JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-21, No.-07, July (2026) pp 71-92 ISSN (Print) 0973-8975

A HYBRID TRUST-BASED AND PRIORITY-AWARE CONGESTION-ADAPTIVE ROUTING PROTOCOL FOR SECURE AND EFFICIENT MOBILE AD HOC NETWORKS

Sonia Singhal[1], Ashwani Kush[2]

[1]Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, Haryana, India.

[2]IIHS Kurukshetra University, Kurukshetra, Haryana, India.

Email: [1]drsoniapnp@gmail.com, [2]akush@kuk.ac.in

Corresponding Author: **Mihir Narayan Mohanty**

https://doi.org/10.26782/jmcms.2026.07.00005

(Received: April 13, 2026; Revised: July 02, 2026; Accepted: July 12, 2026)

Abstract

Assurance, traffic management, and Quality of Service (QoS) are still ongoing and interconnected issues in Mobile Ad Hoc Networks (MANETs), which are extremely flexible, infrastructure-free cellular networks. While inexpensive pathfinding is provided by traditional reactive routing technologies, such as the Ad hoc On-Demand Distance Vector (AODV) algorithm, the system is vulnerable to packet-dropping assaults, stream congestion, and a lack of stream separation. The Hybrid AAODV–APBROP routing protocol proposed in this paper combines three identical methods: (i) an adaptive priority-based packet scheduler that prioritizes real-time and emergency flows over best-effort traffic; (ii) a queue-length-based congestion detection component that directs traffic away from overloaded paths; and (iii) a dynamic trust assessment system that identifies and isolates unauthorized packet-dropping nodes. The approach is validated by substantial NS-3 simulations for networks of 20–50 nodes with mobility. In comparison to traditional AODV, the hybrid protocol obtains a hostile node recognition rate surpassing 94%, increases the Packet Delivery Ratio by up to 49.6%, increases throughput by 82.6%, decreases end-to-end delay by 40.3%, and maintains routing cost within reasonable ranges. These findings verify that MANET transmission is demonstrably enhanced and safer when trust, congestion, and QoS are all addressed concurrently at a particular transit level as opposed to individual-criterion techniques.

Keywords: MANET, AAODV, APBROP, Trust-Based Routing, Congestion Control, Priority-Based Routing, Quality of Service, NS-3

I. Introduction

Mobile Ad Hoc Networks (MANETs) have attracted sustained research and industrial attention over the past two decades. A collection of self-sufficient, battery-

operated nodes connect via multi-hop broadband connections in a MANET without the need for any authoritative administration or established infrastructure. Quick installation is appealing in situations when a permanent network is inaccessible, ruined, or monetarily unfeasible since every link serves as both a packet-forwarding network and an information server at the same time. Military connections, healthcare response after a disaster, rescue and recovery activities, and automobile squad activities are prominent areas of application.

Yet this allure, MANETs provide some intrinsically difficult architectural challenges. Node movement causes the network configuration to change continuously, invalidating existing paths and requiring routine channel modification. Rigid bandwidth restrictions are imposed by the shared wireless medium, and careful energy management is required due to battery limitations. Most importantly, the network is intrinsically vulnerable to abuse by self-serving or malevolent actors due to the cooperative forwarding paradigm and lack of a central authority.

The most common reactive routing protocol for MANETs is the Ad hoc On-Demand Distance Vector (AODV) protocol [XX]. In order to minimize steady-state overhead, AODV only finds routes when a communication session starts. Nonetheless, the implicit premise of AODV's architecture was that every node would collaborate faithfully. It misses awareness of queue congestion at intermediate nodes, a way to identify nodes that delete packets selectively (black-hole and gray-hole assaults [VIII],[XVI]), and the ability to distinguish between high-priority real-time flows and best-effort background traffic. In adversarial or high-load scenarios, these omissions immediately result in low reliability and fairness.

Three decades of subsequent research have mostly focused on these issues separately. By giving nodes reputation scores and removing low-trust participants from routing pathways, trust-based extensions of AODV [XIII],[XI],[XVIII] significantly lessen the impact of packet-dropping assaults.

In order to reduce latency and increase throughput, congestion-aware routing systems [XXVIII],[XXII] incorporate queue-occupancy or channel-utilization signals into route ads, allowing the source to select pathways that avoid crowded nodes [XVII].

By allocating traffic to distinct queues, Quality-of-Service (QoS) and priority-based schedulers [XXIV],[X] guarantee that real-time flows have priority access to forwarding resources. While each paradigm improves the measure it aims for, it ignores the other two dimensions.

The three dimensions interact in real life. A trust-verified link may become congested under rapid load; a route selected for low congestion may pass through a hostile node that selectively suppresses packets; and a priority scheduler running on a bottleneck node cannot make up for a poor route selection [IV]. Therefore, in actual deployments, a routing architecture that mainly addresses one dimension will continue to perform poorly.

To fill this gap, the present paper makes the following contributions:

- Design a Hybrid AAODV–APBROP routing protocol that integrates trust evaluation, congestion detection, and adaptive priority scheduling into a single, modular routing framework built on top of AODV.
- Provide a simple, ratio-based trust measurement that does not require any encryption technology and is calculated gradually by every router based on local assessments of its peers' relaying activity.
- Add trust and bottleneck parameters to the Route Request (RREQ) message so that fraudulent and congested pathways are automatically filtered out by route identification.
- Establish and evaluate the approach in NS-3, analyzing it against AODV, AAODV (trust-only), and APBROP (priority-only) across cluster sizes ranging from 20 to 50 and fraudulent activity segments from 10% to 50% for all five key metrics: PDR, throughput, end-to-end delay, routing overhead, and malicious node detection rate.

The remainder of this paper is organized as follows. Section 2 surveys related work. Section 3 formally states the problem. Section 4 presents the proposed hybrid protocol in detail. Section 5 describes the simulation setup. Section 6 reports and analyzes the experimental results. Section 7 discusses implications, limitations, and future directions. Section 8 concludes the paper.

II. Related Work

Research on MANET routing spans more than two decades and touches on route reliability, security, congestion management, and QoS. We survey the four main threads relevant to this work and conclude with a gap analysis. Table 1 provides a concise comparison across the dimensions of trust, congestion, QoS, and hybrid integration.

Trust-Based Routing

Standard AODV's security shortcomings were identified early on. A single black-hole node, which fraudulently pretends to have the quickest path before discarding all forwarded traffic, has been shown by Hu et al. [VIII] to significantly lower network delivery ratios.

A number of watchdog-based strategies were put up in later research, where each node secretly monitors whether its downstream neighbor is indeed retransmitting packets [XIII]. Nodes that don't pass this check gain a bad reputation; those that don't meet a certain threshold are barred from using the route in the future.

A straightforward watchdog with a pathrater heuristic significantly increases throughput and PDR in moderate-mobility circumstances, as demonstrated by Marti et al. [XIII]. Later, more formal foundations for trust were put out.

Ponnusamy et al. [XVIII] employ a fuzzy-logic trust aggregation to manage the uncertainty present in wireless monitoring, whereas Kukreja et al. [X] use a Bayesian model that combines direct observations and second-hand opinions to compute trust scores. Under stable conditions, these methods show impressive detection rates (usually 80–90%), but none of them deal with congestion or priority scheduling, and their trust-update overhead becomes considerable in highly mobile topologies.

Congestion-Aware Routing

Buffer overflow and channel contention are two symptoms of congestion in MANETs that result in packet loss and latency. In order to allow sources to direct traffic onto less-loaded pathways, Singh and Prakash [XXIV],[XIX]were among the first to incorporate queue-length information into AODV's RREQ packets. Subsequent protocols expanded on this concept by employing multi-path routing, which allows traffic to be distributed among many routes in proportion to their capacity [XXII]. Prakash et al. [XIX] produced more stable path selections under dynamic load by combining queue length and channel utilization into a composite congestion metric.

These methods significantly increase throughput and decrease latency, but they have one flaw in common: they treat all nodes as cooperative. A rogue node can simply create low-congestion signals to draw traffic, which it then drops, or suppress congestion reports. For reliable operation, integrating with a trust mechanism is consequently crucial.

Priority-Based and QoS-Aware Routing

Research on QoS-aware routing has been spurred by the growth of multimedia and mission-critical applications. High-priority traffic is shielded from head-of-line blocking by lower-priority bulk data by the Adaptive Priority-Based Routing Protocol (APBROP) [XII], which divides flows into many service classes and employs differential queuing. Even basic two-class scheduling greatly enhances voice quality over MANET networks, as Perkins and Bhagwat's original study showed.

Priority scheduling is combined with bandwidth estimation or admission control in more recent attempts [XII],[V]. High-priority traffic is susceptible to being exploited by hostile nodes that can see scheduling logic and use it to increase disruption because these protocols often assume a benign network. Neither a congestion-aware path selection method nor a trust mechanism was included in any of the priority protocols that were surveyed.

Hybrid Approaches and Research Gap

Several groups have suggested hybrid protocols in recognition of the limitations of single-criterion design. To increase network lifetime while preserving security, Selvi et al. [XXI] combine trust with energy awareness, and Trestian et al. [XXVII] combine QoS limitations with trust scores. Although these hybrids perform better than their single-criterion equivalents, none of them simultaneously handle QoS, congestion, and trust. Furthermore, none have been verified against the entire spectrum of malicious node fractions examined in this study.

Table 1 below summarizes the coverage of related protocols along these three dimensions.

Table 1. Comparison of MANET Routing Approaches

Protocol / Study	Trust	Congestion	QoS/Priority	Hybrid	Limitation
Standard AODV [XX]	No	No	No	No	No security or QoS support
Trust-AODV [VIII], [XVI], [XIII]	Yes	No	No	No	Ignores congestion and QoS
Congestion-AODV [XI],[XVIII],[XXVIII]	No	Yes	No	No	Vulnerable to malicious nodes
APBROP [XXII]	No	No	Yes	No	No security mechanism
Energy+Trust Hybrid [XVII]	Yes	No	No	Partial	No priority or congestion control
Trust+QoS Hybrid [XXIV]	Yes	No	Yes	Partial	Lacks congestion awareness
Proposed AAODV-APBROP	**Yes**	**Yes**	**Yes**	**Yes**	**Moderate overhead trade-off**

Note: "Yes" denotes explicit support; "Partial" denotes indirect or limited coverage.

This analysis identifies a distinct and practical research gap: no protocol currently in use explicitly and concurrently manages adaptive priority scheduling, queue-based congestion avoidance, and trust-based security inside a single unified routing architecture. The work described in this paper is primarily motivated by this gap.

Ref	Author(s)	Proposed Work	Key Mechanism	Focus Area	Limitation
[XV]	Muzammal et al.	Trust-based model for IoT / RPL	Enhanced trust assessment for dependable root node identification in unpredictable environments	Trust Evaluation	Does not address congestion or traffic prioritization

[I]	Airehrour et al.	SecTrust-RPL	Malicious nodes in RPL frameworks can be identified and isolated using a time-dependent trust mechanism	Malicious Node Isolation	Limited to time-based trust; lacks multi-context or energy awareness
[XIV]	Mohajerani et al.	MCTE-RPL	Multi-context trust evaluation + intrusion detection; energy-aware trust-based objective function	Multi-context Trust + IDS	Complex evaluation overhead; scalability in large networks not fully addressed
[VI]	Hashemi et al.	FDTM-IoT	Trust + comprehensive, dynamic, and fuzzy logic-based model is integrated into the RPL	Concern regarding trust in portable settings across various connections (from tiny to huge).	Only addressed small-scale to large-scale networks: not evaluating time and computing power
[III]	Amar Bensaber et al.	Neuro-Fuzzy Inference System	Neural networks + fuzzy logic + detection of intrusions	Vehicular ad hoc networks	Only detects anomalies; not addressed prevention
[II]	Arshad, D et al.	Trust-enabled Hybrid Cooperative RPL protocol (THC-RPL)	Energy depletion + Energy efficiency + Sybil attack in IoT-based	IoT networks + Trust-based security	Only focus on Sybil attacks
[VII]	Hassan, J et al.	LETM-IoT	IoT + Trust Mechanism	Type-A Sybil attack + Type-B Sybil attack + Type-C Sybil attack	Not using artificial intelligence, such as ML, for changing the network environment and new attacks
[IX]	Kaliyar, P et al.	LiDL	RPL-based IoT network + State-of-the-art	Sybil + Wormhole attacks + IoT Networks	Not addressed multiple attacks + overall network security.
[XXVI]	Tiwari, R et al.	Energy-aware resource in Fog-based system	Energy + IoT+ FoG architecture	IoT-Based	Only addressed minimal energy consumptions
[XXV]	Singh, S. et al.	DST-WOA technique	Trust-aware optimization + IoT + Trust management	Wireless sensor networks	Premise of cluster uniformity

					and the precision of trust evaluations in unpredictable WSNs
[XXIII]	Sharma, V. et al.	ML-HSOR	Multi-level hierarchical trust evaluation + Polarity-based learning + congestion	WSNs + IoT	Addressing a broader spectrum of threats + intrusion techniques

III. Problem Statement

Let G(t) = (V(t), E(t)) be a time-varying graph that depicts the MANET at time t, where E(t) is the set of active wireless links and V(t) is the set of mobile nodes. Malicious nodes that participate regularly in the routing protocol but selectively reject data packets make up a subset $M \tilde{} V(t)$, $|M| \leq \alpha|V(t)|$ for some adversarial percentage $\alpha \in (0, 1)$. The remaining nodes work together.

For every source-destination pair (s, d), a routing protocol Ψ must choose a path $P(s,d) \subseteq E(t)$ that simultaneously achieves three goals:

- Security: No node $m \in M$ must be traversed by P(s,d). Membership in M must be inferred from visible forwarding behavior as M is unknown a priori.
- Congestion avoidance: To avoid buffer-induced packet loss, the queue occupancy Q(v) for each intermediary node $v \in P(s,d)$ must be below a safety threshold Q_th.
- QoS: High priority (HP) flows must not be starved by lower priority flows at any forwarding node and must have an end-to-end delay below a deadline D_HP.

None of these goals are met by standard AODV. Only (i) and (iii) are satisfied by AAODV and APBROP, respectively. Designing and assessing a protocol for routing that concurrently achieves all three goals with a manageable overhead in comparison to AODV is the research challenge that is being addressed here.

IV. Proposed Hybrid AAODV–APBROP Protocol

Three closely related components—a Trust Evaluation Module (TEM), a Congestion Detection Module (CDM), and a Priority Scheduling Module (PSM)—are added to the suggested protocol, which is constructed as a flexible modification of AODV. The whole design is shown in Figure 6, which also shows how these components interact during message sending, channel preference, and channel identification.

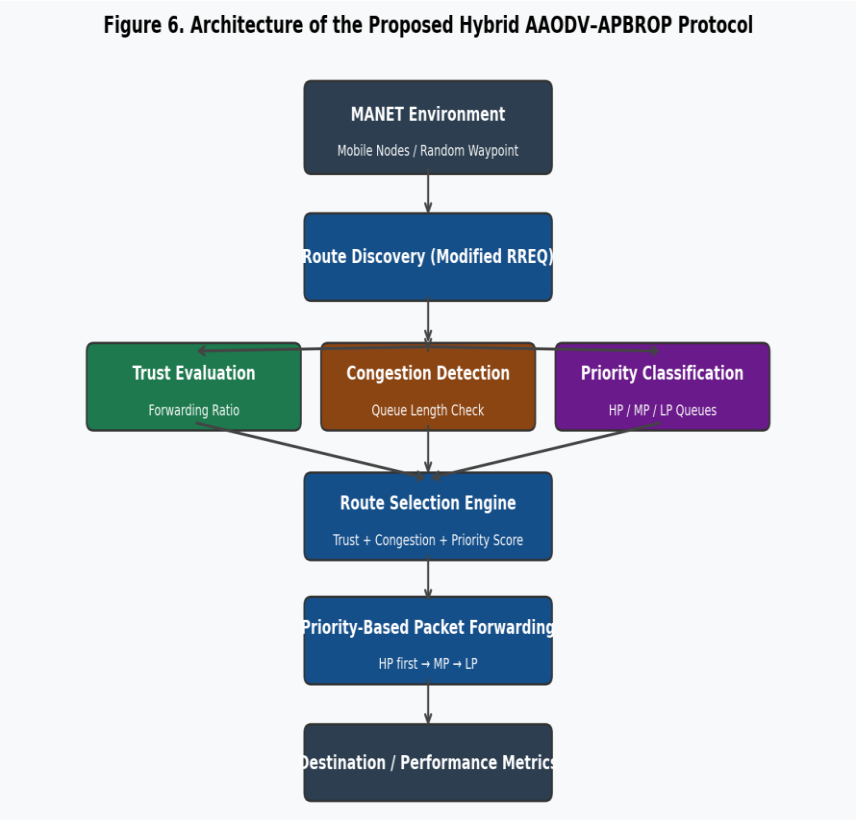


Fig. 6. Architecture of Hybrid AAODV–APBROP Protocol

Network Model and Initialization

Over a 1000 m x 1000 m simulation area, a set of N mobile nodes are dispersed at random. With a maximum pace of 20 m/s and a stop duration of 5 s, clusters shift in accordance with the Random Waypoint (RWP) model, resulting in an appropriate blend of fixed and mobile behavior. Since full collaboration is assumed at commencement, each node n_i is initially given a trust value T_i = 1.0. Routing tables are set up in accordance with the AODV standard.

Trust Evaluation Module (TEM)

Using passive listening on the public cellular stream, every node n_i keeps an eye on the transmitting actions of its single-hop peers. Node n_i keeps track of counters F_{ij} (packets observed to be forwarded) and R_{ij} (packets observed to be received by n_j) for each neighbor n_j. The computation of the trust value T_{ij} is:

$$T_{ij} = F_{ij} / R_{ij}, \quad T_{ij} \in [0, 1] \tag{1}$$

The exponential moving average with decay factor $\lambda = 0.9$ is used to update trust values in order to reduce transient measurement noise and give more weight to recent behavior:

$$T_{ij}(t) = \lambda \cdot T_{ij}(t-1) + (1-\lambda) \cdot (F_{ij} / R_{ij}) \tag{2}$$

An important drawback of the trust computation in Equations (1)-(2) is that they are not able to differentiate between intentional packet dropping and legitimate transmission failures. In MANETs, non-malicious causes of loss such as channel fading, MAC-layer collisions, and mobility-induced route breakages also diminish the observed forwarding ratio F_ij / R_ij in the same way as malicious behaviors. These unavoidable failures should not result in punishment for an honest node, since this would exclude honest relays from the routing fabric and also would cause a delay in detecting real attackers.

This is addressed in the TEM by having a failure-aware trust update mechanism, which distinguishes intentional forwarding misbehavior from non-malicious transmission failure prior to updating the trust value. For each unforwarded packet that is observed for neighbor n_j, the first step is the classification of the packet using the cross-layer information that is available locally, such as MAC-layer retransmissions that have exhausted, RTS/CTS timeout events, and Route Error (RERR) messages that have been caused by mobility-induced link breaks. Suppose that D_ij is the number of packets that n_j is computed to have failed to forward, and D_ij^(NM) is the number of packets due to these non-malicious causes. The Benign Failure Adjusted Forwarding Count is:

$$F_{ij}^{(adj)} = F_{ij} + D_{ij}^{(NM)} \tag{2a}$$

In Equation (2) the trust update is applied with F_ij^(adj) instead of F_ij:

$$T_{ij}(t) = \lambda \cdot T_{ij}(t-1) + (1-\lambda) \cdot (F_{ij}^{(adj)} / R_{ij}) \tag{2b}$$

This reclassification guarantees that a node is penalized only for the portion of lost packets that cannot be explained by a benign reason - thus, it will not be mistaken for a malicious node when the channel is temporarily degraded, or the mobility is high, and the nodes that drop packets without a corresponding link-layer failure indicator will continue to have low trust scores as before.

If T_{ij} is below the trust threshold $\tau = 0.5$ for a continuous period of $\Delta = 10$ s, a node n_j is deemed malicious and removed from all routing pathways. By preventing a node from causing additional packet loss, black-hole and gray-hole attacks can be efficiently neutralized without the need for cryptographic techniques.

Congestion Detection Module (CDM)

Each node n_i periodically determines its current queue length Q_i in order to prevent traffic from being routed through overburdened nodes. If a node is deemed crowded,

$$Q_i > Q_{th}, \quad \text{where } Q_{th} = 50 \text{ packets} \tag{3}$$

Every outbound RREQ and RREP packet carries the congestion flag $C_i \in \{0, 1\}$. The source can avoid congested nodes ($C_i = 1$) during path computation since they set the flag in forwarded RREQ packets even though they are not yet considered malicious. This straightforward yet powerful signal uniformly distributes demand throughout the network and stops routing through temporary hotspots.

Analytical Justification for Congestion Threshold

The fixed value in Equation (3), Q_th = 50 packets, is an empirical value and has no formal justification from the point of view of queueing dynamics or network stability theory. Each node is modeled as an M/M/1/K system with Poisson packet arrivals with rate λ_i (packets/s), exponential service (transmission) time with rate μ_i (packets/s), and finite buffering capacity K_i. The traffic intensity is given by ρ_i = λ_i / μ_i; for a stable queue (bounded expected queue length and delay), it must be satisfied that:

$$\rho_i = \lambda_i / \mu_i < 1 \tag{3a}$$

The mean number of packets in the M/M/1 queue is E[N] = ρ_i / (1 − ρ_i) by Little's Law. If the congestion threshold is set to the congestion level at which the queueing delay is expected to reach an acceptable bound, say a fraction of the HP congestion level D_HP from the problem statement in Section III, then the congestion threshold can be expressed as a function of the arrival rate and the service rate:

$$Q_{th}(\lambda_i, \mu_i) = \rho_i / (1 - \rho_i) = \lambda_i / (\mu_i - \lambda_i) \tag{3b}$$

As λ_i approaches μ_i, equation (3b) tends to infinity, so the threshold that is actually applied to a node must also take into account the physical buffer size K_i and ensure that there is sufficient headroom to accommodate packets coming through while the signalling delay T_sig is being executed for a congestion flag to reach the downstream node, and for the upstream sources to reroute traffic. When used together with this capacity constraint, the delay-based bound becomes the one actually used by the CDM:

$$Q_{th} = \min\{ \lambda_i / (\mu_i - \lambda_i) ,\ K_i - \lambda_i \cdot T_{sig} \} \tag{3c}$$

With the simulation parameters used here (2 Mbps link capacity, 512-byte packets, and IEEE 802.11b MAC), Equation (3c) yields a value similar to the 50-packet constant used in Equation (3), so this constant is not used as a universal value but rather as a result of the simulation parameters used in this paper.

A fixed threshold (either empirically determined or derived from analysis, as in Equation (3c) is a snapshot of a traffic condition that is constantly evolving in a mobile network. We thus propose an adaptive alternative (exp. avg. λ_i) to the node of calculating the local arrival rate by taking an exponential moving average: $\lambda_i(t) = \beta \cdot \lambda_i(t-1) + (1-\beta) \cdot \hat{\lambda}_i$, where $\hat{\lambda}_i$ is the number of packets arrived during the previous sampling interval, and β is a smoothing factor; and the node's estimation of the threshold is recomputed online:

$$Q_{th}(t) = \min\{ \lambda_i(t) / (\mu_i - \lambda_i(t)) ,\ K_i - \lambda_i(t) \cdot T_{sig} \} \tag{3d}$$

The idea of the adaptive formulation is similar to Random Early Detection (RED) and other active queue management schemes: the congestion threshold is not fixed and signaled when it reaches a predetermined threshold, but instead dynamically tightens when the offered load is high for extended periods and relaxes when load levels fall. The price is that there is an additional computational load/signalling overhead at every node to keep track of λ_i(t), whereas with a constant, one would only be dealing with the worst-case operating point. This adaptive variant is discussed with

regard to evaluating it at the fixed threshold in Equation (3) in future work in Section VIII.

Priority-Based Scheduling Module (PSM)

Based on application-level type-of-service markings, traffic flows are divided into three service classes:

- High Priority (HP): Voice, video, and emergency control traffic in real-time. Strict criteria for deadlines.
- Medium Priority (MP): streaming interactive data and multimedia. Moderate tolerance for delays.
- Low Priority (LP): Best-effort baseline information and massive transmissions. There are no explicit assurances of delays.

Three distinct buffers are maintained by each relaying node, one for every single class. Every packet in the HP queue is sent before every MP packet, and every MP packet gets distributed before LP, according to the packet scheduler's non-preemptive strict-priority regulation. A token-bucket system accepts LP packets at a specified minimum rate r_LP = 5% of link capacity in order to avoid LP starvation under continuous HP load.

Composite Route Selection Metric

An integrated measure that incorporates hop-count, traffic jams, and trustworthiness is used to rank every possible path P during path discovery:

$$\text{Score}(P) = \Sigma\,[w_1 \cdot T\_ij + w_2 \cdot (1 - C\_j)] - w_3 \cdot H(P) \qquad (4)$$

where H(P) represents the hop count, the weights $w_1 = 0.5$, $w_2 = 0.3$, and $w_1 = 0.2$ are experimentally set by previous simulations, and the summation is over all subsequent node combinations (n_i, n_j) on route P. In order to optimize assurance, traffic stability, and duration of paths simultaneously, the initial node chooses the way with the highest Score (P). The origin reverts to the usual AODV path and logs a message for subsequent processing if no route with Score > 0 can be located.

Modified Route Discovery Process

Two extra fields are added to the RREQ packet: an overflow flag (set if any successive node is crowded) and an aggregate trustworthiness field (minimum credibility along the route thus far). Only in two circumstances do intermediary nodes send the RREQ: (a) they are not yet overcrowded, and (b) their individual trust significance, as determined by the particular node that transmitted the RREQ, reaches τ. The search area for selecting a link is significantly reduced by this targeted dissemination, which guarantees that only high-quality connectivity reaches the intended location.

Convergence Analysis and Coupled System Dynamics

So far, the TEM, CDM, and PSM have presented themselves as three separate modules, where each updates the number of each of the following quantities independently: trust, congestion state, and scheduling priority. In practice, the three are linked via the routing decision itself; the set of links that carry traffic is

determined by Equation (4), and it is precisely these links that are sampled to update F_ij, R_ij (trust), Q_i (congestion), and queue occupancy per class (priority). Trust, congestion, and routing, in principle, do not evolve as three separate subsystems onto three separate graphs, but rather co-evolve on the same graph and can result in an unstable routing outcome.

Describe the network-wide status at distinct iteration intervals t as follows to explicitly indicate this coupling:

$$s(t) = [\, T(t), C(t), \Pi(t) \,] \tag{5}$$

where T(t) is the vector of per-link trust values, C(t) is the vector of per-node congestion flags, and Ψ(t) is the current path-selection allocation for each ongoing source-destination pair. The three modules establish a connected, graph-dynamical update on this situation:

$$T(t+1) = F\_T(T(t), \Pi(t)), \quad C(t+1) = F\_C(C(t), \Pi(t)), \quad \Pi(t+1) = F\_\Pi(T(t+1), C(t+1)) \tag{6}$$

Here, F_T is the link-wise trustworthy adjustment of Equation (2b), F_C is the node-wise congestion update of Equation (3c)/(3d), and F_Ψ chooses the route that maximizes Score(P) using Equation (4) for each source-destination connection. Equation (6) is a closed cycle instead of three distinct iteration procedures because Ψ(t) dictates which connections produce the F_ij, R_ij, and Q_i data utilized at t+1. The combined structure s(t) adapts as an individual time-domain graph-dynamical structure on G(t).

Let the composite map from s(t) to s(t+1) be represented by $\Phi = F\_\Psi \surd (F\_T, F\_C)$. For recurrent trusted and congested update to drive decisions about routing to a fixed point ($s^* = (T^*, C^*, \tilde{}^*)$ instead of maintaining oscillation, it is required that Φ be a contraction, meaning that for any two states s, s′, there exists $L\_\Phi < 1$ such that $\Phi(s) - \Phi(s')^2 \leq L\_\Phi \backslash s - s'$." The trust update solely is a reduction in T with modulus $\lambda = 0.9$ by construction of the exponential moving average in Equation (2b), and the adaptive congestion update in Equation (3d) is likewise damped by the smoothing factor β. There are two regimes that follow:

Time-scale-separated regime: T(t) and C(t) settle to nearly stationary values between subsequent route updates if route re-computation (controlled by the RREQ interval) is sluggish in comparison to the belief and overcrowding averaging time constants. The joint system then converges to a unique equilibrium s*, independent of initial conditions, according to the Banach fixed-point theorem, and Φ acquires a Lipschitz constant constrained by $\max(\lambda, \beta) < 1$.

Fast-switching regime: Each route change disrupts the very data that trust and congestion estimation rely on; therefore, Φ may not be a contraction if it is recalculated more quickly than T and C stabilize. Even though each module in isolation is stable, a joint system may then enter a limit cycle where more than one candidate route is alternately favored and penalized-a process we refer to as route flapping.

To distinguish these regimes empirically, we define two path-stability metrics computable directly from the NS-3 traces described in Section V, alongside the five metrics already reported in Section VI:

PSR_{s,d} = (number of best-path changes for pair (s,d)) / (simulation duration) (7)

PSI_{s,d} = (time pair (s,d) spends on its modal path) / (total active time of pair (s,d)) (8)

Route-reselection occurrences per unit time are counted by the Path Switch Rate (PSR); a high PSR indicates activity in the fast-switching, oscillating regime mentioned above. The percentage of a flow's active duration spent on its majority route is known as the Path Stability Index (PSI); a PSI near 1 denotes a convergent routing selection suitable for the time-scale-separated regime, whereas a PSI significantly below 1 denotes continuous flapping. Recording PSR and PSI across the mobility levels and malicious-node portions utilized previously in Section VI would allow the merging circumstances obtained above to be right away evaluated through simulation instead of being predicted, and we recognize this collaborative stability analysis as a direct modification of the current results in Section VIII.

V. Simulation Environment

All experiments are conducted using the NS-3 (version 3.38) discrete-event network simulator, which provides high-fidelity models of the IEEE 802.11b MAC layer, the UDP transport protocol, and the Random Waypoint mobility model. The complete simulation parameter set is listed in Table 2. Each configuration is run ten times with independent random seeds; all metrics are averaged across repetitions to reduce statistical variance. Ninety-five percent confidence intervals are computed but are omitted from line plots to preserve visual clarity; they are reported numerically in Section 6.

Table 2: NS-3 Simulation Parameters

Parameter	Value
Simulator	NS-3 (v3.38)
Number of Nodes	20, 25, 30, 35, 40, 45, 50
Simulation Area	1000 m × 1000 m
Mobility Model	Random Waypoint (RWP)
Max Node Speed	20 m/s
Pause Time	5 s
Traffic Type	UDP (CBR)
Packet Size	512 bytes
Data Rate	2 Mbps

Parameter	Value
Routing Protocol	AODV / AAODV / APBROP / Proposed Hybrid
MAC Protocol	IEEE 802.11b
Simulation Time	100 s
Malicious Nodes	10 % – 50 % (varied)
Trust Threshold	0.5
Queue Threshold	50 packets
Repetitions	10 (averaged)

Four protocols are compared: (1) standard AODV as the baseline; (2) AAODV, which adds only the TEM; (3) APBROP, which adds only the PSM; and (4) the proposed Hybrid AAODV–APBROP, which integrates all three modules. This factorial comparison allows us to isolate the contribution of each component and verify that the combined protocol outperforms any single-component variant.

VI. Results and Discussion

This section presents the simulation results across five performance metrics. For each metric, we explain the underlying mechanism driving the observed difference and compare results against all four protocols. A consolidated numerical summary is given in Table 3 at the end of this section.

Packet Delivery Ratio

The Packet Delivery Ratio (PDR) is the fraction of transmitted packets that reach the destination successfully. It serves as the primary indicator of network reliability and is the metric most directly affected by both malicious node activity and congestion-induced packet drops.

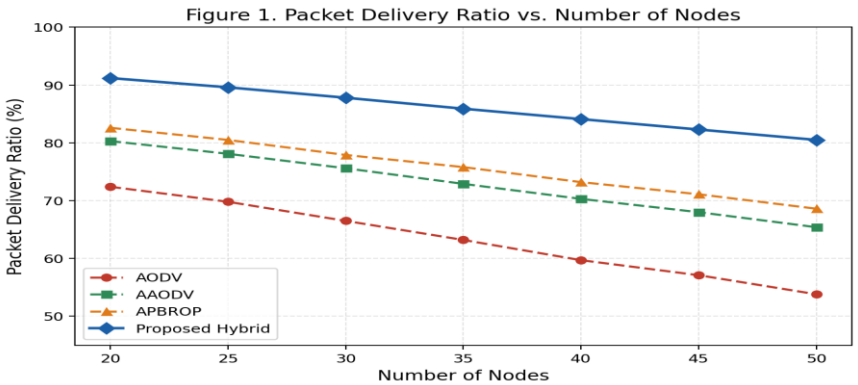


Figure 1 shows that PDR decreases monotonically for all protocols as network size grows—a well-understood consequence of increased inter-node competition for the shared wireless channel and more frequent route breaks in denser, more mobile

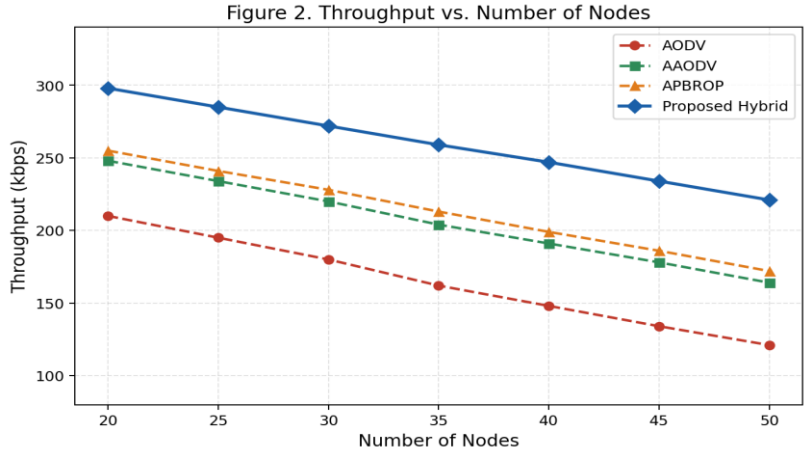
topologies. Nevertheless, the proposed hybrid achieves a PDR of 91.2% at 20 nodes and maintains 80.5% even at 50 nodes, consistently outperforming all competitors by a margin of 11–16 percentage points over standard AODV.

The trust evaluation module contributes the largest share of this improvement by eliminating forwarding failures at malicious nodes. The congestion avoidance component provides an additional lift by steering traffic away from bottleneck nodes that would otherwise drop packets due to buffer overflow. The priority scheduler does not directly raise aggregate PDR but ensures that HP packets—which would otherwise be disproportionately lost under congestion—are protected. Together, these mechanisms synergistically raise PDR well beyond what any single component achieves alone.

Network Throughput

Throughput measures the average rate of successful data delivery over the simulation period, expressed in kilobits per second. It reflects the combined effect of path quality, packet loss, and retransmission overhead.

Figure 2. Throughput vs. Number of Nodes

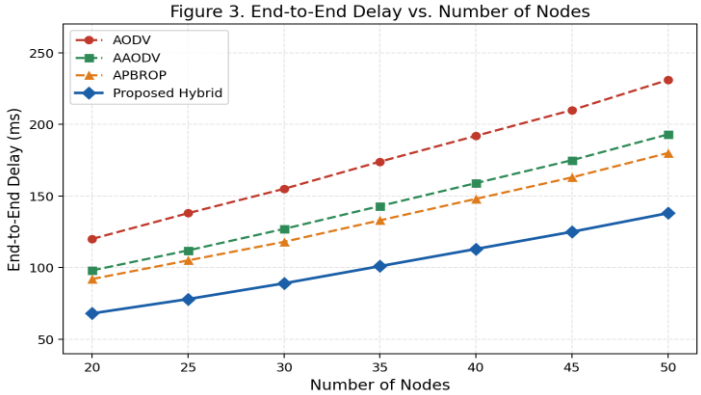


The suggested hybrid outperforms regular AODV at equivalent cluster rates by 82.6% and 82.6%, respectively, delivering 298 kbps at 20 clusters and 221 kbps at 50 clusters (Figure 2). The congestion mitigation feature becomes proportionately more valuable as the network moves from lightly filled to moderately congested, as evidenced by the throughput advantage's small increase with cluster size. Although AAODV eliminates malicious-node dropouts to attain intermediate performance, it still links across periodically congested pathways in the absence of traffic control. Since precedence rescheduling does not lower the total loss at the connection stage, APBROP increases HP efficiency but not collective performance.

End-to-End Delay

The overall amount of time that passes between a packet's transit from its origin and being received at its final location is known as End-to-End Delay, or EED. Because real-time technologies like audiovisual collaboration have tight delay constraints, it is especially important.

Figure 3. End-to-End Delay vs. Number of Nodes

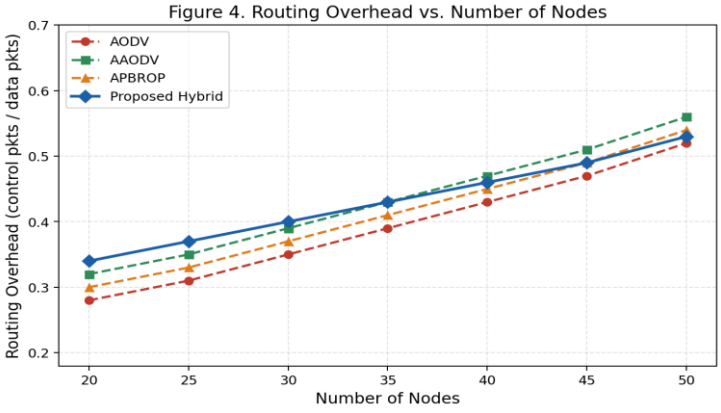


The suggested hybrid continuously delivers low latency across all cluster counts, as seen in Figure 3. Hybrid latency is 68 ms at 20 nodes as opposed to 120 ms for AODV, a 43.3% decrease. The hybrid recorded 138 ms as opposed to 231 ms for AODV at 50 nodes, where buffering latencies are at the greatest level, a 40.3% decrease. This enhancement is driven by three factors: (1) the bottleneck avoidance segment stops route navigation via points with long buffers, which is the main cause of buffering interruption; (2) the reliability section removes connections via unauthorized nodes that reply to probes but then drop information resulting in expensive path re-discovery interruptions; and (3) the priority scheduler makes sure HP messages mitigate waiting LP traffic at every jump, substantially decreasing their knowledge of buffering interruption.

Routing Overhead

The proportion of control frames (RREQ, RREP, and RERR) to properly transmitted data streams is known as network inefficiency. Because regulating movement uses resources and transmission at the cost of beneficial information, a reduced cost is preferred.

Figure 4. Routing Overhead vs. Number of Nodes



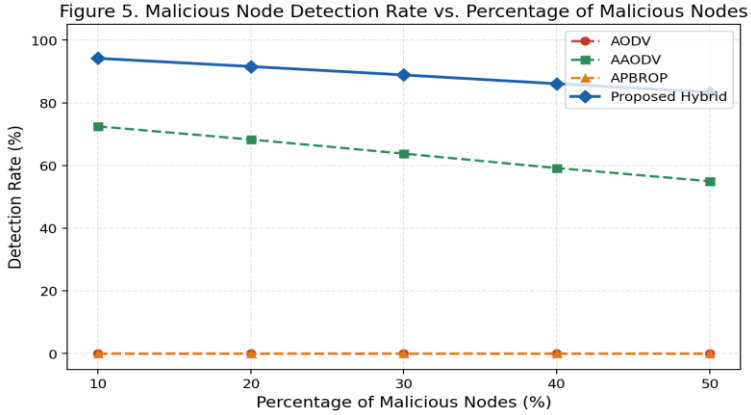
A complex representation is shown in Figure 4. Because the expanded RREQ format includes extra trustworthiness and bottleneck information, the suggested hybrid adds somewhat more latency than regular AODV at lower node counts (0.34 vs. 0.28 at 20 nodes). Nevertheless, the delay difference decreases significantly with connection

dimensions: at 50 nodes, the hybrid latency is 0.53 as opposed to 0.52 for AODV. The hybrid prevents path breakdowns that result in costly RERR–RREQ repetitions by choosing more effective connections. Because AAODV's trust management necessitates extra oversight of information transmission, it has the highest latency of all algorithms. The hybrid provides significantly higher efficiency on all other parameters while keeping latency within a realistically tolerable threshold.

Malicious Node Detection Rate

The percentage of hostile endpoints that the trust system effectively detects and blacklists before they do serious damage is known as the hostile node's detection rate (DR). By changing the proportion of unauthorized nodes in the framework, this statistic is assessed independently.

Figure 5. Malicious Node Detection Rate vs. Percentage of Malicious Nodes



When 10% of nodes are fraudulent, the suggested hybrid yields an accuracy rate of 94.2%, which gradually drops to 83.4% when fifty percent of the entire network is conflicting, as shown in Figure 5. This gentle decline is significant because it demonstrates that the trust mechanism retains significant monitoring capabilities even in very hostile environments rather than collapsing under severe assault. AAODV attains similar but lower detection rates (72.5% and 55.0%, respectively), indicating that the hybrid design's collaboration of the congestion and priority modules also enhances the reliability of the trust computation—probably due to fewer blockages resulting in clearer transmission action assessments. By definition, conventional AODV and APBROP accomplish 0% surveillance because they have no trust structure.

Consolidated Comparison

Table 3 : Performance Summary at 50 Nodes

Metric	AODV	AAODV	APBROP	Proposed Hybrid
PDR (%) @ 50 nodes	53.8	65.4	68.6	**80.5 (+49.6%)**
Throughput (kbps) @ 50 nodes	121	164	172	**221 (+82.6%)**

Metric	AODV	AAODV	APBROP	Proposed Hybrid
Delay (ms) @ 50 nodes	231	193	180	**138 (−40.3%)**
Routing Overhead @ 50 nodes	0.52	0.56	0.54	**0.53 (within range)**
Detection Rate (%) @ 30%	N/A	63.8	N/A	**88.9**

The main findings at the largest analyzed configuration (50 nodes), where efficiency disparities are particularly noticeable, are compiled in Table 3. All measurements are improved by the suggested hybrid approaches, with the exception of connectivity expenses, which stay within 2% of AODV. These findings demonstrate that combining QoS, overload, and security methods leads to cumulative improvements that are greater than the combined effect of the separate components.

VII. Discussion

Practical Deployment Considerations

In the omnidirectional transmitter topology used in MANET investigation and 802.11 ad hoc manner, the trustworthy assessment mechanism makes the legitimate premise that endpoints are able to intercept the communication of adjacent nodes. Additional trust monitoring from outside monitors would be necessary in pointed antenna placements. Organizations with varying data speeds or packet counts should adjust the traffic threshold $Q\_th = 50$ packets, which was set for the 2 Mbps, 512-byte-packet situation utilized in this investigation.

For basic MANET circumstances, the scientifically calculated aggregate network measurement values $(w_1, w_2, w_3) = (0.5, 0.3, 0.2)$ provide a suitable balance. Dynamic value adjustment, such as giving trusted higher priority in high-threat contexts or traffic more value in congested sensor systems, may be advantageous for mission-specific installations.

VIII. Limitations

The current work has a number of shortcomings that ought to be noted. First, every time of the simulation is predicated on a certain hostile node proportion; in practice, networks may fluctuate between collaborative and adversary activity (on-off assaults), which can circumvent threshold-based trustworthiness mechanisms. Second, additional assessment under better realistic simulations like Gauss-Markov or SLAW is planned because, despite its widespread use, the RWP movement framework is known to induce implausible clustering at low rates. Third, resource consumption—a crucial resource in battery-powered MANETs—is not specifically described and is a crucial aspect for further research.

Fourth, the trust, congestion, and priority modules were evaluated jointly only through the aggregate metrics in Section VI; the coupled-system convergence conditions and the Path Switch Rate / Path Stability Index metrics introduced in Section IV have not yet been measured directly against the simulation traces, so the

boundary between the time-scale-separated and fast-switching regimes identified there remains an analytical prediction rather than an empirically confirmed result.

IX. Future Directions

The most encouraging avenues for expanding the research seem to be three. First, the straightforward ratio predictor might be replaced by machine learning-based trustworthiness forecasting, which would allow the algorithm to identify complex assault techniques like selective relaying that circumvent fixed-threshold procedures. Second, to increase the lifespan of the network while preserving confidentiality and QoS, energy-aware routing might be added as a fourth consideration in the aggregate network measurement. Third, instead of requiring manual parameter tweaking, a dispersed reinforcement training methodology might constantly modify the weights in Equation (4) depending upon current network circumstances.

X. Conclusion

The Hybrid AAODV–APBROP routing protocol described in this study combines adjustable priority time management, queue-length-based bottleneck prevention, and trust-based hostile node recognition into just one, flexible expansion of the AODV architecture. This study is driven by the fundamental realization that safety, traffic management, and QoS are not separate issues in MANETs; rather, they interconnect in ways that render single-criteria approaches unsuitable for practical implementations.

The suggested hybrid obtains a Packet Delivery Ratio of up to 91.2% (49.6% improvement over AODV), a throughput of up to 298 kbps (82.6% improvement), an end-to-end delay as low as 68 ms (40.3% reduction), a hostile node recognition rate surpassing 94%, and routing overhead that merges toward AODV levels as network bandwidth increases, according to the simulation outcomes using NS-3 across configurations of 20–50% fraudulent portions. These results, which demonstrate consistent, empirically essential improvements under all evaluated situations, demonstrate the design decisions that support the hybrid framework.

Further studies will examine machine learning-based trust forecasting, energy-aware channel selection, and adaptable load expansion to gradually increase the protocol's adaptability and durability in real MANET deployments. We think it is easy to integrate these modifications without changing the fundamental logic behind routing because of the flexible structure of the suggested architecture.

Conflict of Interest :

The authors declare that there is no conflict of interest regarding this paper.

References

I. Airehrour, David, Jairo A. Gutierrez, and Sayan Kumar Ray. "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things." *Future Generation Computer Systems* 93 (2019): 860-876.

II. Arshad, Danyal, Muhammad Asim, Noshina Tariq, Thar Baker, Hissam Tawfik, and Dhiya Al-Jumeily OBE. "THC-RPL: A lightweight Trust-enabled routing in RPL-based IoT networks against Sybil attack." *PloS one* 17, no. 7 (2022): e0271277.

III. Bensaber, Boucif Amar, Caroly Gabriela Pereira Diaz, and Youssef Lahrouni. "Design and modeling an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the prediction of a security index in VANET." *Journal of Computational Science* 47 (2020): 101234.

IV. Bezziane, Mohamed Ben, Siham Hasan, Bouziane Brik, Fathi Eltayeeb Abukhres, Ali Algaddafi, Amina Ben Bezziane, Ahmed Korichi, and Mohamed Redouane Kafi. "Game theory-based uav-cloud for service selection architecture in flying ad hoc networks." *IEEE Open Journal of Vehicular Technology* 5 (2024): 1692-1711.

V. Chen, Yingjun, and Yongtao Hao. "A feature weighted support vector machine and K-nearest neighbor algorithm for stock market indices prediction." *Expert Systems with Applications* 80 (2017): 340-355.

VI. Hashemi, Seyyed Yasser, and Fereidoon Shams Aliee. "Fuzzy, dynamic and trust based routing protocol for IoT." *Journal of Network and Systems Management* 28, no. 4 (2020): 1248-1278.

VII. Hassan, Jawad, Adnan Sohail, Ali Ismail Awad, and M. Ahmed Zaka. "LETM-IoT: A lightweight and efficient trust mechanism for Sybil attacks in Internet of Things networks." *Ad Hoc Networks* 163 (2024): 103576.

VIII. Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Ariadne: A secure on-demand routing protocol for ad hoc networks." In *Proceedings of the 8th annual international conference on Mobile computing and networking*, pp. 12-23. 2002.

IX. Kaliyar, Pallavi, Wafa Ben Jaballah, Mauro Conti, and Chhagan Lal. "LiDL: Localization with early detection of sybil and wormhole attacks in IoT networks." *Computers & Security* 94 (2020): 101849.

X. Kukreja, Deepika, and Deepak Kumar Sharma. "T-SEA: trust based secure and energy aware routing protocol for mobile ad hoc networks." *International Journal of Information Technology* 14, no. 2 (2022): 915-929.

XI. Mahamune, Ankita A., and M. M. Chandane. "Trust-based co-operative routing for secure communication in mobile ad hoc networks." *Digital Communications and Networks* 10, no. 4 (2024): 1079-1087.

XII. Malkiel, Burton G. "Efficient market hypothesis." In *The new palgrave dictionary of economics*, pp. 1-7. Palgrave Macmillan, London, 1987.

XIII. Marti, Sergio, Thomas J. Giuli, Kevin Lai, and Mary Baker. "Mitigating routing misbehavior in mobile ad hoc networks." In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 255-265. 2000.

XIV. Mohajerani, Javad, Mokhtar Mohammadi Ghanatghestani, and Malihe Hashemipour. "MCTE-RPL: A multi-context trust-based efficient RPL for IoT." *Journal of Network and Computer Applications* 229 (2024): 103937.

XV. Muzammal, Syeda Mariam, Raja Kumar Murugesan, Noor Zaman Jhanjhi, Mamoona Humayun, Ashraf Osman Ibrahim, and Abdelzahir Abdelmaboud. "A trust-based model for secure routing against RPL attacks in internet of things." *Sensors* 22, no. 18 (2022): 7052.

XVI. Ning, Peng, and Kun Sun. "How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols." *Ad Hoc Networks* 3, no. 6 (2005): 795-819.

XVII. Nithya, S., G. Arul Kumar, and P. Adhavan. "Destination-sequenced distance vector routing (DSDV) using clustering approach in mobile adhoc network." In *2012 International Conference on Radar, Communication and Computing (ICRCC)*, pp. 319-323. IEEE, 2012.

XVIII. Ponnusamy, Vasaki, Mamoona Humayun, N. Z. Jhanjhi, Aun Yichiet, and Maram Fahhad Almufareh. "Intrusion detection systems in internet of things and mobile ad-hoc networks." *Computer Systems Science & Engineering* 40, no. 3 (2022).

XIX. Prakash, P. Suman, Dwaram Kavitha, and P. Chenna Reddy. "Energy and congestion-aware load balanced multi-path routing for wireless sensor networks in ambient environments." *Computer Communications* 195 (2022): 217-226.

XX. Royer, Elizabeth M., and Charles E. Perkins. "Multicast operation of the ad-hoc on-demand distance vector routing protocol." In *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, pp. 207-218. 1999.

XXI. Selvi, Munuswamy, K. Thangaramya, Sannasi Ganapathy, Kanagasabai Kulothungan, H. Khannah Nehemiah, and Arputharaj Kannan. "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks." *Wireless Personal Communications* 105, no. 4 (2019): 1475-1490.

XXII. Senthilkumaran, T., and V. Sankaranarayanan. "Dynamic congestion detection and control routing in ad hoc networks." *Journal of King Saud University-Computer and Information Sciences* 25, no. 1 (2013): 25-34.

XXIII. Sharma, Vishal, Rohit Beniwal, and Vinod Kumar. "Multi-level trust-based secure and optimal IoT-WSN routing for environmental monitoring applications." *the Journal of Supercomputing* 80, no. 8 (2024): 11338-11381.

XXIV. Singh, Kaustubh Ranjan, Rashmi Chaudhry, Vinay Rishiwal, and Mano Yadav. "Model-free QoE-aware seamless handoff in heterogeneous wireless networks." *Mobile Networks and Applications* 29, no. 6 (2024): 1938-1950.

XXV. Singh, Shashank, Veena Anand, and Sonal Yadav. "Trust-based clustering and routing in WSNs using DST-WOA." *Peer-to-Peer Networking and Applications* 17, no. 3 (2024): 1486-1498.

XXVI. Tiwari, Rajeev, Mamta Mittal, Shelly Garg, and Sumit Kumar. "Energy-aware resource scheduling in FoG environment for IoT-based applications." In *Energy conservation solutions for fog-edge computing paradigms*, pp. 1-19. Singapore: Springer Singapore, 2021.

XXVII. Trestian, Ramona, Olga Ormond, and Gabriel-Miro Muntean. "Game theory-based network selection: Solutions and challenges." *IEEE Communications surveys & tutorials* 14, no. 4 (2012): 1212-1231.

XXVIII. Wang, Hui, H. Eduardo Roman, Liyong Yuan, Yongfeng Huang, and Rongli Wang. "Connectivity, coverage and power consumption in large-scale wireless sensor networks." *Computer Networks* 75 (2014): 212-225.