Future Technology
Open Access Journal
ISSN 2832-0379

February 2026| Volume 05 | Issue 01 | Pages 168-179

Journal homepage: https://fupubco.com/futech

https://doi.org/10.55670/fpll.futech.5.1.15

Future Publishing LLC

Article

Trust and adaptiveness enhancements to PRFDRA for secure metaheuristic path selection in MANETs

Augustina Dede Agor[1]*, Lawrence Kwami Aziale[1], Frank Kataka Banaseka[1], Kwabena Owusu-Agyemang[2], Selasie Aformaley Brown[1], Benjamin Tei Partey[2]

[1]Department of Information Technology Studies, University of Professional Studies, P. O. Box LG 149, Accra, Ghana
[2]Department of Computer Science, Kwame Nkrumah University of Science and Technology, Private Mail Bag, University Post Office, Kumasi, Ghana

ARTICLE INFO

Article history:
Received 10 August 2025
Received in revised form
15 October 2025
Accepted 18 November 2025

Keywords:
Security, Trust, Adaptive, SFD-MFD Switching, PRFDRA, MANETs

*Corresponding author
Email address:
augustinadede.agor@upsamail.edu.gh

DOI: 10.55670/fpll.futech.5.1.15

ABSTRACT

In Mobile Ad Hoc Networks (MANETs), the Power-Aware River Formation Dynamics Routing Algorithm (PRFDRA) enhanced energy efficiency by forming power-aware paths and facilitating multi-flow diffusion. It remained vulnerable to internal misbehavior. RFDTrust added trust metrics to mitigate malicious activity, but applied them only in neighbor selection along downhill gradients. This limited path diversity and adaptiveness. This paper proposes TA-PRFDRA (Trust-Adaptive-Power-Aware River Formation Dynamics Routing Algorithm), a trust- and adaptiveness-enhanced version of PRFDRA. TA-PRFDRA integrates trust evaluation into all routing stages. It applies dynamic switching between Single Flow Direction (SFD) and Multi-Flow Direction (MFD) based on trust-weighted gradient variance. The algorithm utilizes a composite trust model that takes into account node energy reliability, packet forwarding behavior, route participation, and delay consistency. Trust is applied in gradient, erosion, altitude, sediment transport, and path cost computations. Simulation results show that, compared with PRFDRA, RFDTrust, RFDManet, and TORA, TA-PRFDRA achieved up to 1.33% higher packet delivery ratio (PDR). Average end-to-end delay (AE2ED) decreased by 0.14 s. Detection rate (DR) increased by up to 30.38%. Energy consumption (EC) was reduced by up to 15.94 J. Statistical analysis confirmed that improvements over RFDTrust were significant. These results demonstrate that integrating trust into all routing processes with adaptive flow control enhances reliability, latency performance, security, and energy efficiency in MANETs.

1. Introduction

Mobile Ad Hoc Networks (MANETs) are decentralized, self-organizing networks in which mobile nodes communicate over wireless links without relying on fixed infrastructure [1]. Their dynamic topologies, limited energy resources, and vulnerability to internal attacks make secure and efficient routing a significant challenge [2]. MANETs are increasingly deployed in mission-critical applications such as disaster recovery, military coordination, and vehicular networks. These scenarios require routing protocols that maintain reliability and efficiency in high-mobility environments, as well as in the presence of potential insider threats. Nature-inspired metaheuristic algorithms have been explored for routing in decentralized networks. Models such as Ant Colony Optimization (ACO) [3], Intelligent Water Drops (IWD) [4], and River Formation Dynamics (RFD) [5] simulate natural processes to guide path selection. While these metaheuristics are adaptive in principle, most MANET implementations remain static or only partially adaptive. RFD models the flow of rivers, where paths evolve through erosion and sedimentation. Its distributed design provides a foundation for energy-efficient routing strategies. Agor et al. [1] introduced the Power-Aware River Formation Dynamics Routing Algorithm (PRFDRA) for MANETs. PRFDRA extends RFD by incorporating energy-aware and performance-based parameters across its routing mechanisms. Node-selection probabilities are computed for all neighbors, including those with positive, negative, and flat gradients, to enable probabilistic multi-flow diffusion. This design increases path diversity compared with single-flow RFDTrust. However, it does not incorporate trust or behavioral integrity metrics, which leaves it vulnerable to malicious nodes. RFDTrust [6] uses trust to guide neighbor selection via decreasing-gradient metrics. While this improves security, trust is not embedded in all RFD mechanisms. Packets follow a primarily downhill path, ensuring loop-free routing but limiting path diversity.

This restricts adaptiveness in flat or deceptive topologies and reduces resilience under collusive attacks. To address these limitations, this study proposes the Trust-Adaptive-Power-Aware River Formation Dynamics Routing Algorithm (TA-PRFDRA). TA-PRFDRA integrates trust evaluation into all PRFDRA stages, including gradient computation, erosion assignment, altitude adjustment, sediment dynamics, and path cost calculation. A composite trust score is computed using packet forwarding ratio, energy reputation, route participation frequency, and routing metric consistency. High-trust nodes are favored, while untrusted nodes are penalized throughout the routing process.

TA-PRFDRA also introduces adaptive switching between Single Flow Direction (SFD) and Multiple Flow Direction (MFD) modes. Switching is based on trust-weighted gradient variance. This allows the protocol to respond dynamically to local network conditions, distribute load across multiple paths, and improve resilience against congestion and route manipulation. Embedding trust in all routing stages while enabling adaptive flow control enhances security, reliability, and energy efficiency in MANETs. Accordingly, this study is guided by the following objectives:

- Integrate trust metrics into all PRFDRA routing processes, including gradient, erosion, altitude, sediment transport, and path cost, to favor reliable nodes and penalize untrusted nodes.
- Enhance path selection adaptiveness through dynamic SFD and MFD switching based on trust-weighted gradient variance to ensure responsiveness under varying network conditions.

The remainder of the manuscript is structured as follows: Section 1.1 gives the problem statement. Section 1.2 discusses the security of MANETs, while Section 2 provides a literature review. Section 3 describes the methodology, while Section 4 gives the results. Finally, Section 5 concludes the study.

1.1 Problem statement

Routing in MANETs is challenged by frequent topology changes, limited node energy, and internal misbehaviour [7]. PRFDRA improves energy-aware routing but assumes all nodes behave cooperatively, exposing routes to malicious disruptions. RFDTrust introduces trust evaluation to address this issue, but restricts forwarding choices, reducing path diversity and adaptability under flat or colluding topologies. Other existing RFD-based approaches do not combine trust evaluation with all routing processes. They also lack adaptive flow control using SFD and MFD switching [6]. These gaps result in an insecure and inefficient path, underscoring the need for a unified, trust-adaptive, and energy-efficient routing framework in MANETs.

1.2 MANETs security

Security attacks in MANETs are classified into two types: external and internal, as shown in Figure 1. External attacks are further classified into two types: attacks based on the attackers' actions and attacks based on operational ideologies. The one based on attackers' actions is also classified into three main groups: passive, active, and collaborative attacks. Active attacks can take various forms, including modification, dropping, timing, and fabrication. Attacks can also be classified based on the layered protocol stack. Figure 2 lists the major kinds of attacks that affect the various layers. Not all enumerated MANET security attacks have been included in the classification diagrams, as only representative, structurally distinct attack vectors were illustrated to optimize taxonomic clarity.

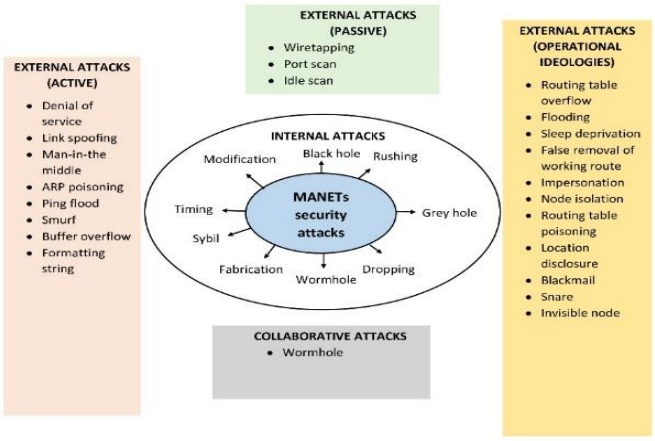

Figure 1. External and internal attacks

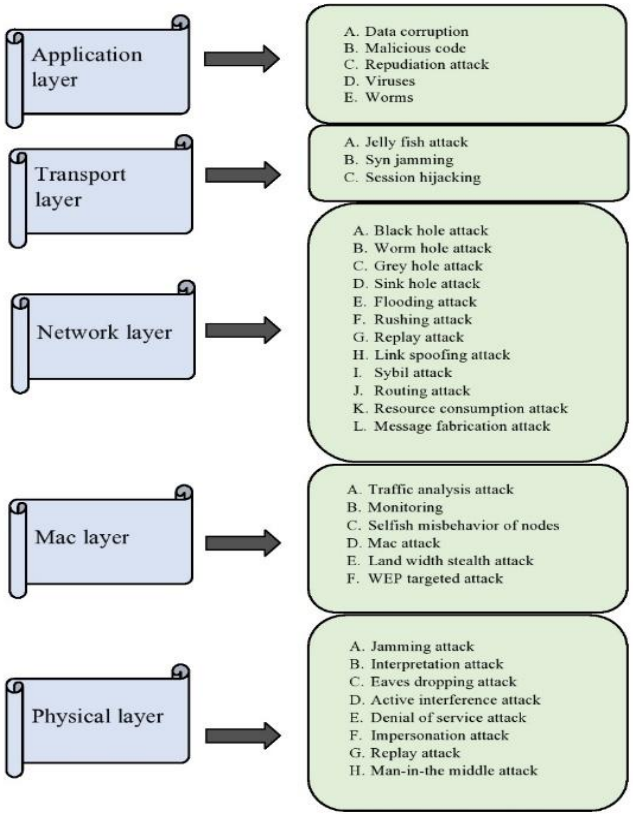

Figure 2. Attacks at the various layers

1.3 Security schemes

As shown in Figure 3, several approaches can be used to detect or prevent security attacks in MANETs. These include game theory, cryptographic systems, reputation mechanisms, credit-based schemes, secure multicasting, secure routing, privacy-aware and position-based routing, key management, intrusion detection systems, artificial intelligence, metaheuristic optimization, trust models, blockchain, formal protocol verification, incentive-based frameworks, and physical security. These schemes may operate individually, synergistically, or in combined configurations.

Artificial intelligence: Artificial intelligence introduces techniques that enable networks to make intelligent decisions, defend nodes, and address protocol-related challenges. It aims to transform nodes into autonomous

decision-makers. The main branches used in MANET security include machine learning, neural networks, deep learning, and fuzzy logic [8].

Blockchain approach: This approach uses decentralized consensus mechanisms, cryptographic techniques, and immutable data storage. It helps maintain the integrity of network operations, prevents data tampering or unauthorized access, and supports transparent and auditable interactions among network participants.

Credit approach: Credit-based schemes, such as the packet purse and packet trade models, distribute credit inside packets as they move through intermediate nodes. In the packet-purse model, credit decreases at each hop until the packet reaches its destination. In the packet trade model, intermediate nodes "trade" packets by buying and selling them, which incentivizes cooperation.

Cryptography approach: Cryptographic systems encode information into unintelligible forms to prevent unauthorized access. Decryption requires a valid key. Encryption may be symmetric, using one shared key, or asymmetric, using different keys for the sender and the receiver [9].

Formal methods for protocol verification: This approach applies formal methods and model-checking techniques to verify security properties and correctness in MANET protocols. It ensures protocol robustness, resistance to attacks, and adherence to security specifications.

Game theory approach: Game theory contributes significantly to MANET security by offering computational efficiency and probabilistic analysis of strategic interactions. It includes cooperative models, where players follow binding agreements, and non-cooperative models, where participants may alter strategies independently [9].

Incentive approach: Incentive-based strategies encourage cooperative node behaviour and discourage selfish or malicious actions.

Intrusion Detection System (IDS) approach: An IDS monitors system activities, detects intrusions, and responds to breaches. IDS designs include anomaly-based, misuse-based, and signature-based detection systems, each with its unique strengths and limitations [10].

Key management approach: Key management solutions, such as Certified Authority (CA) mechanisms, address node mobility challenges. They reduce control overhead and improve reliability in secure communication [11,12].

Metaheuristic optimization approach: Metaheuristic techniques improve MANET resilience by enhancing resource allocation, optimizing routing behaviour, and reducing vulnerabilities. This lowers the attack surface and increases robustness.

Physical security: Physical security measures, such as tamper-resistant hardware, secure deployment, and node authentication, protect nodes from physical attacks.

Privacy and position-based routing approach: This method secures communication by combining position broadcasting with privacy techniques. Approaches like PPBR use dynamic pseudo-identifiers to minimize route overhead and ensure end-to-end anonymity among nodes [11].

Reputation approach: Reputation systems compute node reputation based on direct and indirect interactions. They help detect suspicious behaviour and guide routing decisions. Watchdog detects misbehaviour, while Pathrater mitigates routing misbehaviour in MANETs [9].

Secure multicasting approach: Secure multicasting protects multicast traffic from DoS attacks using architectures such as DIPLOMA. It works with multicast routing protocols, allocates network resources fairly during attacks, and ensures both sender and receiver access to the multicast group while controlling bandwidth use.

Secure routing approach: Secure routing mechanisms address authentication, prevent route fabrication, and improve protocol responsiveness. They aim to maintain network resilience against various routing attacks.

Trust approach: Trust models address security challenges by assessing the trustworthiness of nodes. They help detect and mitigate malicious behaviour by evaluating factors such as reputation, behaviour history, and local or network-wide observations [13].

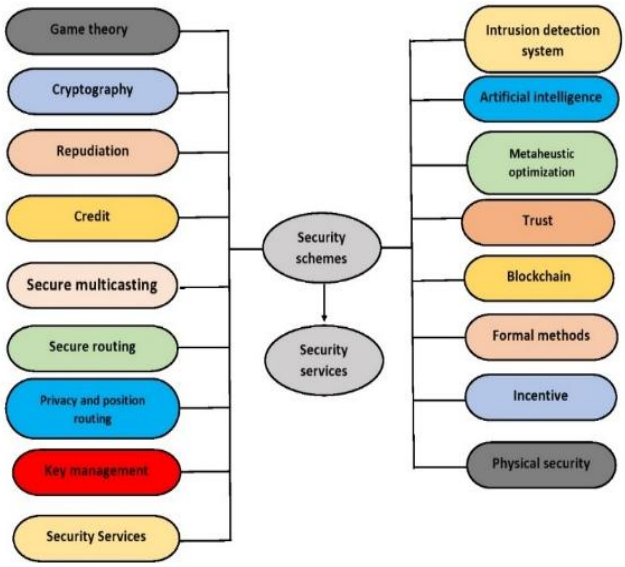

Figure 3. MANETs security schemes

To provide a secure relationship between nodes, security schemes used in MANETs must provide the following services, as illustrated in Figure 4: authentication, authorization, availability, integrity, anonymity, non-repudiation, and confidentiality [14].

- Authentication: Authentication ensures that only authorized nodes are involved in the exchange of information, preventing malicious nodes from impersonating trusted ones and disrupting communication within the network [15].
- Authorization: Authorization involves providing entities with credentials that detail their granted privileges and permissions, ensuring their authenticity and non-repudiation by the certificate authority [16].
- Availability: A node consistently offers the services it's intended for, with a significant focus on thwarting denial-of-service attacks, while certain self-serving nodes render specific network services inaccessible [14].
- Integrity: Integrity ensures that message content can only be altered by authorized users, maintaining message integrity during transmission. Unauthorized actions, such as modifying messages, removing data streams, or unnecessary data replication, compromise integrity [14].
- Anonymity: Anonymity conceals any data that could identify present or owning client nodes, ensuring that such information remains private and is not disclosed by the network device/software or the node itself [17].
- Non-repudiation: Non-repudiation ensures that both the sender and receiver of a message cannot deny having transmitted or received the message, which is crucial for

determining whether a node within a network has been compromised or not [15].

- Confidentiality: Confidentiality guarantees authorization by limiting access to legitimate information to authorized users, thereby safeguarding data privacy [14].

Figure 4. MANETs security schemes

2. Related work

Early Research on secure and adaptive routing in MANETs has evolved across several methodological directions, each with specific strengths and limitations. For foundational trust-based routing without metaheuristics or adaptiveness, early approaches focused on evaluating node behavior through forwarding reliability and historical interactions. Sivaranjani et al. [18] proposed FLEATM, a fuzzy logic-based decision rule framework that updates trust ratings using direct observations and neighbor recommendations, but lacks adaptive routing and metaheuristic optimization. Sen [19] introduced a distributed trust-reputation framework that emphasizes malicious node detection while remaining non-adaptive and not energy-aware. Govindaraj and Arumugam [20] enhanced AOMDV using a trust-based next-hop selection model to counter blackhole attacks, yet the technique does not support energy efficiency or adaptiveness. Cordasco et al. [21] promoted trust-based routing as an alternative to cryptographic mechanisms, although it retains static behavior. Pathan et al. [22] developed TSQRS, which employs social and QoS trust metrics to secure routing but is non-adaptive and lacks metaheuristic mechanisms. These solutions demonstrate that static trust-based routing cannot cope with dynamic and adversarial MANET environments.

In the context of machine learning and hybrid optimization approaches, Hassan et al. [23] introduced FLSTMT-LAR, incorporating federated learning, LSTM-based trust prediction, and NSGA-III optimization. Despite high detection capability and energy efficiency, the model exhibits high computational complexity and partial adaptiveness. Arulselvan and Rajaram [24] integrated deep reinforcement learning with a dolphin-cat optimizer, achieving improved delay and trust estimation but limited real-time adaptiveness. Priya et al. [25] combined GA, PSO, reinforcement learning, and quantum-resistant cryptography to enhance security, though the approach remains centralized, heavy, and only partially adaptive. These hybrid approaches highlight gains in intelligence but struggle to deliver fully dynamic, lightweight, and distributed adaptiveness.

A distinct category involves metaheuristic routing with trust but partial adaptiveness, where trust mechanisms exist but are only loosely connected to the optimization process. Veeramani et al. [2] used FFWHO with LF-SSO-DSR, incorporating intelligent dynamic trust yet keeping trust static and disconnected from metaheuristic decision-making. Kondaiah and Sathyanarayana [26] integrated fuzzy-firefly and PSO for intrusion detection, but trust is applied post-selection rather than proactively guiding routing decisions. Prabaharan and Ponnusamy [27] proposed a hybrid ACO that improves energy consumption and mitigates selfish behavior, although the lack of structured trust limits security. Krishnaveni and Angel [28] used IHSO for trusted-node identification but without adaptive reactivity. Dudala et al. [29] combined WOA with differential evolution to mitigate Byzantine and wormhole attacks, remaining detection-oriented and partially adaptive. Alappatt and Prathap [30] employed LF-SSO and SH2E encryption for secure multipath routing, but adaptiveness is still limited. In these works, trust and metaheuristics coexist but do not interact deeply, limiting proactive routing resilience.

A related yet more advanced category consists of trust-integrated metaheuristic mechanisms with partial adaptiveness, where trust is directly embedded into the optimization process. These approaches differ from the prior category because trust actively influences the metaheuristic cost, selection, or fitness functions, even though adaptiveness remains incomplete. Veeraiah et al. [31] integrated fuzzy trust clustering with C-SSA, improving energy and security but using trust mainly for detection rather than preventive adaptiveness. Vishwakarma et al. [32] combined fuzzy butterfly optimization with chaotic grey wolf optimization, embedding trust values and encryption, but retaining partial adaptiveness. Brar et al. [33] used TrustOpt (ACO-WOA hybrid) with dynamic trust updating, yet the method remains detection-heavy. Vellingiri et al. [34] applied fuzzy trust evaluation with harmony search, GA, and cuckoo search for DSR, but trust integration is still limited. Karanje and Eklarker [35] developed GLBO, which combines energy and trust metrics in optimization, but lacks a full adaptiveness model. Sankaran and Hong [36] used cuckoo search for trust-aware routing, but static RSSI restricts dynamic response. These strategies demonstrate progress toward integrating security with optimization, but still lack continuous state-based adaptiveness.

Another relevant category includes metaheuristic clustering-based trust routing with partial adaptiveness, where metaheuristics optimize cluster formation rather than end-to-end routing. Kumari et al. [37] proposed RTO-TV, using modified group optimization and trust-based security for cluster-head selection, achieving partial adaptiveness but lacking dynamic path re-evaluation. Aravindan and Rajaram [38] combined reinforcement learning with spider monkey optimization for secure cluster routing, offering trust support but limited dynamic re-routing. These methods provide security and energy efficiency, but do not deliver a metaheuristic, trust-adaptive path selection framework. Toward full integration, adaptive trust–metaheuristic mechanisms have emerged. Prasanna and Ramesh [39] used ASO and hybrid cat swarm optimization for trust-aware routing, offering a degree of adaptiveness but suffering encryption overheads. Kamboj and Dalip [40] incorporated grey wolf optimization and cuckoo search with machine learning for malicious detection, but the strategy remains partially adaptive and threat-detection-focused rather than preventive. These works signal a shift towards adaptiveness

but still do not achieve continuous trust-driven dynamic optimization. Finally, the RFD-based baselines from which the proposed method derives show key limitations. Amin et al. [6] presented RFDTrust, embedding trust into the RFD paradigm using trust_forwarding and trust_goodness scores. However, path selection is restricted to lower-altitude neighbors, preventing full exploitation of the network topology and limiting both energy efficiency and trust propagation. Agor et al. [1] improved this with PRFDRA, enabling selection among higher, equal, and lower altitudes to enhance network longevity. However, PRFDRA remains non-secure and only partially adaptive. These limitations collectively motivate the proposed TA-PRFDRA, which integrates multi-stage trust evaluation directly into the RFD metaheuristic, employs adaptive SFD-MFD switching, and enables dynamic, preventive, and energy-efficient path selection beyond the capabilities of prior methods. Table 1 presents a comparative summary of representative MANET routing protocols, highlighting trust mechanisms, metaheuristic integration, adaptiveness, and key limitations relative to TA-PRFDRA.

3. Methodology

3.1 Overview and framework of TA-PRFDRA

The proposed TA-PRFDRA is developed as an enhancement of the PRFDRA proposed by Agor et al. [1]. PRFDRA itself is derived from the RFD model introduced by Rabanal et al. [5]. TA-PRFDRA retains the energy-aware and delay-optimized structure of PRFDRA but integrates trust into all routing computations. It also presents an adaptive SFD-MFD switching mechanism to improve resilience under dynamic and deceptive network conditions.

3.2 Trust estimation module

This module evaluates node reliability through four dimensions: forwarding ratio, route participation, energy reputation, and routing metric consistency. Each submetric contributes to a composite trust score T_{ij} for neighbour j as perceived by the node i defined in equations 1 to 4:

Forwarding ratio (α_{ij}):

$$\alpha_{ij} = {}^{F_{ij}}\!/_{R_{ij}} \quad (1)$$

where F_{ij} is the number of packets forwarded by the node j from node i, and R_{ij} is the number of packets received by j from node i. This metric, rooted in watchdog and path-rater trust frameworks, helps identify packet-dropping behaviors associated with blackhole attacks [19].

Route Participation Ratio (β_j):

$$\beta_j = {}^{RPF_j}\!/_{RP_{total}} \quad (2)$$

where RPF_j is the number of valid routes that include the node j and RP_{total} is the total number of valid routes that are observed. This monitors how frequently j appears in valid routes and penalizes nodes that rarely participate in routing. Low participation suggests non-cooperation or instability.

Energy reputation (γ_j):

$$\gamma_{j=}{}^{E_j}\!/_{E_{init}} \quad (3)$$

where E_j is the residual energy and E_{init} is the initial energy. This extends the energy-aware metrics of PRFDRA [1].

Routing metric consistency (δ_j):

$$\delta_j = 1 - {}^{(|reported\ (TD_j) - measured(TD_j)|)}\!/_{measured\ (TD_j)} \quad (4)$$

Table 1. Comparative Summary of Representative MANET routing Protocols and key limitations relative to TA-PRFDRA

Study	Trust Mechanism	Metaheuristic/ Optimization	Adaptiveness	Main Limitation
Foundational trust-based routing (non-adaptive)- [18-22]	Fuzzy, reputation, or social trust	None	None	Static trust; lacks metaheuristic and adaptive behavior
Hybrid ML/ Optimization trust routing (partial adaptiveness)- [23-25]	Learning-based trust	Multiobjective or hybrid ML-optimization	Partial	High computational overhead; delay; limited real-time adaptiveness
Metaheuristic routing with trust but partial adaptiveness [26-30]	Static or loosely coupled trust	Nature-inspired	Partial	Trust not embedded in optimization; largely detection-based
Trust-integrated metaheuristic routing with partial adaptiveness [31-36]	Fuzzy or behavioural trust	Hybrid metaheuristics	Partial	Limited preventive adaptiveness; static elements restrict dynamic response
Metaheuristic clustering-based trust routing (partial adaptiveness) [37,38]	Cluster or RL-based trust	Nature-inspired	Partial	Adaptiveness limited to cluster management
Adaptive trust metaheuristic routing (partial adaptiveness) [39,40]	Behavioral and ML-assisted trust	Hybrid metaheuristics	Partial	Detection-focused; lacks continuous pre-emptive adaptiveness
RFD variant without trust [1]	None	RFD metaheuristic	Partial	Energy-aware; no trust
RFD variant with trust [6]	Behavioral trust	RFD metaheuristic	Partial	Trust propagation constrained; limited energy efficiency
Proposed TA-PRFDRA	Continuous multi-stage trust integration	RFD metaheuristic with SFD-MFD switching	Dynamic	Adaptive, preventive, trust, and energy-efficient route selection

This validates reported delay values to identify manipulation of common wormholes and grey hole attacks. Here, $reported\ (TD_j)$ refers to the delay value that the node j advertises its current packet transmission time. $measured(TD_j)$, on the other hand, represents the actual time delay inferred by the node j through empirical observation. TD_j captures the queuing and forwarding latency of the node j, which rises with congestion. Therefore, consistent discrepancies between reported and observed delays may indicate intentional misreporting, as observed in wormhole or grey hole attacks.

The composite trust score is computed as:

$$T_{ij}^{new} = w_1.\alpha_{ij} + w_2.\beta_j + w_3.\gamma_j + w_4.\delta_j \quad (5)$$

with weight vector $[w_1, w_2, w_3, w_4]$ = [0.4, 0.2, 0.2, 0.2], emphasizing forwarding reliability while balancing participation, energy and consistency. The exponentially weighted moving average (EWMA), $T_{ij}(t)$ is computed as:

$$T_{ij}(t) = \lambda.T_{ij}(t-1) + (1-\lambda).T_{ij}^{new},\ \lambda\epsilon[0.6, 0.9] \quad (6)$$

λ is a smoothing factor that determines the weight given to historical data. The EWMA produces smoothed trust scores to prevent rapid fluctuations and improve decision stability. Equations (1) to (6) are original formulations developed in this study to quantify node trust. They are conceptually informed by trust models in wireless networks [41–46], but mathematically defined for the TA-PRFDRA framework.

3.3 Trust-augmented gradient computation

In PRFDRA, the neighbour $gradient(i,j)$ is based on altitude difference, time delay (TD) energy (E) and number of hops (N_{Hops}). TA-PRFDRA modifies it to account for trust in equation 7.

$$gradient_{trust}(i,j) = \left[\left(altitude_{trust}(i) - altitude_{trust}(j)\right).TD_j.T_{ij}\right] \Big/ [\mathrm{E}_j.N_{Hops}(i,j)] \quad (7)$$

This formulation penalises low-trust neighbors while maintaining the energy, hop count and latency considerations inherited from PRFDRA.

3.4 Adaptive SFD–MFD switching logic

Whereas PRFDRA employs only an SFD strategy, TA-PRFDRA introduces a variance-driven switching mechanism, as defined in equations 8 and 9.

$$\mu_{gradient_{trust}} = {}^{1}\!/_{|N(i)|} \sum_{j\in N(i)} gradient_{trust}(i,j) \quad (8)$$

$$\sigma^2_{gradient_{trust}} = {}^{1}\!/_{|N(i)|} \sum_{j\in N(i)} (gradient_{trust}(i,j) - \mu_{gradient_{trust}})^2 \quad (9)$$

If $\sigma^2_{gradient_{trust}} < \theta$ the algorithm switches to MFD mode; otherwise, it remains in SFD mode as defined in equations (10) to (11). This allows dynamic control of forwarding strategies based on local variation in gradients. In SFD mode, the node with the highest $gradient_{trust}(i,j)$ is deterministically chosen.

If $\sigma^2_{gradient_{trust}} < \theta \rightarrow$ MFD mode (gradients are similar) (10)

Else → SFD mode (one clear path dominates) (11)

3.5 Trust-Based Probabilistic Flow Assignment in MFD Mode

When MFD mode is active, forwarding probabilities for each neighbor are calculated using the normalized formulae defined in equations 12 to 14 of Table 2.

Table 2. Trust-based probabilistic flow assignment under MFD

Neighbor Set	Probability Equation	Equations
$V_k(i)$	$[gradient_{trust}(i,j).TD_j]/\Sigma\ E_j.\ N_{Hops}(i,j)$	(12)
$U_k(i)$	$[\omega\ /gradient_{trust}(i,j)|).TD_j]$	(13)
$F_k(i)$	$[\delta.TD_j]\ /\ \Sigma\ E_j N_{Hops}(i,j)$	(14)

These probabilistic assignments extend PRFDRA's neighbour selection mechanism by introducing trust-weighted flow control.

3.6 Trust-conscious erosion mechanism

Erosion is adjusted based on the selected mode defined in equations 15 to 17 of Table 3.

- SFD: Apply erosion to the selected neighbor only.
- MFD: Distribute erosion proportionally to each neighbour.

This ensures reinforcement of trusted paths and degradation of malicious ones.

Table 3. Trust-weighted erosion distribution formulas

Neighbor Set	Erosion Equation	Equation
$V_k(i)$	$[\varepsilon_V.\text{gradient}_{trust}(i,j).TD_j]/[(N-1).M.E_j.N_{Hops}(i,j)]$	(15)
$U_k(i)$	$[\varepsilon_U.TD_j]/[|gradient_{trust}(i,j)|.(N-1).E_j.N_{Hops(i,j)}]$	(16)
$F_k(i)$	$[\varepsilon_F.TD_j]\ /\ [(N-1).M.E_j.\text{NHops}(i,j)]$	(17)

3.7 Trust-conscious altitude mechanism

Altitude reduction is scaled based on the target node's trustworthiness. Nodes with lower trust scores cause less erosion, discouraging traffic through untrusted nodes and vice versa. The amount of sediment deposited is influenced by the trust level of the node j. Less sediment is transferred to low-trust nodes, reflecting reduced confidence in their long-term reliability. Equation 18 computes $altitude_{trust}(i)$ as:

$$altitude_{trust}(i) = altitude_{trust}(i) \pm \left(\left(erosion_{trust}(i,j).T_{ij}\right)\Big/_N\right) \quad (18)$$

In Equation 19, blocked drops increase a node's altitude more when the node is untrustworthy, discouraging future selection.

$$altitude_{trust}(l) = altitude_{trust}(l) + paramBlockedDrop.carriedsediment_{trust}.T_{ij} \quad (19)$$

3.8 Trust-focused sedimentation process

Trust modulates the erosion contribution to carried sediment, further limiting the role of low-trust nodes in the sediment transportation process.

Equations 20 and 21 compute $sediment_{trust}(i,j)$ and $carriedSediment_{trust}(i,j)$.

$$sediment_{trust}(i,j) = (\beta.(altitude_{trust}(i) - altitude_{trust}(j)).carriedSediment_{trust}(i,j).TD_j.T_{ij})/(E_j.N_{Hops}(i,j)) \quad (20)$$

$$carriedSediment_{trust}(i,j) = carriedSediment_{trust}(i,j) + erosion_{trust}(i,j).T_{ij} - sediment_{trust}(i,j) \quad (21)$$

3.9 Route cost with trust penalty

To discourage untrusted paths, the final cost function includes a trust-based penalty. Equation 22 defines $cost_{trust}(i,j)$ as:

$$cost_{trust}(i,j) = \sigma \cdot TD + \mu \cdot [1/Min(E)] + \tau \cdot [1/N_{Hops}] + \varphi.[1/T_{min}] \quad (22)$$

In which $T_{min} = min_{\ell \in P} T_\ell$ to severely punish routes that have even an untrusted link.

3.10 Trust-embedded iteration is the best solution

Solutions passing through high-trust nodes are preferred. Low-trust paths incur a higher normalized cost and are less likely to be selected as the best path. This ensures that trust governs not only local forwarding but also global route convergence. The iteration-best trust-weighted solution is computed as ${T_{trust}}^{IB}$ in equation 23.

$${T_{trust}}^{IB} = arg\ min\ \forall T^{Drop} cost_{trust}(i,j) \quad (23)$$

3.11 Provenance of equations and notation

Equations (1) to (11) are original formulations developed in this study to model trust computation and adaptive SFD-MFD control. Equations (12) to (23) are adapted and extended from PRFDRA [1]. Trust scaling and adaptive logic represent new extensions. Table 4 summarizes the symbols and parameters used in the TA-PRFDRA formulations. Parameters already defined in the text are not repeated.

4. Results and discussion

This section presents a comparative evaluation of TA-PRFDRA against PRFDRA, RFDTrust, RFDManet, and TORA using four performance metrics: packet delivery ratio (PDR), average end-to-end delay (AE2ED), detection rate (DR), and energy consumption (EC). Simulations were conducted across varying source node densities (10–60 active sources) to represent diverse traffic conditions in MANETs. A hybrid adversary model was employed to assess robustness under internal threats, with 10–20% of nodes randomly designated as malicious during initialization. Blackhole nodes dropped all data packets after path establishment, while grayhole nodes selectively forwarded ~70% and dropped 30% of packets. These behaviors were implemented via packet-forwarding suppression events in NS-3, affecting path selection without altering metric computations.

The trust-based framework mitigated malicious influence through distributed neighbor evaluation, where each node computed its local trust based on the forwarding ratio, residual energy reliability, reporting consistency, and route participation frequency. Nodes with cumulative trust below the threshold $\tau = 0.5$ were penalized in gradient, erosion, and flow probability calculations, reducing their impact on subsequent path selection. Statistical significance testing was performed between TA-PRFDRA and the trust-based baseline (RFDTrust) for all four metrics using paired t-tests at a 95% confidence level. This focused comparison aligns with established evaluation practices, avoiding redundant pairwise testing [47,48]. Tables 4–6 present the key simulation parameters, averaged results, and statistical test outcomes, respectively.

Table 4. Simulation parameters

Simulator	NS-3
Routing Protocols	TA-PRFDRA, PRFDRA, RFDTrust, RFDManet, TORA
Simulation Time (S)	1500
Simulation Area	1500 m x1500 m
Mac Layer Protocol	IEEE 802.11
Nodes Number	250
Transmission Range (m)	250
Mobility Model	RWP
Highest Node Speed	10 m/s
Data Packet Size	512 bytes
Traffic	CBR
Initial Node Energy (J)	100

4.1 Packet delivery ratio (PDR)

As shown in Figure 5, TA-PRFDRA maintains a consistently high PDR across all source counts, recording 99.64 % at 10 active sources and remaining above 98 % throughout, achieving 98.87 % at 60 sources. The average PDR values for TA-PRFDRA, PRFDRA, RFDTrust, RFDManet, and TORA are 99.54 %, 99.42 %, 99.34 %, 99.20 %, and 98.21 %, respectively. Accordingly, the corresponding improvement rates of TA-PRFDRA over PRFDRA, RFDTrust, RFD, and TORA are 0.12 %, 0.20 %, 0.33 %, and 1.33 %. The paired t-test confirms that the improvement over RFDTrust is statistically significant (p = 0.022, Table 6).

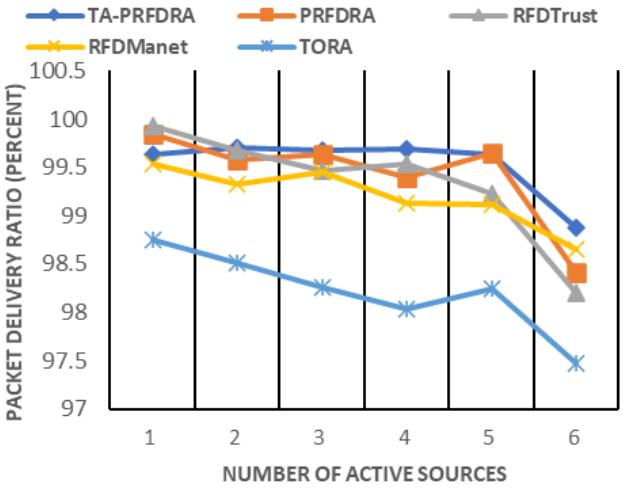

Figure 5. Packet delivery ratio against the number of sources

4.2 Average end-to-end delay (AE2ED)

Figure 6 illustrates the AE2ED performance of all algorithms. TA-PRFDRA achieves an average end-to-end delay of 0.087 s, compared with 0.113 s, 0.128 s, 0.137 s, and 0.225 s for PRFDRA, RFDTrust, RFDManet, and TORA, respectively. The corresponding improvement rates of TA-PRFDRA over PRFDRA, RFDTrust, RFD, and TORA are 0.026 s, 0.041 s, 0.050 s, and 0.138 s. The paired t-test confirms that the delay reduction relative to RFDTrust is statistically significant (p = 0.010).

Table 5. Averaged performance metrics of TA-PRFDRA and baseline protocols under varying numbers of active sources

Scenario					
Number of Active Sources	**PDR in percent**				
	TA-PRFDRA	**RFDTrust**	**PRFDRA**	**RFD**	**TORA**
10	99.64	99.93	99.84	99.53	98.75
20	99.71	99.68	99.58	99.33	98.51
30	99.67	99.47	99.63	99.45	98.26
40	99.69	99.53	99.4	99.13	98.03
50	99.63	99.23	99.65	99.12	98.24
60	98.87	98.2	98.41	98.65	97.47
Number of Active Sources	**AE2ED in seconds**				
	TA-PRFDRA	**RFDTrust**	**PRFDRA**	**RFD**	**TORA**
10	0.07	0.1	0.07	0.09	0.19
20	0.07	0.12	0.09	0.11	0.2
30	0.08	0.13	0.11	0.12	0.21
40	0.08	0.14	0.13	0.16	0.25
50	0.09	0.11	0.09	0.15	0.22
60	0.13	0.17	0.19	0.19	0.28
Number of Active Sources	**DR in percent**				
	TA-PRFDRA	**RFDTrust**	**PRFDRA**	**RFD**	**TORA**
10	60.4	55.02	51.13	46.7	39.6
20	63.25	58.5	52.66	47.65	41.63
30	69.53	63.22	57.32	48.01	42.08
40	78.02	75.57	58.19	49.3	44.3
50	81.65	75.9	59	49.88	44.92
60	81.95	80.06	59.77	50.25	44.98
Number of Active Sources	**EC in joules**				
	TA-PRFDRA	**RFDTrust**	**PRFDRA**	**RFD**	**TORA**
10	46.34	50.81	48.38	53.14	63.16
20	48.51	52.22	49.95	54.08	62.77
30	48.69	51.8	49.8	53.21	61.5
40	48.47	53.31	51.41	55.3	63
50	49.1	54.88	51.69	55.99	62.43
60	46.62	50.17	46.82	51.4	64.91

Table 6. Statistical significance of TA-PRFDRA compared with the trust baseline protocol

Metric	Compared Strategy	Mean difference (TA-baseline)	RFDTest used	P_value	Significant (α =0.05)
PDR (%)	RFDTrust	+0.20	Paired t	0.022	Yes
AE2ED (s)	RFDTrust	-0.04	Paired t	0.010	Yes
DR (%)	RFDTrust	+4.10	Paired t	0.008	Yes
EC (J)	RFDTrust	-4.84	Paired t	0.006	Yes

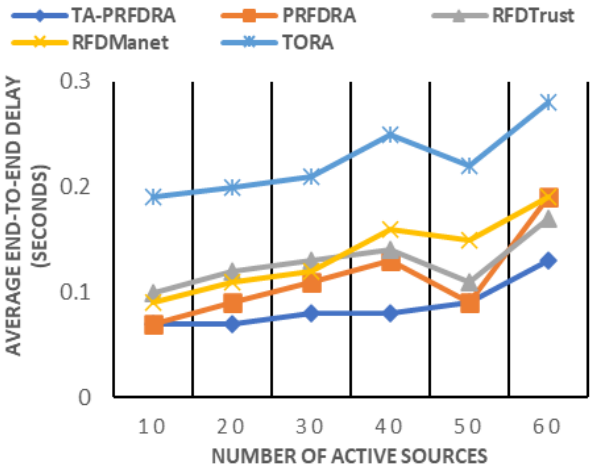

Figure 6. Average end-to-end delay against the number of sources

4.3 Detection rate (DR)

As shown in Figure 7, TA-PRFDRA consistently achieves higher DR across all source counts. The average DR is 72.47 %, compared with 55.51 %, 68.05 %, 48.30 %, and 42.09 % for PRFDRA, RFDTrust, RFDManet, and TORA, respectively. The improvement rates of TA-PRFDRA over PRFDRA, RFDTrust, RFD, and TORA are 16.96 %, 4.42 %, 24.17 %, and 30.38 %. The paired t-test indicates that the improvement over RFDTrust is statistically significant ($p = 0.008$).

4.4 Energy consumption (EC)

Figure 8 compares the EC of all algorithms. TA-PRFDRA records 47.36 J, while PRFDRA, RFDTrust, RFDManet, and TORA consume 49.68 J, 52.20 J, 53.52 J, and 63.63 J, respectively. The corresponding improvement rates of TA-PRFDRA over PRFDRA, RFDTrust, RFD, and TORA are 2.32 J, 4.84 J, 6.16 J, and 16.27 J. The paired t-test confirms that the reduction relative to RFDTrust is statistically significant ($p = 0.006$).

4.5 Discussion

The combined results validate that the proposed TA-PRFDRA protocol maintains high delivery reliability, low latency, strong security awareness, and energy efficiency under dynamic MANET conditions. Its performance superiority is especially evident under high source densities, indicating excellent scalability and resilience. PRFDRA selects paths using residual energy and performance metrics, but assumes all nodes behave reliably [1]. Its gradient and flow-probability computations are energy-aware but trust-neutral. This allows unstable or malicious nodes to influence path formation, causing route oscillations and packet losses. TA-PRFDRA integrates a composite trust score into gradient and flow-probability calculations. This produces more stable path selection and reduced latency compared with PRFDRA.

RFDTrust evaluates node reputation only prior to node selection [6]. Packets primarily follow downhill paths, limiting path diversity and restricting adaptiveness in flat or deceptive topologies. TA-PRFDRA embeds trust evaluation across all RFD stages and applies adaptive switching between single-flow and multi-flow modes based on trust-weighted gradient variance. This allows rapid isolation of low-trust nodes while preserving multiple routing options. RFDManet relies solely on altitude differences and erosion dynamics without energy or trust weighting [6]. Paths may include energy-depleted or malicious nodes, resulting in instability, high retransmissions, and increased energy consumption. TA-PRFDRA combines energy and trust weights in gradient and move-probability calculations. This ensures selected paths are more reliable and sustainable under dynamic conditions.

TORA employs a link-reversal mechanism and maintains multiple routes, but it treats all links equally and does not consider trust [49]. Frequent control messages and uniform link treatment increase delay and energy use, especially when nodes behave maliciously. TA-PRFDRA concentrates forwarding along high-trust links, which reduces unnecessary reversals and enhances route reliability. TA-PRFDRA has some limitations. The trust update process increases computation on nodes with limited resources. The algorithm may also scale poorly in very large networks because more nodes require more trust and gradient evaluations. Future work will reduce this cost through lighter trust updates and more efficient gradient processing to support larger topologies.

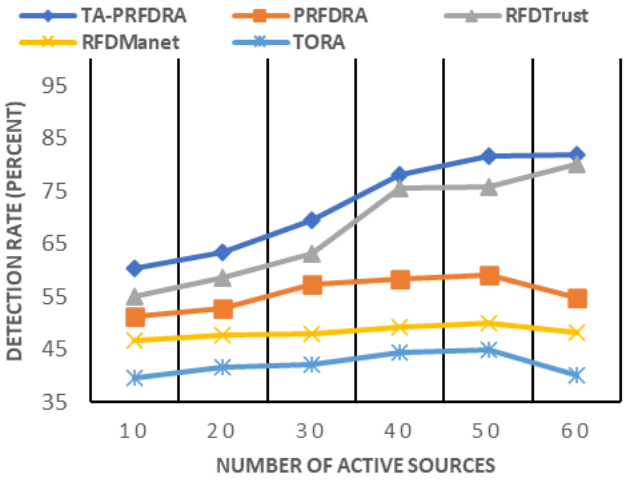

Figure 7. Detection rate against the number of sources

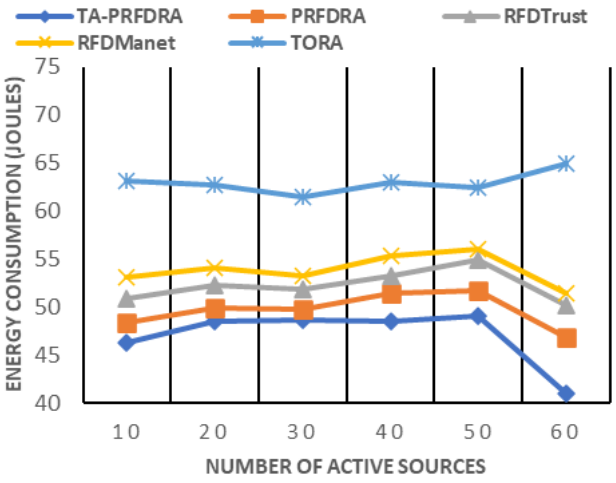

Figure 8. Energy consumption against the number of sources

5. Conclusion

This paper presented TA-PRFDRA, a trust and adaptive enhanced version of PRFDRA for secure and energy-efficient routing in MANETs. TA-PRFDRA incorporated behavioral trust evaluation into all PRFDRA stages and applied dynamic SFD–MFD switching based on trust-weighted gradient variance. Simulation results showed that, compared with PRFDRA, RFDTrust, RFDManet, and TORA, TA-PRFDRA achieved up to 1.33% higher PDR, reduced AE2ED by 0.14 s, increased DR by up to 30.38 %, and lowered EC by up to 15.94 J. Statistical analysis confirmed that improvements over RFDTrust were significant. Future work will extend statistical validation to all comparative protocols and improve computational efficiency. Additional performance metrics such as routing overhead, throughput, and false positive rate will also be evaluated in dense MANET settings. Future studies may explore the integration of blockchain-supported trust mechanisms and IoT-based architectures to strengthen secure distributed routing.

Ethical issue

The authors are aware of and comply with best practices in publication ethics, specifically regarding authorship (avoidance of guest authorship), dual submission, manipulation of figures, competing interests, and compliance with research ethics policies. The authors adhere to publication requirements that the submitted work is original and has not been published elsewhere.

Data availability statement

The manuscript contains all the data. However, more data will be available upon request from the authors.

Conflict of interest

The authors declare no potential conflict of interest.

References

[1] Agor AD, Asante M, Hayfron-Acquah JB, Ami-Narh JT, Aziale LK, Peasah KO. A power-aware river formation dynamics routing algorithm for enhanced longevity in MANETs. International Journal of Computer Networks and Applications 2024;11:274–89. https://doi.org/10.22247/ijcna/2024/17.

[2] Veeramani R, MadhanMohan R, Mahesh C. Energy Efficient and QoS Aware Trustworthy Routing Protocol for Manet Using Hybrid Optimization Algorithms. Computer Science 2025;26:1–31. https://doi.org/10.7494/CSCI.2025.26.1.5135.

[3] Dorigo M, Maniezzo V, Colorni A. Ant system: Optimization by a colony of cooperating agents. IEEE Transactions on Systems, Man, and Cybernetics-Part B Cybernetics, vol. 26, IEEE; 1996, p. 29–41. https://doi.org/10.1109/3477.484436.

[4] Hosseini HS. Problem solving by intelligent water drops. 2007 IEEE Congress on Evolutionary Computation, 2007, p. 3226–31. https://doi.org/10.1109/CEC.2007.4424885.

[5] Rabanal P, Rodríguez I, Rubio F. Using river formation dynamics to design heuristic algorithms. In Unconventional Computation: 6th International Conference, UC 2007, Kingston, Canada: Springer Berlin Heidelberg; 2007.

[6] Amin SH. Optimising routing and trustworthiness of ad hoc networks using swarm intelligence. Brunel University School of Engineering and Design PhD Theses, 2014.

[7] Papadimitratos P, Haas ZJ. Secure Link State Routing for Mobile Ad Hoc Networks. Proceedings - 2003 Symposium on Applications and the Internet Workshops, SAINT 2003 2024:379–83. https://doi.org/10.1109/SAINTW.2003.1210190.

[8] Khalfaoui H, Farchane A, Safi S. An overview of the security improvements of artificial intelligence in MANET. International Conference on Cybersecurity, Cybercrimes, and Smart Emerging Technologies, Cham: Springer International Publishing; 2022, p. 135–46. https://doi.org/10.1007/978-3-031-21101-0_11.

[9] Khan UIB, Olanrewaju RF, Anwar F, Najeeb AR, Yaacob M. A survey on MANETs: Architecture, Evolution, Applications, Security Issues and Solutions. Indonesian Journal of Electrical Engineering and Computer Science 2018;12:832–42. https://doi.org/10.11591/ijeecs.v12.i2.pp832-842.

[10] Popli R, Sethi M, Kansal I, Garg A, Goyal N. Machine learning based security solutions in MANETs: State of the art approaches. Journal of Physics: Conference Series 2021;1950:1–7. https://doi.org/10.1088/1742-6596/1950/1/012070.

[11] Ali MA, Sarwar Y. Security issues regarding MANET (Mobile Ad Hoc Networks): challenges and solutions. Blekinge Institute of Technology, 2011.

[12] Hussain MZ, Hasan MZ. Collective study on security threats in MANET. International Journal of Scientific & Technology Research 2017;6:32–7.

[13] Saha HN, Bhattacharyya D, Banerjee B, Mukherjee S, Singh R, Ghosh D. A review on attacks and secure routing protocols in MANET. International Journal of Innovative Research and Review 2013;1:12–36.

[14] Joshi K, Kumar K. Security breaches of mobile ad-hoc networks (MANET) - A review. Educational Administration Theory and Practice 2024;30:2656–65. https://doi.org/10.53555/kuey.v30i4.1912.

[15] Yadav N, Chug U. Secure Routing in MANET: A Review. 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (Com-IT-Con), 2019, p. 1–5. https://doi.org/10.1109/COMITCon.2019.8862238.

[16] Panda N, Patra B, Hota S. MANET routing attacks and their countermeasures: A survey. Journal of Critical Reviews 2020;7:2777–92. https://doi.org/10.31838/jcr.07.13.428.

[17] Agarwal S, Kaur R, Agarwal T. MANET expansion security challenges attacks and intriguing future trends. International Journal of Computer Sciences and Engineering 2018;6:906–15. https://doi.org/10.13140/RG.2.2.22483.84005.

[18] Sivaranjani R, Shankar R, Duraisamy S. FLEATM: Fuzzy Logic-Based Energy-Aware Trust Based Routing in MANETs. Communications in Computer and Information Science 2025;2426 CCIS:144–59. https://doi.org/10.1007/978-3-031-86296-0_12.

[19] Sen J. A Distributed Trust and Reputation Framework for Mobile Ad Hoc Networks. International Conference on Network Security and Applications, Springer Berlin Heidelberg; 2010, p. 538–47.

[20] Govindaraj M, Arumugam S. Enhancing IoT Security with Trust-Based Mechanism for Mitigating Black Hole Attacks. International Journal of Safety and Security Engineering 2023;13:917–23. https://doi.org/10.18280/ijsse.130515.
[21] Cordasco J, Wetzel S. Cryptographic Versus Trust-based Methods for MANET Routing Security. Electronic Notes in Theoretical Computer Science 2008;197:131–40. https://doi.org/10.1016/J.ENTCS.2007.12.022
[22] Pathan MS, Zhu N, He J, Zardari ZA, Memon MQ, Hussain MI. An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs. Future Internet 2018;10:16. https://doi.org/10.3390/FI10020016.
[23] Hassan SM, Mohamad MM, Muchtar FB, Dawoodi FBYP. Enhancing MANET Security Through Federated Learning and Multiobjective Optimization: A Trust-aware Routing Framework. IEEE Access 2024. https://doi.org/10.1109/ACCESS.2024.3505236.
[24] Arulselvan G, Rajaram A. Routing attacks detection in MANET using trust management enabled hybrid machine learning. Wireless Networks 2025;31:1481–95. https://doi.org/10.1007/S11276-024-03846-7/METRICS.
[25] Priya SS, Vijayabhasker R, Rajaram A. Advanced Security and Efficiency Framework for Mobile Ad-Hoc Networks Using Adaptive Clustering and Optimization Techniques. Journal of Electrical Engineering and Technology 2025;20:1815–26. https://doi.org/10.1007/S42835-024-02119-9/METRICS.
[26] Kondaiah R, Sathyanarayana B. Trust Factor and Fuzzy-Firefly Integrated Particle Swarm Optimization based Intrusion Detection and Prevention System for Secure Routing of Manet. International Journal of Computer Networks & Communications (IJCNC) 2018;10. https://doi.org/10.5121/ijcnc.2018.10102.
[27] Prabaharan SB, Ponnusamy R. Secure and energy efficient MANET routing incorporating trust values using hybrid ACO. 2016 International Conference on Computer Communication and Informatics, ICCCI 2016, Coimbatore, India: Institute of Electrical and Electronics Engineers Inc.; 2016, p. 1–8. https://doi.org/10.1109/ICCCI.2016.7479933.
[28] Krishnaveni S, Angel N. Energy Efficient MANET by Trusted Node Identification Using IHSO Optimization. Smart Network Inspired Paradigm and Approaches in IoT Applications 2019:239–53. https://doi.org/10.1007/978-981-13-8614-5_15.
[29] Dudala DSS, Patamsetti R, Nuli PB, Nagendranath M. WOA-DE Hybrid for Energy-Efficient and Secure Routing in MANETs. IJSAT - International Journal on Science and Technology 2025;16:1–8. https://doi.org/10.71097/IJSAT.V16.I1.3034.
[30] Alappatt V, Prathap J. Trust-Based Energy Efficient Secure Multipath Routing in MANET Using LF-SSO and SH2E. International Journal of Computer Networks and Applications (IJCNA) 2021;8:400–11. https://doi.org/10.22247/ijcna/2021/209706.
[31] Veeraiah N, Khalaf OI, Prasad CVPR, Alotaibi Y, Alsufyani A, Alghamdi SA, et al. Trust aware secure energy efficient hybrid protocol for MANET. IEEE Access 2021;9:120996–1005. https://doi.org/10.1109/ACCESS.2021.3108807.
[32] Vishwakarma RK, Sahu M, Sharma D. Performance evaluation of MAC protocol in mobile ad-hoc wireless network. International Journal of Research Publication and Reviews 2022;3:55–61.
[33] Brar MK, Singh S, Singh S. TrustOpt: An optimized trust-based approach for integrated attacks in MANETs. Proceedings - 2nd International Conference on Advancement in Computation and Computer Technologies, InCACCT 2024, Gharuan, India: Institute of Electrical and Electronics Engineers Inc.; 2024, p. 534–40. https://doi.org/10.1109/INCACCT61598.2024.10551211.
[34] Vellingiri E, Kalimuthu VK, Samydurai G. Fuzzy Logic Based DSR Trust Estimation Routing Protocol for MANET Using Evolutionary Algorithms. Tehnički Vjesnik 2021;28:2006–14. https://doi.org/10.17559/TV-20200612102818.
[35] Karanje P, Eklarker R. Trust and Energy-aware Multipath Selection in MANET for Ensuring Quality-of-service Using the Optimization Protocol. International Journal on Artificial Intelligence Tools 2023;32. https://doi.org/10.1142/S0218213023500239.
[36] Sankaran KS, Hong SP. Trust Aware Secured Data Transmission Based Routing Strategy Using Optimal Ch Selection in Mobile Ad-Hoc Network. Mobile Networks and Applications 2024;29:385–97. https://doi.org/10.1007/S11036-023-02259-8/METRICS.
[37] Kumari SV, Sibi SA, Selvan SM, Nadar KP. RTO-TV: Routed Tree Optimization and Trust-Value-Based Security Scheme to Prevent Black Hole Attack in MANET. Journal of Sensors 2024;2024:3363923. https://doi.org/10.1155/2024/3363923.
[38] Aravindan S, Rajaram A. Energy-aware multi-attribute trust modal for secure MANET-IoT environment. Multimedia Tools and Applications 2024;83:85637–62. https://doi.org/10.1007/S11042-024-20075-4/METRICS.
[39] Prasanna KS, Ramesh B. Multiobjective Secure Trust Aware Redundant Array Shifting Encryption and Clustering Based Routing in Mobile Ad Hoc Networks. International Journal of Communication Systems 2025;38:e6074. https://doi.org/10.1002/DAC.6074.
[40] Kamboj N, Dalip. Secure And Energy-Efficient Multi-Objective MetaHeuristic Routing Protocol for MANET. 2024 15th International Conference on Computing Communication and Networking Technologies, ICCCNT 2024, Kamand, India: Institute of Electrical and Electronics Engineers Inc.; 2024, p. 1. https://doi.org/10.1109/ICCCNT61001.2024.10725180.
[41] Vikas, Wahi C, Sagar BB, Manjul M. Trusted Energy-Aware Hierarchical Routing (TEAHR) for Wireless Sensor Networks. Sensors 2025, Vol 25, Page 2519 2025;25:2519. https://doi.org/10.3390/S25082519.
[42] Udhaya Sankar SM, Dhinakaran D, Deboral CC, Ramakrishnan M. Safe Routing Approach by

Identifying and Subsequently Eliminating the Attacks in MANET. International Journal of Engineering Trends and Technology 2022;70:219–31. https://doi.org/10.14445/22315381/IJETT-V70I11P224.

[43] Mandale RJ, Kavethekar AM, Thorat SA. A survey on trust based MANET routing. 6th International Conference on Advanced Computing & Communication Technologies (ICACCT-2012), Panipat,Haryana, India: Asia Pacific Institute of Information Technology SD India; 2012, p. 73–80.

[44] Shafiuddin S, Krishna KH. TrustRIDR-Net: A Hybrid Trust-Aware Routing Framework Using RFO and DRL for Scalable IoT Networks. Engineering, Technology & Applied Science Research 2025;15:27421–9. https://doi.org/10.48084/etasr.12294.

[45] Yang H. A Study on Improving Secure Routing Performance Using Trust Model in MANET. Mobile Information Systems 2020;2020:1–17. https://doi.org/10.1155/2020/8819587.

[46] Venkata M, Reddy K, Kiran Kumar G, Terlapu PV, Jayaram D, Samreen S. Trust Enabled Secure Routing in Vehicular Adhoc Networks. The International Arab Journal of Information Technology 2025;22:592–613. https://doi.org/10.34028/iajit/22/3/13.

[47] Demšar J. Statistical comparisons of classifiers over multiple data sets. Journal of Machine Learning 2006;7:1–30.

[48] Zhang J, Chen N. Bidirectional Dynamic Adaptation: Mutual Learning with Cross-Network Feature Rectification for Urban Segmentation. Applied Sciences 2025;15:1–22. https://doi.org/10.3390/APP151810000.

[49] Sharma A, Kumar R. Performance comparison and detailed study of AODV, DSDV, DSR, TORA and OLSR routing protocols in ad hoc networks. 2016 4th International Conference on Parallel, Distributed and Grid Computing, PDGC 2016 2016:732–6. https://doi.org/10.1109/PDGC.2016.7913218.

Symbols and parameters

$gradient_{trust}(i,j)$	Trust-based gradient from node i to j
$altitude_{trust}(i)$	Trust-based altitude of node i
$erosion_{trust}(i,j)$	Trust-based erosion of nodes along the path from i to j
$sediment_{trust}(i,j)$	Trust-based sediment added to node j's altitude
$carriedsediment_{trust}$	Sediment carried from node i to j based on trust
$\text{cost}_{trust}(\text{i},\text{j})$	Trust-integrated route cost function
TD_j	Time delay at node j
$N_{Hops}(i,j)$	Number of hops between node i and j
Min(E)	Minimum residual energy along the evaluated path
E_j	Residual energy at node j
$paramBlockedDrop$	Parameter indicating a blocked sediment drop (1 if blocked)
$\sigma, \mu, \tau, \varphi$	Cost-function weight parameters
T^{Drop}	Outcome per iteration
μ_G, σ_G^2	Mean and variance of trust-based gradients for SFD-MFD switching
θ	Threshold controlling transition between SFD and MFD
$\varepsilon_V, \varepsilon_U, \varepsilon_F$	Erosion constants for positive, negative, and flat gradients
ω, δ	Specific small values in Trust-based Probabilistic MFD mode equations
$V_k(i)$. $U_k(i)$, and $F_k(i)$	Set of neighbors with positive, negative and flat gradients
Sum	Sum of numerator weights of all neighbors
i, j, l, n	Node indices
$N(i)$	Set of neighbors of node i
T_{min}	Minimum trust among nodes on a route