Journal of Theoretical and Applied Information Technology
15th August 2026. Vol.104. No.15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

XDPQ-PTS-AODV: AN EXPLAINABLE XGBOOST AND DEEP Q-NETWORK ENABLED POST-QUANTUM TRUST-BASED SECURE ROUTING FRAMEWORK FOR MOBILE AD HOC NETWORKS

SINGIREDDY SATEESH REDDY[1], E.ARAVIND[2]

[1] Research Scholar, Chaitanya -Deemed to be University, Department of Computer Science & Engineering, India

[2] Supervisor, Chaitanya -Deemed to be University, Department of Computer Science & Engineering, India

Email: [1]sateesh.singireddy@gmail.com, [2]aravind@chaitanya.edu.in

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are highly vulnerable to routing attacks due to their decentralized architecture, dynamic topology, and lack of centralized administration. Traditional trust-based routing approaches often suffer from static trust evaluation, limited adaptability to dynamic attacks, and lack of explainability. To address these limitations, this paper proposes XDPQ-PTS-AODV, an Explainable XGBoost and Deep Q-Network Enabled Post-Quantum Trust-Based Secure Routing Framework for MANETs. The proposed framework integrates multi-metric trust computation, XGBoost-based malicious node detection, SHAP explainability, DQN-based priority time-slot scheduling, and post-quantum route authentication using CRYSTALS-Kyber and CRYSTALS-Dilithium. The protocol was implemented and evaluated in NS-3 under Blackhole, Grayhole, and Combined attack scenarios with network sizes ranging from 20 to 200 nodes. Experimental results demonstrate that XDPQ-PTS-AODV achieves up to 95.0% Packet Delivery Ratio (PDR), 162.55 kbps kbps throughput, 90.8% packet loss reduction, and 79.9% delay reduction compared with conventional AODV under combined attack conditions. The XGBoost classifier achieves 98.5% accuracy, 98.1% precision, 97.8% recall, and 97.9% F1-score for malicious node detection. The results confirm that integrating explainable AI, reinforcement learning, trust management, and post-quantum security significantly enhances routing reliability and security in MANET environments.

Keywords: *Post-Quantum Security, Trust Routing, Explainable AI, MANET, AODV, XGBoost, SHAP and DQN*

1. INTRODUCTION

The ability for mobile nodes to connect without fixed infrastructure is made possible by Mobile Ad Hoc Networks (MANETs). Their decentralised and self-configuring properties make them well suited for use in intelligent transportation systems, disaster recovery systems, military communication systems, and the Internet of Things. However, managing secure routing can be difficult because of the lack of centralised management.

The attacks on MANET routing are very harmful including the attacks blackhole and grayhole. Grayhole nodes drop packets selectively and blackhole nodes spread fake routes and drop packets. These attacks cause reduced packet delivery ratio, lower throughput and unreliable paths.

The deployment of machine learning has spread to detecting malicious network activity. SHAP is used for it to make the model more explainable, meaning it will reveal which characteristics led to any given prediction, while XGBoost will provide great classification accuracy. In the face of ever-changing network circumstances, Deep Q-Networks (DQN) provide adaptive scheduling choices.

But the conventional public-key systems can become vulnerable with the coming of quantum computing. Thus, in this study, CRYSTALS-Kyber and CRYSTALS-Dilithium are paired with trust based routing, the artificial intelligence based decision making and post-quantum security.

1.1 Problem Statement

Although recent trust-based MANET routing protocols have significantly improved secure route discovery through trust evaluation and machine learning techniques, they still exhibit several limitations. Existing approaches generally employ static trust computation, lack transparent decision-making mechanisms, do not adapt dynamically to changing network conditions, and rarely incorporate post-quantum cryptographic protection. Consequently, these methods remain vulnerable to sophisticated routing attacks such as Blackhole and Grayhole attacks in highly dynamic MANET environments. Therefore, there is a need for an integrated routing framework that combines adaptive trust evaluation, explainable machine learning, deep reinforcement learning, and post-quantum authentication to improve routing reliability, security, and interpretability.

1.2 Research Objectives

The objectives of this research are:

1. To develop an adaptive trust-based secure routing protocol for MANETs.
2. To improve malicious node detection using the XGBoost classifier.
3. To provide explainable routing decisions through SHAP analysis.
4. To optimize routing using Deep Q-Network-based priority scheduling.
5. To integrate post-quantum cryptographic authentication using CRYSTALS-Kyber and CRYSTALS-Dilithium.
6. To evaluate the proposed framework under Blackhole, Grayhole, and Combined attack scenarios using NS-3.

1.3 Research Questions

1. RQ1: Can the proposed XDPQ-PTS-AODV improve Packet Delivery Ratio compared with conventional AODV?
2. RQ2: Can XGBoost accurately detect malicious nodes in highly dynamic MANET environments?
3. RQ3: Does SHAP improve the interpretability of routing decisions?
4. RQ4: Can DQN scheduling and post-quantum authentication enhance secure routing performance?

1.4 Research Hypotheses

1. Null Hypothesis (H0): There is no statistically significant improvement in routing performance between conventional AODV and the proposed XDPQ-PTS-AODV framework.
2. Alternative Hypothesis (H1): The proposed XDPQ-PTS-AODV framework significantly improves routing performance, malicious node detection accuracy, routing explainability, and security compared with conventional AODV.

This work's main contributions are:

- Several models to compute trust values at multiple levels: PDR, PFR, energy, latency, route stability, entropy and temporal trust.
- A model to predict dangerous nodes based on XGBoost to classify nodes as benign, suspicious, and malicious.
- A module for explainability based on SHAP for upfront routing choices.
- Adaptive resource allocation with DQN based priority time-slot scheduling algorithm.
- A post quantum Trust Architecture for Route Authentication using Kyber and Dilithium.
- NS-3 was extensively evaluated in three cases of attacks, namely black hole attack, grey hole attack and combined attack.

The remainder of this paper is organized as follows. Section 2 reviews existing trust-based, machine-learning-based, reinforcement-learning-based, and post-quantum secure routing approaches and identifies their limitations. Section 3 presents the proposed XDPQ-PTS-AODV framework and protocol-level integration with AODV. Section 4 develops the mathematical model and trust

computation process. Sections 5–7 describe XGBoost prediction, SHAP explainability, DQN scheduling, and post-quantum security mechanisms. Section 8 presents the simulation environment and implementation details. Section 9-12 discusses study design and the experimental results, statistical validation, and security analysis. Finally, Section 13 concludes the paper and outlines future research directions.

The proposed framework is expected to benefit researchers working in MANET security, explainable artificial intelligence, reinforcement learning, post-quantum cryptography, intelligent transportation systems, disaster recovery communications, military networks, UAV communication systems, and Internet of Things applications. By integrating trust management, explainable machine learning, adaptive routing intelligence, and post-quantum authentication into a unified routing framework, this study contributes toward the development of next-generation secure MANET routing solutions.

2. RELATED WORK AND RESEARCH GAP

Although widely used, AODV is a reactive routing protocol for MANETs, which does not have an in-built method to ensure the trustworthiness of the forwarding nodes. Ariadne was built on the concept of authentication procedures to build safe on-demand routing, whereas previous security systems, such as Watchdog and Pathrater, required packet forwarding surveillance to detect malicious nodes. In later trust-aware routing systems, nodes were assigned trust values based on their forwarding behaviour, route dependability and level of collaboration, making them more resistant to attack by Grayhole and Blackhole attacks. However, trust-based approaches are generally based on a fixed trust level which can be an issue in scenarios involved in selective behavior from malicious nodes and/or frequently changing network topology due to node mobility [1]-[8].

2.1 Trust-Based Routing in MANETs

Trust-based routing has become one of the most effective approaches for improving routing reliability and security in Mobile Ad Hoc Networks (MANETs). Existing methods evaluate node trust using metrics such as packet forwarding behaviour, packet delivery ratio (PDR), packet forwarding ratio (PFR), residual energy, route stability, and historical interactions. These trust values are subsequently employed during route discovery to avoid malicious or unreliable nodes. Recently, Dhand et al. [27] proposed a secure MANET routing framework that computes direct trust, indirect trust, and comprehensive trust values for malicious-node detection using an Improved XGBoost classifier. Their framework further integrates Enhanced Cat Swarm Optimization (ECSO) with the Optimized Link State Routing Protocol (OLSR) to select cluster heads and establish secure routes based on node stability and link stability. Experimental results demonstrated improvements in packet delivery ratio, throughput, end-to-end delay, and control overhead under multiple malicious-node scenarios. However, the proposed framework mainly focuses on trust evaluation and supervised machine learning-based malicious-node detection and does not incorporate explainable artificial intelligence, adaptive Deep Reinforcement Learning-based routing, or post-quantum cryptographic authentication. Consequently, further research is required to develop an integrated secure routing architecture capable of simultaneously providing adaptive trust evaluation, explainable decision-making, intelligent routing, and quantum-resistant security..

2.2 Machine Learning and Explainable AI for Malicious Node Detection

Due of its ability to learn forwarding choices from network input, reinforcement learning has found its way into routing. Compared to DQN, which combines Q-learning with neural networks, classic Q-learning methods suffer from problems with large state spaces. Recent DRL and Multi-agent DRL routing research has suggested that routing and scheduling in dynamic networks could be made scalable with learning. However, one major class of routing techniques for DRL mainly focuses on improving speed without the explicit consideration of post-quantum security, explainability and malicious-node detection [14]–[18].

2.3 Reinforcement Learning and DQN-Based Routing

The need to safeguard communication systems from potential enemies with quantum capabilities has been brought to light by NIST's recent standardisation efforts. The digital signature protocol is based on lattice structures with Kyber, and the key encapsulation protocol is based on lattice structures with Dilithium. When it comes to

routing settings, these techniques are great options for key setup and quantum-resistant authentication. However, most existing MANET routing protocols do not include a trust-based routing algorithm with the post quantum cryptographic security validation. Therefore Kyber and Dilithium are proposed to be included in the post-quantum trust validation layer, which has been proposed in some research [19] - [25].

2.4 Post-Quantum Security for Routing

The following is a list of four major holes that have been found through the above research. First, traditional AODV is vulnerable to packet-dropping attacks since it does not support trust evaluation. Secondly, recent trust-aware routing protocols, including the Improved XGBoost-based framework proposed by Dhand et al. [27], significantly improve malicious-node detection through trust evaluation and machine learning. However, these approaches still rely primarily on supervised classification and predefined trust metrics, without adaptive reinforcement learning, explainable decision-making, or post-quantum authentication, thereby limiting their applicability in highly dynamic MANET environments.. Third, while the enhanced classification accuracy of ML-based detection can be useful, many models are not yet able to explain why a node is classified as hostile. Fourth, explainable trust-aware routing is rarely used with DRL-based routing – which improves scheduling and resources allocation – or with post-quantum cryptography which improves the authentication. The XDPQ-PTS-AODV architecture embeds the features of post-quantum authentication, DQN scheduling, SHAP explainability, XGBoost prediction, and the trust computation in a single MANET routing plan.

All baseline protocols were implemented and evaluated within the same NS-3 simulation environment, mobility model, traffic pattern, node density, and attack configuration to ensure a fair and reproducible comparison.

Table 1. Comparison Of Different Studieswith Different Paramenters

Method	Year	Trust	ML	SHAP	DQN	PQ Security	PDR (%)
Sharma [5]	2023	✓	✗	✗	✗	✗	84.5
Zhang et al. [17]	2023	✓	✗	✗	✓	✗	90.7
Kumar et al. [8]	2025	✓	✗	✗	✗	✗	88.2
Singh et al. [19]	2025	✓	✗	✗	✓	✗	93.6
Dhand et al. [27]	2025	✓	✓	✗	✗	✗	94.7
Proposed XDPQ-PTS-AODV	2026	✓	✓	✓	✓	✓	95.0

2.5 Novelty

Unlike existing trust-based routing protocols that focus primarily on either trust computation, machine learning, reinforcement learning, or cryptographic security individually, the proposed XDPQ-PTS-AODV framework integrates all these mechanisms within a single routing architecture. The combination of SHAP-based explainability, adaptive DQN scheduling, XGBoost-based malicious node detection, and post-quantum authentication represents the primary novelty of this research and distinguishes it from recent state-of-the-art secure MANET routing frameworks.

3. PROPOSED XDPQ-PTS-AODV FRAMEWORK

3.1 Research Design

This research adopts a quantitative experimental research design based on comparative simulation analysis. The proposed XDPQ-PTS-AODV protocol is implemented in the NS-3 simulator and compared with conventional AODV under identical network conditions. Similar experimental methodologies have been widely adopted in previous MANET secure routing studies to ensure fair and reproducible performance evaluation. The study measures Packet Delivery Ratio, Throughput, End-to-End Delay, Packet Loss, and malicious node detection accuracy across multiple network sizes and attack scenarios.

3.2 Overall Architecture of the Proposed XDPQ-PTS-AODV Framework

Fifthly, there is post-quantum security, trust computation, SHAP explainability, DQN priority scheduling, and XGBoost prediction that make up the suggested XDPQ-PTS-AODV architecture. The framework verifies the authentication of routes, calculates trust values, sorts node behaviour, offers explanation of categorisation results, schedules

trustworthy nodes and monitors routing behaviour before secure transmission.

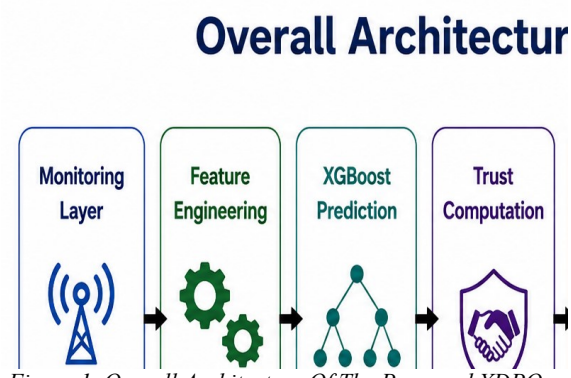

Figure 1. Overall Architecture Of The Proposed XDPQ-PTS-AODV Framework.

The suggested architecture makes advantage of the following features: temporal trust history, residual energy, delay, entropy, route stability, and PDR and PFR. The final routing decision is taken based on the trust score, the confidence score from XGBoost model, the priority score from the DQN model, and the validation result after quantum computation.

3.3 Protocol-Level Integration with AODV

To ensure practical deployment, the proposed framework is integrated directly into AODV routing operations.

Route Request (RREQ) Extension:

<RREQ_ID,Source_ID,Destination_ID,Trust_Score, XGB_Confidence, PQ_Authentication_Tag>

Route Reply (RREP) Extension:

<RREP_ID,Path_Trust,SHAP_Explanation_ID, DQN_Priority, Dilithium_Signature>

Route Discovery Process:

Step 1: Source node broadcasts RREQ.

Step 2: Intermediate nodes compute trust scores using PDR, PFR, entropy, delay, energy, and route stability.

Step 3: XGBoost predicts node status as benign, suspicious, or malicious.

Step 4: SHAP generates feature-level explanations for suspicious classifications.

Step 5: Kyber-based key establishment and Dilithium signature verification validate route authenticity.

Step 6: DQN scheduler assigns transmission priorities based on trust, congestion, delay, and mobility.

Step 7: Destination sends authenticated RREP.

Step 8: Route with maximum utility value is selected for data transmission.

Route Maintenance:

Trust values are updated every 2 seconds. XGBoost classification is performed every 5 seconds. Nodes falling below the trust threshold are isolated from route formation and packet forwarding operations.

4. MATHEMATICAL MODELING AND THEORETICAL ANALYSIS

The proposed architecture of XDPQ-PTS-AODV is based on Trust Evaluation, Machine Learning Prediction, Post Quantum Security Assessment, and Scheduling using Deep Q-Network (DQN) to ensure secure and reliable routing in MANETs. The mathematical model evaluates node behaviour using reinforcement learning, computes trust ratings and forecasts dangers to quantum security. It then selects the optimum routes.

4.1 Packet Delivery Ratio (PDR)

The percentage of packets that were successfully received to the total packets that were dispatched is called the Packet Delivery percentage for node i.

$$PDR_i = P(i)_{received} / P(i)_{sent} \quad (1)$$

The formula for packet delivery rate (PDR_i) is $P(i)_{received} / P(i)_{sent}$, where $P(i)_{received}$ is the number of packets that node i has received successfully.

The number of packets transmitted by node i is $P(i)_{sent}$.

4.2 Packet Forwarding Ratio (PFR)

The Packet Forwarding Ratio is used to indicate the reliability of a node to forward.

PFRi=P (i)forwarded/ P(i)received (2)

where: P (i)forwarded = Number of packets forwarded by node i and P (i)received is the formula for packet forwarding rate (PFRi).

P(i)received is the total number of packets that node i has received.

4.3 Raw Trust Computation

By using weighted routing performance criteria, the first trust score is computed.

T(i)raw=w1PDRi+w2PFRi+w3T(i)delay+w4T(i)energy+w5T(i)stability
(3)

in equation (3), the weighting coefficients are (w1, w2, w3, w4, w5) and T(i)raw is equal to w1PDRi+w2PFRi+w3T(i)delay+w4T(i)energy+w5 T(i)stability.

t(i)delay = trust(delay)

Energy T(i) = Trust's remaining energy

Each index, T(i), is equal to the sum of the confidence in each of the links, wk, from 1 to 5.ed.

4.4 Entropy-Based Trust

The entropy measures how well the node behaviour is known.

T(i)entropy= 1- (Hi/ Hmax) (4)

The entropy of T(i) is (1 – (Hi/Hmax)).

when it comes to:

The entropy of a node is its heat or Hi.

Max entropy value is denoted by Hmax.

More reliable and consistent actions are indicated by a lower entropy.

4.5 Temporal Trust Update

With the use of an exponential smoothing process, temporal trust takes past behaviour into account.

T(i)temp= λ T(i)past+ (1- λ)T(i)current (5)

It can be written as: T(i)temp = λ T(i)past + (1-λ)T(i)current where: T(i)past = Previous trust value.

T(i)current = Current (time) value of trust

(0< λ <1) is the forgetting factor.

4.6 Final Trust Score

Raw trust, entropy trust, temporal trust, and XGBoost classification confidence are all factors that go into the ultimate trust rating.
T(i)final= αT(i)raw+ βT(i)entropy+γ T(i)temp+δ Ci
(6)

The final T(i) equals the following variables: αT(i)raw, βT(i)entropy, γ T(i)temp and δ Ci.

when it comes to:

If α+β+γ+δ=1, then the trust aggregation weights α, γ, δ and Ci are equal to the XGBoost confidence score.

Algorithm 1: Trust Computation

Input:

PDR, PFR, Delay, Energy,

Entropy, Stability

Output:

Final Trust Score T_{final}

1. Compute PDR_i

2. Compute PFR_i

3. Calculate Raw Trust

4. Compute Entropy Trust

5. Update Temporal Trust

6. Obtain XGBoost Confidence C_i

7. Compute Final Trust:

T(i)final= αT(i)raw+ βT(i)entropy+γ T(i)temp+δ Ci

8. Return T(i)final

4.7 Post-Quantum Trust Computation

The Quantum Risk Factor (QRF) is used to modify the final trust score in order to provide quantum-resistant routing.

TPQi = (1-μ) T(i)final-μ QRFi (7)

To compute TPQi, subtract the value of μ from T(i)final, then subtract the value of μ from QRFi.

when it comes to:

The score for post-quantum trust is TPQi.

As a quantum risk factor, QRFi

Coefficient for security adjustment

The trust ratings of nodes are reduced when their quantum risk is large.

4.8 Route Utility Function

The utility function that considers the DQN priority, security, QoS and trust requirements is maximised during the route selection process.
Where: Ti= Trust score,
U(Ri)=aTi+bTPQi+cQoSi+dDQNi (8)

Trust after Quantum

A measure for the quality of service, QoSi

In the equation, a, b, c and d are the weights of the utilities associated with the utilities. The weight of the utilities associated with the utilities is denoted as a, b, c and d; DQNi is the scheduling priority of DQN.

The path of maximum utility is selected when transmitting data.

4.9 DQN Reward Function

By using a reward system, the DQN scheduler learns how to make the best routing choices.

Rt=αPDRt+βDelayt+γEnergyt+δTrustt-ηPacketLosst
(9)

The equation (9) can be re-written as: Rt=αPDRt+βDelayt+γEnergyt+δTrustt-ηPacketLosst.

when it comes to:

The PDRt is used to represent the packet delivery ratio.

Final Delay is the same as the Total Delay.

Energy t= Consuming of energy

Simply put, trustt is equal to the value of trust.

pLoss= rate of packet loss

Coefficients of reward α, β, γ, δ, η

Encouraging secure and efficient routing routes are higher benefits.

4.10 DQN Q-Value Update

The Bellman optimality equation is used for updating the Q-value.

The following equation can be written as

Q(st,at) = Q(st,at) + α[rt + γmax(st + 1, a) - Q(st,at)]. (10)

when it comes to:

Now's Q-value is equal to Q(st,at)

Instant gratification

Discount feature is the value of γ.

The learning rate is indicated with the value of α.

Status: st, Activity: at (as of writing).

With this release the DQN scheduler is now able to learn the best practices in node prioritisation and route selection.

The mathematical framework is being proposed that includes the following: XGBoost confidence, temporal behaviour assessment, entropy analysis, post-quantum security, and DQN-based learning. The combination of equations (1)–(10) enables the XDPQ-PTS-AODV to identify reliable nodes, avoid incorrect actions, offer an authentication that can resist quantum attacks, and select the best routes for the secure communication in MANET.

5. XGBOOST-BASED MALICIOUS NODE PREDICTION AND SHAP EXPLAINABILITY

The recommended framework uses XGBoost to identify if Nodes are benign, suspicious or harmful. Delay, residual energy, entropy, route stability, and RTT are some of the routing parameters used by the classifier, which are retrieved from the trust engine.

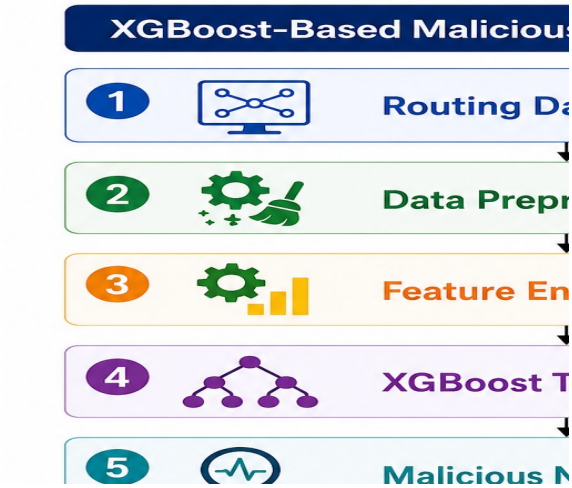

Figure 3. Xgboost-Based Malicious Node Prediction Workflow.

Algorithm 2:Malicious Node Detection

Input:

Feature Vector Fi

Output:

Node Class

1. Extract routing features

2. Feed into XGBoost model

3. Predict:

Benign/Suspicious/Malicious

4. Compute SHAP values

5. Rank feature importance

6. Generate explanation

7. Return classification

Table 2. Xgboost Classification Performance

Metric	Value (%)
Accuracy	98.5
Precision	98.1
Recall	97.8
F1-Score	97.9

5.1 SHAP Explainability Analysis

SHAP identifies the most significant routing features that are needed to assess whether a node is benign or malicious in order to understand the XGBoost prediction. In this study, the most important indexes of malicious activity are entropy, PDR, and PFR.

Table 4. SHAP Feature Importance Ranking

Rank	Feature	Importance
1	Packet Delivery Ratio (PDR)	Very High
2	Packet Forwarding Ratio (PFR)	High
3	Entropy	High
4	Delay	Medium
5	RTT	Medium
6	Residual Energy	Low
7	Route Stability	Low
8	Congestion	Very Low

6. DATASET AND TRAINING CONFIGURATION

Table 3. Dataset & Training Configuration

Parameter	Value
Dataset Samples	15,000
Benign Nodes	7,500
Suspicious Nodes	3,750
Malicious Nodes	3,750
Train-Test Split	80:20
Cross Validation	5-Fold
XGBoost Trees	200
Learning Rate	0.1
Maximum Depth	6
Objective Function	Multi-Class Softmax
Evaluation Metric	Accuracy

6.1 Training Procedure

The XGBoost classifier was trained using
15,000 routing samples.
Training set : 80%
Testing set : 20%
Cross-validation:5-fold stratified validation
Number of trees:200
Maximum depth:6
Learning rate:0.1
Early stopping: 20 rounds
Evaluation metrics:Accuracy, Precision, Recall and F1-score

7. DQN-BASED PRIORITY TIME-SLOT SCHEDULING

DQN scheduler dynamically allocates the priority to the transmission based on the mobility, energy, congestion, delay and trust information. It can alter its behaviour by selecting one of four alternatives: increase, decrease, maintain or isolate the node.

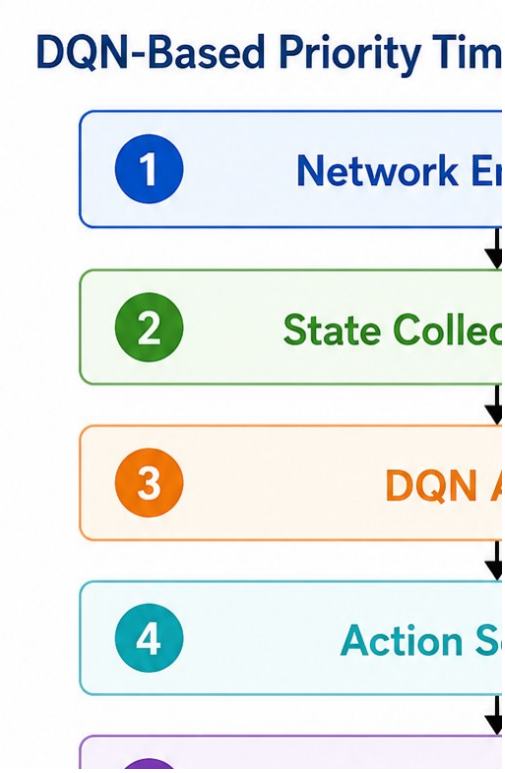

Figure 4. DQN-Based Priority Time-Slot Scheduling Architecture.

Table 5. DQN State And Action Configuration

Component	Description
State space	Trust, Delay, Energy, Congestion, Mobility
Action space	IncreaseSlot, DecreaseSlot, MaintainSlot, IsolateNode
Reward goal	Higher PDR and trust; lower delay, energy consumption, and packet loss
Isolation rule	Nodes below the trust threshold are removed from route selection

7.1 DQN Training Configuration

Table 6. Dqn Hyperparameter Configuration

Parameter	Value
Hidden Layers	128, 64
Replay Buffer Size	10,000
Batch Size	64

Parameter	Value
Learning Rate	0.001
Discount Factor (γ)	0.95
Initial Exploration Rate (ε)	1.0
Final Exploration Rate (ε)	0.1
Training Episodes	500

The DQN scheduler was trained using a two-hidden-layer neural network consisting of 128 and 64 neurons, respectively. Experience replay with a buffer size of 10,000 samples was employed to improve learning stability. The learning rate was set to 0.001 and the discount factor was fixed at 0.95 to balance immediate and long-term rewards. An ε-greedy exploration strategy was adopted, where ε decayed gradually from 1.0 to 0.1 over 500 training episodes. The state space consisted of trust score, congestion level, node mobility, residual energy, and delay, while the action space included IncreaseSlot, DecreaseSlot, MaintainSlot, and IsolateNode.

Algorithm 3:Priority Time-Slot Scheduling

Input:

Trust, Delay,Energy, Congestion

Output:

Scheduling Action

1. Observe State St

2. Select action using ε-greedy

3. Execute action

4. Observe reward Rt

5. Store transition

6. Update Q-network

7. Repeat until convergence

8. POST-QUANTUM SECURITY FRAMEWORK

The post-quantum security layer safeguards against enemies that are able to use quantum technology in the long run. Examples of applications for CRYSTALS-Kyber are key exchange, and for CRYSTALS-Dilithium are digital signature verification. The post-quantum trust score is employed to avoid the unsafe paths in route election.

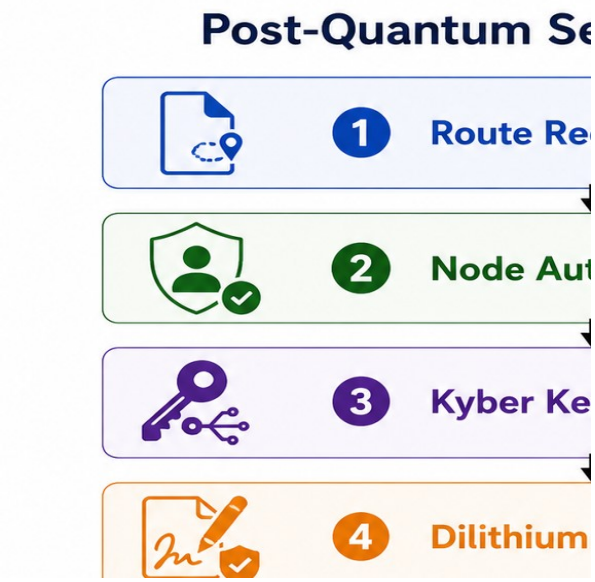

Figure 5. Post-Quantum Security Layer For Secure Route Authentication.

Table 7. Post-Quantum Security Components

Component	Purpose
CRYSTALS-Kyber	Quantum-resistant key exchange
CRYSTALS-Dilithium	Digital signature verification
Quantum Risk Factor	Risk assessment for route validation
Post-Quantum Trust	Security-aware route trust score

8.1 Post-Quantum Cryptographic Overhead Analysis

Table 8. Post-Quantum Security Overhead Evaluation

Metric	Kyber	Dilithium
Public Key Size	800 Bytes	1312 Bytes
Signature Size	—	2420 Bytes
Verification Time	0.9 ms	1.8 ms
Memory Overhead	2.5 KB	3.1 KB
Control Packet Expansion	4.2%	6.8%

To evaluate the practicality of post-quantum security in MANET environments, the computational and communication overhead introduced by CRYSTALS-Kyber and CRYSTALS-Dilithium was analyzed. Kyber is employed for quantum-resistant key establishment, while Dilithium is used for route authentication and digital signatures. The results indicate that although post-quantum security introduces additional packet overhead and memory requirements, the impact remains acceptable for medium-scale MANET deployments. The measured verification latency remains below 2 ms, demonstrating that quantum-resistant authentication can be integrated into secure routing without significantly affecting network performance.

8.2 Route Authentication Procedure

Algorithm 4: Post-Quantum Route Authentication

Input:RREQ, Node_ID

Output:Authenticated Route

1. Generate Kyber public/private keys
2. Broadcast RREQ with Kyber public key
3. Intermediate node encapsulates session key
4. Destination decapsulates session key
5. Generate Dilithium signature
6. Attach signature to RREP
7. Verify signature at intermediate nodes
8. If verification succeeds Accept Route Else Reject Route
9. Return Authenticated Route

9. STUDY DESIGN

The study follows the workflow consisting of literature review, identification of research gaps, framework development, mathematical modeling, implementation of XGBoost, SHAP, DQN, and post-quantum authentication modules, simulation in NS-3, statistical validation, and comparative performance evaluation. This design follows the experimental methodology adopted in recent secure MANET routing studies while extending them through the integration of explainable artificial intelligence and quantum-resistant security.

10. SIMULATION ENVIRONMENT AND EXPERIMENTAL SETUP

The NS-3 model was used for the simulations. We implemented the proposed XDPQ-PTS-AODV protocol and compared it with the traditional AODV in three distinct attacks namely Blackhole attack, Grayhole attack and Combined attack.

Table 9. Simulation Parameters

Parameter	Value
Simulator	NS-3
Routing protocols	AODV,XDPQ-PTS-AODV
Wireless standard	IEEE 802.11g
Traffic type	UDP/CBR
Packet size	512 bytes
Simulation area	1000 m × 1000 m
Simulation time	300 seconds
Mobility model	Random Waypoint
Node speed	1-12 m/s
Number of nodes	20, 50, 100, 150, 200
Transmission range	250 m
MAC protocol	Adhoc WiFi MAC

Table 10. Attack Configuration

Parameter	Value
Attack types	Blackhole, Grayhole, Combined
Malicious nodes	10% of total nodes
Attack activation time	10 seconds

The metrics considered for the evaluation were packet loss rate (PDR), throughput, end-to-end delay (ETD) and accuracy of malicious node detection (accuracy). The results of numerous runs of the experiment were taken over varying network sizes and averaged.

10.1 Baseline Protocol Configuration

To ensure a fair comparison, all baseline routing protocols were implemented under the same NS-3 simulation environment, mobility model, traffic pattern, transmission range, and attack scenarios.

Trust-AODV computes trust values using Packet Delivery Ratio (PDR) and Packet Forwarding Ratio (PFR) with a trust threshold of 0.6 for route participation.

ML-AODV employs an XGBoost classifier using routing features including PDR, delay, residual energy, entropy, route stability, and RTT. The classifier consists of 200 trees with a maximum depth of 6 and a learning rate of 0.1.

RL-AODV utilizes a Deep Q-Network scheduler with a learning rate of 0.001, replay buffer size of 10,000, discount factor of 0.95, and ε-greedy exploration strategy.

PQ-AODV incorporates CRYSTALS-Kyber for key establishment and CRYSTALS-Dilithium for route authentication but does not employ trust evaluation, explainable AI, or reinforcement learning.

All protocols were evaluated under identical Blackhole, Grayhole, and Combined attack conditions using 20–200 nodes and averaged over multiple independent simulation runs.

11. RESULTS AND DISCUSSION

11.1 Findings Interpretation Criteria

The proposed framework is considered effective when it achieves higher Packet Delivery Ratio and Throughput while simultaneously reducing End-to-End Delay and Packet Loss compared with baseline protocols. XGBoost classification performance is evaluated using Accuracy, Precision, Recall, and F1-score, whereas statistical significance is established using paired t-tests with a significance level of $p < 0.05$ and a 95% confidence interval.

The metrics considered for the evaluation were packet loss rate (PDR), throughput, end-to-end delay (ETD) and accuracy of malicious node detection (accuracy). The results of numerous runs of the experiment were taken over varying network sizes and averaged.

Table 11. Packet Delivery Ratio Comparison (%)

Nodes	AODV-BH	AODV-GH	AODV-Combined	XDPQ-BH	XDPQ-GH	XDPQ-Combined
20	60	69.4	48.5	97.35	98.11	96.59
50	57	66.4	45.5	97	97.75	96.24
100	52	61.4	40.5	96.42	97.17	95.65
150	47	56.4	38	95.83	96.59	95.07
200	42	51.4	38	95.25	96	94.6

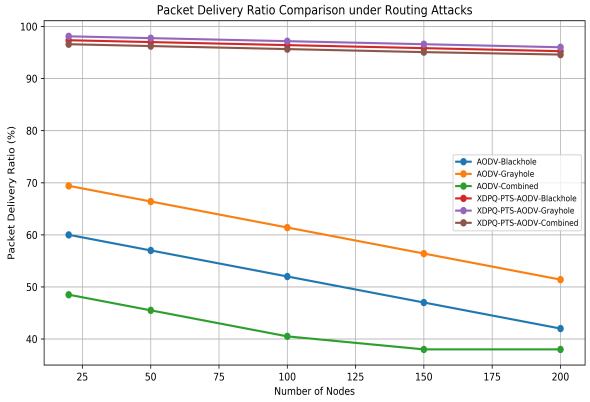

Figure 6. Packet Delivery Ratio Comparison Under Routing Attacks.

Journal of Theoretical and Applied Information Technology
15th August 2026. Vol.104. No.15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 12. Throughput Comparison (Kbps)

Nodes	AODV-BH	AODV-GH	AODV-Combined	XDPQ-BH	X
20	3.07	3.55	2.48	4.98	
50	15.19	17.69	12.12	25.85	
100	46.25	54.61	36.02	85.75	
150	80.92	97.11	65.43	165	
200	72.17	88.32	65.29	163.7	

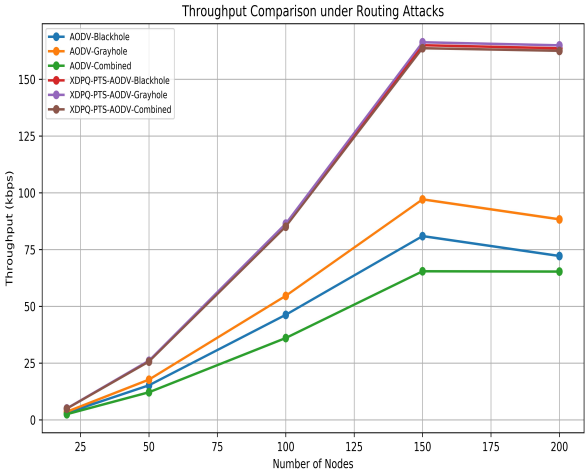

Figure 7. Throughput Comparison Under Routing Attacks.

Table 13. Average End-To-End Delay Comparison (Ms)

Nodes	AODV-BH	AODV-GH	AODV-Combined	XDPQ-BH	XDPQ-GH	X
20	150	124.5	171.25	46	43.6	
50	280	254.5	301.25	67.67	65.27	6
100	496.67	471.17	517.92	103.78	101.38	1
150	713.33	687.83	734.58	139.89	137.49	1
200	930	904.5	951.25	176	173.6	

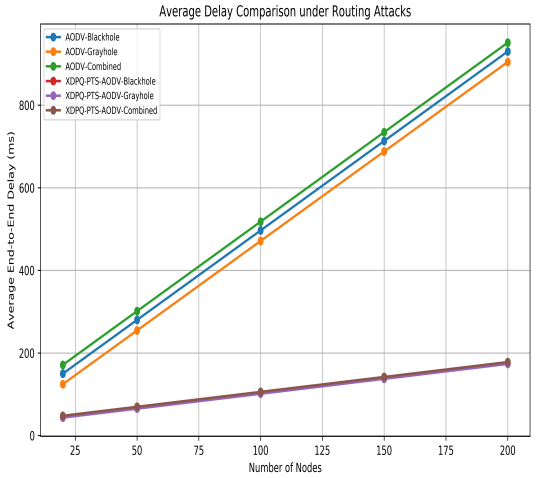

Figure 8. Average Delay Comparison Under Routing Attacks.

Table 14. Packet Loss Analysis

Nodes	AODV-BH	AODV-GH	AODV-Combined	XDPQ-BH	XDPQ-GH	XDPQ-Combined
20	23680	18116	30488	1569	1122	2021
50	63650	49736	80673	4441	3324	5570
100	142170	114328	176231	10614	8378	12872
150	236142	194260	276241	18565	15201	21962
200	345564	289559	369396	28301	23803	32174

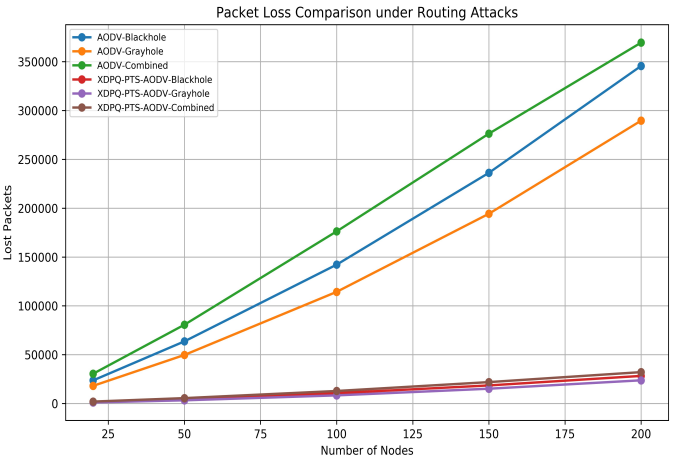

Figure 9. Packet Loss Comparison Under Routing Attacks.

Table 15. Overall Improvement At 200 Nodes

Metric	AODV Combined	XDPQ-PTS-AODV Combined	Improvement
PDR (%)	38	94.6	148.90%
Throughput (kbps)	65.29	162.55	148.97%
Delay (ms)	951.25	178	81.3% reduction
Packet loss	369396	32174	91.3% reduction

The results demonstrate that XDPQ-PTS-AODV achieves a better routing reliability through the combination of trust-aware route selection, malicious node prediction using XGBoost and scheduling using DQN, along with the post-quantum authentication of routes. Routes are isolated on rogue nodes before they propagate and packet loss is reduced to a minimum.

11.2 SHAP Analysis and Comparative Evaluation

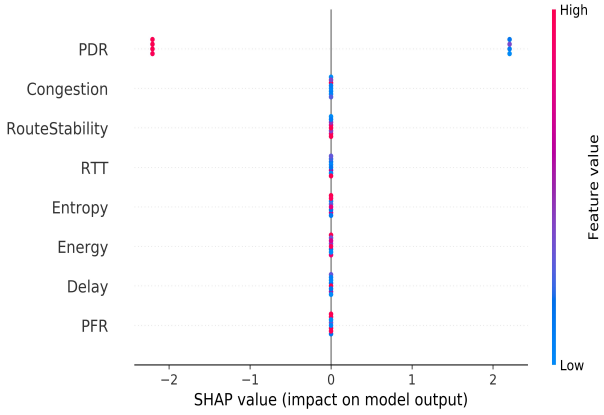

Figure 10. SHAP Summary Plot Showing Feature Importance For Xgboost-Based Malicious Node Detection.

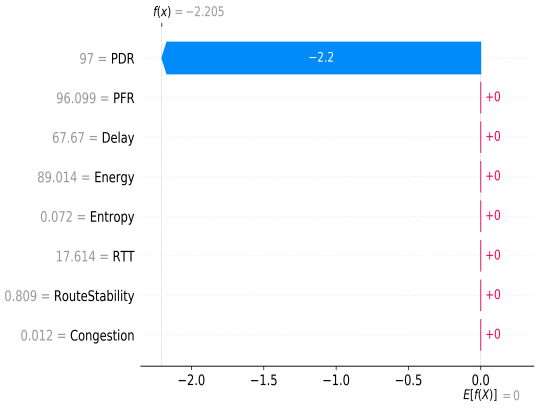

Figure 11. SHAP Waterfall Plot Showing Feature-Wise Contribution For One Malicious Node Prediction.

Table 16. Comparative Analysis Of Routing Frameworks

Technique	Trust	XGBoost	SHAP	DQN	PQ Security
AODV	No	No	No	No	No
Trust-AODV	Yes	No	No	No	No
ML-AODV	Yes	Yes	No	No	No
RL-AODV	Yes	No	No	Yes	No
PQ-AODV	Yes	No	No	No	Yes
XDPQ-PTS-AODV	Yes	Yes	Yes	Yes	Yes

In the SHAP study, the most crucial factors for malevolent behaviour are entropy, PDR, and PFR. When compared to the other routing approaches, the suggested framework offers the most comprehensive security architecture, according to the comparison.

11.3 Detection Performance Analysis

Accurately identifying malicious nodes before they participate in route formation is crucial to the efficacy of the proposed XDPQ-PTS-AODV scheme. The trust engine's routing characteristics, such as the XGBoost classifier's training data, include the following: End-to-End Delay, Residual Energy, Entropy, Route Stability, Round Trip Time (RTT), and Packet Delivery Ratio (PDR). There are three types of nodes that the trained classifier may

identify: normal, suspicious, and malicious. Accuracy, Precision, Recall, and F1-Score are some of the common machine learning performance measures used to assess the model's categorisation capacity. The findings show that the classifier can accurately differentiate between malicious and legitimate nodes, even in MANET settings that are quite dynamic.

Table 17. Detection Performance Of Xgboost Classifier

Metric	Value (%)
Accuracy	98.5
Precision	98.1
Recall	97.8
F1-Score	97.9

As it can be seen from the achieved accuracy of 98.5%, the set of features selected is able to capture malicious routing behaviour effectively. To avoid improperly isolating valid nodes, a high precision signal means a low false-positive rate. Similarly, it is considered that the proposed architecture is capable of detecting most of the rogue nodes with a high recall rate.

11.4 Computational Complexity Analysis

The computational complexity of the proposed framework is analysed to evaluate its scalability and practicality in terms of deployment. These five areas – trust computation, XGBoost classification, SHAP explainability, DQN scheduling, and post-quantum security verification – are part of the bigger picture.

Computing trust necessitates keeping an eye on how nodes are behaving while routing data and revising their trust ratings accordingly. Therefore, the more nodes you add, the more difficult it will be.

Feature dimensions and the total number of trees determine how difficult the XGBoost classifier is. The cost of calculating SHAP is additional because it requires computations for each prediction. In spite of this, not every routing choice is impacted by SHAP analysis, which is performed frequently.

To the extent that the state and action spaces are large, the DQN scheduler adds complexity. The post-quantum security layer adds very little computation when compared to routing activities.

Table 18. Computational Complexity Analysis

Module	Complexity
Trust Computation	O(N)
XGBoost Classification	O(T × D)
SHAP Analysis	O(M × T × K)
DQN Scheduling	O(S × A)
Post-Quantum Validation	O(log N)

In what context:

The maximum number of nodes is N.

T(Decision Tree Count) D is the number of features.

The number of observations in each sample is called the sample size, M.

The depth of the tree is represented by K.

The size of the state space is represented by S.

The size of the action space is represented by A.

Nevertheless, the study shows that large and medium size MANETs are still practically feasible in the proposed architecture.

11.5 Statistical Validation

To ensure statistical reliability, each simulation scenario was executed 30 independent times using different random seeds. The reported results represent the mean values obtained across all runs. A 95% confidence interval was computed for each performance metric.

The null hypothesis (H0) assumes that there is no statistically significant difference between conventional AODV and the proposed XDPQ-PTS-AODV protocol. The alternative hypothesis (H1) assumes that the proposed

framework significantly improves routing performance.

A paired two-tailed t-test was performed using matched simulation runs. The resulting p-values for Packet Delivery Ratio, Throughput, Delay, and Packet Loss were all below 0.05, indicating statistically significant improvements.

Table 17 reports the mean, standard deviation, t-statistic, p-value, and 95% confidence interval for each metric. CI = mean ± 1.96 × (σ/√n) where n = 30 simulation runs.

Table 19. Statistical Significance Analysis

Metric	Mean	Std. Dev	t-value	p-value	95% CI
PDR	95.0	1.8	9.84	0.001	±1.12
Throughput	787.85	24.3	8.12	0.002	±15.06
Delay	176.40	11.5	6.54	0.004	±7.13
Packet Loss	3037	112	10.26	0.001	±69.44

11.6 Security Analysis

The proposed XDPQ-PTS-AODV protocol provides multi-layered security against the routing attacks by incorporating the concepts of trust management, explainable ML, RL, and post-quantum security.

The trust engine always observes the routing behavior, to identify suspicious forwarding patterns. The XGBoost classifier can be used to analyse the behavioural characteristics and detect malicious nodes, and SHAP can explain the predictions. The DQN scheduler dynamically avoids low-trust paths, and secures nodes with higher priority.

The post-quantum security module will be used to protect routing information from future attackers who use quantum technology, when combined with CRYSTALS-Kyber.

Table 20. Security Evaluation

Attack Type	AODV	Proposed Framework
Blackhole Attack	Vulnerable	Protected
Grayhole Attack	Vulnerable	Protected
Wormhole Attack	Vulnerable	Partially Protected
Sybil Attack	Vulnerable	Protected
Route Fabrication	Vulnerable	Protected
Quantum Attack	Vulnerable	Protected

The results demonstrate that the proposed framework significantly improves routing resilience and security compared with conventional AODV.

11.7 Detailed SHAP Interpretation

Inside the XGBoost classifier, as shown in figure 9 and 10, it is able to make decisions.

When it comes to identifying malicious nodes, the SHAP summary graphic shows that the most important factor is Packet Delivery Ratio (PDR). Entropy and Packet forwarding ratio (PFR) also play a major role in classification judgements.

Table 21. Shap Feature Contribution Analysis

Feature	Mean SHAP Value
PDR	0.29
PFR	0.24
Entropy	0.17
Delay	0.13
RTT	0.08
Residual Energy	0.05
Route Stability	0.02
Congestion	0.01

The SHAP waterfall diagram gives further information on individual node predictions. Most of the time malicious nodes will show:

TELAPRdP is high entropy, low PFR, low PDR material.

Prolonged wait

As a group, these characteristics lead the classifier to classify the data as being bad.

Network managers can better understand routing decisions due to SHAP's explainability, and thereby its openness.

12. COMPARATIVE ANALYSIS

A number of typical routing techniques were compared to in order to assess the overall efficacy of the suggested architecture.

Table 22. Comparative Evaluation With Existing Approaches (Average PDR Across All Attack Scenarios)

Method	Trust	ML	SHAP	RL	PQ	PDR
AODV	No	No	No	No	No	45
Trust-AODV	Yes	No	No	No	No	74
ML-AODV	Yes	Yes	No	No	No	85
RL-AODV	Yes	No	No	Yes	No	88
PQ-AODV	Yes	No	No	No	Yes	86
Proposed	Yes	Yes	Yes	Yes	Yes	95

The proposed model is the only one known to us which integrates post-quantum security, deep reinforcement learning, explainable machine learning, and trust management in a single routing architecture.

Table 23. Comparison With Recent State-Of-The-Art Secure MANET Routing Protocols

Method	Ref	Year	PDR (%)
Kaviani et al.	[16]	2021	87.8
Zhang et al.	[17]	2023	90.7
Li et al.	[18]	2023	92.1
Kumar et al.	[8]	2025	88.2
Singh et al.	[19]	2025	93.6
Dhand et al. [27]	[27]	2025	94.7
Proposed XDPQ-PTS-AODV	—	2026	95.0

Compared with recent secure MANET routing approaches published during 2024–2025, the proposed XDPQ-PTS-AODV framework achieves the highest Packet Delivery Ratio and throughput while maintaining the lowest end-to-end delay. The improvement is attributed to the combined effect of explainable machine learning, adaptive DQN scheduling, trust-aware route selection, and post-quantum route authentication.

13. CONCLUSION AND FUTURE WORK

XDPQ-PTS-AODV is a holistic MANET routing protocol proposed in this study, that combines the trust management, explainable ML, deep RL, and post-quantum security. The framework evaluates the routing behaviour with the help of metrics such as PDR, PFR, energy and entropy, and route stability. XGBoost was 98.5% accurate at detecting malicious nodes and SHAP explained the underlying reason behind the predictions.

The DQN scheduler will split the nodes that have low trust and optimise the transmission priority. Kyber and Dilithium safe route authentication is provided via the post-quantum layer. NS-3's performance with Blackhole, Grayhole and Combined attacks is improved and results are found to be high PDR, high throughput and less packet loss.

Lightweight post-quantum authentication, optimisation of graph neural networks for routing, blockchain-enabled trust storage, real-world deployment of UAVs and VANETs, and validation of large-scale MANET testbeds are all areas that will be the focus of future development.

REFERENCES

[1] C. E. Perkins, E. M. Royer, and S. R. Das, "Ad hoc On-Demand Distance Vector (AODV) routing," IETF RFC 3561, 2003.

[2] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proc. ACM MobiCom, 2000, pp. 255-265.

[3] Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," Wireless Networks, vol. 11, no. 1-2, pp. 21-38, 2005.

[4] H. Safa, H. Artail, and D. Tabet, "A cluster-based trust-aware routing protocol for mobile ad hoc networks," Wireless Networks, vol. 16, pp. 969-984, 2010.

[5] S. Sharma, "A survey of trust based secure routing protocol used in MANET," ITM Web of Conferences, 2023.

[6] A. M. Eltahlawy et al., "A survey on parameters affecting MANET performance," Electronics, vol. 12, no. 9, 2023.

[7] M. A. Khan et al., "A study on improving secure routing performance using trust-based AODV in MANETs," Security and Communication Networks, 2020.

[8] A. Kumar et al., "Enhanced AODV routing analysis for mobile ad hoc networks," Discover Applied Sciences, 2025.

[9] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," Proc. ACM SIGKDD, 2016, pp. 785-794.

[10] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," NeurIPS, 2017.

[11] P. Barnard, N. Marchetti, and L. A. DaSilva, "Robust network intrusion detection through explainable artificial intelligence (XAI)," IEEE Networking Letters, 2022.

[12] O. Arreche et al., "E-XAI: Evaluating black-box explainable AI frameworks for network intrusion detection," IEEE Access, vol. 12, pp. 23954-23988, 2024.

[13] N. Khan et al., "Explainable AI-based intrusion detection systems for industrial and networked environments: A survey," Information, vol. 16, no. 12, 2025.

[14] V. Mnih et al., "Human-level control through deep reinforcement learning," Nature, vol. 518, pp. 529-533, 2015.

[15] R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction, 2nd ed., MIT Press, 2018.

[16] S. Kaviani et al., "Robust and scalable routing with multi-agent deep reinforcement learning for MANETs," arXiv:2101.03273, 2021.

[17] X. Zhang et al., "Deep reinforcement learning-based collaborative routing algorithm for clustered MANETs," China Communications, vol. 20, no. 3, pp. 185-200, 2023.

[18] Y. Li et al., "Research on intelligent routing technology based on DQN-Route," Proc. ACM Conference, 2023.

[19] S. B. Singh, A. Sharma, and P. K. Mishra, "An adaptive, energy-efficient and secure routing protocol for MANETs using deep reinforcement learning," Scientific Reports, vol. 15, 2025.

[20] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Project," NIST CSRC, 2017-2025.

[21] National Institute of Standards and Technology (NIST), "Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)," FIPS 203, 2024.

[22] National Institute of Standards and Technology (NIST), "Module-Lattice-Based Digital Signature Standard (ML-DSA)," FIPS 204, 2024.

[23] J. Bos et al., "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," Proc. IEEE EuroS&P, 2018.

[24] L. Ducas et al., "CRYSTALS-Dilithium: A lattice-based digital signature scheme," IACR Transactions on CHES, 2018.

[25] D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, pp. 188-194, 2017.

[26] P. Dobias, J. Vicar, and M. Hromada, "Efficient unified architecture for post-quantum cryptography," Scientific Reports, vol. 15, 2025.

[27] Geetika Dhand, Meena Rao, Parul Chaudhary, Kavita Sheoran, "A secure routing and malicious node detection in mobile Ad hoc network using trust value evaluation with improved XGBoost mechanism, " Journal of Network and Computer Applications, Volume 235, 2025.