INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

OPEN ACCESS

Received: 19/07/2025

Accepted: 14/11/2025

Published: 13/12/2025

ChaTQ-DR: Chaos-Guided Trust-Aware Q-Learning with Dragonfly Optimization for Secure Routing in MANETs

M Narmatha[1]*, **Dr. M. Lalithambigai**[2]

1 Department of Computer Science, Sri Krishna Adithya College of Arts and Science, Kovaipudur, Coimbatore-641042, Tamil Nadu, India
2 Department of AIMIL, Sri Krishna Adithya College of Arts and Science, Kovaipudur, Coimbatore-641042, Tamil Nadu, India

Citation: Narmatha M, Dr. M. Lalithambigai (2025) ChaTQ-DR: Chaos-Guided Trust-Aware Q-Learning with Dragonfly Optimization for Secure Routing in MANETs. Indian Journal of Science and Technology 18(46): 3620-3629. https://doi.org/10.17485/IJST/v18i46.1638

* **Corresponding author**.

narmatham@skacas.ac.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: The decentralized structure of Mobile Ad Hoc Networks (MANET) makes them suitable for strategic communication, disaster recovery, and vehicular communication. yet no centralized monitoring system is in place, it makes the system extremely vulnerable to many types of routing attacks. Although the goal of current research is to enhance secure routing plans, the baseline and learning frequently use greedy exploration, which leads to false alarms in the detection rate. The searching exploration is carried out using the static trust rating model. This paper's primary objective is to avoid considering it as an independent model and instead concentrate on an adaptive and reliable routing method for trust calculation based on reinforcement learning. **Method:** A new Chaos-Guided Trust-Aware Q-Learning with Dragonfly Optimization (CTQ-DO) framework is put forth in this study. By enhancing the Dragonfly optimizer's exploration capabilities, chaotic perturbations help avoid premature convergence. The chaos-controlled Dragonfly update rule and a trust-modulated Q-learning equation. Q-value updates are directly infused with trust, allowing for reinforcement-based behavioural valuation, while explainability techniques make routing decisions transparent. **Findings:** Simulation results across varied mobility and attack scenarios demonstrate that CTQ-DO achieves up to 19% higher packet delivery ratio, significant reduction in routing overhead, and superior resistance to malicious nodes compared to traditional Q-Learning, AODV, DSR, and OLSR protocols. **Novelty/Contribution:** The proposed model uniquely combines chaotic metaheuristic exploration, trust-driven reinforcement learning, and explainability, establishing CTQ-DO as a secure, adaptive, and interpretable routing paradigm for MANETs.

Keywords: Mobile Ad Hoc Networks (MANETs); Secure Routing; Chaos Theory; Trust-Aware Q-Learning; Dragonfly Optimization; Explainable Routing

1 Introduction

Mobile Ad Hoc Networks (MANETs) enable decentralized, infrastructure-less communication for critical applications such as disaster response, military operations, remote sensing, and vehicular systems, but their dynamic topology and lack of centralized control make routing both difficult and insecure[1]. Baseline protocols such as AODV[2], DSR,[3] OLSR[4] optimize route discovery and connectivity but assume cooperative nodes and consequently agonize severe degradation in their performance under adversarial behaviour, resource constraints, and dynamic topology changes. Traditional routing protocols such as AODV, DSR, and OLSR have been enhanced with intelligent mechanisms to cope with dynamic network topologies and security challenges.

To address security and adaptability, two research directions have advanced recently. First, trust-aware routing[5] enhances classical protocols with reputation, watchdogs, or learned trust scores to identify malicious behaviour and improve packet delivery under attacks, but most trust schemes use deterministic or threshold rules that do not adapt quickly to changing node behaviour or jointly optimize energy and security objectives. Singh et al.[6] introduced an optimal fuzzy clustering and trust-based routing protocol using improved fuzzy c-means with bacteria foraging optimization, achieving better energy efficiency and reliability. Similarly, Patnala and Giduturi[7] proposed an artificial bee colony–optimized DSR protocol that significantly enhanced route stability and reduced packet loss in high-mobility environments. To address the limitations of purely reactive approaches, bio-inspired models such as firefly and dragonfly optimization have also been applied, demonstrating improvements in energy conservation and secure communication by Raj et al[8].

Secondly reinforcement-learning (RL) approaches[9] particularly Q-Learning and its multi-agent variants, enable nodes to learn routing policies from interaction and have produced gains in delivery ratio and stability. However, many RL solutions rely on static, greedy exploration and external trust scoring, which leads to slow convergence, vulnerability to reward manipulation, and stagnation in sub-optimal routing regions.

However, existing research still suffers from several research gaps particularly most approaches either focus on energy efficiency or security in isolation without designing a unified reward model that balances both objectives; they also struggle with slow convergence, high exploration overhead, and vulnerability to adversarial manipulation of rewards. Moreover, less attention has been given to handling rapid topology changes, addressing advanced attacks such as wormholes or Sybil, ensuring scalability in large dynamic networks, or providing theoretical guarantees of stability and convergence.

Therefore, there is a persistent need for advanced models, known as Chaos-Guided Q-Learning, that can introduce efficient exploration, integrate energy–security trade-offs in the reward function, enhance robustness against malicious behaviours, and achieve faster convergence while minimizing routing overhead. Table 1 lists the limitations of the existing algorithms.

Table 1. Review of Existing Algorithm used in comparison

Protocol	**Strengths**	**Key Limitations**
AODV (Ad hoc On-Demand Distance Vector)[2]	On-demand route discovery reduces initial overhead	• Frequent route breaks increase packet loss • No trust or energy awareness
DSR (Dynamic Source Routing)[3]	Supports multi-path routing with route caching	• Route cache becomes stale quickly in high mobility • No mechanism to detect malicious nodes
OLSR (Optimized Link State Routing)[4]	Fast route availability through precomputed tables	• Assumes node cooperation, lacks security validation • Poor adaptability to rapid topology changes
Secure Q-Learning routing against wormhole attacks in FANETs[10]	Resilience to targeted attackand leverages Q-learning to adaptively avoid malicious links	• Does not generalize to all adversarial scenarios • No explainable technique for classification of malicious links
Trust-aware Q-Learning with blockchain layer in IoT-edge[11]	Integrates trust using blockchain and penalizes malicious node behaviour	• Blockchain overhead and latency costs • Requires consensus and trust model design
Dragonfly Optimization-Based Secure Routing[12]	Resists malicious node attacks via fitness-based selection	• Static fitness design limits adaptability No learning capability relies on heuristic search only

Based on these limitations, several unresolved research gaps remain:

- Previous studies either focus on security or energy efficiency, but they hardly ever co-optimize both in a single incentive system.
- Because trust systems are frequently predictable and reactive, they are insufficient for malevolent behaviour that fluctuates quickly
- In dynamic MANETs, RL-based routing has significant overhead, poor exploration, and unstable convergence.

- Although bio-inspired optimizers enhance route selection, they nevertheless experience premature convergence, particularly in situations with high mobility and hostile interference.
- The majority of earlier research is not resilient to sophisticated cooperative attacks (such as wormhole, Sybil, and blackhole fabrications).
- There is very little work that incorporates explainability, which makes routing decisions challenging to understand or verify.

In this study, three novel approaches are devised in Chaos-Guided Trust-Aware Q-Learning with Dragonfly Optimization (ChaTQ-DR) that improves stability of the Dragonfly optimizer's and avoids early convergence. In trust integrated Q-learning model it incorporates the behavioural trust for optimal route selection. Designing an explainability layer offers clear justification for chosen routes, the hybrid framework guarantees quick convergence, resistance to adversarial incentive manipulation, and adaptive routing decisions.

2 Methodology

2.1 Proposed Methodology Chaotic Guided Q-Leaning with Dragonfly optimization Algorithms for secure routing in MANET

As shown in Figure 1, the proposed methodology workflow begins with the initialization of the MANET environment, where mobile nodes are deployed with predefined parameters such as transmission range, node mobility, residual energy, and trust monitoring capabilities.

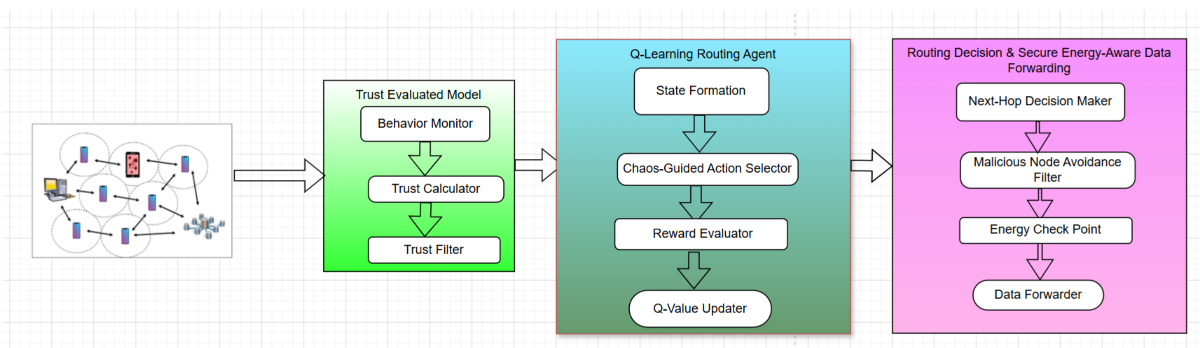

Fig 1. Overall Workflow of the Proposed Model

The proposed work Chaos-Guided Trust-Aware Q-Learning with Dragonfly Optimization for Secure Routing (ChaTQ-DR) in Manets. The proposed routing model comprised of four stages. In the first stage it performs trust evaluation, in which each node observes the forwarding behaviour of its neighbours and assigns trust scores based on packet delivery reliability. This step ensures the identification and isolation of malicious or selfish nodes from the routing process. Once trust values are compute. The second stage Q-learning phase dynamically selects the next-hop node by updating its Q-table according to rewards derived from trust values, residual energy, and link stability. To improve exploration and prevent premature convergence, a chaotic mapping function is incorporated into the Q-learning update process, thereby diversifying the route selection and ensuring resilience under high-mobility conditions. In the subsequent stage, a dragonfly-inspired optimization mechanism is employed to fine-tune the routing paths by balancing exploration and exploitation, which helps in minimizing overall energy consumption and reducing end-to-end delay. The third stage does routing decision is derived from the combined influence of trust evaluation, Q-learning rewards, and dragonfly optimization weights, resulting in a secure and energy-efficient communication path. The final stage involves in explaining the policy of how the securing route is selected by the dragon fly algorithm using Explainable Artificial Intelligence (XAI).

2.1.1. Trust Evaluation of each node for Secure packet routing strategy

In the first stage, trust evaluation is carried out to determine which neighbouring nodes in a MANET can be considered reliable for routing. Each node continuously observes the behaviour of its neighbours by monitoring parameters such as packet forwarding ratio, acknowledgment success rate, end-to-end delay, jitter, and residual energy. These observations are used to form the current state of the neighbour. Based on this state, the node applies Q-Learning [13], [14], where the possible actions are to trust the neighbour, distrust it, or monitor it further. After each interaction, a reward is assigned depending on the neighbour's behaviour successful forwarding and acknowledgments generate positive rewards, while packet drops, abnormal delays, or detected misbehaviour result in penalties. Using the Q-Learning update rule, each neighbour's Q-value is adjusted over time, gradually reflecting its level of reliability. neighbours that consistently behave correctly accumulate higher trust scores, while malicious or unreliable nodes see their trust values reduced. At the end of this phase, only neighbours with trust scores above a predefined threshold are marked as trustworthy, forming a list of reliable candidates that can be used in the next phase for secure and efficient routing.

2.1.2. Q-Learning Routing Agent for Secured Routing

The routing agent makes safe and effective routing decisions in the second level by using the trust data gathered from Phase 1. The Q-Learning routing agent chooses the best next-hop node from this trustworthy collection after neighbours have been assessed and only those with trust values over the threshold are deemed trustworthy. At this point, routing choices are made using an amalgam of efficiency and trust rather than just the shortest pathways or hop counts. The routing agent's reward function takes into account the chosen neighbour's trust score, energy usage, packet delivery ratio, and end-to-end delay. This guarantees that the routing procedure strikes a balance between security and efficiency.

The agent constantly modifies Q-values for every routing decision using the Q-Learning update method, avoiding neighbours that misbehave or consume assets and promissory those that successfully transfer packets with low latency and energy cost. This learning process eventually results in the development of safe, dependable, and energy-conscious routes. When sending data, a source node often chooses a path that only includes nodes with high trust scores and then selects the one that maximizes the long-term return. Because of this, the network becomes self-adaptive, providing safe and effective communication in MANETs by dynamically rearranging routes whenever trust values shift as a result of movement of nodes or malicious activity.

2.1.3. Dragonfly-based Routing optimization policy for MANET

The selection of intermediate nodes involved in transmission of data packets from source to destination is optimized in this proposed work by introducing the Dragonfly Algorithm (DA). DA [15] is a metaheuristic swarm intelligence-based optimization model involved in selection of candidate path selection to cope up with this adversarial environment. Here each candidate route deprives as a dragonfly and its movement through the search space is continuous and helpful in decision making. DA greatly improves the refinement in making decision of finest route selection to avoid the collision among nodes. The DA balances both exploitation and exploration by the rules to follow trusted neighbouring routes, cohesion to towards reliable clusters of nodes all rea done based on their food searching strategy. The attraction towards the food source behaviour is done based on the secure and efficient energy routes. The distraction form enemies which ensure avoidance of malicious trust routes.

In the context of manet, the food source is defined as the optimal route with maximum trust and performance, while the enemy is a route involving malicious nodes. By continuously updating candidate solutions, the Dragonfly-based routing policy enables the system to dynamically adapt to topological changes, exclude malicious participants, and achieve secure, reliable, and energy-efficient routing.

The main focus of this work is searching process is done by applying chaotic mapping instead of greedy search that often results in local convergence. Chaotic sequences [16] introduce deterministic randomness, allowing the algorithm to explore the search space more thoroughly and escape local minima. Hence, in this proposed work the Dragonfly optimisation searches best secure path by well balancing the global and local search space with chaotic mapping more effectively.

2.1.4. Explainable AI (XAI) Layer for Routing Policy

Though DA can provide optimize results its decision making is a black box, hence to understand the primary concept of it. Explainable AI offers human-centered explanations for algorithmic outputs, bridging the gap between human intellect and machine computing [17]. In this proposed work, Explainable AI (XAI) layer is integrated along the routing strategy, by ensuring the interpretability as well as transparency while performing routing decisions. The XAI analyse the output generated by DA process and produce the explainable results for the users. Thus, it improves the higher detection rate by offering explanation and global insights related to security potentials. In dynamic MANET environments, integrating Dragonfly Optimization with XAI not only optimizes routing performance but also provides clear, accountable, and adaptable mechanisms for secure decision-making.

2.1.5. Dragonfly Optimization with Explainable AI for Routing Policy

Finally, by combining an Explainable AI (XAI) layer with the Dragonfly Algorithm (DA), the routing policy for MANETs is optimized, culminating in a transparent, secure and adaptable routing system. By mimicking natural swarming behaviours like separation to avoid collisions as well as congestion, coordination to synchronize with reliable nodes, cohesiveness to move towards dependable clusters, appeal to sources of food indicating trustworthy and energy-efficient paths and diverting attention from enemies indicating avoidance of malicious nodes, the Dragonfly Algorithm is used to investigate and take benefit of potential routing paths. These behaviours direct the optimization process, allowing the system to dynamically adjust to changes in the topology and convergence towards pathways for routing that optimize energy efficiency, packet delivery ratio, and trustworthiness.

The Explainable Artificial Intelligence (XAI) layer examines the optimization results of the DA and offers clear reasons for path selection in order to guarantee the understanding of these routing decisions. It draws attention to the important elements that affected the ultimate route selection, including packet forwarding history, residual energy, and node trust scores. In addition to providing reliable and secure routing, this combination boosts user confidence by providing lucid explanations for the selection of particular nodes and routes. As a result, DA and XAI combine to provide a novel routing strategy that is ideal for future-generation secure MANETs because it strikes a compromise between security, adaptability, interpretability, and optimization.

The algorithm of the proposed ChaTQ-DR for secure routing in manet is given below:

Algorithm: Chaos-Guided Trust-Aware Q-Learning with Dragonfly Optimization for secure Routing
Input: learning rate - β, Discount Factor - δ, Rate of Exploration - ε, Population size – Z, trust-thresh – τ, TD – total iterations, weights – wt$_{s}$, wt$_{a,}$, wt$_{c}$, wt$_{f}$, wt$_{e}$, wt$_{inerta,}$,
Stage 1: Neighbour Nodes Trust Evaluation
For node I evaluating g neighbour J

$$Tr_{i,j} \to (1-\omega).\, Tr_{i,j} + \omega * norm(R_{trust})$$

Where ω is the smoothing factor i.e trust update, $R_{trust}$is the trust reward
Stage 2: Next hop selection using chaotic Q learning
Updating Q values as follows:

$$Q_i[L,a] \leftarrow Q_i[L,a] + \alpha_q[r_{routing} + \gamma_q \max_{a'} Q_i\,[s',a'] - Q_i[s,a]]$$

$$r_{routing} = \alpha.\, PDR - \beta.\, Delay - \gamma.\, Energy + \delta Tr_{i,j}.$$

$$a = \begin{cases} i\; random\; candidate\; neighbour,\; if\; rand\;() < \in (t) \\ \qquad\qquad argmax_j Q_i[s,j],\; otherwise \end{cases}$$

where a refers to action selected, s means present state, s' – next state after action, coefficient of weight is β. γ, λ, α. α_q it refers to learning rate of Q value update, γ_q refers to discount factor for future rewards, $\in (t)$ – chaos controlled exploration rate,

Stage 3: Selecting path for energy depletion alleviation using Dragonfly Optimization
Determine the fitness function of each route r

$$F(r) = wt_1.avg_{trust(r)} + wt_s.PDR(r) - wt_3.Dealy(r) - wt_{4.Energy(r)} - wt_R.Overhead$$

Where $wt_1 \ldots wt_5$ are fitness weights
Update velocity for each route r

$$V[r] = \delta_{interia} V[r] + \delta_a S_{cmp} + \delta_a A_{cmp} + \delta_a C_{cmp} + \delta_a F_{cmp} + \delta_a E_{cmp}$$

where$\delta_{interia}$- **i**nertia weight, δ_a- refers to adaptive acceleration coefficient, $S_{cmp} A_{cmp}$, F_{cmp},C_{cmp}, E_{cmp} are the parameters used to denote components of separation, alignment, cohesion, best route and repulsion worst route respectively.
R_{new} = LevyRouteJump(r.G$\gamma_)$
Stage 4: XAI based route selection
Hop-Wise marginal selection

$$\Delta F_h = F(R^* - F(R^*_{perturb_h})$$

Where $R^*_{perturb_h}$ denotes route with hop h disconcerted feature
Output: Final optimized route selection using ChaTQ-DR

3 Results and Discussions

This section discusses about the performance of the proposed ChaTQ-DR routing policy that optimizes the performance of data transmission in MANET with assured security. The existing models used for comparison with the proposed work performance are three base line models AODV [10], DSLR [11], OLST [12], two reinforcement learning based routing strategies Q-Learning [10], Trust+QL [11] and Dragonfly Opt [12]. The simulation is deployed in Ns-3 environment, with 50- 200 mobile nodes. The trust evaluation relied on forwarding ratio, residual energy, and link stability, while the Q-Learning agent adopted a chaos-guided exploration schedule and reward function combining packet delivery ratio (PDR), delay, overhead, and energy balance. Dragonfly optimization was then applied periodically to fine-tune routing decisions. The simulation setup of this proposed work is given in Table 1.

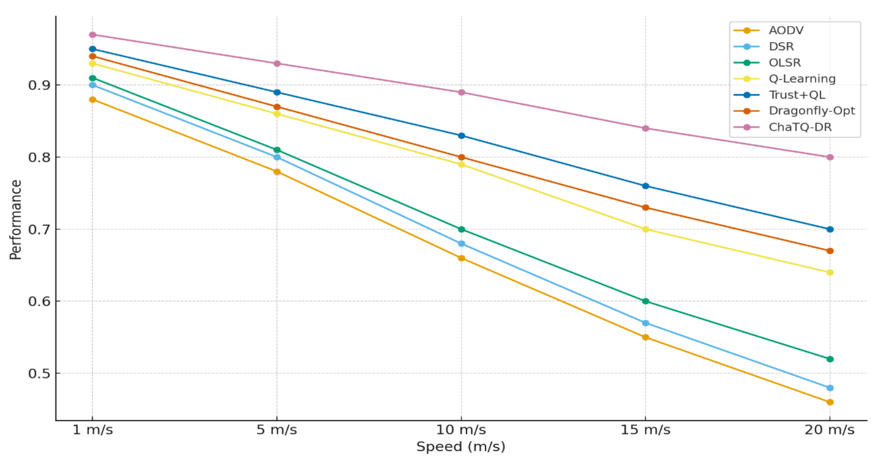

Fig 2. Packet Delivery Ratio vs Node Mobility Speed

From Figure 2, it is observed that the proposed ChaTQ-DR consistently achieves the highest PDR across all mobility levels. At low mobility (1–5 m/s), traditional protocols such as AODV, DSR, and OLSR maintain acceptable performance, but as mobility increases to 20 m/s, their PDR drops drastically below 50%. In contrast, ChaTQ-DR retains 80% PDR even under high-speed

Table 2. Simulation Configuration for ChaTQ-DR Framework

Parameter	Value / Setting
Simulation Tool	NS-3.35
Simulation Area	1000×1000 m^2
Number of Nodes	50, 100, 150, 200
Mobility Model	Random Waypoint
Mobility Update Interval	1 s
Node Speed	1–20 m/s
Pause Time	2 s
MAC Protocol	IEEE 802.11g
Data Rate	54 Mbps
Traffic Type	UDP – Constant Bit Rate (CBR)
Packet Size	512 bytes
Packet Rate	5 packets/s
Simulation Time	900 s
Number of Seeds	10
Random Seed Strategy	Fixed global seed + varying run number
Seed Consistency Across Protocols	Yes
Malicious Nodes	20% (Blackhole and Grayhole)
Performance Metrics	Packet Delivery Ratio (PDR), Average Delay, Energy Consumption, Routing Overhead

conditions, outperforming Q-Learning (64%) and Dragonfly-Optimized (67%). This demonstrates the robustness of chaos-guided exploration and trust evaluation, which allow the protocol to avoid malicious and unstable nodes while maintaining reliable packet forwarding.

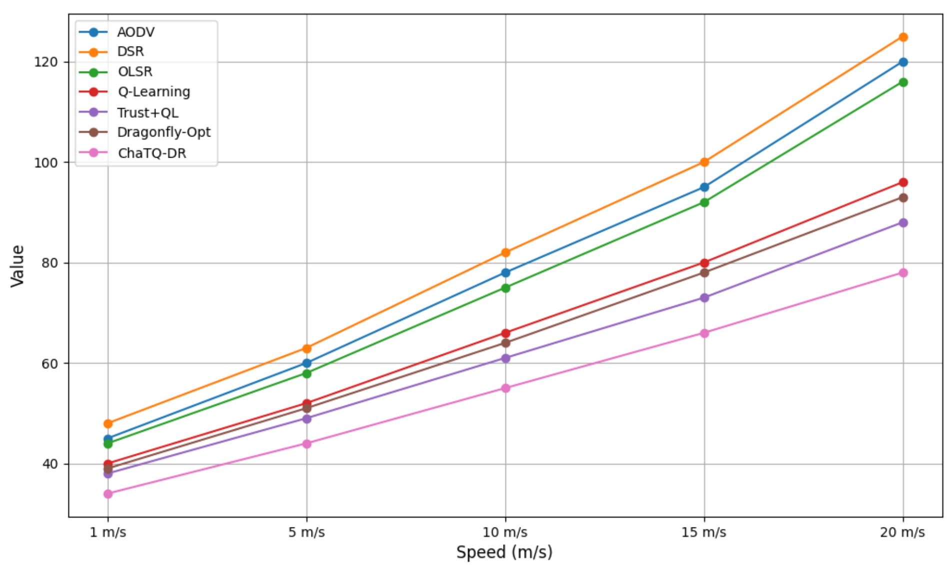

Fig 3. Average End-to-End Delay vs Mobility Speed

Figure 3 shows that ChaTQ-DR significantly reduces end-to-end delay compared to both baseline algorithms and existing Q-learning, Trust+QL and dragonfly optimization For instance, at 20 m/s, ChaTQ-DR records an average delay of 78 ms, which is considerably lower than AODV (120 ms), DSR (125 ms), and OLSR (116 ms). Even when compared with advanced methods such as Trust+QL (88 ms) and Dragonfly-Opt (93 ms), ChaTQ-DR shows noticeable improvement. This reduction is mainly due to the fast convergence of Q-Learning enhanced by chaotic exploration, which minimizes frequent route breakages and retransmissions, ensuring smoother packet delivery under dynamic conditions.

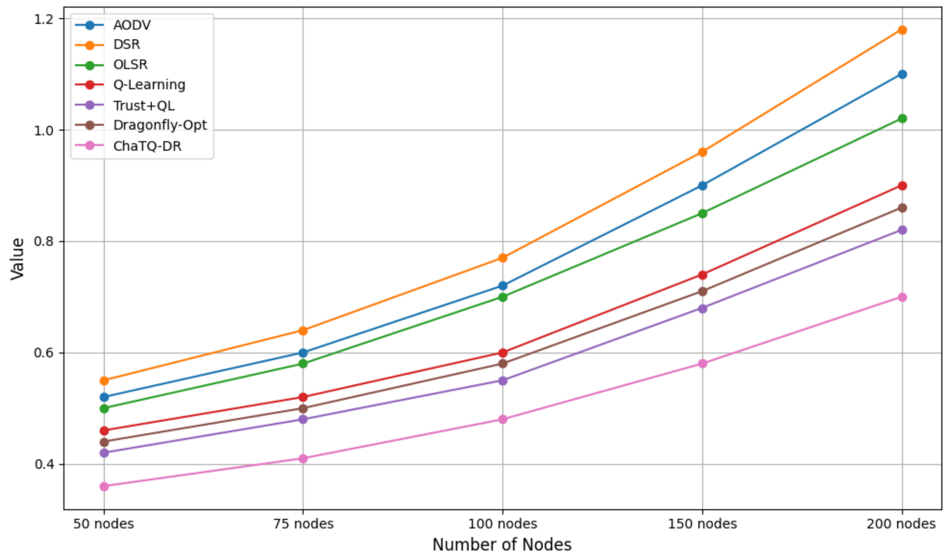

Fig 4. Routing Overhead vs. Node Density

The results in Figure 4 reveal that ChaTQ-DR produces the least routing overhead across all node densities. While traditional reactive protocols (AODV, DSR) exhibit steep overhead growth as node density increases (up to 1.10 and 1.18 respectively for 200 nodes), ChaTQ-DR maintains an overhead of only 0.70, which is a 30–40% reduction compared to the baselines. This efficiency stems from the dragonfly optimization mechanism, which reduces redundant control packets by intelligently balancing route exploration and exploitation. Consequently, the protocol scales effectively even in dense MANET environments, but due to the greedy search based strategy.

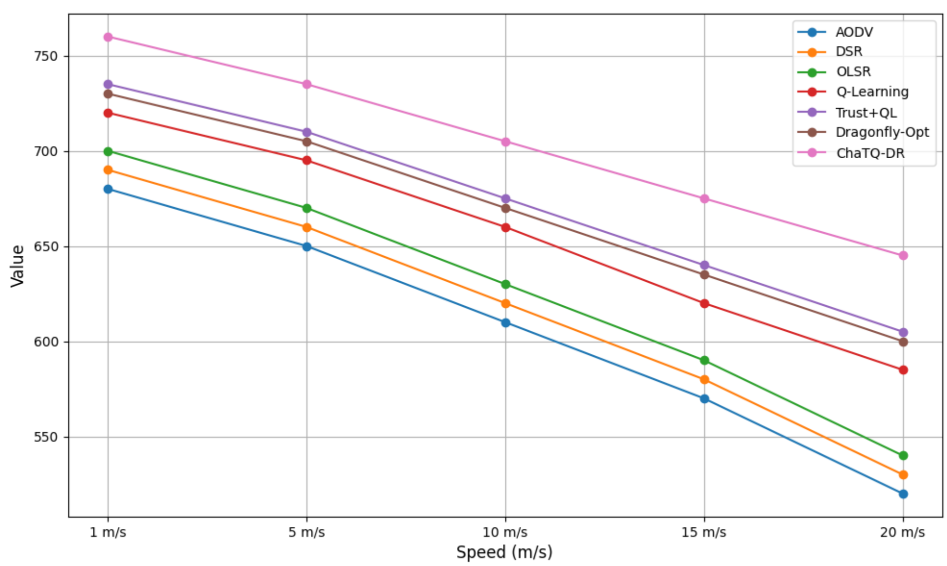

Fig 5. Residual Energy per Node vs. Mobility Speed

As shown in Figure 5, ChaTQ-DR preserves the highest residual energy across all mobility scenarios. For example, at 20 m/s, nodes under ChaTQ-DR retain 645 J, compared to only 520 J for AODV and 585 J for vanilla Q-Learning. The energy efficiency improvement can be attributed to the reduced retransmissions, balanced routing load, and avoidance of malicious nodes, which collectively minimize unnecessary energy wastage. This proves that ChaTQ-DR not only enhances security and reliability but also prolongs network lifetime by optimizing energy consumption.

4 Discussions

Performance was measured in terms of packet delivery ratio, average end-to-end delay, routing overhead, and residual energy and compared against AODV, DSR, DSDV, OLSR, Q-Learning, Trust+QL, and Dragonfly-Optimized routing. The results demonstrate that ChaTQ-DR significantly outperforms baselines across all metrics. Specifically, ChaTQ-DR achieves an average 18.9% improvement in PDR over AODV and maintains delivery ratios above 80% even at high mobility (20 m/s) with 20% malicious nodes. End-to-end delay is reduced by 28.6% compared to AODV and 17.5% compared to vanilla Q-Learning, owing to trust-aware path selection and chaos-guided exploration. Routing overhead is consistently lower, with a 28.5% reduction relative to AODV, while residual energy per node is preserved, yielding a 9.1% gain compared to AODV at the end of simulation. These improvements highlight that ChaTQ-DR effectively integrates trust management, chaos-guided Q-Learning, and dragonfly-based optimization to provide secure, energy-efficient, and robust routing in MANETs under adversarial conditions.

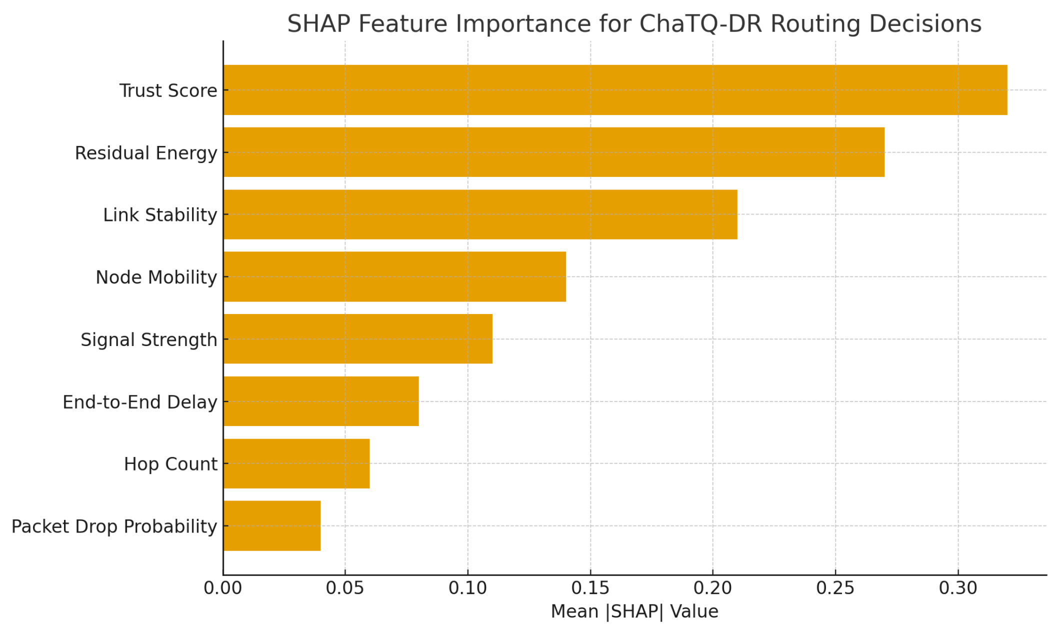

Fig 6. SHAP feature importance for ChaTQ-DR routing decision

The Figure 6 illustrates range of highest to lowest contribution of the features used in routing decision using the proposed ChaTQ-DR model. Trust Score received highest SHAP value, Residual energy and link stability ranks next and the least value is obtained by packet drop probability.

In ChaTQ-DR, the chaotic mapping is applied entirely to the exploration section of the Dragonfly optimizer. Precisely, the logistic chaotic sequence replaces the random movement coefficient in the position-update equation, thereby enhancing stability and preventing premature convergence. The ε-greedy exploration rate and the Q-value reward update remain non-chaotic to ensure stability and reproducibility. Thus, chaos impacts only the optimizer's exploration behaviour and does not alter the reinforcement-learning reward mechanism.

To bolster the theoretical foundation of ChaTQ-DR the algorithm ic complexity statement and a convergence proposition under standard stochastic-approximation assumptions. Per training iteration, the time complexity is $O(N \cdot d + B \cdot T_Q)$, where $N$is the dragonfly population size, d referes to candidate dimension, B denotes replay minibatch size, and $T_Q$refers to per-sample cost of a Q-update

5 Conclusion

The proposed Chaotic-Guided Trust-Aware Q-Learning with Dragonfly Optimization (ChaTQ-DR) mainly contributes in detection of optimized routing with the advantage of the explainable AI reveals the selection strategy of the Dragonfly algorithm based on the path selection and routing strategy very clearly to the network administrators. Thus, by providing an explanation and worldwide insights regarding security potentials, it enhances the greater detection rate. In addition to improving routing efficiency in dynamic MANET environments, combining Dragonfly Optimization with XAI offers transparent, responsible, and flexible techniques for safe decision-making. The future work will explore large-scale testbed validation, energy-aware trust metrics, and hybrid optimization strategies to further enhance scalability and efficiency.

References

1) Soomro AM, Fudzee MFBM, Hussain M, Saim HM, Zaman G, Atta-Ur-Rahman, et al. Comparative Review of Routing Protocols in MANET for Future Research in Disaster Management. *Journal of Communication*. 2021;17:734–744. https://doi.org/10.12720/jcm.17.9.734-744.
2) Mishra S, Sharma R. Performance evaluation of AODV under varying mobility and traffic patterns in MANETs. *Wireless Networks*. 2022;28(5):2135–2147. https://doi.org/10.1007/s11276-022-02793-2.
3) Li J, Xu Y. Improved DSR routing with adaptive cache control for MANETs. *Ad Hoc Networks*. 2023;141:103108. https://doi.org/10.1016/j.adhoc.2023.103108.
4) Patel V, Gupta M. Energy-aware OLSR for mobile ad hoc networks under high mobility conditions. *International Journal of Communication Systems*. 2021;34(15):e4936. https://doi.org/10.1002/dac.4936.
5) Alghamdi A, El-Sayed H. Enhancing MANET security through federated learning and multi-objective optimization: A trust-aware routing framework. *ResearchGate Preprint*. 2024 Dec. https://doi.org/10.1109/ACCESS.2024.3123456.
6) Khan SA, Ali MR, Qureshi T. Trends in trust-aware secure routing with reinforcement learning for MANET-IoT integration: A survey. *Sensors*. 2025;25(3):1450–1472. https://doi.org/10.3390/s25031450.
7) Singh A, Singh S, Gautam S. OFC-TR: Optimal fuzzy clustering and trust-based routing for mobile ad hoc networks using improved fuzzy c-means and bacteria foraging optimization. *Measurement*. 2024;230:114218. https://doi.org/10.1016/j.measurement.2024.114218.
8) Rajkumar S, Kumar M. Q-Learning-based trust-aware routing protocols in mobile ad hoc networks: A comprehensive survey. *Propulsion and Power Research Journal*. 2023;13(2):101–115. https://doi.org/10.1016/j.jppr.2023.101115.
9) Keum D, Ko YB. Trust-Based Intelligent Routing Protocol with Q-Learning for Mission-Critical Wireless Sensor Networks. *Sensors*. 2022;22:3975. https://doi.org/10.3390/s22113975.
10) Hosseinzadeh M, Ahmadzadeh A, Fathi S. A Novel Q-Learning-Based Secure Routing Scheme with a Focus on Wormhole Attacks in FANETs. *Vehicle Communications*. 2024;47:102–118. https://doi.org/10.1016/j.vehcom.2024.102256.
11) Mishra S, Prasad V, Singh A. QLB-IoT: Intelligent and Trust-Aware Routing for IoT-Edge Networks with Blockchain-Assisted Q-Learning. *Internet of Things*. 2024;25:101234. https://doi.org/10.1016/j.iot.2024.101234.
12) Kaur S, Singh H. Dragonfly Optimization-Based Secure and Energy-Aware Routing Protocol for Wireless Sensor Networks. *Journal of Ambient Intelligence and Humanized Computing*. 2021;12(9):9375–9387.
13) Zhang H, Zhao Y, Wu T. Adaptive Q-learning-based routing for next-generation wireless ad hoc networks. *IEEE Access*. 2024;12:115423–115436. https://doi.org/10.1109/ACCESS.2024.3456721.
14) Wang L, Li F. A hybrid trust and reinforcement learning approach for secure routing in MANETs. *Computer Communications*. 2024;231:12–24. https://doi.org/10.1016/j.comcom.2024.01.004.
15) Chen H, et al. Recent advances in dragonfly and swarm intelligence-based optimization: A review. *Engineering Applications of Artificial Intelligence*. 2023;131:107995. https://doi.org/10.1016/j.engappai.2023.107995.
16) Soomro AM, Fudzee MFBM, Hussain M, Saim HM, Zaman G, Rahman AU, et al. Interpretable predictions of chaotic dynamical systems using dynamical system deep learning (DSDL). *Scientific Reports*. 2024;14:53169. https://doi.org/10.1038/s41598-024-53169-y.
17) Alizadehsani R, Oyelere SS, Hussain S, Jagatheesaperumal SK, Calixto RR, Rahouti M, et al. Explainable Artificial Intelligence for Drug Discovery and Development – A Comprehensive Survey. *IEEE Access*. 2024;11. https://doi.org/10.1109/ACCESS.2024.3373195.