Journal of Advanced Robotics, Autonomous Systems and Human-Machine Interaction ISSN: 3070-6491

PRIME OPEN ACCESS

**Volume 2, Issue 2**

**Research Article**

**Date of Submission:** 06, March, 2026
**Date of Acceptance:** 06 April, 2026
**Date of Publication:** 16 April, 2026

# Negative Effects of Selfish Nodes in Mobile Ad Hoc Networks (MANETs): A Comprehensive Review and Analytical Framework

**Ebenezer Amakeh***

Department of Computer Science, Monroe University, King Graduate School, USA

***Corresponding Author:** Ebenezer Amakeh, Department of Computer Science, Monroe University King Graduate School, USA.

**Citation:** Amakeh, E. (2026). Negative Effects of Selfish Nodes in Mobile Ad Hoc Networks (MANETs): A Comprehensive Review and Analytical Framework. *J Adv Robot Auton Syst Hum Mach Interact, 2*(2), 01-09.

**Abstract**

Mobile ad hoc networks (MANETs) rely on multi-hop cooperation: mobile devices act not only as end hosts but also as routers that relay packets for other users. In practice, however, nodes may behave selfishly to conserve scarce resources such as battery energy, bandwidth, CPU time, and buffer capacity. Unlike overtly malicious attacks that aim to harm the network even at a cost, selfish behavior is often economically rational and may be intermittent, selective, and context dependent. These properties make selfishness difficult to detect and, importantly, allow it to degrade performance in ways that are easily mistaken for normal mobility or wireless losses. This paper synthesizes the negative effects of selfish nodes in MANETs and explains how local non-cooperation propagates into network-wide degradation. We provide a taxonomy of selfish behaviors across layers (routing misbehavior, selective forwarding, route misreporting, resource hoarding, and MAC-layer misbehavior), and then analyze downstream impacts on packet delivery ratio, delay/jitter, routing overhead, energy consumption, fairness, and the risk of network partitioning. To support interpretation, we introduce simple analytical models that relate selfishness severity and path length to end-to-end delivery probability and illustrate how reduced effective cooperative density increases partition risk. Finally, we present a reproducible evaluation template (protocol choices, selfishness models, metrics, and statistical reporting) to guide rigorous empirical studies. The synthesis underscores a central finding: selfishness frequently creates reinforcing feedback loops—loss triggers rerouting, rerouting increases control traffic, control traffic consumes energy and bandwidth, and these pressures can induce further selfishness. Therefore, the cost of selfish behavior is not limited to dropped packets; it can shorten network lifetime and compromise mission-critical applications even when only a fraction of nodes defect.

**Keywords:** Mobile Ad Hoc Networks, Selfish Nodes, Cooperation, Routing, Trust, Reputation, Incentive Mechanisms, Quality of Service, Network Partitioning

## Introduction

Mobile ad hoc networks (MANETs) are infrastructure-less, self-organizing wireless networks formed by mobile nodes that communicate over multi-hop links. MANETs are valuable in environments where fixed infrastructure is unavailable, damaged, or undesirable—such as disaster response, tactical operations, temporary events, and mobile IoT edge scenarios. In these settings, routing must be performed in a distributed manner while nodes move, links break, and the wireless medium fluctuates. A core assumption behind classical MANET routing protocols is that nodes will forward packets for others. Yet forwarding is not free: transmitting and receiving consume battery power; storing packets consumes buffer space; processing control traffic consumes CPU time; and contending for the wireless medium increases delay. Because individual devices are resource constrained and owned by users with their own objectives, nodes face a tension between individual utility (saving resources) and collective utility (maintaining connectivity). When a node refuses to forward packets, drops route requests, or manipulates routing and MAC behavior to reduce its burden, it becomes a selfish node. Selfishness differs from purely malicious behavior. Malicious nodes aim to damage the network even if they expend resources, whereas selfish nodes typically seek to maximize their own long-term utility and may cooperate when it benefits them. This rational and intermittent nature is exactly what makes selfishness dangerous: it can be widespread, difficult to attribute, and capable of degrading the network without triggering obvious security alarms. Understanding the negative effects of selfish behavior is essential for two reasons. First, selfishness can degrade performance even when the fraction of selfish nodes is modest, because MANET routing depends on a small set

of high-betweenness relays and on shared control-plane operations. Second, mitigation mechanisms—reputation and trust systems, acknowledgment schemes, credits, or learning-based detection—introduce overhead and trade-offs. Without a clear articulation of how selfishness harms MANETs, designers' risk either under-protecting (leading to poor reliability) or over-engineering defenses (consuming resources and causing false accusations). This paper focuses on the negative effects of selfish nodes and contributes: (1) a taxonomy of selfish behaviors across protocol layers; (2) an impact analysis that traces how non-cooperation propagates into QoS degradation, unfairness, and partition risk; (3) a lightweight analytical framework illustrating nonlinear degradation with hop count and cooperative density; and (4) a reproducible methodology template for empirical evaluation.

## Background: MANET Routing and the Cooperation Assumption

MANETs differ from traditional infrastructure networks in several key aspects. Nodes are mobile and may join or leave at any time; links are unstable; and routing must be decentralized. Common routing protocols include reactive (on-demand) protocols such as AODV and DSR, proactive protocols such as OLSR, and hybrid approaches that combine proactive neighborhood maintenance with on-demand discovery. In many MANET designs, intermediate nodes forward both data packets and control packets (route requests and replies, hello messages, link-state updates, and route error notifications). Therefore, forwarding behavior influences not only a single flow but also the ability of many nodes to discover and maintain routes. For example, if a node drops route requests or refuses to rebroadcast them, route discovery coverage shrinks; if a node withholds route errors, stale routes persist and cause repeated losses. Selfish behavior has been studied since early work on routing misbehavior and watchdog-based detection [1]. and economic incentives to stimulate cooperation [2]. More recent studies quantify selfishness impacts and examine hybrid trust-aware routing and detection mechanisms. Shan et al. (2021), for example, studied energy-consumption-driven dynamic selfishness in MANETs and reported substantial impacts on packet loss, delay, and throughput across mobility and density settings. Survey work organizes mitigation approaches into reputation-based, credit-based, acknowledgment-based, and game-theoretic families [3]. Across this literature, one theme is consistent: selfish behavior is not a local nuisance. It changes the effective topology by removing relays, increases route instability, and can create cascading degradations such as repeated route discoveries, energy waste, congestion, and (in extreme cases) network partitioning. Rigorous analysis of negative effects is therefore a prerequisite for designing balanced mitigation strategies.

## Illustrative Example of Selfish Forwarding Disruption

Figure 1 illustrates a simple multi-hop route where a selfish intermediate node refuses to forward traffic, breaking end-to-end communication.

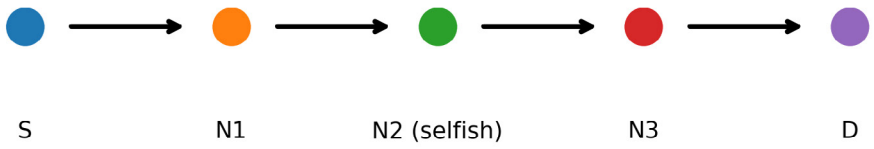


**Figure 1: A Multi-Hop Path Disrupted by A Selfish Forwarding Node**

## Taxonomy of Selfish Node Behaviors

Selfishness in MANETs can be expressed at multiple protocol layers and with varying intensity. A practical taxonomy can be organized by (a) the action taken, (b) selectivity, and (c) the layer affected.

### Action Types Include:

- **Forwarding Refusal:** refusing to relay data packets and sometimes control packets.
- **Selective Forwarding:** forwarding some packets but dropping others based on source, destination, flow, hop count, or perceived benefit.
- **Delay and Jitter Injection:** forwarding packets but intentionally delaying them (e.g., aggressive sleep scheduling) to conserve energy or reduce contention.
- **Routing Misreporting:** manipulating routing control information to avoid being selected as a relay, to reduce route maintenance burden, or to shift load to others.
- **Resource Hoarding:** limiting queue space for transit traffic, discarding packets under congestion in a biased manner, or refusing to buffer opportunistic traffic.
- **MAC-Layer Selfishness:** manipulating contention parameters or transmission behavior to capture more channel time or reduce cooperative cost [4].

Selectivity matters because selective behavior can evade simplistic detectors. A node may cooperate for its own traffic but not for transit traffic (free-riding), or it may switch between cooperative and selfish modes based on residual energy thresholds (dynamic selfishness), which Shan et al. (2021) model explicitly. Layer matters because the same goal (saving resources) can be pursued in different ways: network-layer selfishness directly affects routing and path stability; MAC-layer selfishness affects medium access fairness and collision rates; and application-level selfishness can involve refusing to share sensed data or to participate in distributed services.

Figure 2 summarizes a conceptual chain from selfishness drivers to behaviors and observed impacts.

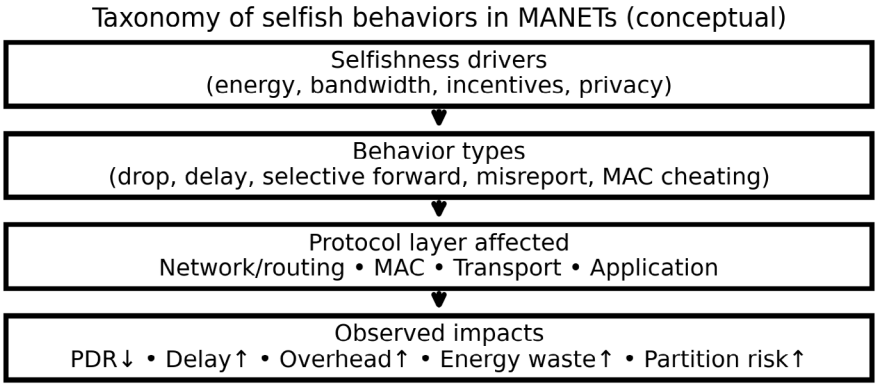


**Figure 2: Conceptual Taxonomy and Impact Chain for Selfish Behaviors in Manets**

## Negative Effects of Selfish Nodes

Selfish nodes degrade MANETs through a combination of direct forwarding failures and indirect control-plane feedback. The following subsections analyze major negative effects and explain how they reinforce each other. Packet delivery ratio and reliability. The most immediate effect is reduced packet delivery ratio (PDR). If a selfish node lies on a critical cut of the connectivity graph, it can drop or refuse to forward traffic, making certain destinations effectively unreachable. Even when alternate paths exist, route discovery may repeatedly select paths that include selfish nodes because local knowledge is incomplete and routes are chosen based on metrics that assume cooperation. Quantitative evaluations report that delivery degrades as selfish fraction increases and that the effect depends strongly on mobility and node placement [5]. End-to-end delay and jitter. When selfishness causes route failures or forces rerouting to longer detours, latency increases. Delay also rises when nodes intentionally introduce waiting before forwarding. Jitter is particularly damaging for real-time traffic (voice, telemetry, control) and can induce transport-layer retransmissions and timeouts that further increase load. Routing overhead and control storms. Loss caused by selfish nodes is often indistinguishable from mobility-induced link breaks, so sources initiate new route discoveries. Reactive protocols respond with broadcast route requests and propagate errors. If selfish nodes also drop control traffic, route discovery becomes less effective and repeated broadcasts follow. This feedback loop inflates routing overhead, consumes bandwidth, and can precipitate congestion collapse. Energy waste and shortened network lifetime. Selfish nodes may save their own energy, but the network as a whole can expend more energy. Repeated discoveries, retransmissions, and longer paths increase total radio usage among cooperative nodes. Hot-spot relays deplete faster, which can trigger secondary selfishness as more nodes reach low-energy states—an instance of tragedy-of-the-commons dynamics. Fairness and load imbalance. Selfishness shifts the forwarding burden to a smaller set of cooperative nodes, creating hot spots with higher contention and queueing. Fairness can be quantified using per-node forwarding rates, energy depletion, or Jain's fairness index. Unfair burden also changes incentives: if the same nodes are exploited, rational users may defect unless compensated. Connectivity degradation and partitioning. By removing relays from the forwarding fabric, selfish nodes reduce effective cooperative density. If selfish nodes are clustered or occupy bridge positions, the network can split into disconnected components. Shan et al. (2021) emphasize that partition risk depends jointly on density, mobility, and the proportion and selection of selfish nodes. Figure 6 illustrates a conceptual relationship between selfish fraction, density, and partition risk. Security and mission risk. Although selfishness is not always malicious, its outcomes resemble denial-of-service: critical messages fail to deliver, routes become unstable, and control traffic floods the network. Moreover, selfish and malicious behaviors can coexist. This overlap motivates integrated security approaches such as danger-theory-based immune systems and intrusion detection frameworks that treat non-cooperation as a security-relevant event [6,7]. Application-level consequences. In mission-oriented deployments, unreliable communication can cause coordination breakdowns, delayed situational awareness, and increased physical risk. In IoT edge settings, selfishness can reduce the availability of sensed data and degrade closed-loop control. Overall, selfishness harms MANET performance through multiple pathways that reinforce each other. The next section formalizes these relationships using simple analytical models.

| Selfish behavior | Primary negative effect | Typical metrics | Notes |
|---|---|---|---|
| Forwarding refusal / drop | PDR decrease; reachability loss | PDR, PLR, throughput | High impact when node is a bridge or high-centrality relay |
| Selective forwarding | Unreliable flows; biased loss patterns | Flow PDR, loss bursts, RTT variance | Harder to detect; can target specific victims |

| | | | |
|---|---|---|---|
| Delay injection / sleep | Delay and jitter increase | Avg delay, jitter, TCP timeouts | May resemble benign duty-cycling if not modeled carefully |
| Control packet dropping | Route discovery failure; control storms | RREQ/RERR counts, overhead bytes | Amplifies overhead and energy waste |
| MAC-layer cheating | Unfair medium access; collisions | Channel utilization, collision rate, fairness index | Can degrade neighbors even without dropping data |
| Resource hoarding (buffers) | Congestion and queue drops | Queue occupancy, drop rate, delay | Often interacts with traffic load and burstiness |

**Table 1: Mapping of Selfish Behaviors to Negative Effects and Observable Metrics**

## Cross-Layer Effects and Confounders

Cross-layer negative effects deserve special attention because selfishness can originate at one layer and manifest as harm at another. MAC-layer selfishness. Nodes can manipulate contention behavior to gain more channel access (e.g., shorter backoff) or to reduce cooperative retransmission cost. Such behavior increases collisions and delays for neighbors and can appear as unexplained throughput collapse. Kyasanur and Vaidya (2005) show that MAC misbehavior can be as damaging as network-layer misbehavior because it distorts the shared medium, which is a single point of contention for the entire neighborhood. Transport and application interactions. Packet drops and jitter induced by selfishness can trigger TCP congestion control and retransmission timeouts, shrinking throughput and increasing delay. For UDP real-time flows, jitter and loss degrade perceptual quality. Importantly, application-level adaptation (e.g., increasing send rate to compensate for loss) can exacerbate congestion, creating a self-reinforcing loop. Energy management as a confounder. Some behavior that resembles selfishness is legitimate energy management: duty-cycling, sleep schedules, and adaptive transmit power. Therefore, a negative-effect analysis must consider the boundary between rational energy saving and protocol violation. Dynamic selfishness models [5]. Help clarify this boundary by making the switching rule explicit.

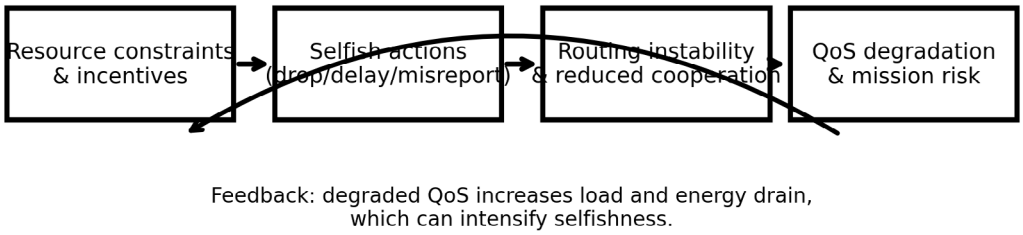


**Figure 3: Conceptual Impact Pathway from Selfish Behavior to System-Level Harm**

## Analytical Framework for Interpreting Degradation

Analytical models help explain why modest selfishness can cause disproportionate harm. While real MANETs include mobility, interference, and protocol complexity, simple probability models capture the sensitivity of multi-hop delivery to cooperation. End-to-end delivery probability. Consider a path of h hops between source and destination. Let p denote the fraction of nodes that are selfish. Suppose selfish nodes forward a transit packet with probability q (0 <= q <= 1), representing partial cooperation (e.g., forwarding only under incentives or when energy is above a threshold). A conceptual approximation is that each hop succeeds with probability (1 - p) + p*q = 1 - p*(1 - q).

## The end-to-end delivery probability along an h-hop path is then:

Delivery ≈ (1 - p*(1 - q)) ^h. Figure 4 plots this relationship for representative q values. The exponential dependence on h explains why longer paths are fragile: even moderate selfishness yields large delivery losses. Effective path length and rerouting. When paths containing selfish nodes fail, routing protocols often select alternate paths that avoid detected or suspected nodes, which can increase hop count. Longer paths increase cumulative loss and delay. Additionally, repeated rerouting increases control overhead. The result is a coupled system: selfishness reduces delivery, reduced delivery increases routing churn, and routing churn consumes the very resources that nodes are trying to preserve. Partition risk. Connectivity in random geometric graphs depends on node density and communication range. Selfish behavior reduces effective relay density because selfish nodes do not act as forwarding intermediaries. A conceptual indicator of partition risk is therefore increasing in p and decreasing in density. Figure 6 shows one such conceptual surface and highlights that sharp transitions can occur as cooperative density approaches a percolation threshold. Interpretation and limitations. These models are intentionally simplified. They do not capture spatial clustering of selfish nodes, correlated behaviors, or protocol-specific mechanisms such as route caching. Nonetheless, they clarify two key insights: (1) multi-hop reliability declines nonlinearly with selfishness and hop count, and (2) harm is amplified by protocol reactions

(rerouting, retransmissions, and control flooding).

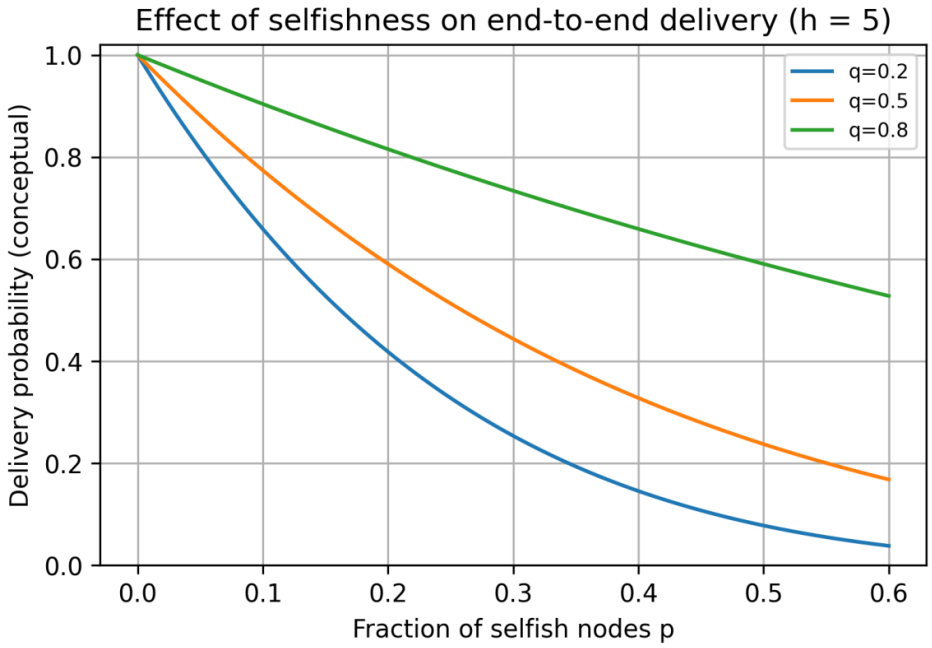


**Figure 4: Conceptual Relationship Between Selfish-Node Fraction and End-To-End Delivery Probability.**

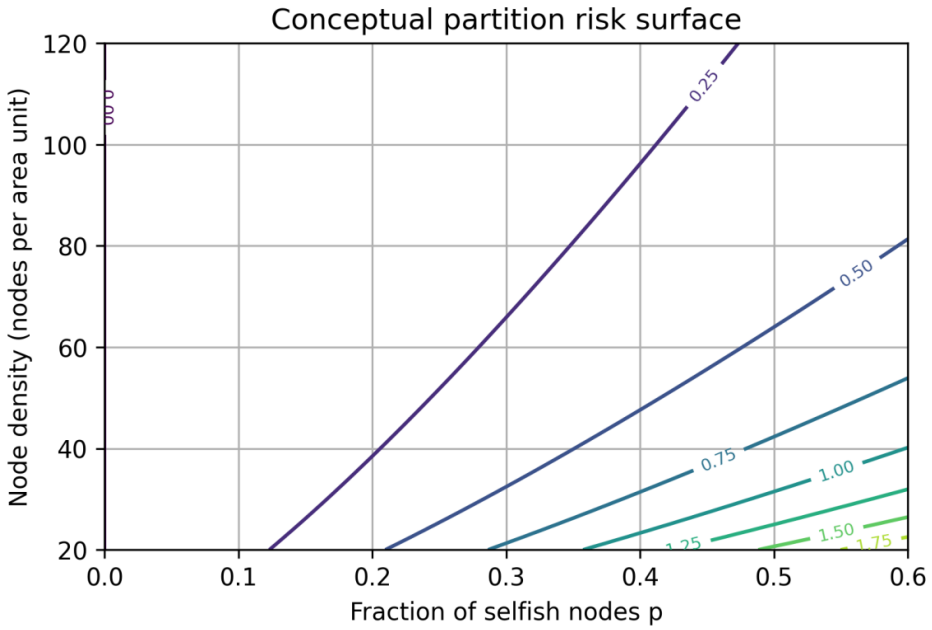


**Figure 6: Conceptual Surface Relating Selfish-Node Fraction, Density, and Partition Risk.**

## Related Work and Research Trends

Research on selfishness in MANETs spans three overlapping threads: measurement of impact, detection of non-cooperation, and incentives for cooperation. Early work highlighted that routing misbehavior can severely degrade delivery and proposed watchdog/path rater mechanisms [1]. Because watchdog-style approaches require promiscuous monitoring and can be unreliable in the presence of collisions and asymmetric links, acknowledgment-based schemes such as TWOACK were proposed to detect forwarding failures more robustly [8]. In parallel, reputation systems such as CORE and CONFIDANT emphasized social enforcement: nodes maintain reputations based on observed behavior and isolate or deprioritize misbehaving nodes [9,10]. These approaches address repeated selfishness but face challenges such as false accusations, slow reputation convergence, and dynamic mobility. OCEAN proposed using only first-hand observations to reduce the trust-management burden (Bansal & Baker, 2003). Economic and credit-based systems treat forwarding as a service that should be compensated. Buttyan and Hubaux (2003) introduced mechanisms to stimulate cooperation, and Sprite proposed a cheat-proof credit system using receipts and a trusted authority (Zhong et al., 2003). These mechanisms directly acknowledge the rational incentives behind selfishness and provide an interpretation

bridge between networking performance and user utility. Recent studies extend these ideas with optimization and learning. Survey work categorizes detection techniques and highlights the need for hybrid approaches that combine trust, acknowledgments, and context [3]. Trust-aware clustering and routing protocols aim to select reliable relays while controlling overhead [13,14]. Machine learning approaches attempt to distinguish selfish behavior from legitimate losses by extracting features from routing, MAC, and traffic statistics [15]. Security-oriented work integrates selfishness into broader intrusion detection, recognizing that selfish behavior can resemble or enable denial-of-service [6,7]. Across these threads, impact studies consistently show that selfishness increases routing churn and energy waste, suggesting that mitigation evaluations should report not only detection accuracy but also end-to-end system cost.

## Methodology Template for Reproducible Impact Studies

Because selfishness effects depend on mobility, density, traffic, and protocol details, experimental methodology must be explicit and reproducible. This section outlines a study design template. Study objectives and hypotheses. A typical impact study can test: (H1) increasing selfish node fraction reduces PDR; (H2) the impact strengthens as average hop count increases; (H3) selfishness increases routing overhead disproportionately in reactive protocols; and (H4) dynamic energy-driven selfishness is less harmful than static refusal but still degrades performance.

**• Selfishness models. At minimum, include:**

• Static selfishness: the node refuses to forward transit packets throughout the run.
• Dynamic selfishness: the node switches to selfish mode below an energy threshold or under queue pressure [5].
• Selective selfishness: the node forwards only its own traffic or traffic from trusted peers.
• MAC-layer selfishness (optional): the node manipulates contention behavior to gain channel access [4].

Protocols and scenarios. Evaluate at least one reactive protocol (AODV or DSR) and one proactive protocol (OLSR) under multiple mobility models (Random Waypoint, Gauss-Markov, group mobility) and node densities. Explicitly state radio and propagation parameters and traffic patterns (UDP CBR, TCP flows, bursty traffic).

**Metrics. Report a core set:**

• Packet delivery ratio (PDR) and packet loss rate.
• End-to-end delay and jitter.
• Routing overhead (control packets or bytes per delivered data packet).
• Energy consumption per delivered bit and a network lifetime proxy (time until X% of nodes are depleted).
• Fairness metrics (Jain's index for forwarding load or energy depletion).

Statistical analysis. Use multiple random seeds and report confidence intervals. When comparing conditions, report effect sizes (e.g., percent change relative to baseline) and avoid over-interpreting small differences. Threats to validity. Internal validity threats include unrealistic selfishness models and implementation artifacts. External validity threats include obstacles and hardware heterogeneity in real deployments. Construct validity threats include selecting metrics that do not match mission goals. Figure 5 shows a workflow template for reproducible studies.


**Figure 5: Reproducfcible Workflow for Simulating and Evaluating Selfishness Impacts**

## Discussion and Design Implications

Several cross-cutting insights emerge.

First, selfishness amplifies protocol overhead. Routing protocols interpret losses as mobility or channel issues and respond with rediscovery and retransmissions. When selfishness causes loss, these reactions can consume more resources than the original traffic. This is why network-level energy cost can rise even if selfish nodes save energy individually. Second, placement matters as much as proportion. Two networks with the same selfish fraction can behave very differently depending on where selfish nodes appear. If selfish nodes coincide with high-betweenness relays or bridges between groups, harm is larger. Evaluations should therefore vary not only fraction but also selection strategy (random, centrality-based, clustered). Third, dynamic selfishness is realistic and policy-relevant. Energy-driven and queue-driven selfishness (nodes defect under stress) reflects real devices and can still trigger cascading congestion and route churn. Quantifying intermediate behaviors helps distinguish mitigation needs for benign energy management versus adversarial manipulation. Fourth, privacy and observability constraints are central. Many detection approaches rely on promiscuous listening and neighbor monitoring. Encryption, duty-cycling, directional antennas, and heterogeneous hardware can reduce observability and increase false positives. False accusations are harmful: they can exclude cooperative nodes and further reduce connectivity. Finally, impacts are application dependent. Tactical and emergency networks prioritize reliability and timeliness; IoT networks prioritize lifetime; and vehicular or aerial networks prioritize low-latency control. Therefore, the most important negative effects should be evaluated using mission-oriented utility functions rather than single metrics.

## Mitigation Landscape (Context for Impact Interpretation)

Although this paper emphasizes negative effects, mitigation strategies provide context for why effects matter and what trade-offs arise. The literature groups defenses into: (1) reputation and trust systems (e.g., CORE, CONFIDANT), (2) watchdog and acknowledgment schemes (e.g., watchdog/pathrater, TWOACK-style mechanisms), (3) incentive and credit systems (e.g., nuglets and Sprite), (4) game-theoretic cooperation enforcement, and (5) learning-based detection and hybrid security frameworks.Reputation systems attempt to estimate a neighbor's willingness to forward and then prefer high-reputation relays [9,10]. Acknowledgment approaches add control packets to verify forwarding [8]. Credit systems reward forwarding using tokens or micropayments [2]. Game-theoretic approaches frame cooperation as a repeated game and design strategies that make cooperation a best response [11,12]. More recent work explores trust-aware routing with optimized clustering and learning-based detection in IoT-MANET environments [13,15]. Each approach incurs cost: monitoring consumes energy, credits require accounting, and learning requires features and data. Importantly, mitigation mechanisms can themselves reduce performance if misconfigured (e.g., false accusations can exclude healthy nodes and increase partition risk). Therefore, understanding negative effects is essential to choosing proportionate and mission-appropriate defenses.

## Case Study Scenarios

Practical deployments highlight why the negative effects of selfishness are mission critical.

Disaster response. In a post-disaster area, first responders may deploy handheld radios or smartphones forming an ad hoc network. If some devices reduce forwarding to preserve battery for critical voice communications, the network may exhibit intermittent partitions. The most harmful effects are delayed delivery of situational reports, reduced reachability of command nodes, and an increase in control traffic that drains already scarce batteries. Tactical patrol and reconnaissance. In tactical MANETs, a subset of nodes may have higher-value missions and attempt to minimize forwarding load to preserve stealth and energy. If those nodes occupy bridge positions, non-cooperation can split the network into isolated squads. Even when routes exist, jitter and loss can compromise time-sensitive coordination. Edge and IoT data collection. In IoT-style MANETs (e.g., mobile sensors or drones collecting data), nodes may refuse to relay data to conserve energy. Here the negative effect is incomplete data coverage and biased datasets: cooperative nodes contribute more observations, while selfish nodes still consume network services. This can degrade downstream analytics and decision-making.

## Recommendations for Research and Practice

### Design recommendations derived from the negative-effect analysis include:

- Measure harm with mission-oriented metrics. In addition to PDR, include delay, jitter, energy per delivered bit, and fairness. Mission utility often depends on timeliness as much as reliability.
- Evaluate both proportion and placement. Random selfishness may underestimate harm relative to strategic placement at high-centrality nodes. Include clustered and centrality-based selfish-node selections.
- Separate benign energy saving from protocol violations. Include dynamic selfishness models where nodes defect below energy thresholds and report those thresholds. Compare to benign duty-cycling baselines.
- Report overhead of mitigation. Detection accuracy alone is insufficient; mitigation must be evaluated on total cost (additional control traffic, energy consumption, false exclusions) and on whether it reduces partition risk.
- Use reproducible methodology. Provide simulator version, parameters, traffic seeds, mobility traces, and code availability. Reproducibility is essential because selfishness effects depend on many interacting factors.

## Limitations and Future Work

This paper provides a comprehensive review and analytical framework, but several limitations should be noted. First, the analytical models are simplified and do not capture spatial correlations, interference dynamics, or protocol-specific behaviors. Second, because this work is a synthesis, it does not present new simulation results; instead, it provides a methodology and conceptual models to guide reproducible empirical studies. Third, the literature varies in definitions of selfishness and in measurement setups, which complicates direct comparison. Future work should focus on standardized selfishness models and benchmark scenarios across simulators, reproducible open-source implementations of detection and incentive mechanisms, evaluation under realistic mobility traces and heterogeneous radios, privacy-aware cooperation enforcement, and joint optimization of detection accuracy and overhead under mission constraints.

## Conclusion

Selfish nodes undermine the cooperative foundation of MANETs. Their negative effects extend beyond dropped packets: selfishness increases delay, inflates routing overhead, wastes energy for cooperative nodes, creates unfair load distributions, and can induce network partitions. Because selfish behavior is often rational and intermittent, it is difficult to detect and can be amplified by protocol mechanisms designed to cope with mobility.

By organizing selfish behaviors into a clear taxonomy, tracing pathways from local defection to system-level harm, and presenting analytical relationships that explain nonlinear degradation with hop count and cooperative density, this paper provides a foundation for rigorous evaluation and design. The included methodology template offers a roadmap for future studies to quantify impacts across protocols, mobility models, densities, and selfishness severities. Ultimately, mitigating selfishness requires balanced mechanisms that improve cooperation without imposing prohibitive overhead or unfairly penalizing benign energy-saving behavior.

## References


1. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 255-265).
2. Buttyán, L., & Hubaux, J. P. (2003). Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Networks and Applications, 8(5), 579-592.
3. Vanday Baseri, M., & Fatemidokht, H. (2022). Survey of different techniques for detecting selfish nodes in MANETs. Journal of Mahani Mathematical Research, 11(2), 45–59.
4. Kyasanur, P., & Vaidya, N. H. (2005). Selfish MAC layer misbehavior in wireless networks. IEEE transactions on mobile computing, 4(5), 502-516.
5. Shan, A., Fan, X., Wu, C., Zhang, X., & Fan, S. (2021). Quantitative study on the impact of energy consumption based dynamic selfishness in MANETs. Sensors, 21(3), 716.
6. Jim, L. E., Islam, N., & Gregory, M. A. (2022). Enhanced MANET security using artificial immune system-based danger theory to detect selfish nodes. Computers & Security, 113, 102538.
7. Nirmala Bai, K. S., Subramanyam, M. V., & others. (2025). Integrated intrusion detection design with discretion of leading agent using machine learning for efficient MANET system. Scientific Reports.
8. Balakrishnan, K., Deng, J., & Varshney, V. K. (2005, March). TWOACK: preventing selfishness in mobile ad hoc networks. In IEEE Wireless Communications and Networking Conference, 2005 (Vol. 4, pp. 2137-2142). IEEE.
9. Michiardi, P., & Molva, R. (2002). CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Communications and Multimedia Security (pp. 107–121). Springer.
10. Buchegger, S., & Le Boudec, J.-Y. (2002). Performance analysis of the CONFIDANT protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks. In Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc).
11. Li, Z., & Shen, H. (2012). Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks. IEEE Transactions on Mobile Computing, 11(8), 1287–1303.
12. Khan, B. U. I., Anwar, F., Olanrewaju, R. F., Pampori, B. R., & Mir, R. N. (2020). A game theory-based strategic approach to ensure reliable data transmission with optimized network operations in futuristic mobile adhoc networks. Ieee Access, 8, 124097-124109.
13. Nirmaladevi, K., & Prabha, K. (2023). A selfish node trust aware with optimized clustering for reliable routing protocol in MANET. Measurement: Sensors, 28, 100680.13
14. Jeganathan, S., & others. (2025). Trust-aware routing protocol using Hierarchical Manta Ray Foraging Optimization Algorithm with selfish node detection in MANET. International Journal of Communication Systems.
15. Ghosh, S., Banerjee, A., Sufian, A., Gupta, S. K., Alsamhi, S. H., & Saif, A. (2023). Efficient selfish node detection using SVM in IoT-MANET environment. Transactions on Emerging Telecommunications Technologies.
16. Akhbari, A., Fattahi, A., & others. (2021). Selfish node detection based on fuzzy logic and Harris hawk's optimization algorithm in MANET. Security and Communication Networks, 2021, 2658272.
17. Bansal, S., & Baker, M. (2003). Observation-based cooperation enforcement in ad hoc networks. arXiv preprint cs/0307012.
18. Fayaz, M., Mehmood, G., Khan, A., Abbas, S., & Gwak, J. (2022). Counteracting selfish nodes using reputation-based system in mobile ad hoc networks. Electronics, 11(2), 185.
19. Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In Mobile computing (pp. 153-181). Boston, MA: Springer Us.
20. Perkins, C. E., & Royer, E. M. (1999). Ad-hoc on-demand distance vector routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA) (pp. 90–100).
21. Varga, A., & Hornig, R. (2008, March). An overview of the OMNeT++ simulation environment. In Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops (pp. 1-10).
22. Wu, C., Gerla, M., & van der Schaar, M. (2017). Social norm incentives for network coding in manets. IEEE/ACM Transactions on Networking, 25(3), 1761-1774.
23. Zhong, S., Chen, J., & Yang, Y. R. (2003, March). Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428) (Vol. 3, pp. 1987-1997). IEEE.
24. Lupia, A., & De Rango, F. (2016, April). A probabilistic energy-efficient approach for monitoring and detecting malicious/selfish nodes in mobile ad-hoc networks. In 2016 IEEE Wireless Communications and Networking Conference (pp. 1-6). IEEE.
25. Rehman, G. U., Ghani, A., Zubair, M., Naqvi, S. H. A., Singh, D., & Muhammad, S. (2019). Ips: Incentive and punishment scheme for omitting selfishness in the internet of vehicles (iov). IEEE Access, 7, 109026-109037.


## Appendices

**Appendix A:** Example Parameter Template for Selfishness Impact Simulations
Topology: square area L x L (e.g., 1000 m x 1000 m)
Node count: N = {30, 50, 80, 120}
Radio range: R = {150 m, 250 m}
Mobility model: Random Waypoint (speed 1–20 m/s, pause 0–30 s) and Group Mobility
Routing protocols: AODV, DSR, OLSR

Traffic: UDP CBR (512-byte packets) at {2, 4, 8} flows; optional TCP flows
Simulation time: 900 s
Selfish fraction p: {0, 0.1, 0.2, 0.3, 0.4}
Selfish model: static refusal; dynamic threshold (defect if energy < 20%); selective (drop transit only)
Energy model: initial energy 1000 J; Tx/Rx power per simulator defaults; report energy per delivered bit
Replications: 20 random seeds; report 95% confidence intervals

**Appendix B:** Pseudocode for a Simple Selfish Forwarding Model

```
OnReceive (Packet pkt):
if pkt. destination == self:
DeliverToUpperLayer(pkt)
return
if IsControlPacket(pkt):
# optional: selfish nodes may also drop control traffic
ForwardControl(pkt) # or drop based on control_drop_rate
return
# Data packet for transit forwarding
if selfish_mode == STATIC_REFUSAL:
Drop(pkt)
else if selfish_mode == DYNAMIC_THRESHOLD:
if ResidualEnergy() < ENERGY_THRESHOLD:
Drop(pkt)
else: Forward(pkt)
else if selfish_mode == SELECTIVE:
if pkt.source == self or pkt. flow in trusted_flows:
Forward(pkt)
else: Drop(pkt)
```

**Appendix C:** Metric Definitions
Packet delivery ratio (PDR) = delivered data packets / sent data packets.
Average end-to-end delay = mean(receive_time - send_time) over delivered packets.
Routing overhead = total control packets (or bytes) / delivered data packets.
Energy per delivered bit = total energy consumed by all nodes / total delivered payload bits.
Fairness (Jain) = (sum x_i)^2 / (n * sum x_i^2), where x_i is per-node forwarding load or energy depletion.