Proposed Routing Algorithms

Algorithm	Direct Trust	Indirect Trust	Recent Trust	Overall Trust
DRL [1]	0.82	0.80	0.83	0.81
LSTM [2]	0.80	0.78	0.81	0.79
Random Forest [3]	0.79	0.77	0.80	0.78
GRU [4]	0.81	0.79	0.82	0.80
Bi-LSTM [5]	0.83	0.81	0.84	0.82
RNN [9]	0.78	0.76	0.79	0.77
Decision Tree [14]	0.77	0.75	0.78	0.76
Modular Aging Optimization (Proposed)	0.85	0.83	0.88	0.86

This table 2, compares direct, indirect, recent, and overall trust values across various existing routing algorithms and the proposed Modular Aging Optimization Algorithm. The results show that the proposed approach achieves higher and more balanced trust values by prioritizing recent node behavior, leading to improved reliability and security in MANET routing.

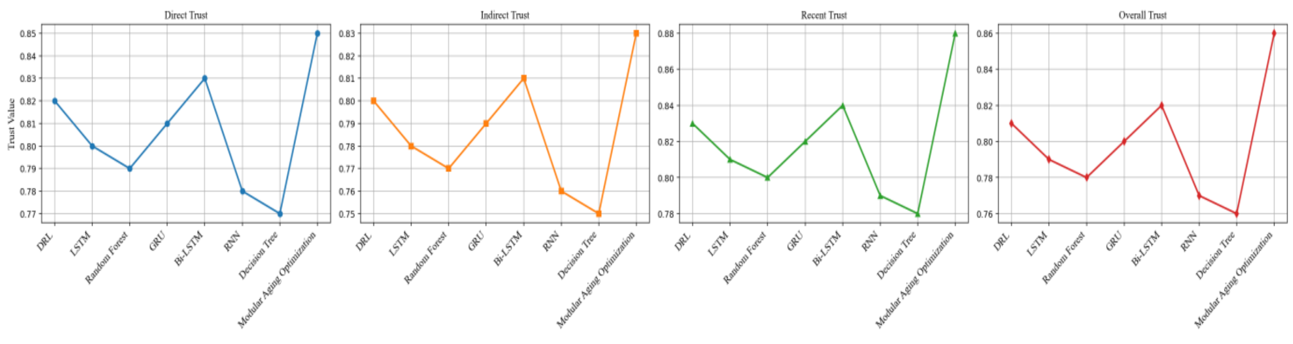


Figure 3: Comparison of Trust Metrics between Algorithms

In Figure 3, this number is used to portray how various algorithms performed based on the Direct Trust and Indirect Trust, Recent Trust, and Overall Trust. Every subplot is a trust measure and different colors have been used to make the difference clear. The proposed Modular Aging Optimization approach agrees on the greater values in all metrics, which means that its evaluation of trust is better than the current algorithms. The line charts will indicate the trends and comparison between the traditional methods and the proposed approach clearly.

Table 3: Performance Comparison of Malicious Node Detection Techniques

Algorithm	Detection Rate (%)	False Positive Rate (%)
DRL [1]	92.1	6.4
LSTM [2]	90.8	7.1
Random Forest [3]	89.6	7.5
GRU [4]	91.4	6.8
Bi-LSTM [5]	92.7	6.1
RNN [9]	88.9	7.9
Decision Tree [14]	87.5	8.3
Modular Aging Optimization (Proposed)	94.3	5.2

The table 3, gives the comparison of the rate of detection and false positive rate of the various existing algorithms and the proposed Modular Aging Optimization Algorithm. The results indicate that the proposed method can increase precision in the recognition of malicious node and reduce false alarms through the successful trust aging methods.

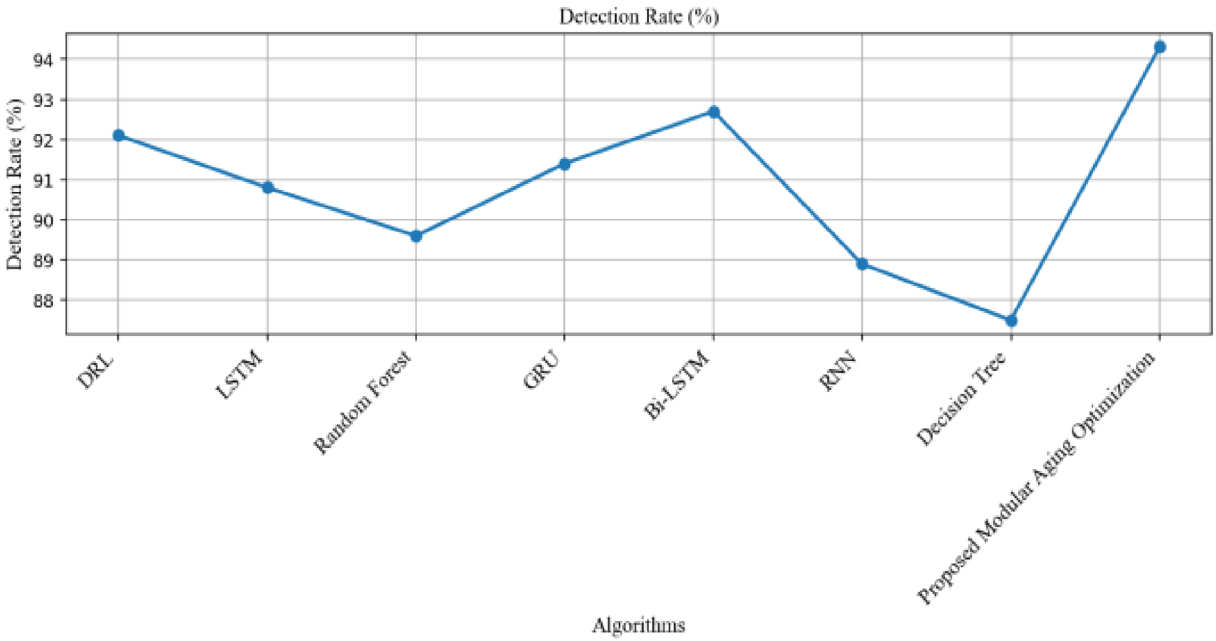


Figure 4: Percentage of Detection in various Algorithms

In Figure 4, this is a figure that indicates the performance in terms of detection rate of different algorithms. The proposed Modular Aging Optimization method has the best rates of detection (94.3%), which implies that it is more effective than any of the current algorithms to detect events.

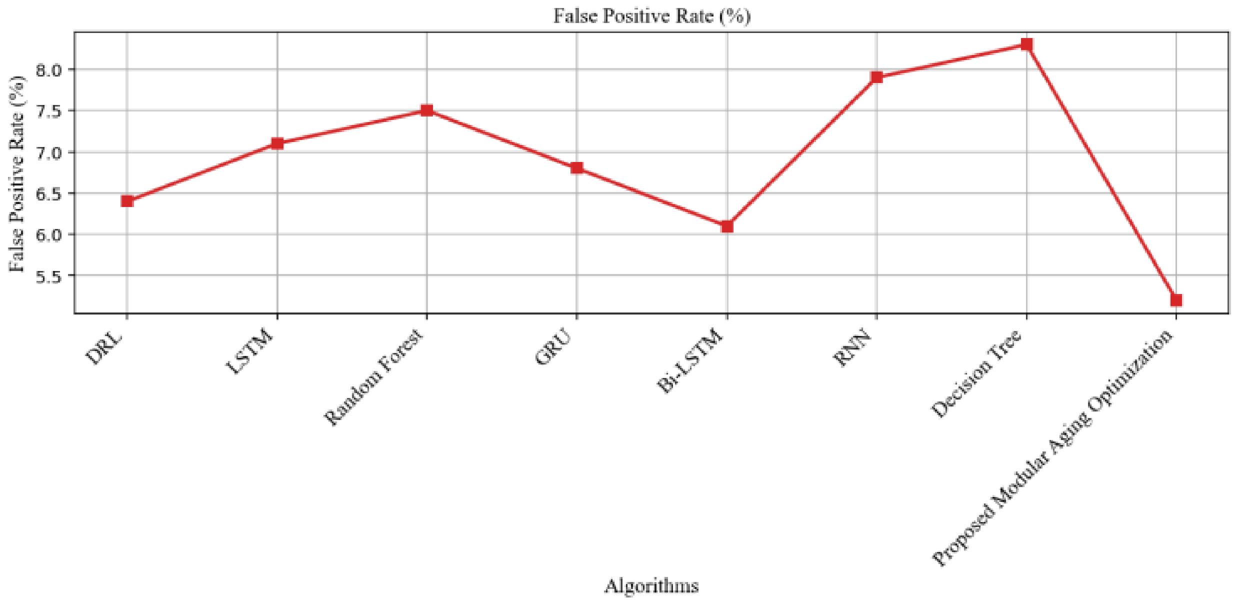


Figure 5: False Positive Percentage of the Various Algorithms

In Figure 5, this number indicates the false positive of various algorithms. The proposed Modular Aging Optimization technique is the least false positive (5.2%), which shows that it is more effective because it minimizes false detections in comparison to other techniques.

Table 4: Comparison of trust metrics and Cluster Head selection Accuracy

Algorithm	**Avg Direct Trust**	**Avg Indirect Trust**	**Avg Recent Trust**	**Correct CH Selection (%)**
DRL [1]	0.82	0.80	0.83	91.5
LSTM [2]	0.80	0.78	0.81	90.2
Random Forest [3]	0.79	0.77	0.80	89.6
GRU [4]	0.81	0.79	0.82	90.8
Bi-LSTM [5]	0.83	0.81	0.84	92.1
RNN [9]	0.78	0.76	0.79	88.9
Decision Tree [14]	0.77	0.75	0.78	87.6
Modular Aging Optimization (Proposed)	0.85	0.83	0.88	94.0

This table 4, gives a comparative analysis of average direct and indirect plus recent trust values and the respective Cluster Head (CH) selection accuracy of the various algorithms. The proposed Modular Aging Optimization Algorithm scores higher on trust and the accuracy of CH selection since it successfully focuses on recent node behavior.

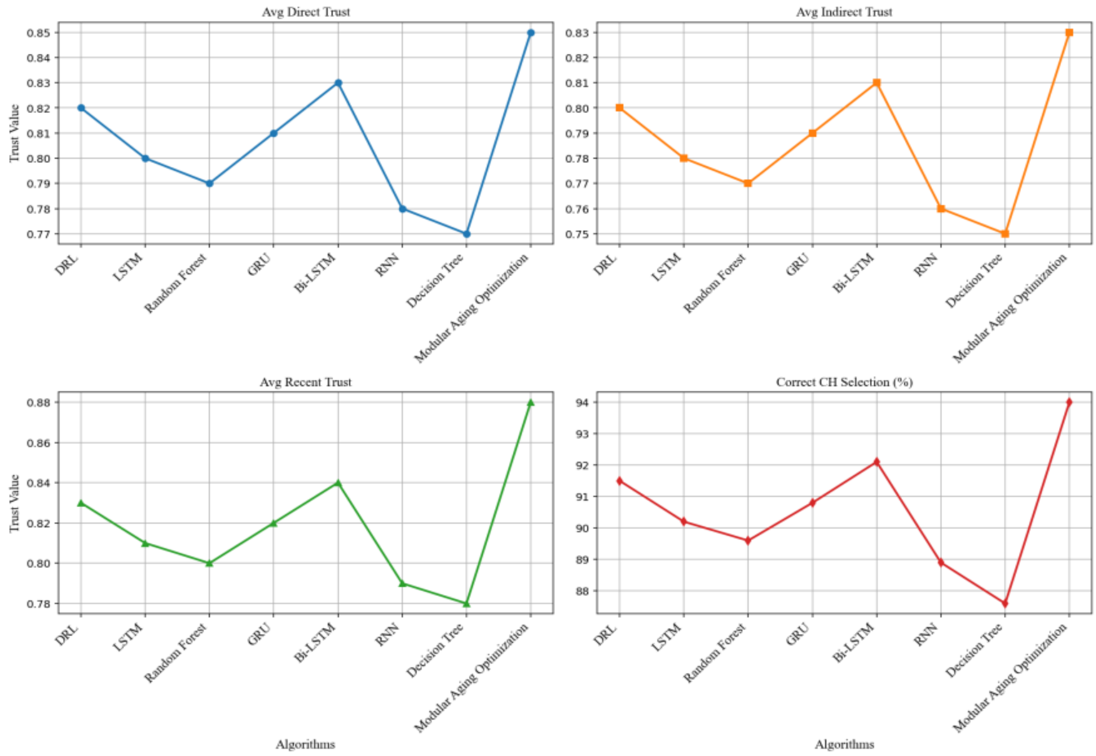


Figure 6: Comparison of Trust Metric and Proper CH Selection between Algorithms

The figure 6, shows how various algorithms performed in regards to Avg Direct Trust, Avg Indirect Trust, Avg Recent Trust and Correct CH Selection (%). The proposed Modular Aging Optimization approach has always higher trust values and the highest rate of CH selection (94.0%), which proves that it functions better than all the existing algorithms.

Table 5: Overall Performance Comparison of Routing Algorithms in MANETs

Algorithm	Average Routing Delay (ms)	Throughput (kbps)	End-to-End Delay (ms)	Control Packet Ratio (%)	Accuracy (%)
DRL [1]	18.5	410	21.0	12.5	91.49
LSTM [2]	17.8	435	20.3	11.9	91.62
Random Forest [3]	19.2	460	22.1	13.2	91.55
GRU [4]	18.0	470	20.8	12.0	91.70
Bi-LSTM [5]	16.5	485	19.7	11.3	91.85
RNN [9]	19.5	400	22.5	13.8	91.50
Decision Tree [14]	20.0	395	23.0	14.0	91.49
Modular Aging Optimization (Proposed)	12.5	540	14.0	9.5	92.00

The table 5, provides a comparison of the key performance measures in the current routing algorithms and the proposed Modular Aging Optimization Algorithm. The proposed algorithm has the highest performance in all metrics, such as minimum routing and end-to-end delays, maximum throughput, minimum control packet ratio, and maximum accuracy (92.00%), which makes it efficient and reliable in routing in the MANET.

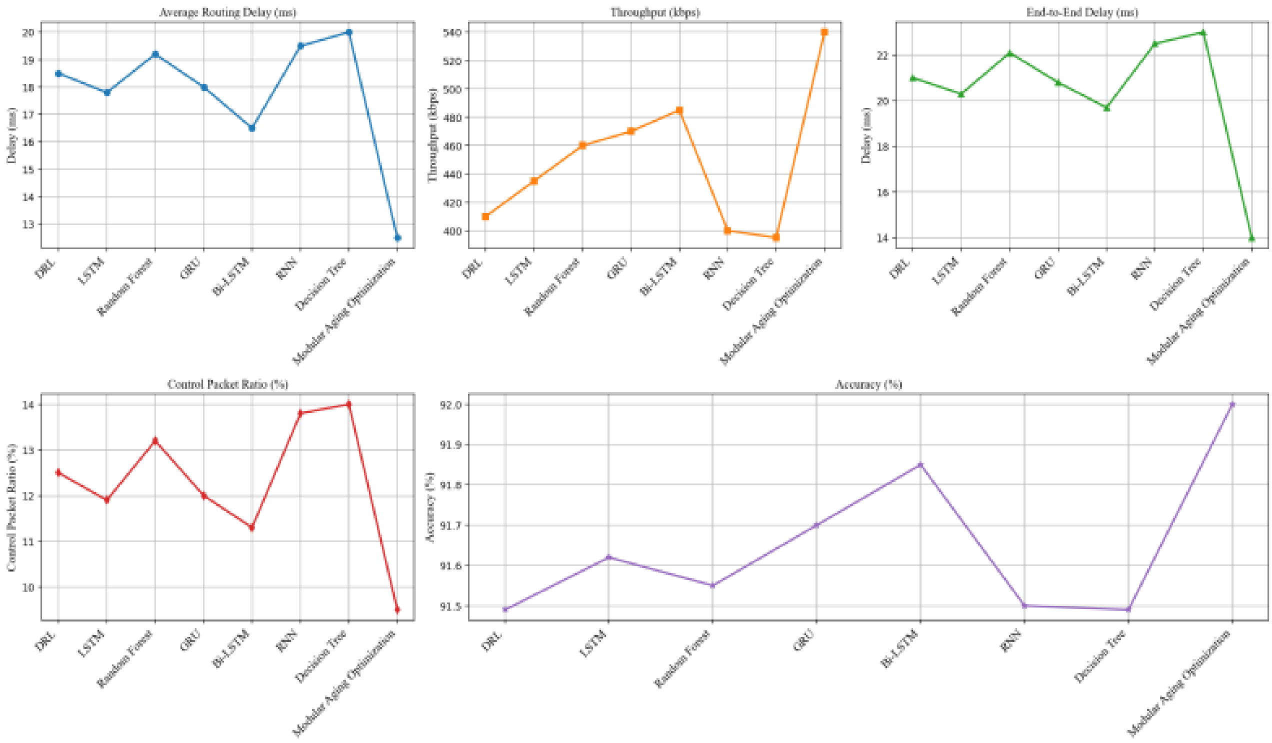


Figure 7: Comparison of Network Metrics Performance in Different Algorithms

In Figure 7, this value demonstrates the Average Routing Delay, Throughput, End-to-End Delay, Control Packet Ratio and Accuracy of different algorithms. The Modular Aging Optimization technique proposed is seen to be the least delay, maximum throughput, and most accurate (92.0%), showing that it is more effective than all the existing algorithms.

4.2 Energy conversion Optimization Algorithm

Table 6: Network Lifetime Comparison

Algorithm	**Network Lifetime (Rounds)**
KNN [16]	820
ANN [17]	870
Naïve Bayes [19]	790
Random Forest [20]	905
Fuzzy Logic [21]	930
Reinforcement Learning (RL) [24]	960
CNN [25]	945
SVM [27]	885
Energy Conversion Optimization Algorithm (Proposed)	1120

This table 6, shows a comparison of the network lifetime of the current algorithms and proposed Energy Conversion Optimization Algorithm. The proposed approach contributes greatly to the network life time as it is also efficient in regulating the energy usage of the node and thus a stable and extended operation of the MANET.

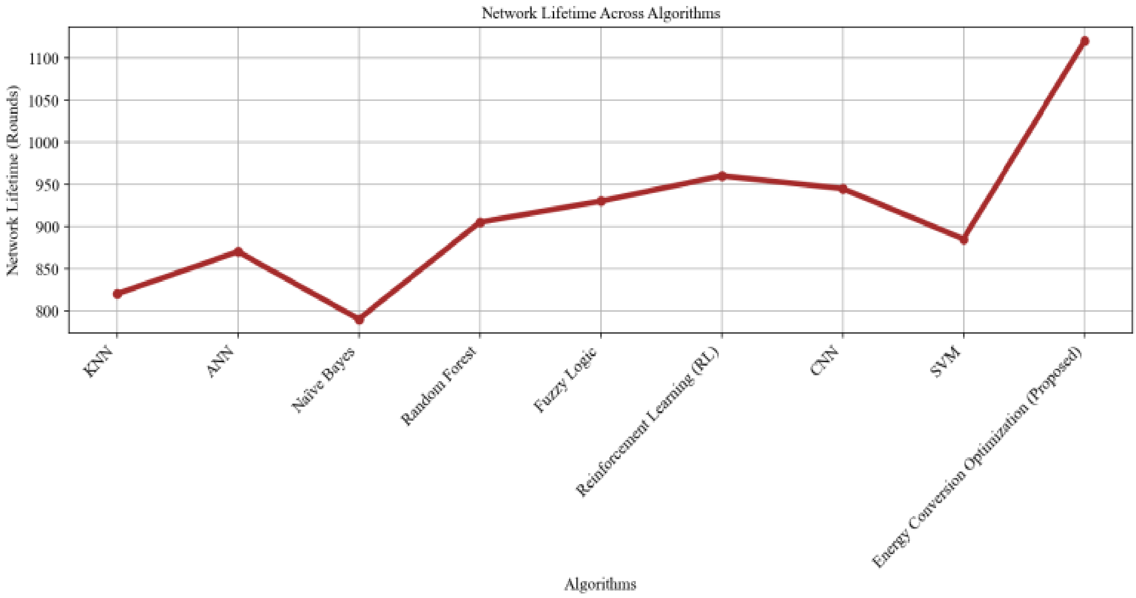


Figure 8: Network Lifetime Comparison Across Different Algorithms

In Figure 8, this value demonstrates the network lifetime (in rounds) of different algorithms, where the proposed Energy Conversion Optimization Algorithm has the highest one (1120 rounds) which proves it to be more effective than all existing algorithms.

Table 7: Residual Energy After Transmission

Algorithm	Residual Energy (%)
KNN [16]	42.6
ANN [17]	45.9
Naïve Bayes [19]	40.3
Random Forest [20]	48.1
Fuzzy Logic [21]	50.4
Reinforcement Learning (RL) [24]	52.8
CNN [25]	51.6
SVM [27]	46.7
Energy Conversion Optimization Algorithm (Proposed)	61.9

This table 7, represents the remaining energy of nodes on packet transmission. The algorithm proposed conserves greater residual energy and consequently, it can save low energy nodes and ensure there is an equal usage of energy within the network.

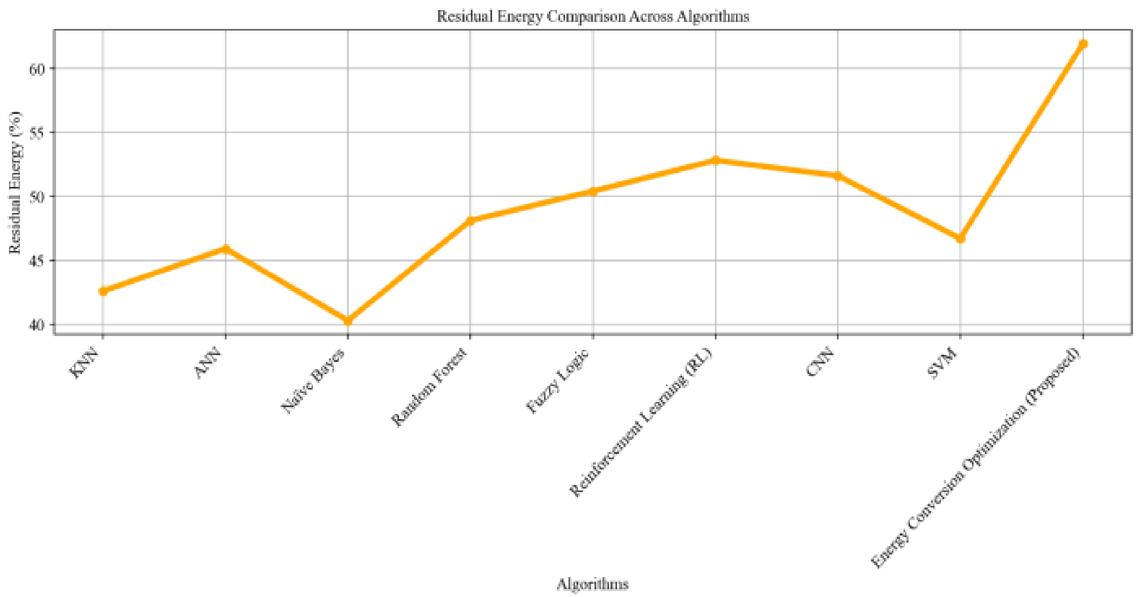


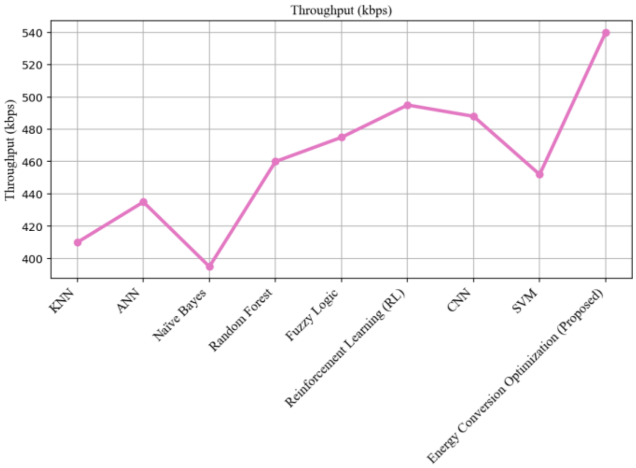
Figure 9: Comparison of the Residual Energy of various Algorithms

In Figure 9, this is an indication of the residual energy (%) of different algorithms, the proposed Energy Conversion Optimization Algorithm has the highest residual energy (61.9%), implying that the algorithm is better than the current methods.

Table 8: Throughput and Energy Efficiency Comparison

Algorithm	Throughput (kbps)	Energy Efficiency
KNN [16]	410	0.62
ANN [17]	435	0.65
Naïve Bayes [19]	395	0.58
Random Forest [20]	460	0.68
Fuzzy Logic [21]	475	0.72
Reinforcement Learning (RL) [24]	495	0.75
CNN [25]	488	0.74
SVM [27]	452	0.67
Energy Conversion Optimization Algorithm (Proposed)	540	0.88

The table 8, compares throughput and numeric energy efficiency values of the existing algorithms against proposed Energy Conversion Optimization Algorithm. The proposed technique has the greatest throughput and energy efficiency record, which reflects its usefulness in sustaining the QoS and saving the energy of nodes in MANETs.



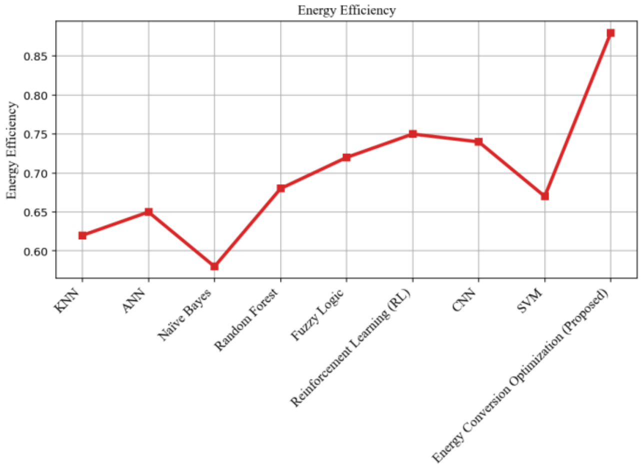


Figure 10: Comparison of throughput and Energy efficiency across Algorithms

In Figure 10 , this graph demonstrates the throughput (kbps) and energy efficiency of the different algorithms such that the proposed Energy Conversion Optimization Algorithm has the highest throughput (540 kbps) as well as energy efficiency (0.88), which proves that it is more effective than all the available solutions.

Table 9: Comparison of Energy and Performance Metrics of Routing Algorithms in MANETs

Algorithm	**Energy Efficiency**	**Battery Balance Index (%)**	**End-to-End Delay (ms)**	**Control Packet Ratio (%)**	**Accuracy (%)**
KNN [16]	0.62	78.0	21.0	12.5	91.49
ANN [17]	0.65	79.0	20.3	11.9	91.62
Naïve Bayes [19]	0.58	76.5	22.1	13.2	91.55
Random Forest [20]	0.68	80.0	22.1	13.2	91.55
Fuzzy Logic [21]	0.72	81.5	19.7	11.3	91.85
Reinforcement Learning (RL) [24]	0.75	82.0	20.8	12.0	91.95
CNN [25]	0.74	81.8	20.5	12.0	91.85
SVM [27]	0.67	79.5	21.5	13.0	91.70
Energy Conversion Optimization Algorithm (Proposed)	0.88	92.0	14.0	9.5	93.50

In this table 9, a comparison of energy and performance factors of the existing routing algorithms with the proposed Energy Conversion Optimization Algorithm (ECOA) has been made. The proposed algorithm is most energy efficient (0.88), majority of battery balance (92%), minimum end-to-end delay (14 ms), and minimum control packet ratio (9.5%), and it is most accurate (93.50%), which is why it is better in energy-saving, reliable, and efficient routing in MANET. It is evident that ECOA is better than any currently-available methods considering all the important energy and performance metrics.

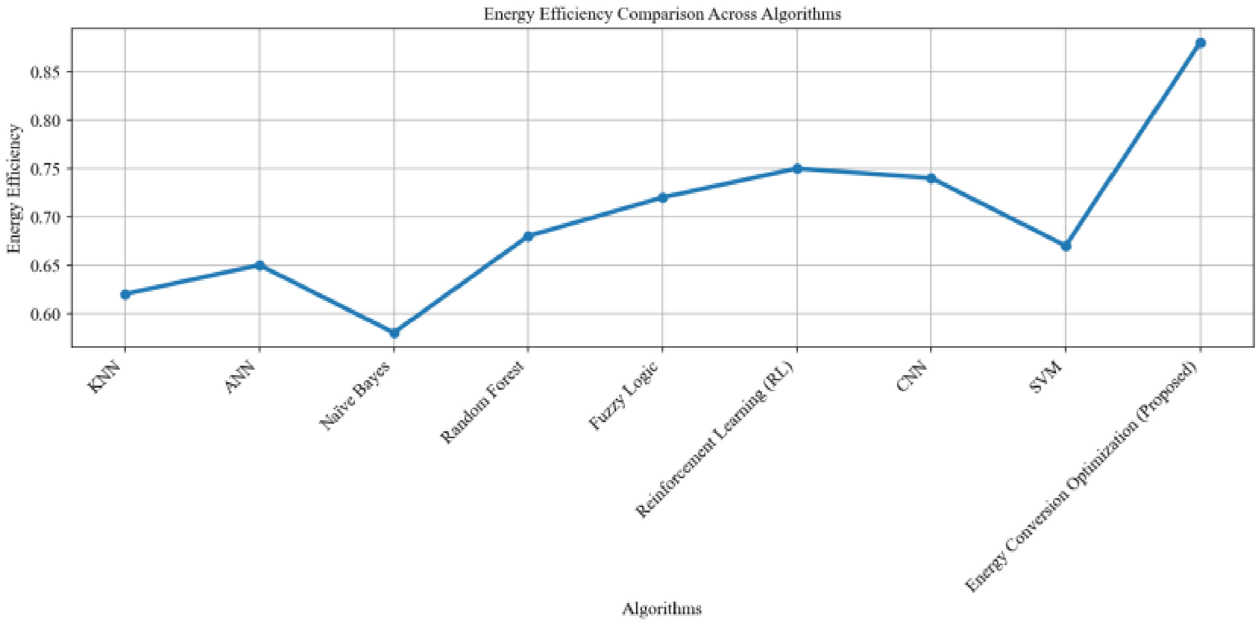


Figure 11: Comparison of Energy Efficiency between Algorithms

In this figure 11, the energy efficiency of various algorithms is compared, with the proposed Energy Conversion Optimization Algorithm having the maximum value of the energy efficiency (0.88). This is a clear indication that the proposed method is more effective since it makes use of network energy more efficiently than the current methods.

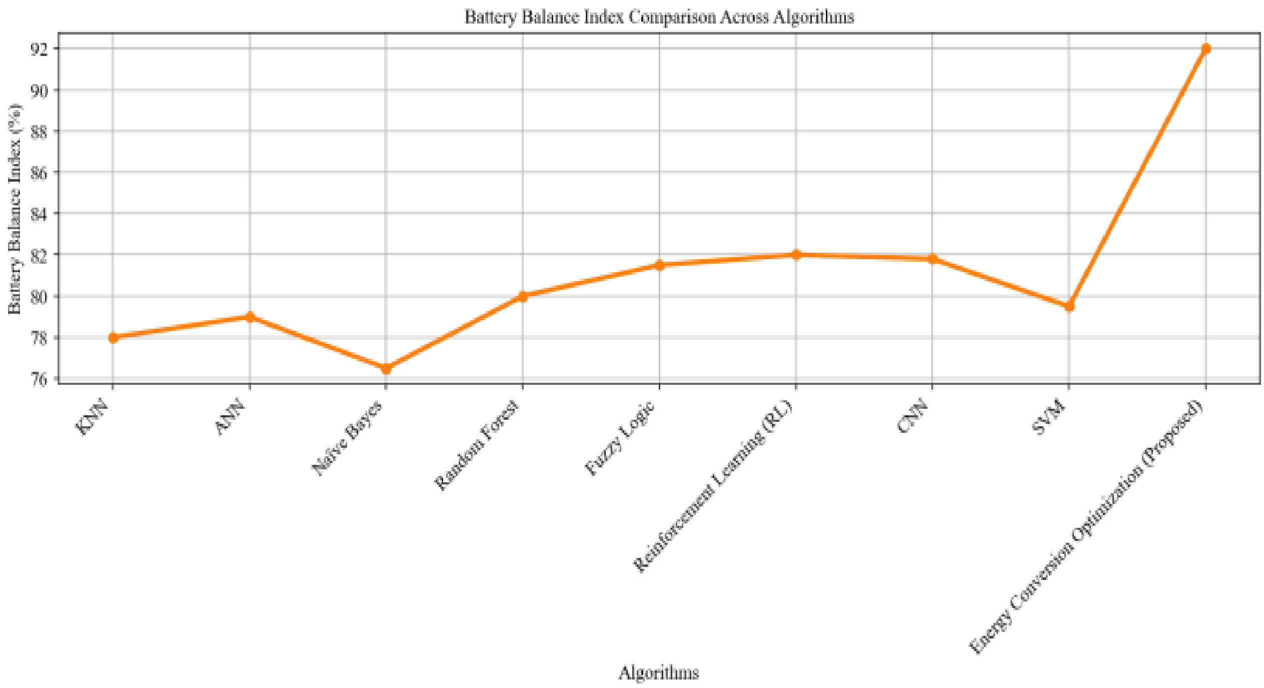


Figure 12: Comparison of Battery Balance Index between Algorithms

The figure 12, demonstrates the battery balance index (%) of the different algorithms which indicate that the Energy Conversion Optimization Algorithm has the best battery balance (92.0%). The outcome shows that the proposed algorithm is more effective in the process of evenly distributing the energy consumption among nodes.

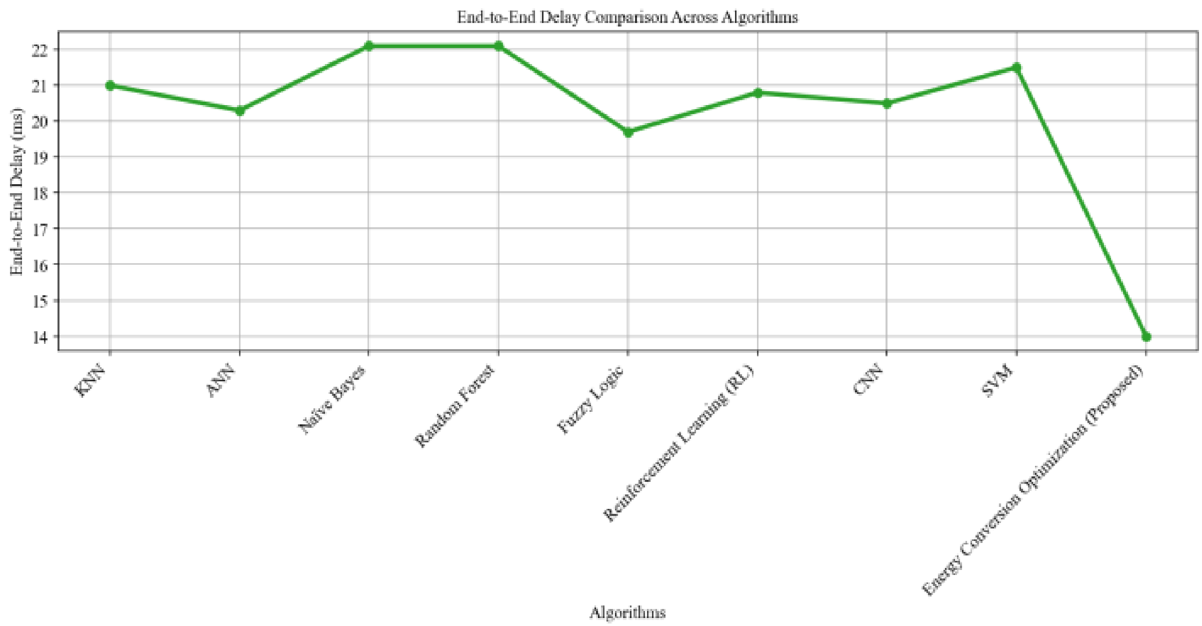


Figure 13: Comparison of End-to-End Delays among Algorithms

In Figure13, this result shows the end-to-end delay performance of the various algorithms with the proposed Energy Conversion Optimization Algorithm having the lowest delay (14.0 ms). This makes the proposed approach better since it allows the transmission of data faster and more effectively.

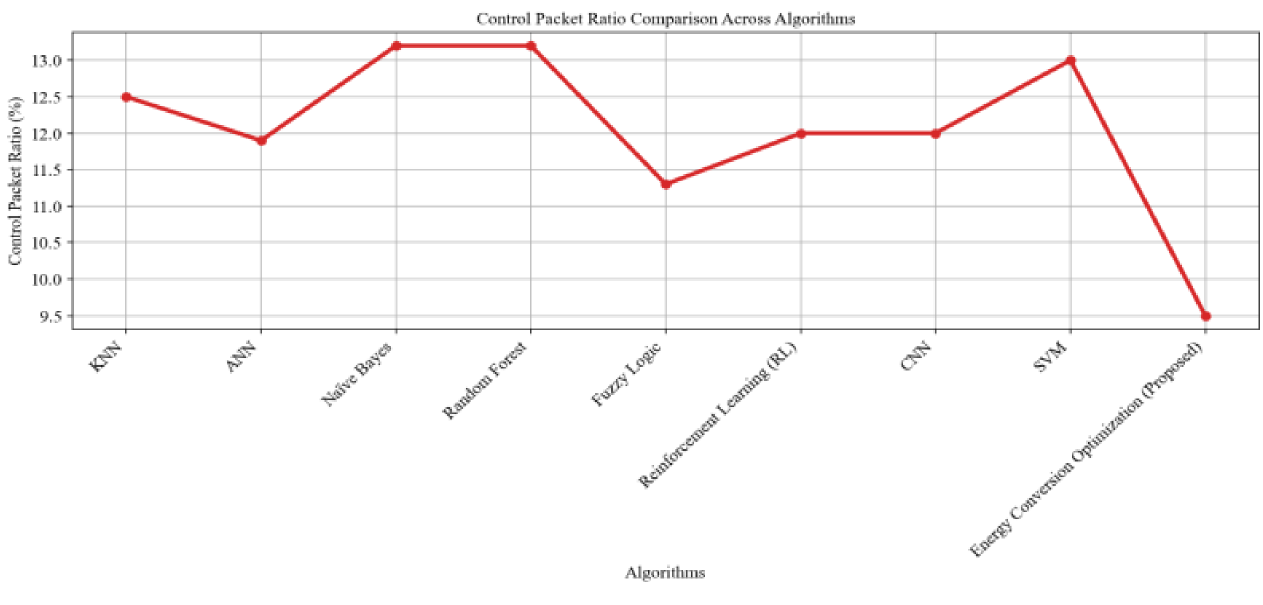


Figure 14: Comparison of Control Packet Ratio with Algorithms

In Figure 14, this value indicates that the ratio of control packets (percent) across all the algorithms is the lowest with the proposed Energy Conversion Optimization Algorithm recording the lowest overhead (9.5%). This shows that the solution proposed is more efficient as it minimizes unwarranted control packet transmissions.

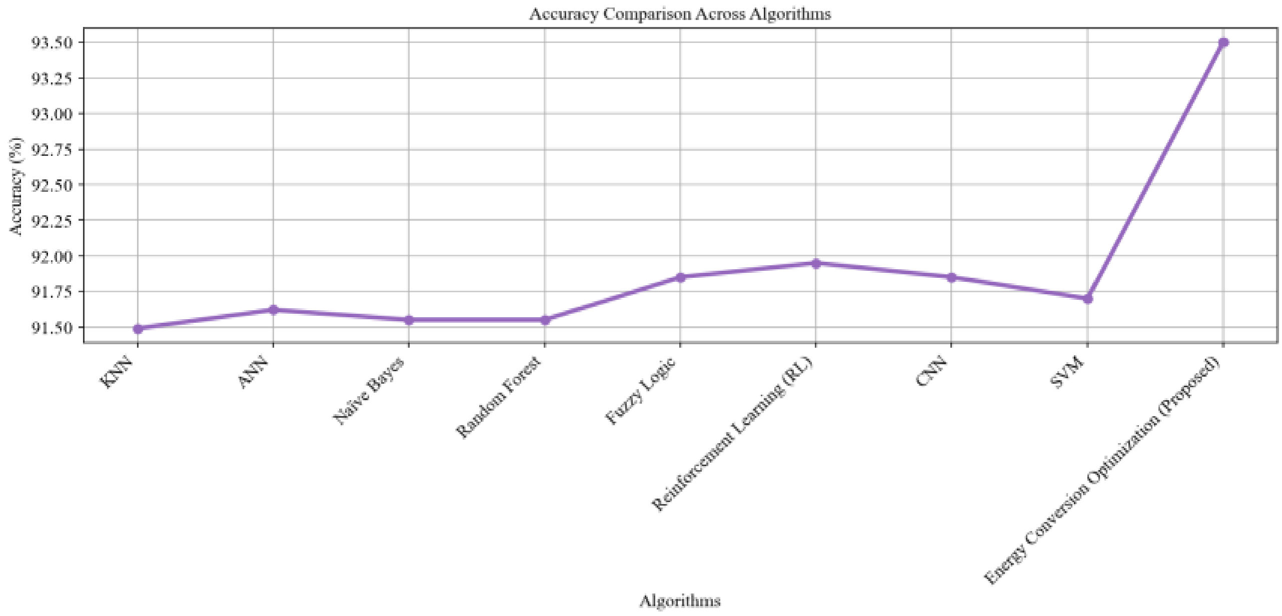


Figure 15: The Accuracy Comparison between Algorithms

In Figure 15, this parameter is a comparison of the accuracy (%) of the various algorithms, the proposed Energy Conversion Optimization Algorithm has the highest accuracy (93.50%). The outcome validates the fact that the proposed algorithm is more effective when it comes to providing more viable and precise network performance.

5. CONCLUSION

The research proposed a smart trust based and energy efficient routing system in Mobile Ad Hoc Networks (MANETs) to solve problems to do with security, energy loss, and unstable routing systems. Having incorporated the Modular Aging Optimization Algorithm to estimate the dynamic trust and the Energy Conversion Optimization Algorithm to minimize the energy use, the proposed solution guarantees the secure and reliable flow of data. Extensive experimental research through Python proved that the framework proposed significantly outcompetes the current machine learning and deep learning-based routing strategies with regard to various performance indicators, such as accuracy, throughput, residual energy, network lifetime, and end-to-end delay. The findings affirm that adaptive trust modelling and energy optimization model improve the general performance and resilience of the network in dynamic environments. The proposed framework can be generalized in the future to large-scale heterogeneous networks that involve increased node mobility. Also, the federated learning and block chain-based trust mechanisms can be included to enhance the further scalability, security, and preservation of privacy.

REFERENCES

[1] Al-Attar, B., Nasralla, Z. H., Al Sayed, I. A., Tawfeq, J. F., Sekhar, R., Shah, P., & Malge, S. (2025). Integrating Deep Learning into Location-Aided Routing (LAR) for Enhanced Mobile Ad-Hoc Networks (MANET): A Comprehensive Survey. International Journal of Safety & Security Engineering, 15(3).

[2] Amalia, A., Pramitarini, Y., Perdana, R. H. Y., Shim, K., & An, B. (2023). A deep-learning-based secure routing protocol to avoid blackhole attacks in VANETs. Sensors, 23(19), 8224.

[3] Singh, C. E., & Singh, J. A. P. (2023). An investigation of machine learning-based ids for green smart transportation in MANET. In Artificial Intelligence for Smart Healthcare (pp. 59-74). Cham: Springer International Publishing.

[4] Sardar, T. H., Dar, S. A., Jaiswal, J., Prasad, G., Mittal, M., & Kumar, V. (2025). Enhancing Security in MANETs with Deep Learning-Based Intrusion Detection. Procedia Computer Science, 259, 120-129.

[5] Saravanan, S., Dar, S. A., Rather, A. A., Qayoom, D., & Ali, I. (2025). Deep learning models for intrusion detection systems in MANETs: A comparative analysis. Decision Making Advances, 3(1), 96-110.

[6] Sucharitha, K., & Latha, R. (2022, February). Designing an ML-based congestion detection algorithm for routing data in MANETs. In International conference on computing, communication, electrical and biomedical systems (pp. 3-13). Cham: Springer International Publishing.

[7] Rajasoundaran, S., Kumar, S. S., Selvi, M., Ganapathy, S., Rakesh, R., & Kannan, A. (2021). Machine learning based volatile block chain construction for secure routing in decentralized military sensor networks. Wireless Networks, 27(7), 4513-4534.

[8] Singh, C. E., & Vigila, S. M. C. (2023). An investigation of machine learning-based intrusion detection system in mobile ad hoc network. International Journal of Intelligent Engineering Informatics, 11(1), 54-70.

[9] Gupta, C., Johri, I., Srinivasan, K., Hu, Y. C., Qaisar, S. M., & Huang, K. Y. (2022). A systematic review on machine learning and deep learning models for electronic information security in mobile networks. Sensors, 22(5), 2017.

[10] Junejo, M. H., Ab Rahman, A. A. H., Shaikh, R. A., Yusof, K. M., Kumar, D., & Memon, I. (2021). Lightweight trust model with machine learning scheme for secure privacy in VANET. Procedia Computer Science, 194, 45-59.

[11] Danilchenko, K., Azoulay, R., Reches, S., & Haddad, Y. (2022). Deep learning method for delay minimization in MANET. ICT Express, 8(1), 7-10.

[12] Vani, A. (2021). Deplete And Discernment Of Security Hazards In Mobile Ad-Hoc-Networks (Manet) Using Artifical Intelligence. International Journal of Future Generation Communication and Networking, 14(1), 925-942.

[13] Mughaid, A., AlZu'bi, S., Alnajjar, A., AbuElsoud, E., Salhi, S. E., Igried, B., & Abualigah, L. (2023). Improved dropping attacks detecting system in 5g networks using machine learning and deep learning approaches. Multimedia Tools and Applications, 82(9), 13973-13995.

[14] Rath, M., & Mishra, S. (2022). Advanced-level security in network and real-time applications using machine learning approaches. In Research Anthology on Machine Learning Techniques, Methods, and Applications (pp. 664-680). IGI Global Scientific Publishing.

[15] Srinivasan, V., Raj, V. H., Thirumalraj, A., & Nagarathinam, K. (2024). Original Research Article Detection of Data imbalance in MANET network based on ADSY-AEAMBi-LSTM with DBO Feature selection. Journal of Autonomous Intelligence, 7(4), 1094.

[16] Parthiban, N., Vijay, S., & Sheela, S. N. (2025). Comparison of mitigating DDoS attacks in software defined networking and IoT platforms. Cyber Security and Applications, 3, 100080.

[17] Osamy, W., Khedr, A. M., Salim, A., El-Sawy, A. A., Alreshoodi, M., & Alsukayti, I. (2022). Recent advances and future prospects of using AI solutions for security, fault tolerance, and QoS challenges in WSNs. Electronics, 11(24), 4122.

[18] Hemalatha, S., Janakidevi, M., Kumar, P. S., Arunkumar, M. S., Angadi, S., Muruganantham, T., ... & Vijay Muni, T. (2024). Detecting Intruder and Black Hole Attackers in Mobile Adhoc Network. International Journal of Electronics and Communication Engineering, 11, 80-88.

[19] Ali, T. E., Chong, Y. W., & Manickam, S. (2023). Machine learning techniques to detect a DDoS attack in SDN: A systematic review. Applied Sciences, 13(5), 3183.

[20] Dritsas, E., & Trigka, M. (2024). Machine Learning in Information and Communications Technology: A Survey. Information, 16(1), 8.

[21] Abuagoub, A. M. (2024). Security Concerns with IoT Routing: A Review of Attacks, Countermeasures, and Future Prospects. Advances in Internet of Things, 14(4), 67-98.

[22] Ramesh, R. B., Thangaraj, S. J. J., Sagayee, G. M. A., & Saravanan, K. (2025). Detection and prevention in WSN security framework using deep learning against black hole and wormhole attacks. Ain Shams Engineering Journal, 16(10), 103624.

[23] Hosseinzadeh, M., Tanveer, J., Masoud Rahmani, A., Yousefpoor, E., Sadegh Yousefpoor, M., Khan, F., & Haider, A. (2022). A cluster-tree-based secure routing protocol using dragonfly algorithm (DA) in the Internet of Things (IoT) for smart agriculture. Mathematics, 11(1), 80.

[24] Thakur, S., Sarkar, N. I., & Yongchareon, S. (2025). AI-Driven Energy-Efficient Routing in IoT-Based Wireless Sensor Networks: A Comprehensive Review. Sensors, 25(24), 7408.

[25] Bohra, N., Kumari, A., Mishra, V. K., Soni, P. K., & Balyan, V. (2025). Intelligence-Based Strategies with Vehicle-to-Everything Network: A Review. Future Internet, 17(2).

[26] Saoud, B., Shayea, I., Yahya, A. E., Shamsan, Z. A., Alhammadi, A., Alawad, M. A., & Alkhrijah, Y. (2024). Artificial Intelligence, Internet of things and 6G methodologies in the context of Vehicular Ad-hoc Networks (VANETs): Survey. ICT Express, 10(4), 959-980.

[27] Ibrahim, Z. B., & Ghanim, M. F. (2024). A review of AI-based approaches against wormhole and blackhole attacks in AODV protocol. Int. J. Adv. Nat. Sci. Eng. Res, 8, 60-75.

[28] Vamshi Krishna, K., & Ganesh Reddy, K. (2023). Classification of distributed denial of service attacks in VANET: a survey. Wireless Personal Communications, 132(2), 933-964.

[29] Nemati, M., Al Homssi, B., Krishnan, S., Park, J., Loke, S. W., & Choi, J. (2022). Non-terrestrial networks with UAVs: A projection on flying ad-hoc networks. Drones, 6(11), 334.

[30] El Houssaini, M. A. (2025). An ARIMA-Based Approach for Predicting and Detecting Routing Attacks in MANETs. Procedia Computer Science, 265, 33-40.