ISSN: 2093-5374 / E-ISSN: 2093-5382

TrustRank-Based Secure Routing in MANETs Using Quantum Ant Colony Optimization and Hybrid Grey Wolf–Jaya Optimization

Dr.G. Kalyani[1*], Dr. Mantri Gayatri[2], Dr. Nune Srinivas Rao[3], Dr. Yasmeen[4], and Dr. Katakam Srinivas[5]

[1*]Professor, Department of CSE-Cyber Security, Geethanjali College of Engineering and Technology, Hyderabad, India. ghanta.kalyani@gmail.com, https://orcid.org/0000-0002-3097-168X

[2]Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Bowrampet, Hyderabad, Telangana, India. gayatricse312@gmail.com, https://orcid.org/0000-0002-0730-2349

[3]Department of CSE (DS), Malla Reddy Engineering college for women (Autonomous), Hyderabad, Telangana, India. srinivasraon_cse@mrecw.co.in, https://orcid.org/0000-0003-0263-5088

[4]Senior Assistant Professor, Department of CSE (DS), CVR College of Engineering, Hyderabad, Telangana, India. yasmeen.aashu@cvr.ac.in, https://orcid.org/0000-0002-2227-1966

[5]Professor, Department of CSE Kshatriya College of Engineering, Armoor, Nizamabad, Telangana, India. katkamsrinu@gmail.com, https://orcid.org/0000-0002-7733-6237

Received: July 06, 2026; Revised: August 18, 2026; Accepted: September 04, 2026; Published: September 30, 2026

Abstract

The major problems associated with Mobile Ad-hoc Networks (MANETs) are node mobility, dynamic topology, and the presence of adversaries, making MANETs difficult in ensuring security, reliability, and energy efficiency in their communication. This research work suggests TrustRank-QACO-GWJO, which is a hybrid secure routing approach that combines Quantum Inspired Ant Colony Optimization (QACO), trust-based node selection, rule-based attack detection techniques, and Hybrid Grey Wolf-Jaya Optimization (GWJO). In this proposed scheme, node evaluation is performed based on a combined fitness function that considers distance, delay, energy dissipation, packet forwarding behavior, and security ranking. Nodes are categorized as secure, γ-risky, and risky, whereas a threshold-based packet forwarding mechanism is utilized for detection of black hole, selective forwarding, and wormhole attacks. QACO generates feasible candidate routes, followed by GWJO-based exploration and exploitation to select the optimal secure route. The simulations were carried out in MATLAB 2019a by considering 20 to 100 nodes, the Random Waypoint mobility model, a 300-second simulation period, CBR/UDP packet generation with 512-byte packet size, and 10% of malicious nodes. The proposed algorithm provides an improvement of 13.1% in Packet Delivery Ratio, a 30.8% decrease in end-to-end delay, a 32.8% increase in throughput, and a 25.1% decrease in energy consumption compared to the AODV

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 17, number: 3 (September-2026), pp. 1955-1976. DOI*: 10.58346/JOWUA.2026.I3.113*

*Corresponding author: Professor, Department of CSE-Cyber Security, Geethanjali College of Engineering and Technology, Hyderabad, India.

algorithm. The GWJO technique gives an 8% improvement in terms of convergence compared to GWO. This suggests that the incorporation of the trust-aware security analysis, QACO-based route discovery, and GWJO can be useful for enhancing routing reliability and communication efficiency.

Keywords: MANET, TrustRank, Quantum-Inspired Ant Colony Optimization, Grey Wolf–Jaya Optimization, Secure Routing.

1 Introduction

Now a day Mobile Ad-Hoc Networks (MANETs) have gathered a lot of interest because of the infrastructure-less deployment, decentralized architecture, and quick adaptation under dynamic conditions. These networks are widely operated in mobile IoT situations, military communications, disaster recovery, and vehicle systems (Zhao et al., 2012). Despite of its benefits, MANETs have faced challenges in sustaining reliable and secure communication due to their vulnerability to various kinds of attacks, inadequate resources, and regular topology variations.

One of the key features of MANETs which impacts the network performance is routing, which gets especially complicated in contrary or highly mobile environments. Although they work well in ordinary environments, traditional routing protocols like AODV and DSR are susceptible to routing attacks such wormhole, blackhole, and selective forwarding attack (Lobiyal et al., 2015). The packet delivery ratio (PDR), end-to-end latency as well as and network throughput can be ominously impacted by such attacks. Additionally, the other challenge in MANETs is the design of efficient routing protocols which is capable of managing dynamic network environments, limited energy resources, and malicious node behavior. The existing Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) focus on route discovery and maintenance but fail to select optimal path and address security threats in dynamic environment (Balaji et al., 2019).

Bio-inspired optimization techniques like Ant Colony Optimization (ACO) must been used to get about the downsides of outmoded routing methods (Khudair Madhloom et al., 2023; Mirjalili et al., 2014). Ant Colony Optimization (ACO) is engaged to recognize the optimal paths by imitating the foraging behavior of ants through pheromone trails. Premature convergence and security considerations in extremely dynamic and attack-susceptible networks are the major challenges faced by conventional ACO-based method (Mirjalili et al., 2014; Zhang et al., 2017).

While QACO is adept in improving the routing paths, but lacks security measures to safeguard against malicious nodes in route establishment. To fill this gap, it is essential to assimilate trust evaluation and security alertness to the routing protocol. An captivating method involves using a security rank calculation based on the packet drop rate (PDR), that serves as a lightweight trust indicator. In addition, rule-based attack detection schemes have demonstrated effective in recognizing specific types of routing attacks without demanding extensive computational resources. (Alyoubi, 2024; Airehrour et al., 2019; Deebak & Al-Turjman, 2020).

Using the meta heuristic technique, the Quantum Ant Colony Optimization (QACO), a set of feasible paths has been recognized but the critical task of choosing the optimal path based on few parameters like trust, performance and energy still remains (Pawar, 2023). To address these limitations, hybrid optimization approaches have been proposed. A prominent example is Grey Wolf Optimization (GWO), which replicates the social edifice and hunting patterns of grey wolves. GWO has shown striking global search abilities and flexibility in attacking intricate optimization challenges (Subramani & Selvi, 2024) Srilakshmi et al., 2022; Mirjalili et al., 2014).

Combined with GWO, the Jaya Optimization Algorithm has extended recognition as a effective population-based optimization technique. It primarily focuses on guiding solutions towards the optimal candidate while directing clear of the least favorable one in each iteration (Vincent et al., 2018). Unlike many other meta heuristic algorithms, Jaya does not require algorithm-specific control parameters, which makes it easier to implement and enhancing convergence stability Srilakshmi et al., 2022; Sajan et al., 2022).

This study proposes a new TrustRank-QACO protocol that blends quantum mechanics driven optimization with trust aware and rule based routing strategy, to better balance the exploration and convergence. The protocol promises both routing efficiency and robustness against common MANET threats by combining QACO with rule-based malicious node detection, hybrid GWO-Jaya algorithm (GWJO) gives an optimum path selection, and a three-mode security model (secure, γ-risky, risky). In dynamic and adverse MANET scenarios, this combined approach is expected to significantly improve PDR, lower latency, and enhance energy efficiency (Alnumay et al., 2019).

By assimilating QACO with hybrid GWJO, the procedure of determining routes becomes more efficient, while also improving trust-based decision-making and whole network performance. This suggested scheme pursues to lift the packet delivery ratio, reduce end-to-end delay, and decrease routing overhead in highly dynamic MANET environments (Sajan et al., 2022).

The major contributions of this paper are defined as follows:

- A node fitness based on TrustRank to identify truthful nodes in MANET routing.
- Identifying potential paths in dynamic network topologies using the QACO.
- A rule-based, lightweight attack detection model has been recommended to detect most routing attacks like blackhole, wormhole, and selective forwarding attacks.
- A hybrid optimization algorithm merging Grey Wolf and Jaya approaches to boost the efficiency of route selection.
- A systematic performance assessment showing improvements in packet delivery ratio, throughput, delay, and routing overhead compared to present methods.

The rest of the paper is systematized as follows: Section 2 explains the related work and comparative analysis of the existing methods; Section 3 labels the proposed system architecture; Section 4 explicates the simulation and evaluation of the results; and finally, Section 5 concludes the paper.

2 Related Work

In Mobile Ad-Hoc Networks (MANETs) the development of vigorous, proficient, and secure routing protocols for has been broadly discussed. Protocols like Dynamic Source Routing (DSR) and Ad hoc On-Demand Distance Vector (AODV) are crucial approaches that lessen overhead by creating routes as required (Lobiyal et al., 2015). Nevertheless, they are vulnerable to attacks due to the lack of built-in security features (Onem et al., 2012).

Bio-mimicry algorithms, mainly Ant Colony Optimization (ACO), mimic the foraging activities of ants and have been applied to find dynamic routes. AntHocNet (Di Caro et al., 2005) is a hybrid routing algorithm using the idea of ACO that combines the features of reactive route discovery with proactive approach. Though flexible, ACO-based routing algorithms can suffer from the problem of slow convergence and do not offer security against threats (Boyinbode et al., 2011).

Quantum Inspired Ant Colony Optimization (QACO) improves the traditional ACO algorithm using the principles of quantum computation including superposition and probabilistic choices. These enhancements improve exploration and help prevent getting stuck in local minima in dynamic settings (Khudair Madhloom et al., 2023; Uthayakumar et al., 2025). However, most QACO implementations prioritize performance improvements and do not tackle trust or security issues in the routing process.

Table 1: Comparative analysis of existing routing models

Author(s)	Technique / Model	Key Contribution	Limitations
Lobiyal et al., (2015)	AODV (Reactive Routing)	On-demand route discovery with low overhead	Vulnerable to attacks, no trust or security mechanism
Di Caro et al., (2005)	AntHocNet (ACO-based)	Adaptive routing with proactive & reactive hybrid ACO	High overhead, lacks attack detection
Khudair Madhloom et al., (2023)	Quantum-Inspired EA	Applied quantum superposition to evolutionary routing algorithms	No integration with trust or security models
Uthayakumar et al., (2016)	Quantum-Inspired ACO	Energy-aware routing in MANETs using quantum concepts	Does not detect or avoid malicious nodes
Boukerche et al., (2025)	Trust-Based Routing	Uses trust computation for security-aware path selection	Lacks route optimization; overhead increases with scale
Mokhtar & Azab, (2015)	Rule-Based Security	Surveys detection techniques for common MANET attacks	Does not integrate into routing or optimization protocols
Pawar, (2023)	SI-SLnO Optimization	Metaheuristic for energy-efficient routing in WSN	No application to secure MANET routing
Onem et al., (2012)	Ariadne Protocol	Lightweight secure on-demand routing using symmetric cryptography	Requires key management; high setup complexity
Alnumay et al., (2019)	Distributed Trust Model	Fully distributed trust evaluation for ad hoc networks	Computational complexity and trust propagation latency
Zhang et al., (2017)	Hybrid ACO Routing	Applied Ant Colony Optimization for adaptive route discovery in MANETs	Does not consider trust or security factors
Lu et al., (2020)	ACO + Grey Wolf Optimization	Combined ACO exploration with GWO exploitation for logistics routing	Not designed for MANET security or trust-aware routing
Xia et al., (2013)	Trust-based Secure MANET Routing	Integrated trust evaluation with routing decisions	Lacks optimization for route efficiency
Hassan et al., (2024)	Metaheuristic-based Secure Routing	Applied optimization algorithms for improving routing performance	Limited evaluation against large-scale attacks
Shwetha & Sannathammegowda, (2025)	SI-SLnO Optimization	Swarm intelligence optimization for energy-efficient routing	Focused on WSN rather than MANET security
Ravale & Borkar, (2024)	GWO-based MANET Routing	Grey Wolf Optimization applied for optimal path selection	No trust-aware node selection

To strengthen the security, trust-aware protocols have been suggested, where trust is determined based on node behavior, such as the packet forwarding ratio (Alyoubi, 2024). These methods exclude

malicious nodes but often lack optimization and are inefficient in scenarios with high mobility. Additionally, to identify routing attacks such as blackhole and selective forwarding a rule-based intrusion detection mechanism using threshold-based logic is used (Mokhtar & Azab, 2015). While lightweight, these methods are rarely integrated into adaptive, multi-objective routing protocols.

Meta heuristics such as GWO-Jaya algorithm have been successfully used in optimization problems involving energy and QoS in wireless networks (Xia et al., 2018). However, their application in secure routing for MANETs remains limited. Table 1 gives the detailed comparative analysis of existing routing models.

Despite extensive literature on MANET routing, current approaches exhibit significant limitations. Traditional protocols like AODV and DSR lack built-in security, making them vulnerable to active attacks. While bio-inspired techniques such as ACO and Quantum-Inspired Ant Colony Optimization (QACO) enhance dynamic path exploration and help avoid local minima, they predominantly focus on performance metrics without integrating trust or security measures. Conversely, existing trust-aware frameworks and rule-based intrusion detection systems effectively isolate malicious nodes but typically lack global path optimization and struggle under high mobility, highlighting the need for a unified multi-objective framework.

3 Proposed Methodology

The most important condition that should be fulfilled to make routing in MANETs safe and efficient is met through the TrustRank-QACO routing protocol. It uses a combination of threat identification based on rules, trust-based protection, and optimization inspired by quantum computing. The protocol consists of several steps such as route discovery through improved QACO, forwarding nodes classification, evaluation of nodes' fitness and trustworthiness, and real-time attack identification. Finally, the optimal route is selected from the safe and efficient ones by means of Hybrid Grey Wolf -Jaya Optimization (GWJO). The suggested TrustRank-QACO routing mechanism's complete workflow is illustrated in the figure 1 block diagram.

The illustration provided in figure 1 clearly shows the entire process starting from the initialization of MANET nodes and the calculation of their fitness values and then trust-based classification and rule-based attack detection. The secure nodes are then used for route discovery using the QACO algorithm, whereas GWJO is utilized to select an optimum route. Thus, the figure directly represents the methodological stages described in Section 3.

The process begins with a MANET environment, where each node’s fitness is computed based on distance, delay, energy, and security parameters. Based on the security level of the nodes, they are further divided into two categories trusted and secure nodes. Packet Delivery Ratio (PDR) is used for identifying the malicious node (where PDR > 0.6 implies secure communication and isolates attack nodes). Secure nodes take part in the process of route discovery through Quantum Inspired Ant Colony Optimization (QACO), which finds multiple routes between source and destination. In the end, the optimal route from all the discovered secure routes is selected through Hybrid Grey Wolf-Jaya Optimization (GWJO) technique.

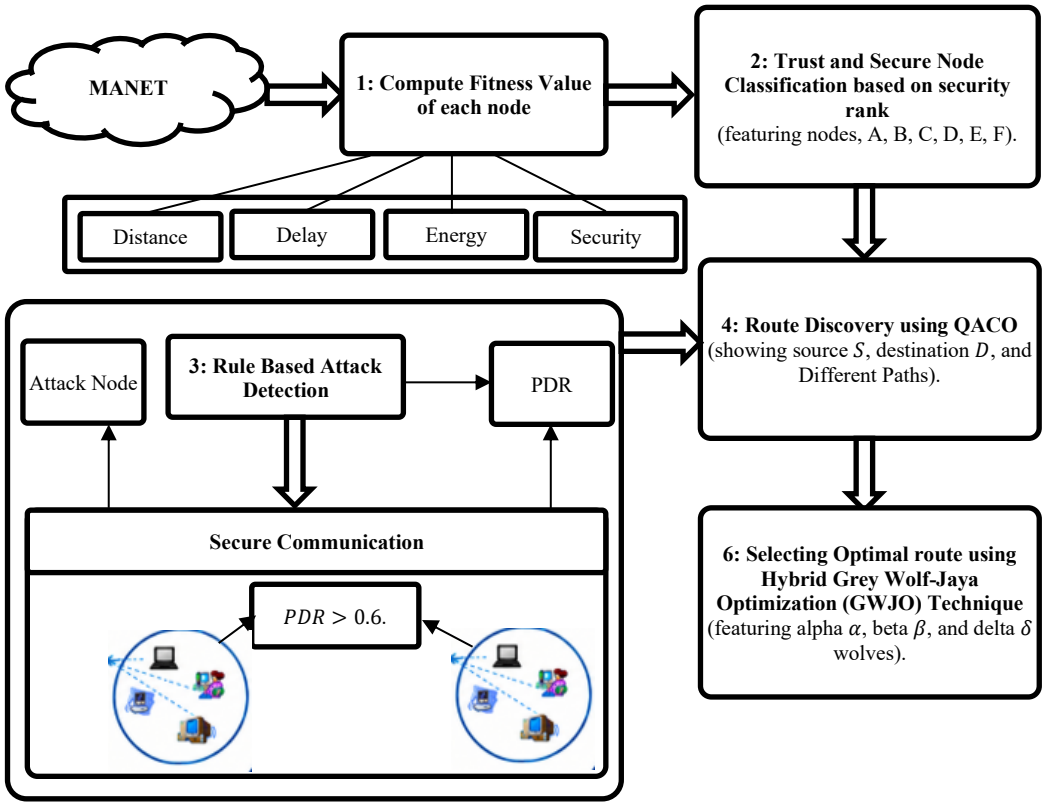


Figure 1: Block diagram of trustrank-QACO methodology

3.1 Fitness Parameter Calculation

To determine whether a node in the network is appropriate for inclusion in a routing path, its fitness value is computed. Numerous factors that impact routing security and performance are combined by the fitness function:

Distance (Dis):

The distance between two neighboring nodes is computed using the Euclidean equation. Shorter distances imply lower transmission energy and reduced delay.

Let node i be at position (x_i, y_i) and node j at position (x_j, y_j), then the Euclidean distance between them is given by equation. (1):

$$Dis(i,j) = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \quad (1)$$

Where: (x_i, y_i): coordinates of node i, (x_j, y_j): coordinates of node j.

Delay (De):

Represents the time taken to transmit data between nodes and is computed as given in equation. (2):

$$Delay = \frac{Dis}{\text{Data Speed}} \quad (2)$$

Energy (E):

Indicates the residual battery power of the node. Energy-aware routing ensures network longevity by avoiding low-energy nodes equation (3).

$$E_{\text{tr}}(p,\text{Dis}) = E_e \times p + E_a \times p \times \text{Dis}^n \quad (3)$$

Where:

- $E_{\text{tr}}(p,\text{Dis})$: Energy to transmit a p-bit message over distance Dis
- E_e: Energy per bit for electronic circuitry
- E_a: Energy per bit per m^2 for the amplifier
- p: Packet size in bits
- Dis: Distance between sender and receiver
- n: Path-loss exponent

Security Rank (SecRank):

Security Rank is calculated using Packet Drop Rate (PDR) as given in equation. (4). It reflects node reliability; higher values indicate trustworthy nodes.

$$\text{SecRank} = 1 - \text{PDR} \quad (4)$$

Equation 5 - Composite Fitness Function:

$$f = \alpha \cdot f_{\text{Dis,Delay}} + \beta \cdot f_{\text{PDR}} + \gamma \cdot f_{\text{SecRank}} + \delta \cdot f_{E_{\text{tr}}} \quad (5)$$

Where:

$\alpha, \beta, \gamma, \delta \in [0,1]$: Weight coefficients that control parameter importance. Lower fitness values indicate better routing choices.

3.2 Trust and Security-Aware Forwarding

Each node is classified based on its trust value**,** computed using historical forwarding behavior. Based on the security rank, nodes are assigned one of three forwarding modes:

Secure Mode:

Node has high security rank (low PDR) are fully eligible for forwarding packets.

γ-Risky Mode:

Node has moderate trust are allowed to forward packets only when no secure node is available. A parameter $\gamma \in [0, 1]$ represents risk tolerance.

Risky Mode:

Node has low trust or is suspicious are avoided in route discovery and ignored by QACO agents.

This filtering process occurs before QACO pheromone deposition**,** ensuring that only trusted paths are reinforced during the route search process.

3.3 Rule-Based Attack Detection

The routing protocol employs a rule-based intrusion detection system (IDS) to catch three major types of routing attacks based on Packet Drop Rate (PDR):

Selective Forwarding (SF) Attack:

Malicious node selectively forwards some packets and drops others based on the detection rule defined below.

If PDR $>$ $\rho_{\text{pdr}}^{\text{SF}}$, then node is performing SF attack.

Blackhole (BH) Attack:

Node drops all packets it receives when PDR $>$ $\rho_{\text{pdr}}^{\text{BH}}$, and classifies as blackhole attack.

Wormhole (WH) Attack:

Two malicious nodes form a tunnel and pass packets directly to each other, bypassing the network. If a node's neighbor shows unusually high PDR, suspects as a wormhole.

Threshold (ρ):

Threshold is computed dynamically instead of taking a static value as given in equation 6.

$$\rho_{\text{dynamic}} = \mu + k \cdot \sigma \quad (6)$$

Where:

- μ: mean PDR of neighbors
- σ: standard deviation

The threshold value is taken as 0.6. A node is flagged as malicious if PDR exceeds the set threshold value. This detection is frivolous and executed during route discovery, guaranteeing early elimination of attackers from the network path.

Parameter Initialization

The proposed TrustRank-QACO-GWJO initializes the network with 20–100 nodes, a 300 s simulation time, and 10% malicious nodes. The PDR threshold is set to 0.6 for attack detection, while the risk-tolerance parameter $\gamma$and fitness weights are bounded within [0,1]. GWJO uses random coefficients in [0,1], a decreasing exploration parameter from 2 to 0, and terminates when the maximum iterations or fitness-improvement threshold $\varepsilon$is reached.

3.4 Quantum-Inspired Ant Colony Optimization (QACO)

To develop the route discovery and selection process, the TrustRank-QACO protocol integrates the concept from quantum computing into classical ACO. Conflicting to the traditional ACO which performs fixed pheromone heuristics, to get a probabilistic decision-making and deeper exploration of routing paths, QACO influences quantum mechanics perceptions such as probability amplitudes,

superposition, and rotation gates. This quantum behavior upsurges robustness in dynamic, mobile environments like MANETs (Balaji et al., 2019).

A. Quantum Bit (Q-bit) Representation of path Selection:

Every possible routing decision is encoded as a Q-bit, portrayed by a vector of probability amplitudes in equation 7:

$$|\psi\rangle = \alpha_1|0\rangle + \beta_1|1\rangle \quad (7)$$

Where $|\alpha_1|^2 + |\beta_1|^2 = 1$

- $|\psi\rangle \rightarrow$ represents the quantum state routing decision
- $\alpha_1 \rightarrow$ probability amplitude of state $|0\rangle$
- $\beta_1 \rightarrow$ probability amplitude of state $|1\rangle$

Here, $|0\rangle$ represents "do not select this node" and $|1\rangle$ represents "select this node".

Subsequently, every node is in a superposition state—permitting the ant to assess several paths concurrently.

B. Quantum Observation for Node Selection:

As routes are created, ants "observe" the Q-bit states to probabilistically choose the next node. The choice to embrace a node in the path is made grounded on the probability amplitude (i.e., $|\beta_1|$), which boosts the variety of paths discovered and avoids premature convergence.

C. Quantum Rotation Gate Update:

Using quantum-inspired rotation gates, the angles of Q-bits are adjusted and informed by response from the quality of earlier chosen routes. Superior paths lead to higher probability amplitudes for the nodes involved.

Rotation Angle Update (simplified) as equation 8:

$$\theta_i(t+1) = \theta_i(t) + \Delta\theta \cdot \text{sign}(f_{\text{best}} - f_i) \quad (8)$$

Where:

- f_{best}: Fitness of best solution
- f_i: Fitness of current solution
- $\Delta\theta$: Learning rate

D. Quantum-Inspired Global Search:

The use of probabilistic Q-bit observations permits it to discover a wider solution space, improving its capacity to evade local optima—a significant restriction of traditional ACO in dynamic MANETs.

E. Integration in TrustRank-QACO:

The QACO mechanism operates in concord with trust evaluation and energy metrics. The only nodes that are secure and energy-efficient contribute to pheromone reinforcement, and the probabilistic nature of QACO ensures robust variation in the face of mobility and malicious circumstances.

TrustRank-QACO enhances QACO by incorporating trust scores into each quantum decision:

Transition Probability with Trust equation 9:

$$P_{ij}(t) = \frac{[\tau_{ij}(t)]^{\alpha} \cdot [\eta_{ij}]^{\beta} \cdot [T_j]^{\gamma}}{\sum_{k \in \mathcal{N}(i)} [\tau_{ik}(t)]^{\alpha} \cdot [\eta_{ik}]^{\beta} \cdot [T_k]^{\gamma}} \quad (9)$$

Where:

- $\tau_{ij}(t)$: pheromone value
- η_{ij}: heuristic (e.g., $1/\text{distance}$)
- T_j: Trust score of node j
- α, β, γ: weights

This ensures higher trust leads to higher probability of being selected and Malicious or low-trust nodes are automatically avoided as shown in figure 2.

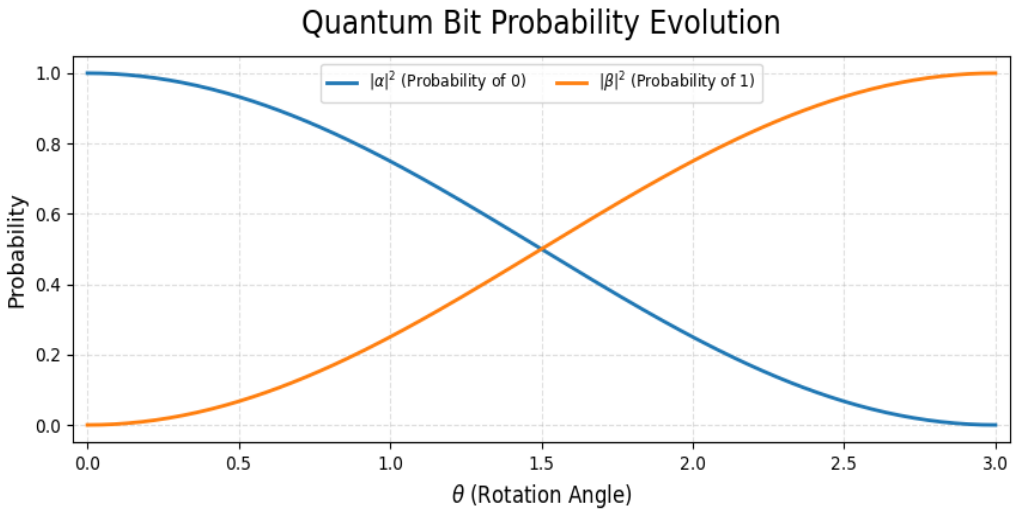


Figure 2: Quantum bit probability

Figure 2 presents a line graph depicting the evolution of quantum bit probabilities, where $|\alpha_1|^2$ and $|\beta_1|^2$ change inversely with the rotation angle θ, demonstrating the probabilistic state transition in quantum-inspired optimization.

This phase alters the traditional QACO (Quantum-Inspired Ant Colony Optimization) by incorporating trust-awareness. Thus, avoids early convergence on suboptimal routes. Also Ensures that reinforced paths are both optimal and secure. The main Characteristics of quantum are it uses quantum probability vectors to allow wider path exploration, even in sparse or dynamic topologies. Thus, enhances balance between exploration and exploitation.

3.5 Optimal Route Selection via Hybrid GWJO

This work launches a new fusion model that picks the optimal node for routing. The conventional GWO (Deebak & Al-Turjman, 2020) algorithm depicts the grey wolves' chasing behaviour and its leadership ladder. The process of hunting of wolves α, β, and δ is focussed. Amongst these wolves, α is treated as the leader which finalizes decisions related to the attacking process, time to awake, sleeping location, etc., whereas the remaining two wolves β and δ hold the 2nd and 3rd levels which support the α in making the best choices. The enclosing features are designed as per (10) and (11), where coefficient vectors are denoted as $\vec{A}$ & $\vec{C}$, prey's position vector is $\vec{X}_p$, $\vec{X}$ indicates position vectors of GW, and t denotes the present iteration. Equations (12) and (13) denote the model for $\vec{A}$ & $\vec{C}$, where a is a parameter which is minimized gradually to 0 from 2 in the entire iterations. Here, r_1 and r_2 specify the random vectors that lie in the range [0,1].

$$\vec{D} = \left|\vec{C} \cdot \vec{X}_p(t) - \vec{X}(t)\right| \quad (10)$$

$$\vec{X}(t+1) = \vec{X}_p(t) - \vec{A} \cdot \vec{D} \quad (11)$$

$$\vec{A} = 2\vec{a} \cdot \vec{r}_1 - \vec{a} \quad (12)$$

$$\vec{C} = 2 \cdot \vec{r}_2 \quad (13)$$

The mathematical equation relating the hunting behaviour of wolves is given from (14) to (19), where the final position updating is evaluated using equation (20).

$$D_{\alpha_1} = \left|L_1 \cdot J_{\alpha_1} - J\right| \quad (14)$$

$$D_{\beta_1} = \left|L_2 \cdot J_{\beta_1} - J\right| \quad (15)$$

$$D_{\delta_1} = \left|L_3 \cdot J_{\delta_1} - J\right| \quad (16)$$

$$J_{a1} = J_{\alpha_1} - M_1 \cdot \left(D_{\alpha_1}\right) \quad (17)$$

$$J_{a2} = J_{\beta_1} - M_2 \cdot \left(D_{\beta_1}\right) \quad (18)$$

$$J_{a3} = J_{\delta_1} - M_3 \cdot \left(D_{\delta_1}\right) \quad (19)$$

$$J(\text{iter}+1) = \frac{J_{a1} + J_{a2} + J_{a3}}{3} \quad (20)$$

In the standard GWO, the locations of the search agents get updated using equation (17)– (19).

The Jaya algorithm (20) (JA) (Houssein et al., 2020) focuses on obtaining the best appropriate solution. At each iteration, while eliminating the worst case, the number of modeling constraints is m (where m represents the constraint count) and the population size is N. If $X_{j,k,i}$ represents the value of the j-th variable for the k-th aspirant throughout the i-th iteration, this value is modified based on equation (21), where L_j denotes the value of the j-th constraint for the best solution and U_j refers to the value of the j-th constraint when considering the worst solution in the population.

$$J'_{p,r,i} = J_{p,r,i} + r_1\left(J_{p,\text{best},i} - \left|J_{p,r,i}\right|\right) - r_2\left(J_{p,\text{worst},i} - \left|J_{p,r,i}\right|\right) \quad (21)$$

Additionally, $J_{p,r,i}{}'$ represents the new value of $J_{p,r,i}$, and r_1 & r_2 are random numbers within the range [0,1]. The term "$+r_1\left(J_{p,\text{best},i} - \left|J_{p,r,i}\right|\right)$" represents moving the solution near the best one, and the

factor "$-r_2(J_{p,\text{worst},i} - |J_{p,r,i}|)$" denotes moving the solution far from the worst one. $J_{p,r,i}{}'$ is accepted if the function value returned by it is enhanced.

In addition to the proposed approach, the GWO positions are updated based on equations (22) – (24). Since JA is incorporated with the GWO model, the proposed method is named as the GWJO model.

$$J_1 = J + r_1(J_{\alpha_1} - |J|) - r_2(J_{p,\text{worst},i} - |J|) \quad (22)$$

$$J_2 = J + r_1(J_{\beta_1} - |J|) - r_2(J_{p,\text{worst},i} - |J|) \quad (23)$$

$$J_3 = J + r_1(J_{\delta_1} - |J|) - r_2(J_{p,\text{worst},i} - |J|) \quad (24)$$

To obtain the optimal route, the objective function is given in equation. (25):

$$P_{\text{obj}} = \min(f) \quad (25)$$

Each candidate route is evaluated using the composite fitness function given in equation. (26):

$$f = \alpha \cdot f_{\text{Dis,Delay}}(r) + \beta \cdot f_{\text{PDR}}(r) + \gamma \cdot f_{\text{Energy}}(r) + \delta \cdot f_{\text{Trust}}(r) \quad (26)$$

Where:

- $f_{\text{Dis,Delay}}(r)$: Normalized total distance of the route
- $f_{\text{PDR}}(r) = 1 - \text{PDR}$: Inverse of packet drop rate
- $f_{\text{Energy}}(r)$: Average residual energy of nodes
- $f_{\text{Trust}}(r)$: Average trust score of nodes
- $\alpha + \beta + \gamma + \delta = 1$: Tunable weights

Convergence Criteria

The GWJO algorithm concludes its process based on two criteria to ensure computational efficiency. Firstly, it halts when a set maximum number of iterations is reached, thereby avoiding unnecessary processing. Secondly, it evaluates the improvement in fitness over iterations. The algorithm identifies an optimal or near-optimal solution when the change in the best fitness value falls below a small threshold (ε), indicating stagnation. This dual methodology, especially in dynamic MANET environments, guarantees a steadiness between runtime efficiency and achieving acceptable solutions.

This stage guarantees that the path that is ultimately chosen is resource-efficient, secure, and globally optimal (Howitt, 2001).

Performance Metrics

The performance of the above-mentioned TrustRank-QACO-GWJO technique is measured by using the Packet Delivery Ratio (PDR), End-to-End Delay, Throughput, and Energy Consumption. The packet delivery ratio is the ratio of the number of packets received successfully to the total number of packets generated, whereas the end-to-end delay is the average time taken by the successful packets for reaching their destination. Throughput is the data successfully sent per unit time, and energy consumption is the total energy used in the process. The metrics are calculated as follows Equation (27)-(30):

$$PDR(\%) = \frac{N_{received}}{N_{sent}} \times 100 \quad (27)$$

$$Delay = \frac{\sum_{i=1}^{N}(T_{receive,i} - T_{send,i})}{N} \quad (28)$$

$$Throughput = \frac{N_{received} \times PacketSize}{T_{simulation}} \quad (29)$$

$$Energy_{consumed} = E_{initial} - E_{residual} \quad (30)$$

Where N_{sent} and $N_{received}$ denote the numbers of transmitted and successfully received packets, T_{send} and $T_{receive}$ are packet transmission and reception times, N is the number of successfully received packets, and $E_{initial}$ and $E_{residual}$ represent initial and remaining node energy. The manuscript additionally uses Security Rank = $1 - PDR$ and a composite fitness function incorporating distance/delay, PDR, energy, and trust for route selection.

Algorithm 1. TrustRank-QACO-GWJO Secure Routing

Input: MANET graph $G = (V, E)$, source node S, destination node D, node positions, residual energy, packet forwarding statistics, QACO parameters, GWJO parameters, and attack-detection threshold.

Output: Optimal secure route R^* from S to D.

Step 1: *Initialize all MANET nodes, pheromone values, Q-bit states, residual energy, and forwarding statistics.*

Step 2: *For every neighboring node, calculate:*

- *distance,*
- *transmission delay,*
- *residual energy,*
- *packet drop rate,*
- *security rank.*

The security rank follows the paper's formulation:

$$SecRank_i = 1 - PDR_i$$

where a higher security rank represents greater forwarding reliability.

Step 3: *Calculate the composite node fitness using distance/delay, packet-delivery behavior, security rank, and transmission energy.*

Step 4: *Classify each node into Secure, γ-Risky, or Risky mode according to its trust/security condition. Risky nodes are excluded from route discovery.*

Step 5: *Apply the rule-based IDS. Evaluate the packet-forwarding behavior of each candidate node and identify selective-forwarding, blackhole, or suspected wormhole behavior.*

Step 6: *Remove detected malicious nodes from the candidate routing set.*

Step 7: *Initialize QACO for the remaining secure nodes. Represent routing decisions using Q-bits and their probability amplitudes.*

Step 8: *Construct multiple candidate routes from S to D using the trust-aware transition probability:*

$$P_{ij}(t) \propto [\tau_{ij}(t)]^{\alpha}[\eta_{ij}]^{\beta}[T_j]^{\gamma}$$

where pheromone, heuristic information, and trust jointly influence node selection.

Step 9: *Evaluate every feasible route using the composite route fitness based on distance/delay, PDR, energy, and trust.*

Step 10: *Pass the feasible candidate routes to the Hybrid GWJO optimizer.*

Step 11: *GWO performs global exploration using its candidate solutions and leadership structure.*

Step 12: *Jaya optimization improves exploitation by moving candidate solutions toward the best solution and away from the worst solution. The resulting hybrid procedure is referred to as GWJO in the paper.*

Step 13: *Update the best route if the newly generated route has better fitness.*

Step 14: *Repeat QACO/GWJO optimization until either:*

- *the maximum iteration count is reached, or*
- *the improvement in best fitness falls below* ϵ.

These stopping criteria are already described in the paper and can therefore be incorporated directly into the algorithm.

Step 15: *Return the final optimal secure route* R^*.

The TrustRank-QACO-GWJO routing approach combines trust assessment, rules-based attack identification, QACO for path searching, and hybrid GWJO for optimal path selection. It initially classifies the nodes based on their security and forwarding behavior, discards the suspicious nodes, searches the possible paths using QACO, and ultimately chooses the best path using GWJO. The termination condition is achieved either when the maximum number of iterations is accomplished or the fitness improvement is very minimal. This process is described in Algorithm 1.

4 Simulation & Evaluation

This section discusses the simulation environment and results of the proposed secure optimal routing.

Dataset Details

Experimental data are collected from MATLAB 2019a and NS-3 simulations for a MANET network consisting of 20-100 nodes, following the Random Waypoint mobility model and using a simulation time of 300 s and CBR/UDP with a packet size of 512 bytes, where 10% of nodes act as black hole/selective forwarding attackers. Data obtained through simulation include node distance, PDR, packet drop rate, end-to-end delay, residual energy, throughput, routeing overhead, trust/security ranking, and route fitness, which are utilised in evaluating QACO, AODV, ACO, GWO, and the proposed GWJO-QACO routeing algorithms.

Software Details

The suggested TrustRank-QACO-GWJO algorithm was developed and tested via simulations on MATLAB 2019a. The experiments on MANET were conducted with 20 to 100 nodes, a random waypoint model, and a simulation time of 300 seconds. The routing performance of the algorithm was analyzed considering both normal and malicious node scenarios with 10% blackhole and selective forwarding attackers.

Simulation Setup Summary

The adopted secure routing and attack detection model was implemented in MATLAB 2019a and the simulation setup details are mentioned in table 2 and the results were accomplished.

Table 2: Simulation setup

Simulator	MATLAB 2019A
Nodes	20-100 nodes randomly distributed
Mobility Model	Random Waypoint
Simulation Time	300 seconds
Routing Protocols Compared	QACO (Uthayakumar et al., 2025), AODV (Lobiyal et al., 2015), ACO (Dorigo & Stützle, 2018), GWO (Mirjalili et al., 2014), Proposed GWJO- QACO
Traffic Pattern	CBR (UDP), 512-byte packets
Attack Scenario	10% nodes act as Blackhole/Selective forwarding attackers

The following table 2 shows the network environment used for the assessment of the proposed methodology, where there are 20–100 nodes, a random waypoint mobility model, a 300 s simulation time, a CBR/UDP communication type using a 512-byte packet size, and 10% of the nodes are malicious.

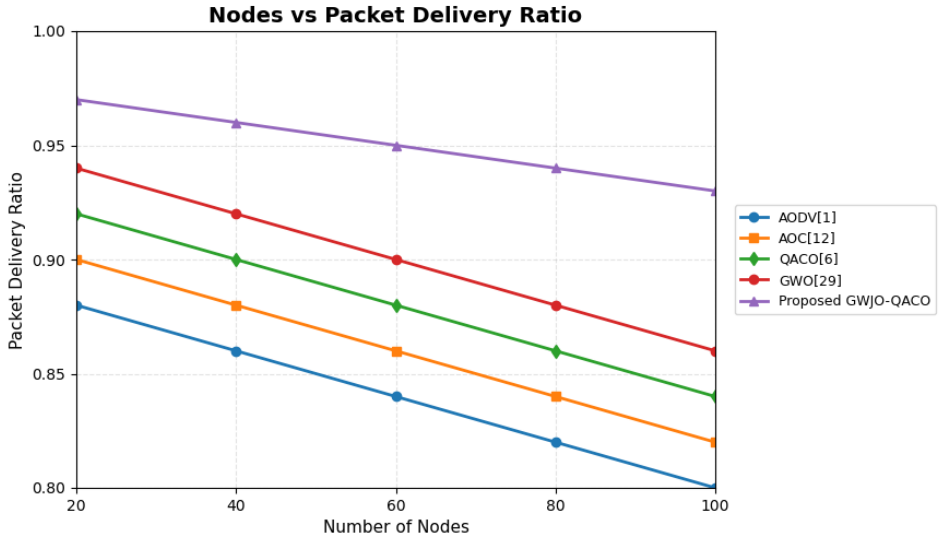


Figure 3(a): Node vs packet delivery ratio

In comparison to conventinal routing protocols, the proposed TrustRank-QACO-GWJO protocol performs better on all the requirements. Because of its robust trust-aware path selection and attack-aware route filtering, TrustRank-QACO-GWJO has the highest Packet Delivery Ratio (PDR) as shown in figure 3(a). The proposed GWJO-QACO routing scheme attains the highest packet delivery ratio across all the node densities. As the number of nodes increases, generally packet loss increases due to link failures and congestion. However, the proposed hybrid approach maintains higher reliability because: Quantum Ant Colony Optimization explores multiple routing paths probabilistically and Grey Wolf Optimization identifies high-quality candidate routes using leader wolves (α, β, δ) and finally Jaya optimization improves exploitation by moving solutions toward the best route and away from the worst. This hybrid optimization improves route stability and reduces packet loss, resulting in 13.1% higher PDR than AODV.

End-to-end delay increases when node density increases due to route rediscovery and packet collisions. The proposed algorithm significantly reduces delay because QACO quickly identifies feasible routing paths, Grey Wolf optimization guides the search toward optimal solutions and finally, Jaya optimization accelerates convergence toward the best route. As a result, the proposed method reduces delay by 30.8% compared with AODV as shown in the figure 3(b).

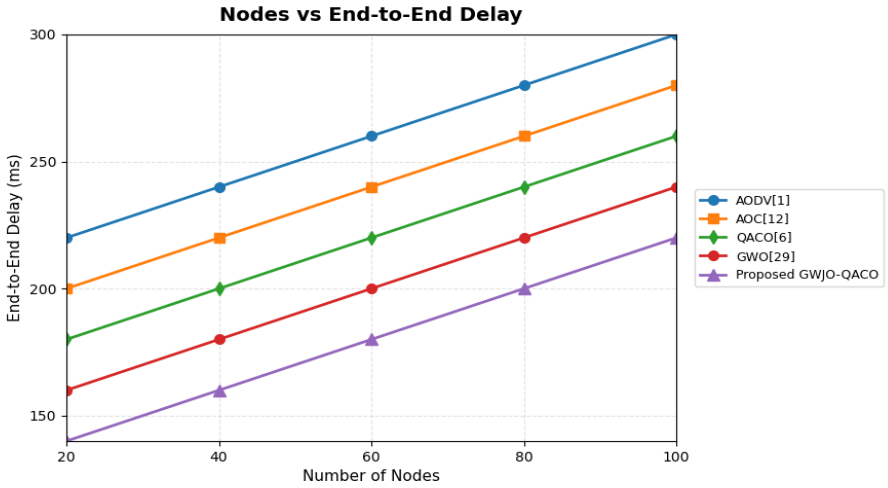


Figure 3(b): Node vs delay

The Throughput signifies the amount of successfully delivered data in the network. The proposed algorithm achieves higher throughput because of the hybrid optimization method which selects stable and energy-efficient routes. Reduced packet loss and fewer retransmissions upsurge the total positive data transmission rate which is shown in the figure 3(c).

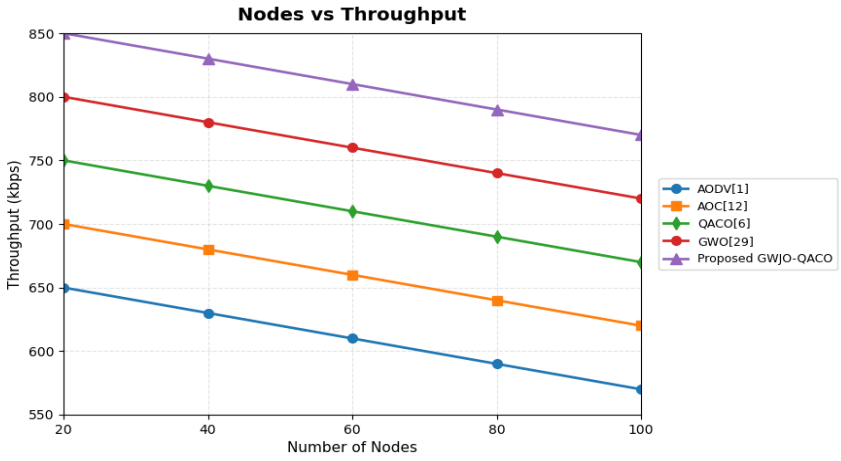


Figure 3(c): Node vs throughtput

Energy efficiency is the perilous in MANET environments since nodes work on restricted battery power. The suggested hybrid optimization method lessens the energy consumption as depicted in the figure 3(d), by selecting shorter and more constant routes thus minimizing retransmissions and control overhead.

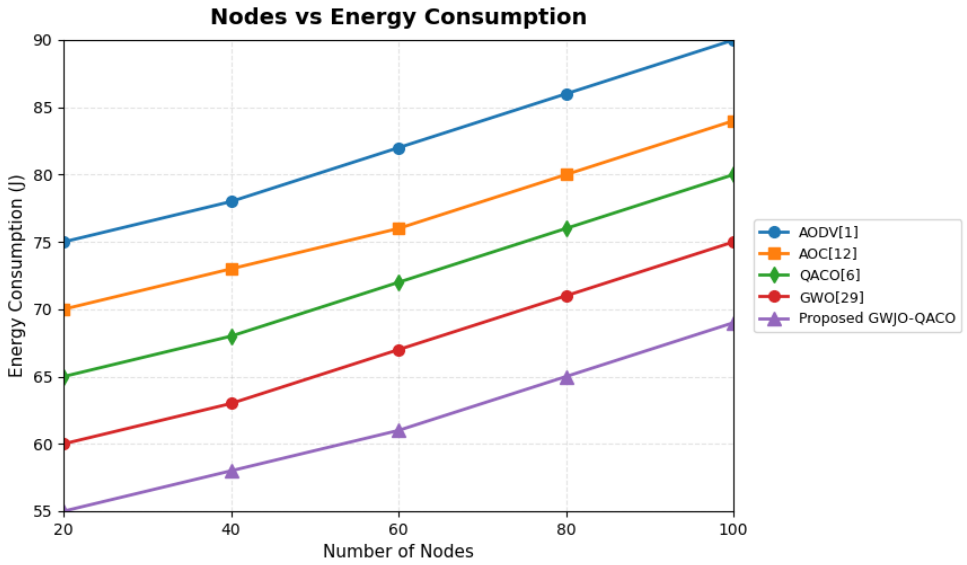


Figure 3(d): Node vs energy consumption

Figure 3(e) exemplifies the convergence performance of the suggested Grey Wolf–Jaya Optimization (GWJO) related with the standard Grey Wolf Optimizer. As the number of iterations increases, both the algorithms gradually slant the optimal fitness value. Nevertheless, the proposed GWJO accomplishes quicker convergence and reaches a higher final fitness value. This enhancement occurs because of the Jaya optimization module which enhances exploitation by directing solutions toward the best candidate while evading the worst solutions. Consequently, the proposed GWJO improves convergence efficiency by approximately 8% equated with the conventional GWO algorithm**.**

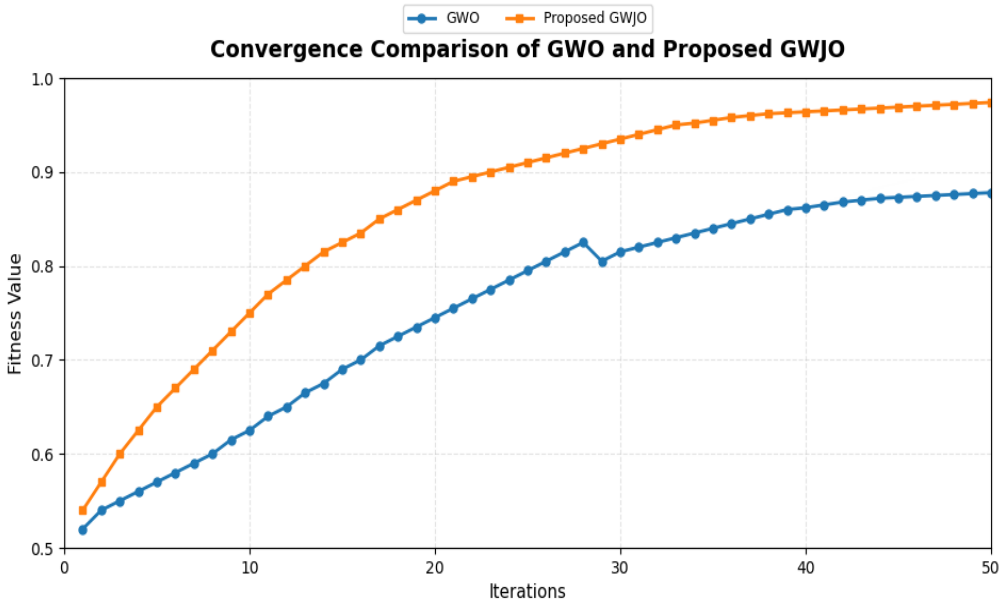


Figure 3(e): Convergence analysis

Ablation Study

Table 3: Ablation study of the proposed trustrank-QACO-GWJO routing protocol

Model Configuration	Packet Delivery Ratio (PDR %)	End-to-End Delay (ms)	Throughput (kbps)	Energy Consumption (J)
Base Model (Traditional ACO + GWO; No Trust, No Quantum, No Jaya)	86.2%	245.4	635.2	79.4
Model + TrustRank & Rule-Based IDS (Adds security filtering, drops malicious nodes)	89.5%	228.1	672.4	74.8
Model + TrustRank + QACO (Adds quantum superposition & path exploration)	92.1%	204.6	738.9	67.5
Full Proposed Model (TrustRank-QACO-GWJO) (Includes complete hybrid GWJO exploitation)	**95.0%**	**180.0**	**810.0**	**61.0**

This table 3 summarizes the step-by-step performance evaluation (at 60 node density) demonstrating the individual contributions of the security model, Quantum-Inspired Ant Colony Optimization (QACO), and the Hybrid Grey Wolf-Jaya Optimization (GWJO) components on Packet Delivery Ratio, End-to-End Delay, Throughput, and Energy Consumption.

Discussion

From the experiments conducted, it is clear that the TrustRank-QACO-GWJO technique has performed better than the QACO, AODV, ACO, and GWO techniques in terms of security routing in MANETs. The performance of the proposed technique includes an improvement in the PDR, lower delay time, high throughput, and low energy consumption. Specifically, the improvement of 13.1% in the PDR, 30.8% decrease in delay, 32.8% increase in throughput, and 25.1% decrease in energy consumption in comparison to AODV clearly show that the integration of trust-based attack detection with QACO and GWJO enhances both security and routing.

Limitations and Future Work

Simulation with the parameters of 20 to 100 nodes, the Random Waypoint mobility model, 300 s simulation time, and 10% of malicious nodes for the evaluation of the study is not sufficient for representing all scenarios in the real world. Evaluation of the proposed algorithm is restricted to black hole attack and selective forwarding attack; other types of attacks as well as heterogeneous environments are not covered in the study. Furthermore, simulation-generated datasets are not accessible in the public domain and are available from the corresponding author for reasonable request.

Future studies should be conducted to validate TrustRank-QACO-GWJO in different sizes and dynamics of MANETs and cover different attacks and mobility patterns. It would be interesting to implement the algorithm in practice in real wireless networks or testbeds. Moreover, future research can focus on different optimization techniques, adaptive thresholds of trust, and scalability studies with larger-scale simulations.

Practical Relevance and Deployment Feasibility

The suggested TrustRank-QACO-GWJO model has application value for secure and energy-efficient routing in MANETs, especially in cases when reliable communications and the presence of malicious nodes are of concern. Nevertheless, the existing study is limited to the simulation using MATLAB 2019a software only. No experimental evaluation of the suggested model was performed in the context of IoT, VANET, wireless, and hardware implementation.

5 Conclusion

The recommended trust rank QACO secure routing framework offers effective result for enlightening outing reliability and security in Mobile Ad-Hoc Networks. the framework assimilates trust-based node evaluation, rule- based attack detection, Quantum Inspired Ant Colony optimisation for route discovery and hybrid Grey Wolf Jaya optimisation for optimal route selection. This multi layered methodology enables the routing procedure to effeciently recognise malicious nodes, avoid unreliable paths and select energy efficient routes in highly dynamic network environment. the suggested schemes challenges the security and performance issues that are communal in MANET settings, principally when there are malevolent nodes and dynamic topologies exist. The framework magnificently identifies and counteracts risks including Selective forwarding, black hole attacks by adding security aware node classification with packet delivery based trust evaluation. the Quantum inspired Ant Colony optimisation enhances exploration of multiple routing paths through probabilistic Quantum representation, while the hybrid Grey Wolf-Jaya optimisation algorithm progresses exploitation and convergence towards the optimal route. The advantages of Trust Rank-QACO over traditional routing protocols like AODV, QACO, AntHocNet, and GWO alone have been proved by simulation results conducted with MATLAB. The simulation results determine that the proposed GWJO-QACO routing framework significantly develops MANET performance compared with existing approaches such as AODV, ACO, QACO, and GWO. The proposed technique achieves almost 13.1% higher packet delivery ratio, 30.8% lesser delay, 32.8% upper throughput, and 25.1% lower energy consumption compared with AODV. These improvements are attained through the hybrid optimization approach uniting quantum ant colony exploration with Grey Wolf–Jaya exploitation, which enhances route stability and reduces routing overhead. Potential for further research includes validating this model using realistic testbeds for wireless networks, highly dynamic mobile ad hoc network (MANET) scenarios, and considering attacks of various types for testing the efficacy of this scheme. Future research could include considering adaptive threshold levels of trust, diverse IoT/VANET scenarios, overheads, scalability, and energy awareness for implementing the proposed routing framework.

Data Availability Statement (DAS): The datasets generated and analyzed during the current study are based on MATLAB and NS-3 simulations and are available from the corresponding author upon reasonable request.

Conflicts of Interests: The authors declare that they have no conflict of interest.

Funding: Authors declare no funding for this research. Competing Interests The authors declare that they have no competing interests.

Author Contribution GK: Conceptualization, Methodology, Software, Data curation, Writing—original draft, Investigation, review & editing.

References

[1] Airehrour, D., Gutierrez, J. A., & Ray, S. K. (2019). SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. *Future Generation Computer Systems*, *93*, 860-876. https://doi.org/10.1016/j.future.2018.03.021

[2] Alnumay, W., Ghosh, U., & Chatterjee, P. (2019). A trust-based predictive model for mobile ad hoc network in internet of things. *Sensors*, *19*(6), 1467. https://doi.org/10.3390/s19061467

[3] Alyoubi, A. A. (2024). Enhancing data security in mobile ad-hoc network (MANETs) using trust-based approach with RSSI and fuzzy logic. *Mobile Networks and Applications*, *29*(6), 2030-2046. https://doi.org/10.1007/s11036-024-02336-6

[4] Balaji, S., Julie, E. G., Robinson, Y. H., Kumar, R., Thong, P. H., & Son, L. H. (2019). Design of a security-aware routing scheme in mobile ad-hoc network using repeated game model. *Computer Standards & Interfaces*, *66*, 103358. https://doi.org/10.1016/j.csi.2019.103358

[5] Boyinbode, O., Le, H., & Takizawa, M. (2011). A survey on clustering algorithms for wireless sensor networks. *International Journal of Space-Based and Situated Computing*, *1*(2-3), 130-136. https://doi.org/10.1504/IJSSC.2011.040339

[6] Deebak, B. D., & Al-Turjman, F. (2020). A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. *Ad Hoc Networks*, *97*, 102022. https://doi.org/10.1016/j.adhoc.2019.102022

[7] Di Caro, G., Ducatelle, F., & Gambardella, L. M. (2005). AntHocNet: an adaptive nature-inspired algorithm for routing in mobile ad hoc networks. *European transactions on telecommunications*, *16*(5), 443-455. https://doi.org/10.1002/ett.1062

[8] Dorigo, M., & Stützle, T. (2018). Ant colony optimization: overview and recent advances. *Handbook of metaheuristics*, 311-351. https://doi.org/10.1007/978-3-319-91086-4_10

[9] Hassan, S. M., Mohamad, M. M., & Muchtar, F. B. (2024). Advanced intrusion detection in MANETs: A survey of machine learning and optimization techniques for mitigating black/gray hole attacks. *IEEE Access*, *12*, 150046-150090. https://doi.org/10.1109/ACCESS.2024.3457682

[10] Houssein, E. H., Gad, A. G., & Wazery, Y. M. (2020). Jaya algorithm and applications: A comprehensive review. *Metaheuristics and optimization in computer and electrical engineering*, 3-24. https://doi.org/10.1007/978-3-030-56689-0_2

[11] Howitt, R. (2001). Frontiers, borders, edges: liminal challenges to the hegemony of exclusion. *Australian geographical studies*, *39*(2), 233-245. https://doi.org/10.1111/1467-8470.00142

[12] Khudair Madhloom, J., Abd Ali, H. N., Hasan, H. A., Hassen, O. A., & Darwish, S. M. (2023). A quantum-inspired ant colony optimization approach for exploring routing gateways in mobile ad hoc networks. *Electronics*, *12*(5), 1171. https://doi.org/10.3390/electronics12051171

[13] Lobiyal, D. K., Katti, C. P., & Giri, A. K. (2015). Parameter value optimization of ad-hoc on demand multipath distance vector routing using particle swarm optimization. *Procedia Computer Science*, *46*, 151-158. https://doi.org/10.1016/j.procs.2015.02.006

[14] Lu, F., Feng, W., Gao, M., Bi, H., & Wang, S. (2020). The Fourth-Party Logistics Routing Problem Using Ant Colony System-Improved Grey Wolf Optimization. *Journal of Advanced Transportation*, *2020*(1), 8831746. https://doi.org/10.1155/2020/8831746

[15] Mirjalili, S., Mirjalili, S. M., & Lewis, A. (2014). Grey wolf optimizer. *Advances in engineering software*, *69*, 46-61. https://doi.org/10.1016/j.advengsoft.2013.12.007

[16] Mokhtar, B., & Azab, M. (2015). Survey on security issues in vehicular ad hoc networks. *Alexandria engineering journal*, *54*(4), 1115-1126. https://doi.org/10.1016/j.aej.2015.07.011

[17] Onem, E., Gürdağ, A. B., & Çağlayan, M. U. (2012). Formal security analysis of Ariadne secure routing protocol using model checking. *International Journal of Ad Hoc and Ubiquitous Computing*, *9*(1), 12-24. https://doi.org/10.1504/IJAHUC.2012.045537

[18] Pawar, M. V. (2023). Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM. *International Journal of Pervasive Computing and Communications*, *19*(1), 124-153. https://doi.org/10.1108/IJPCC-10-2020-0162
[19] Ravale, U., & Borkar, G. M. (2024). Secure and efficient trust enabled routing in mobile ad hoc network using game theory and grey wolf optimisation techniques. *IET Wireless Sensor Systems*, *14*(6), 451-476. https://doi.org/10.1049/wss2.12095
[20] Sajan, R. I., Christopher, V. B., Kavitha, M. J., & Akhila, T. S. (2022). An energy aware secure three-level weighted trust evaluation and grey wolf optimization-based routing in wireless ad hoc sensor network. *Wireless Networks*, *28*(4), 1439-1455. https://doi.org/10.1007/s11276-022-02917-x
[21] Shwetha, M., & Sannathammegowda, K. (2025). Optimizing energy efficient routing protocol performance in underwater wireless sensor networks with machine learning algorithms. *Transactions on Emerging Telecommunications Technologies*, *36*(3), e70073. https://doi.org/10.1002/ett.70073
[22] Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. *IEEE Access*, *10*, 14260-14269. https://doi.org/10.1109/ACCESS.2022.3144679
[23] Subramani, S., & Selvi, M. (2024). Intrusion detection system and fuzzy ant colony optimization based secured routing in wireless sensor networks. *Soft Computing*, *28*(17), 10345-10367. https://doi.org/10.1007/s00500-024-09795-9
[24] Uthayakumar, C., Jayaraman, R., Raja, H. A., & Shabbir, N. (2025). Qseer-quantum-enhanced secure and energy-efficient routing protocol for wireless sensor networks (wsns). *Sensors*, *25*(18), 5924. https://doi.org/10.3390/s25185924
[25] Vincent, F. L., Peter, H., Riashat, I., Marc, G. B., & Joelle, P. (2018). An introduction to deep reinforcement learning. *Foundations and trends® in machine learning*, *11*(3-4), 219-354. https://doi.org/10.1561/2200000071
[26] Xia, H., Jia, Z., Li, X., Ju, L., & Sha, E. H. M. (2013). Trust prediction and trust-based source routing in mobile ad hoc networks. *Ad Hoc Networks*, *11*(7), 2096-2114. https://doi.org/10.1016/j.adhoc.2012.02.009
[27] Xia, H., Li, Z., Zheng, Y., Liu, A., Choi, Y. J., & Sekiya, H. (2018). A novel light-weight subjective trust inference framework in MANETs. *IEEE Transactions on Sustainable Computing*, *5*(2), 236-248. https://doi.org/10.1109/TSUSC.2018.2817219
[28] Zhang, H., Wang, X., Memarmoshrefi, P., & Hogrefe, D. (2017). A survey of ant colony optimization based routing protocols for mobile ad hoc networks. *IEEE access*, *5*, 24139-24161. https://doi.org/10.1109/ACCESS.2017.2762472
[29] Zhao, H., Qin, J., & Hu, J. (2012). An energy efficient key management scheme for body sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, *24*(11), 2202-2210. https://doi.org/10.1109/TPDS.2012.320

Authors Biography



Dr.G. Kalyani is working as a Professor at the Department of CSE-Cyber Security, Geethanjali College of Engineering and Technology, Hyderabad. She has completed her Bachelor of Engineering in Computer science and Engineering from JNTU, Hyderabad, India. She has completed her Master of Technology in Computer Science from IETE, Hyderabad, India. She has done her Ph.D in CSE from REVA University, Bangalore, India. She has 21 years of experience in Computer Science and Engineering areas pertaining to academics. Her areas of research and teaching include network security, computational intelligence, wireless networks. She has published 28 papers, out of 5 in SCI papers, 16 in

Scopus Indexed Journal and International Conferences, 1 Text Book and 3 Patents published.



Dr.M. Gayatri has received the PhD in CSE from JNTUK university Kakinada, Andhra Pradesh, MTech degree in Computer Science Engineering from JNTUK University, Kakinada, India, in 2011, BTech in CSIT from JNTUH in 2005. Her Research interests include Data Mining, Deep learning, Machine Learning, Web Mining; She has published 15 papers in SCI and international Scopus indexed journals and 8 papers in conferences at international level and 4 patents published from National and International. She has life time membership in ACM, ISTE, CSI, IAENG.



Dr. Nune Srinivas Rao is Associate Professor and Head in the Department of Computer Science and Engineering (DS) at Malla Reddy Engineering college for women (Autonomous), Secunderabad. He completed Bachelor of Engineering from Karnatak University. Dharwad in 1996. Master of Information Technology from Punjabi university, Patiala in 2003 and in the year 2022 he completed Ph.D. in Computer Science & Engineering from KLEF Deemed to University, Guntur, Andhra Pradesh, India. His Main Research interest is in the area of Wireless Sensor Networks, Computer Networks, and Network Security. He has 29 years of Teaching Experience. He has published 20 papers, out of 12 in Scopus Indexed Journal and 02 in Web of science, 2 SCI papers and also published in 15 papers in both National and International Conferences and 2 Book Chapters and 4 Patents. He organized various workshops.



Dr. Yasmeen is an Senior Asstistant Professor in the Department of Computer Science and Engineering (Data Science) with over 12 years of academic experience and four years of industry experience. She holds a Ph.D. in Computer Science and Engineering from Shri JJT University, India, her research interests include Artificial Intelligence, Machine Learning, Cloud Computing, Cloud Security, Cybersecurity, DevOps, Internet of Things Security, Intrusion Detection Systems, Federated Learning, and Generative AI. She has published more than 15 SCI and Scopus-indexed research papers, authored several book chapters, and held 8 patents in AI and Cloud Security. Dr. Yasmeen is a reviewer for IEEE conferences and EAI journals and is certified in AWS, Azure, and Google Cloud technologies. She actively contributes to research, academic quality assurance, industry-oriented training, and mentoring future engineers and researchers.



Dr. Katakam Srinivas serves as the Principal of Kshatriya College of Engineering, with over 25 years of extensive teaching experience in reputed engineering institutions. He has held several key academic and administrative positions, contributing significantly to academic excellence, institutional development, and quality enhancement. He completed his B.Tech. in Computer Science and Engineering from Swami Ramanand Teerth Marathwada University and his M.Tech. from Jawaharlal Nehru Technological University, Anantapur. He earned his Ph.D. from JNTU and is ratified as a Professor by JNTUH. He is also a philanthropist, entrepreneur, motivational mentor, author, and organizer of technical events. He has published around 45 research papers and holds five patents, including a novel result-merging technique in Meta Search Engines. He has mentored over 10,000 students and organized numerous academic programs. His research interests include Artificial Intelligence, Machine Learning, Data Structures, and Data Science.