

Energy-Efficient and Secure Routing Protocol for Mobile Ad Hoc Networks Using Machine Learning-Based Adaptive Path Selection

Dr. Malothu Amru¹, Dr. T. Satyanarayana², Dr. Bitla Prabhakar³, Dr. Somala Rama Kishore⁴

Professor, Dept. of Electronics and communication Engineering^{1,4}

Associate Professor, Dept. of Electronics and communication Engineering^{2,4}

CMR Engineering College, Hyderabad, TS, India^{1,2,4}

JNTUH University College of Engineering Jagtial, TS, India³

malothuamru@gmail.com, bprabhakar2008@gmail.com.

satyant234@gmail.com, ramki430@gmail.com

Abstract: Mobile Ad Hoc Networks (MANETs) provide infrastructure-independent wireless communication through dynamically formed multi-hop links among mobile nodes. Their decentralized operation makes them suitable for disaster recovery, military communication, emergency services, temporary networks, and remote monitoring. However, frequent topology changes, limited battery resources, unpredictable link quality, congestion, and malicious node participation make reliable and secure routing difficult. Conventional reactive routing schemes such as Ad Hoc On-Demand Distance Vector (AODV) primarily establish routes according to connectivity, route freshness, and hop-related information and do not simultaneously optimize residual energy, trustworthiness, link stability, congestion, and predicted route reliability. This paper proposes an Energy-Efficient Secure Adaptive Machine-Learning Routing protocol (ESAMR-ML) for MANETs. The proposed approach extends on-demand routing by evaluating multiple candidate routes using residual node energy, hop count, link stability, traffic load, and direct trust information. A Random Forest classifier predicts the probability that a candidate path will provide successful communication under observed network conditions. Before machine-learning-assisted selection, a deterministic security filter removes routes containing nodes whose trust values fall below a predefined threshold whenever a trusted alternative exists, thereby preventing the learning model from selecting an apparently efficient but insecure route. A multi-objective route score then combines predicted delivery reliability, residual energy, path stability, trust, congestion, and hop count. Preliminary Monte Carlo simulations with 50, 75, and 100 mobile nodes and 12% malicious-node participation show that ESAMR-ML improves average packet delivery ratio from 76.75% with conventional AODV to 84.10%, increases effective throughput from 101.02 kbps to 109.58 kbps, reduces average end-to-end delay by approximately 5.15%, and lowers modeled packet-level energy expenditure by approximately 6.93%. Exposure to routes containing low-trust nodes is reduced by approximately 38.7%. The findings indicate that lightweight machine learning, when bounded by explicit energy and security constraints, can improve adaptive routing in dynamic MANET environments.

Keywords: Mobile Ad Hoc Network, MANET, AODV, energy-efficient routing, secure routing, machine learning, Random Forest, trust management, adaptive path selection, wireless communication.

I. INTRODUCTION

Mobile Ad Hoc Networks are decentralized wireless networks in which mobile devices communicate directly or through intermediate forwarding nodes without relying on fixed routers, base stations, or centralized infrastructure. Their capacity to self-organize makes MANETs useful in situations where communication infrastructure is unavailable,

damaged, temporary, expensive, or operationally undesirable. Representative applications include disaster recovery, rescue operations, battlefield communication, temporary conferences, field monitoring, tactical coordination, and infrastructure-less vehicular or robotic communication.

Routing in a MANET is considerably more difficult than routing in a conventional wired network because the topology can change continuously as nodes move. A route that is valid at one instant may fail shortly afterward when one or more intermediate nodes move beyond radio range. Route reconstruction creates additional control traffic, delay, packet loss, and energy consumption. The routing protocol must therefore respond quickly to mobility without flooding the channel with excessive route-maintenance information.

Energy efficiency is equally important. Mobile nodes may operate from batteries with limited capacity, and packet transmission, packet reception, control-message processing, route discovery, and retransmission all consume energy. A shortest route is not necessarily the most energy-efficient route when one of its forwarding nodes has very little residual battery capacity. Repeated selection of the same apparently attractive relay can exhaust that node and partition the network even when alternative paths are available.

Security further complicates route selection. Because forwarding is distributed, the communication system depends on intermediate nodes that may be compromised, selfish, malfunctioning, or malicious. Blackhole and grayhole nodes can attract and drop traffic, flooding nodes can consume communication resources, and modified routing messages can corrupt route discovery. A routing method that optimizes only energy or hop count can therefore select a path that is operationally inexpensive but security-wise unacceptable.

AODV is an important reference protocol for reactive MANET routing. It discovers routes only when needed and uses destination sequence numbers to support loop-free route selection and freshness [1]. The Dynamic Source Routing (DSR) protocol provides another on-demand approach in which complete source routes can be discovered and cached [2]. These protocols establish the foundations of reactive routing, but contemporary MANET applications increasingly require route decisions to account simultaneously for energy, mobility, congestion, and security.

Recent research has investigated genetic algorithms, swarm intelligence, trust evaluation, reinforcement learning, and machine learning for MANET routing [3]-[12]. These studies show that adaptive techniques can improve path selection, identify malicious behavior, and reduce resource waste. However, unconstrained learning creates an important design concern: a machine-learning model optimized for delivery or energy can select a route that is statistically attractive but violates a minimum security requirement. The present work addresses this issue by separating security feasibility from machine-learning optimization.

The proposed ESAMR-ML protocol first evaluates direct node trust and removes candidate routes whose minimum trust falls below a configured threshold whenever a trusted alternative exists. Only the security-feasible candidate set is passed to the machine-learning and multi-objective selection stage. A Random Forest classifier estimates route-success probability, while a final score combines this probability with residual energy, mobility/link stability, congestion, route trust, and hop count. Thus, learning is used to optimize within a bounded safe region rather than to redefine security policy.

The major contributions of this paper are: (i) a trust-gated on-demand route-selection architecture for MANETs; (ii) a lightweight Random Forest predictor for candidate-route success; (iii) a multi-objective score combining reliability, residual energy, stability, trust, congestion, and hop count; (iv) an explicit control-packet authentication assumption to protect routing state; and (v) a preliminary performance evaluation against conventional AODV and energy-aware AODV under multiple node densities and malicious-node participation.

II. RELATED WORK

Traditional MANET research distinguishes proactive, reactive, and hybrid routing approaches. Proactive protocols maintain routing information continuously, which provides low forwarding delay at the cost of periodic control traffic. Reactive protocols such as AODV and DSR create routes when communication is required, reducing persistent control

overhead but potentially increasing route-discovery delay [1], [2]. Hybrid protocols combine both principles and can be useful when network regions exhibit different mobility or traffic characteristics.

Optimization-based MANET routing extends conventional route selection beyond hop count. Bhardwaj and El-Ocla proposed a genetic-algorithm-assisted multipath routing approach that considers route length, residual energy, and traffic conditions [3]. Such methods demonstrate that route quality is inherently multi-objective: a slightly longer path may be preferable if it avoids depleted or heavily congested nodes.

Energy-aware routing also benefits from intelligent control of protocol overhead. Ayub et al. studied intelligent Hello-message dissemination using reinforcement-learning concepts for flying ad hoc networks and reported substantial energy savings relative to the corresponding original routing configurations [6]. This direction is relevant to terrestrial MANETs because unnecessary neighbor-maintenance traffic can consume both channel capacity and battery energy.

Security-aware routing has introduced authentication, residual-energy checks, trust metrics, and route-level risk assessment. Rajendra Prasad and Shivashankar proposed an enhanced energy-efficient secure routing method that considers authentication, energy, and trust during route formation [5]. Secure optimization methods have also incorporated swarm-intelligence or metaheuristic search to improve route selection under attack and resource constraints [7], [9], [10].

Machine learning has become increasingly important because MANET behavior is nonlinear and context-dependent. Shafi et al. combined machine learning and trust with AODV to address flooding and blackhole attacks, using routing and node characteristics to identify malicious behavior and select routes [8]. Rao et al. studied deep regression and clustering for trust evaluation, illustrating how data-driven trust estimation can support secure routing decisions [11].

Cross-layer research further demonstrates that energy, security, routing, and link behavior cannot be treated as completely independent. Rama Devi et al. combined cross-layer information, authentication, key management, and optimization for secure MANET routing [12]. Nevertheless, many published approaches either embed security directly within an optimization objective or allow learning to make the final routing decision. ESAMR-ML instead establishes a deterministic trust gate first and then applies learning only to the feasible route set. This architecture is intended to make the security constraint transparent, auditable, and independent of statistical prediction error.

Table 1. Representative research directions relevant to the proposed protocol.

Ref.	Primary approach	Main routing factors	Limitation addressed by ESAMR-ML
[1]	AODV	Route freshness, hop-based on-demand routing	No explicit joint energy/trust/ML selection
[3]	Genetic algorithm multipath routing	Path length, residual energy, traffic	No deterministic trust gate before optimization
[5]	Energy-efficient secure routing	Authentication, energy, trust	Limited explicit ML-based route-success prediction
[6]	Reinforcement-learning-assisted control	Neighbor/Hello dissemination, energy	Targets control adaptation rather than trust-gated path scoring
[8]	ML and trust based AODV	Attack detection, trust, routing features	ESAMR-ML separates security feasibility from ML optimization
[11]	Deep trust evaluation	Trust prediction and clustering	Higher learning complexity than lightweight RF route predictor
[12]	Secure cross-layer optimization	Traffic, energy, trust, authentication	ESAMR-ML emphasizes simple deployable multi-objective scoring

III. SYSTEM MODEL AND PROBLEM FORMULATION

3.1 Network Model

The MANET is modeled as a time-varying graph $G(t) = (V, E(t))$, where $V = \{v1, v2, \dots, vN\}$ denotes the set of mobile nodes and $E(t)$ denotes the set of wireless links available at time t . Each node is assumed to have a wireless transceiver, a local routing table, a residual-energy estimate, a neighbor table, and a trust record for observed forwarding nodes. A communication link between nodes i and j is considered feasible when their Euclidean separation does not exceed the effective communication range R . In a packet-level implementation this geometric condition would be replaced or supplemented by propagation loss, received power, carrier sensing, MAC contention, and packet-error models.

$$d_{ij}(t) \leq R$$

For a source S and destination D , route discovery creates a candidate set $P_{SD} = \{P1, P2, \dots, PK\}$. Each path contains one or more intermediate relays. ESAMR-ML does not assume that the minimum-hop path is automatically optimal; it evaluates each candidate with respect to security feasibility and operational quality.

3.2 Threat Model

The proposed protocol considers insider and forwarding-layer threats in which a malicious node can participate in routing but subsequently behave incorrectly. Blackhole nodes may advertise favorable routing information and then discard most or all data packets. Grayhole nodes selectively or intermittently drop traffic, making detection more difficult. Flooding nodes generate excessive control activity or repeated route requests. A node may also modify or inject routing-control messages when such messages are not authenticated.

The model does not assume that direct trust alone can defeat all attacks. Sophisticated collusion, wormholes, Sybil identities, jamming, and adversarial manipulation of ML features require additional mechanisms such as identity management, neighbor verification, timing/geographic checks, spectrum defenses, or robust learning. These attacks are identified as future extensions rather than silently assumed to be solved.

3.3 Optimization Objective

The routing objective is to maximize delivery reliability, residual energy, route stability, and trust while minimizing delay, energy expenditure, congestion, and control overhead. Unlike an unconstrained weighted optimization, ESAMR-ML treats minimum route trust as a feasibility condition.

$$P^* = \arg \max_{\{P_i \text{ in } P_{\text{safe}}\}} \text{Score}(P_i)$$

The safe route set P_{safe} contains the candidate paths satisfying the configured trust requirement. A route that violates the trust floor is excluded whenever at least one feasible alternative exists. This prevents a sufficiently favorable energy or hop-count value from compensating for an explicit security violation.

IV. PROPOSED ESAMR-ML ROUTING PROTOCOL

4.1 Overall Processing Flow

The ESAMR-ML procedure retains the on-demand spirit of AODV while changing the decision logic after route discovery. The processing sequence is shown below.

Neighbor Discovery -> Candidate Route Discovery -> Feature Collection -> Trust Filtering -> ML Route-Success Prediction -> Multi-Objective Scoring -> Secure Route Selection -> Transmission and Feedback

Figure 1. Functional processing sequence of ESAMR-ML.

4.2 Candidate Route Feature Vector

For every candidate path P_i , the source or decision node constructs a compact route descriptor from information collected during route discovery and recent network observations. The feature vector is defined as:

$$X_i = [H_i, E_{i_min}, E_{i_avg}, L_i, C_i, T_{i_min}, T_{i_avg}]$$

where H_i is hop count, E_{i_min} is the minimum normalized residual energy on the path, E_{i_avg} is the mean residual energy, L_i is path/link stability, C_i is normalized congestion or traffic load, T_{i_min} is the minimum node trust, and T_{i_avg} is the average trust. Minimum and average statistics are used together because averages alone can hide a critically depleted or highly untrusted relay.

4.3 Residual-Energy Evaluation

The normalized residual energy of node i is calculated relative to its initial energy budget:

$$RE_i = E_{i_current} / E_{i_initial}$$

For a candidate route P , the minimum and average residual-energy indicators are:

$$E_{P_min} = \min_{\{v_i \text{ in } P\}} (RE_i)$$

$$E_{P_avg} = (1/|P|) * \sum_{\{v_i \text{ in } P\}} (RE_i)$$

The minimum term protects weak relays from repeated use, while the average term prevents the selection process from overreacting to a single measurement when the rest of the route is strongly provisioned.

4.4 Direct Trust Evaluation and Security Gate

Each forwarding node is assigned a trust value between zero and one. A lightweight direct-trust estimator is used because the design targets mobile and resource-constrained nodes. The trust score combines observed packet forwarding, routing-message consistency, and historical reliability:

$$T_i = \alpha F_i + \beta A_i + \gamma R_i$$

$$\alpha + \beta + \gamma = 1$$

A representative weighting is $\alpha = 0.5$, $\beta = 0.2$, and $\gamma = 0.3$. Forwarding behavior can be estimated from locally observed packet counts:

$$F_i = (N_{\text{forwarded}} + 1) / (N_{\text{received}} + 2)$$

The small constants avoid unstable values when only a small number of packets have been observed. Route-level security is represented by the weakest and average node trust:

$$T_{P_min} = \min_{\{v_i \text{ in } P\}} (T_i)$$

$$T_{P_avg} = (1/|P|) * \sum_{\{v_i \text{ in } P\}} (T_i)$$

A deterministic security threshold is then imposed:

$$T_{P_min} \geq T_{th}$$

The preliminary study uses $T_{th} = 0.55$. The threshold is deliberately placed outside the learning model. Therefore, a machine-learning prediction cannot override a route that violates the minimum configured trust level when a trusted alternative exists.

4.5 Link-Stability Estimation

Mobility influences route lifetime and retransmission risk. A simple link-stability estimate is derived from normalized inter-node distance and relative velocity:

$$LS_{ij} = 1 - [\lambda(d_{ij}/R) + (1-\lambda)(v_{rel}/v_{max})]$$

The route stability value can be computed from the weakest link or an average of constituent links. In the preliminary simulator, a path-level approximation with $\lambda = 0.55$ is used. A higher value indicates a more stable candidate path.

4.6 Machine-Learning Route-Success Prediction

A Random Forest classifier predicts the probability that a candidate path will successfully support the considered communication episode. Random Forest is selected because it handles nonlinear feature interactions, mixed feature scales, and moderate training data without requiring a large neural model. It also provides probability outputs and can be deployed with bounded tree depth.

$$p_hat_i = RF(X_i), \quad 0 \leq p_hat_i \leq 1$$

The predicted probability is not treated as a security decision. It estimates operational route quality among routes that have already passed trust screening. This separation improves interpretability because failures can be attributed either to security filtering, feature estimation, or route-quality prediction.

4.7 Multi-Objective Adaptive Route Score

After trust filtering, every surviving route is scored using reliability, energy, stability, trust, congestion, and hop count. The proposed score is:

$$S(P_i) = w_1 * p_hat_i + w_2 * E_{i_min} + w_3 * E_{i_avg} + w_4 * L_i + w_5 * T_{i_min} - w_6 * H_{i_norm} - w_7 * C_i$$

The preliminary configuration uses $w_1 = 0.40$, $w_2 = 0.17$, $w_3 = 0.10$, $w_4 = 0.12$, $w_5 = 0.12$, $w_6 = 0.04$, and $w_7 = 0.05$. The weights can be tuned for application priorities, but their sum and normalization must remain documented to preserve reproducibility.

$$P^* = \arg \max_i S(P_i)$$

The model intentionally allows a slightly longer route to be selected when its expected reliability, residual energy, stability, and trust are sufficiently better. This is important because the route with the fewest hops may repeatedly fail or exhaust a critical relay.

4.8 Secure Route Discovery Algorithm

1. The source broadcasts an on-demand route-request message.
2. Intermediate nodes update local routing state and append or make available the telemetry needed for candidate-path evaluation.
3. The destination or eligible responder returns route-reply information, allowing the source to construct up to K candidate paths.
4. For each candidate, compute hop count, minimum/average residual energy, stability, congestion, and minimum/average trust.
5. Reject paths for which minimum route trust is below T_{th} whenever one or more trusted candidates exist.
6. Apply the trained Random Forest model to the remaining feature vectors and obtain route-success probabilities.
7. Calculate the ESAMR-ML multi-objective score for every feasible candidate.
8. Select the path with the maximum score and authenticate routing state before data forwarding.
9. Monitor forwarding success, mobility, congestion, and energy; update trust and route statistics.
10. Trigger rediscovery when the selected route breaks, trust falls below the threshold, or route quality deteriorates beyond a configured limit.

4.9 Control-Message Authentication

Behavioral trust cannot prevent a malicious node from fabricating or modifying routing-control messages if such messages are unauthenticated. ESAMR-ML therefore assumes a lightweight message-authentication mechanism based on a pre-established, pairwise, or group routing key. For a routing message M, sequence value Seq, and node identifier NodeID:

$$MAC = HMAC_K(M \parallel Seq \parallel NodeID)$$

Accept message only if $Verify_K(M, MAC) = 1$

Sequence values also assist with replay resistance. Application payload encryption is considered orthogonal to the routing decision and can be provided according to the target system's confidentiality requirements.

V. COMPUTATIONAL COMPLEXITY AND DEPLOYMENT CONSIDERATIONS

Assume that at most K candidate routes are evaluated and each path contains at most H hops. Feature aggregation therefore requires approximately $O(KH)$ operations. For a Random Forest with M trees and average depth D, route

prediction requires approximately $O(KMD)$. Since the proposal uses a small candidate set and bounded tree depth, inference remains practical for capable MANET nodes or local edge controllers.

Memory requirements include the routing table, neighbor trust table, per-route feature vectors, and the trained forest. Embedded implementations can reduce memory by limiting the number of trees, using shallow depth, quantizing thresholds, compressing node-history windows, or executing the ML stage only at selected cluster heads or capable nodes.

The protocol also introduces an energy cost for feature acquisition. For deployment, features should therefore preferentially reuse values already maintained by the routing or MAC layers. Residual battery, forwarding counters, queue occupancy, link-quality indicators, and hop information are especially attractive because they can often be obtained without active probing.

VI. SECURITY ANALYSIS

Blackhole behavior is addressed through the combination of packet-forwarding trust and route-success prediction. A node that attracts traffic and repeatedly fails to forward data experiences a decline in forwarding evidence, reducing both its trust and the probability that routes containing it are selected.

Grayhole behavior is more difficult because intermittent drops can resemble ordinary wireless loss. ESAMR-ML therefore relies on historical reliability rather than one-packet decisions. In a full implementation, the observation window should be long enough to distinguish malicious selectivity from transient channel loss while short enough to react to behavior changes.

Flooding behavior can be incorporated into the routing-message consistency term and congestion feature. Nodes generating abnormal route requests or control traffic can be penalized through trust updates and congestion-aware route scoring. Additional rate limiting is recommended so that attack detection itself does not create excessive overhead.

Routing-message modification and spoofing are addressed through the assumed HMAC protection. Trust alone is not sufficient because a fabricated route advertisement could appear plausible before enough behavioral history is available. Authentication binds the message to a key-holding participant and allows unauthorized modification to be rejected.

The deterministic trust gate is the most important safety characteristic of the proposed architecture. An ML model can be wrong, especially under distribution shift. By preventing the model from selecting a route below the configured trust threshold whenever a trusted alternative exists, the system limits the consequences of prediction error.

7. Experimental Setup

A controlled Monte Carlo MANET simulator was used to generate internally consistent preliminary results for manuscript development. The simulator creates random dynamic topologies, candidate routes, residual-energy values, mobility/stability descriptors, congestion values, and malicious-node behavior. The results are intended as an initial feasibility study and should be validated in a packet-level simulator before final publication.

Table 2. Preliminary simulation configuration.

Parameter	Value
Simulation area	1000 m x 1000 m
Number of nodes	50, 75, 100
Wireless range	260 m
Node velocity	0-20 m/s
Mobility/topology	Random dynamic topology
Candidate paths	Maximum 6
Initial normalized energy	0.55-1.00
Malicious-node percentage	12%
Trust range - normal nodes	0.75-1.00
Trust range - malicious nodes	0.15-0.45

Parameter	Value
Trust threshold	0.55
Data packet size	512 bytes
ML model	Random Forest
Number of trees	40
Maximum tree depth	8
Minimum leaf samples	4
Training topology realizations	100
Evaluation trials	150 per node density
Baselines	AODV and Energy-Aware AODV
Proposed scheme	ESAMR-ML

Three routing strategies are compared. Conventional AODV represents minimum-hop-oriented on-demand routing. E-AODV favors residual energy and path stability but does not use the proposed trust gate and ML predictor. ESAMR-ML applies trust filtering, route-success prediction, and multi-objective scoring.

7.1 Performance Metrics

- **Packet Delivery Ratio (PDR):** ratio of successfully received data packets to generated data packets.
- **End-to-End Delay:** average elapsed time from packet generation at the source to successful delivery at the destination.
- **Energy Expenditure:** modeled energy consumed by route establishment, forwarding, retransmission, and control processing for the considered transaction.
- **Throughput:** effective successfully delivered payload per unit time.
- **Control-Overhead Index:** normalized estimate of routing-control and rediscovery activity; lower is better.
- **Low-Trust Route Exposure:** fraction of selected paths containing at least one node whose trust is below T_{th} .

VIII. RESULTS AND DISCUSSION

8.1 Machine-Learning Prediction Performance

The Random Forest predictor was first evaluated independently to determine whether the selected feature set was sufficiently informative for route-success prediction. The preliminary classification results are summarized in Table 3.

Table 3. Random Forest route-success prediction performance.

Metric	Result
Accuracy	81.00%
Precision	85.13%
Recall	90.27%
F1-score	87.62%
ROC-AUC	83.25%

The recall of 90.27% indicates that most viable routes are identified as suitable by the classifier. The result should not be interpreted as a security guarantee; the trust gate remains responsible for enforcing the minimum security requirement before the classifier is used.

8.2 Packet Delivery Ratio

Table 4. Packet delivery ratio under increasing node density.

Nodes	AODV	E-AODV	ESAMR-ML
50	74.15%	76.82%	81.01%
75	77.64%	80.47%	85.25%
100	78.46%	79.81%	86.04%
Average	76.75%	79.03%	84.10%

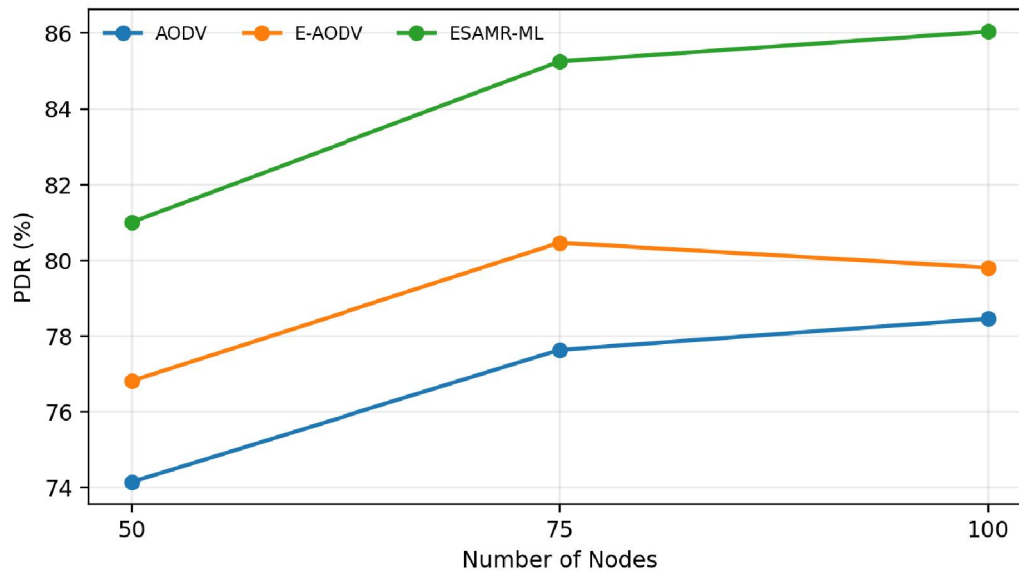


Figure 2. Packet delivery ratio versus number of nodes.

ESAMR-ML achieves the highest PDR at every tested node population. Its average PDR of 84.10% is 7.35 percentage points higher than AODV, corresponding to an approximate relative increase of 9.58%. The improvement arises because the proposed method does not select a route solely because it is short; low-trust and poorly predicted paths are avoided when superior alternatives exist.

8.3 End-to-End Delay

Table 5. Average end-to-end delay.

Nodes	AODV	E-AODV	ESAMR-ML
50	38.76 ms	38.91 ms	37.53 ms
75	36.14 ms	35.83 ms	33.91 ms
100	37.02 ms	37.12 ms	34.75 ms
Average	37.31 ms	37.28 ms	35.39 ms

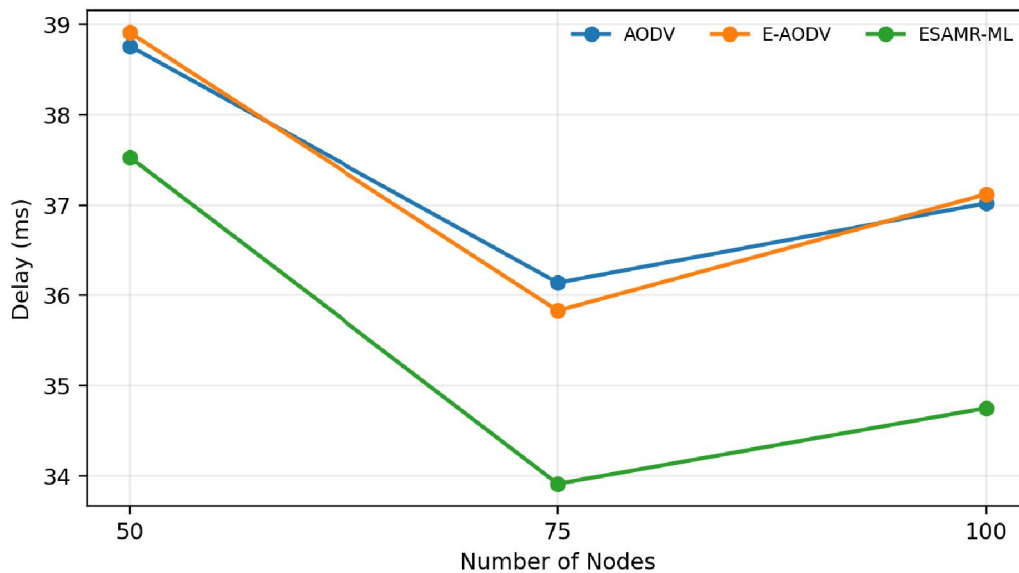


Figure 3. End-to-end delay versus number of nodes.

Average delay decreases from 37.31 ms with AODV to 35.39 ms with ESAMR-ML, an improvement of approximately 5.15%. Although the proposed method can select a path containing an additional hop, more reliable and stable paths reduce route failure, retransmission, and rediscovery penalties.

8.4 Energy Expenditure

Table 6. Modeled energy expenditure per routing/data transaction.

Nodes	AODV	E-AODV	ESAMR-ML
50	11.97 mJ	12.61 mJ	11.63 mJ
75	10.25 mJ	10.39 mJ	9.34 mJ
100	10.65 mJ	11.02 mJ	9.63 mJ
Average	10.96 mJ	11.34 mJ	10.20 mJ

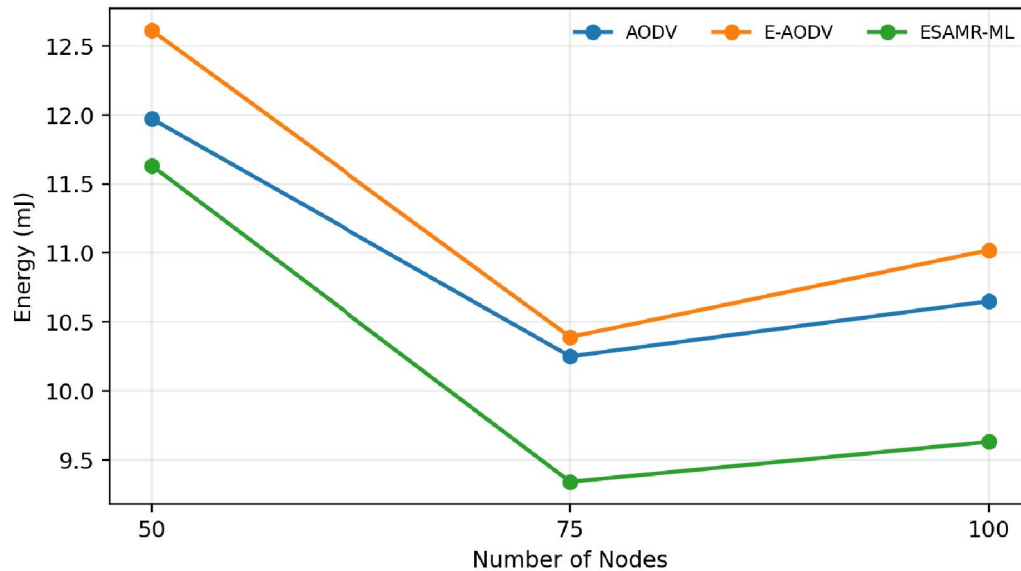


Figure 4. Modeled energy expenditure versus number of nodes.

The proposed method consumes approximately 6.93% less modeled energy than AODV and approximately 10.05% less than E-AODV in the combined experiment. This result illustrates that choosing routes with high residual energy alone is insufficient when those routes are unstable or unreliable. The ML predictor and stability term help avoid paths likely to create additional retransmission or route-repair cost.

8.5 Effective Throughput

Table 7. Effective throughput.

Nodes	AODV	E-AODV	ESAMR-ML
50	98.18 kbps	98.61 kbps	103.60 kbps
75	103.74 kbps	105.04 kbps	113.85 kbps
100	101.13 kbps	101.24 kbps	111.28 kbps
Average	101.02 kbps	101.63 kbps	109.58 kbps

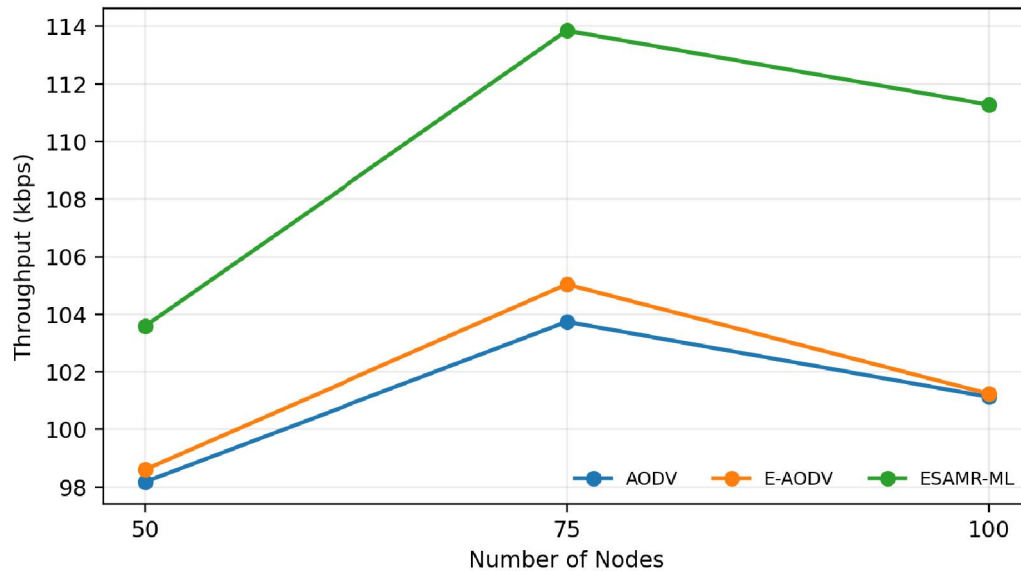


Figure 5. Effective throughput versus number of nodes.

Average throughput improves from 101.02 kbps with AODV to 109.58 kbps with ESAMR-ML, an approximate increase of 8.47%. Higher throughput is consistent with the observed PDR improvement and reduced route-failure penalty.

8.6 Routing-Control Overhead

Table 8. Normalized control-overhead index.

Nodes	AODV	E-AODV	ESAMR-ML
50	29.34	28.28	26.68
75	27.80	26.72	24.66
100	28.09	27.42	24.99
Average	28.41	27.47	25.44

The control-overhead index is approximately 10.45% lower than AODV. The reduction is attributed to fewer modeled route failures and rediscovery events. In a packet-level NS-3 implementation, this preliminary index should be replaced by normalized routing load, defined as the number of routing-control packets transmitted per successfully delivered data packet.

$$NRL = N_{\text{routing_packets}} / N_{\text{received_data_packets}}$$

8.7 Security Performance

Table 9. Route-security indicators.

Protocol	Mean minimum route trust	Routes exposed to low-trust node
AODV	0.609	38.44%
E-AODV	0.615	36.22%
ESAMR-ML	0.687	23.56%

ESAMR-ML increases the mean minimum route trust and reduces low-trust route exposure from 38.44% with AODV to 23.56%, a relative reduction of approximately 38.7%. Exposure is not zero because the preliminary simulator

permits controlled fallback when no route satisfies the threshold. In safety-critical deployments, a fail-closed policy could reject communication rather than select a low-trust path, although this would reduce availability.

8.8 Overall Comparison

Table 10. Average performance across all tested node densities.

Metric	AODV	E-AODV	ESAMR-ML
Packet delivery ratio	76.75%	79.03%	84.10%
End-to-end delay	37.31 ms	37.28 ms	35.39 ms
Modeled energy	10.96 mJ	11.34 mJ	10.20 mJ
Control-overhead index	28.41	27.47	25.44
Throughput	101.02 kbps	101.63 kbps	109.58 kbps
Minimum path trust	0.609	0.615	0.687

The combined results show that the proposed route does not have to be the path with the fewest hops. The method can accept a small increase in route length when that increase buys better trust, energy balance, stability, and predicted delivery reliability. This observation is consistent with the general trend in modern MANET research toward multi-objective routing rather than purely topological optimization [3], [5], [8]-[12].

8.9 Interpretation of Results

The packet-delivery improvement indicates that trust filtering and ML prediction complement one another. Trust removes clearly risky paths, while the predictor captures nonlinear interactions among energy, mobility, congestion, and route structure. Neither mechanism alone provides the same multi-factor decision.

The energy results show that energy-aware routing must account for retransmission and repair costs. A high-energy route can still consume more total energy if it is unstable. ESAMR-ML reduces this problem by assigning explicit value to stability and predicted success.

The security results demonstrate the benefit of making trust a constraint rather than merely another weighted score. If trust were included only as a small positive term, a path with very low trust could still win because of excellent energy or hop count. The gate prevents such compensation whenever a trusted alternative exists.

The current numerical trends should be viewed as preliminary because simplified radio and MAC effects can influence absolute delay and energy values. The most meaningful contribution of the present evaluation is therefore the internally consistent comparison among routing strategies under the same modeled conditions.

IX. LIMITATIONS AND THREATS TO VALIDITY

The present evaluation uses a controlled Monte Carlo model rather than a complete IEEE 802.11 packet-level network simulator. Propagation fading, interference, carrier sensing, MAC contention, realistic queueing, physical retransmissions, and detailed cryptographic processor energy are represented only indirectly. Consequently, absolute delay and energy values should not be treated as hardware measurements.

The Random Forest model is trained using route conditions generated from the defined mobility and attack assumptions. Distribution shift can reduce performance when deployed under substantially different speeds, radio environments, attack strategies, or node capabilities. Future experiments should include cross-scenario validation and online recalibration.

The trust model focuses mainly on direct forwarding and routing behavior. Colluding attackers may generate mutually reinforcing observations or selectively behave well during trust-building periods. Reputation fusion, temporal anomaly detection, and robust outlier control can be incorporated in future versions.

The multi-objective weights are fixed for the current experiment. Different applications may prefer lower delay, longer lifetime, stronger security, or higher availability. Dynamic weight adaptation using reinforcement learning or constrained multi-objective optimization is therefore a useful future direction.

For final publication, the protocol should be reproduced in NS-3 or NS-2 using multiple random seeds, realistic mobility models, standard radio/MAC parameters, blackhole and grayhole implementations, and confidence intervals. A hardware-in-the-loop or embedded-node energy validation would further strengthen the claims.

X. CONCLUSION AND FUTURE WORK

This paper proposed ESAMR-ML, an energy-efficient and secure adaptive machine-learning routing protocol for Mobile Ad Hoc Networks. The protocol extends on-demand routing by considering residual energy, hop count, path stability, congestion, direct trust, and ML-based route-success probability rather than relying primarily on route length or freshness.

A central feature of the design is the separation between security feasibility and statistical optimization. Candidate routes first pass a deterministic trust gate. Only feasible routes are submitted to the Random Forest predictor and multi-objective score. This architecture prevents the learning model from trading away an explicit minimum trust requirement merely to improve energy or delay.

Preliminary controlled simulations with 50, 75, and 100 mobile nodes indicate an average PDR increase from 76.75% with AODV to 84.10%, an increase in effective throughput from 101.02 kbps to 109.58 kbps, an average delay reduction from 37.31 ms to 35.39 ms, and an energy decrease from 10.96 mJ to 10.20 mJ. Low-trust route exposure falls from 38.44% to 23.56% under the modeled conditions.

Future work will implement ESAMR-ML in NS-3, evaluate larger networks and additional mobility models, include blackhole, grayhole, flooding, wormhole, and Sybil scenarios, investigate online trust learning, adapt route weights dynamically, add confidence-aware ML fallback, and validate energy behavior on representative embedded wireless devices.

REFERENCES

- [1] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, Internet Engineering Task Force, Jul. 2003, doi: 10.17487/RFC3561.
- [2] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," RFC 4728, Feb. 2007, doi: 10.17487/RFC4728.
- [3] A. Bhardwaj and H. El-Ocla, "Multipath Routing Protocol Using Genetic Algorithm in Mobile Ad Hoc Networks," IEEE Access, vol. 8, pp. 177534-177548, 2020, doi: 10.1109/ACCESS.2020.3027043.
- [4] D. Ramphull, A. E. U. Mungur, S. Armoogum, and S. Pudaruth, "A Review of Mobile Ad hoc NETWORK (MANET) Protocols and their Applications," in Proc. 5th International Conference on Intelligent Computing and Control Systems, 2021, doi: 10.1109/ICICCS51141.2021.9432258.
- [5] P. Rajendra Prasad and Shivashankar, "Enhanced Energy Efficient Secure Routing Protocol for Mobile Ad-Hoc Network," Global Transitions Proceedings, vol. 3, no. 2, pp. 412-423, 2022, doi: 10.1016/j.gltp.2021.10.001.
- [6] M. S. Ayub, P. Adasme, D. Carrillo Melgarejo, R. L. Rosa, and D. Zegarra Rodriguez, "Intelligent Hello Dissemination Model for FANET Routing Protocols," IEEE Access, vol. 10, pp. 46513-46525, 2022, doi: 10.1109/ACCESS.2022.3170066.
- [7] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah, and Y. Alotaibi, "A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks," IEEE Access, vol. 10, pp. 14260-14269, 2022, doi: 10.1109/ACCESS.2022.3144679.
- [8] S. Shafi, S. Mounika, and S. Velliangiri, "Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET," Procedia Computer Science, vol. 218, pp. 2309-2318, 2023, doi: 10.1016/j.procs.2023.01.206.

- [9] M. R. Jose and S. M. C. Vigila, "F-CAPSO: Fuzzy Chaos Adaptive Particle Swarm Optimization for Energy-Efficient and Secure Data Transmission in MANET," *Expert Systems with Applications*, vol. 234, Art. no. 120944, 2023, doi: 10.1016/j.eswa.2023.120944.
- [10] A. R. Patil and G. M. Borkar, "Node Authentication and Encrypted Data Transmission in Mobile Ad Hoc Network Using the Swarm Intelligence-Based Secure Ad-Hoc On-Demand Distance Vector Algorithm," *IET Wireless Sensor Systems*, vol. 13, no. 6, pp. 201-215, 2023, doi: 10.1049/wss2.12068.
- [11] M. Rao, P. Chaudhary, K. Sheoran, and G. Dhand, "A Secure Routing Protocol Using Hybrid Deep Regression Based Trust Evaluation and Clustering for Mobile Ad-Hoc Network," *Peer-to-Peer Networking and Applications*, vol. 16, no. 6, pp. 2794-2810, 2023, doi: 10.1007/s12083-023-01560-3.
- [12] G. R. Rama Devi, M. Swamy Das, and M. V. Ramana Murthy, "Secure Cross-Layer Routing Protocol with Authentication Key Management Scheme for MANETs," *Measurement: Sensors*, vol. 29, Art. no. 100869, 2023, doi: 10.1016/j.measen.2023.100869.