Engineering and Technology Journal e-ISSN: 2456-3358

Volume 11 Issue 04 April-2026, Page No.-9324-9324

DOI: 10.47191/etj/v11i04.01, I.F. – 8.595

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 ORCID: 0009-0009-5578-1370

ABSTRACT: Mobile ad hoc networks depend upon the multi-hop collaboration of the nodes; that is, the nodes not just act as end systems but also behave as routers to forward the packets of other users. However, in the real world, the nodes might act selfishly to conserve scarce resources such as battery power, bandwidth, CPU time, and buffer space. Unlike other attacks that are intended to destroy the network, selfish behavior might be economically rational, intermittent, and context dependent. Hence, selfish behavior might not always be easy to detect and, more importantly, might cause performance degradation that manifests because of mobility and wireless effects. This paper integrates the impact of selfish nodes on MANETs and shows how local non-cooperative behavior can cause network-wide decline. We present a taxonomy of selfish behavior at different layers of the network such as routing misbehavior, selective forwarding, fake route report generation, resource hoarding, and MAC layer misbehavior. We then show how local selfish behavior can cause network-wide decline about packet delivery ratio, delay, jitter, routing overhead, energy dissipation, fairness, and network partitioning. To facilitate easy understanding of the effects of selfish behavior, we present simple analytical models that relate the level of selfishness and path lengths to the probability of end-to-end packet delivery. We then present a reproducibility template for the evaluation of selfish behavior about the choice of protocols used, the selfish behavior modeling used, the metrics used for evaluation, and statistical reporting of the results. The integration of the effects of selfish behavior highlights that a significant effect of selfish behavior might be the formation of a feedback loop that causes packet loss due to rerouting, which in turn causes more routing overhead that consumes scarce resources such as energy and bandwidth, which might cause other nodes to behave selfishly as well. Hence, the cost of selfish behavior might not just be packeting loss but the possible shortening of the network lifetime and the compromising of mission- critical applications due to the selfish behavior of a small number of nodes.

KEYWORDS: mobile ad hoc networks; selfish nodes; cooperation; routing; trust; reputation; incentive mechanisms; quality of service; network partitioning

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are wireless, infrastructure-free networks where mobile nodes communicate with each other through multi-hop connections. They are particularly useful when there's no infrastructure available or when it's undesirable. Examples include disaster areas, tactical military operations, temporary events, or mobile IoT edge computing. In these environments, routing must be performed in a distributed fashion, given the mobility of the nodes, changing links, and wireless channel conditions. One of the underlying assumptions in traditional MANET routing protocols is that nodes will cooperate by forwarding packets for other nodes. However, there are costs to forwarding, including battery use when sending, battery use when receiving, buffering using memory, processing control packets using CPU, and competing for the wireless channel, which introduces delays. Additionally, these nodes are constrained in resources, are typically user-owned, and have their own objectives, creating a tradeoff between individual utility, or conserving resources, and network utility, or keeping the network connected.

If a node refuses to forward or drops route requests or adjusts routing and MAC parameters to reduce its own burden, then it is selfish. Selfish behavior should not be confused with malicious behavior. Malicious nodes are those that try to impair network performance even at the expense of their own resources. Selfish nodes are those that try to maximize their own benefit. Selfish behavior is a rational behavior that may not always be cooperative. This behavior is dangerous because it can manifest at large scales, be hard to detect, and can cause network degradation without any obvious signs. Selfish behavior in MANETs is important because it can cause network degradation even if a small percentage of nodes are selfish. This is because MANET routing protocols are based on a limited number of high-traffic nodes. In addition, any proposed solutions such as reputation systems, trust systems, or credit systems all have associated costs. Without a good understanding of how selfish behavior impacts MANETs, any proposed solutions may either not protect the network adequately (bad

reliability) or may protect too well (excessive reliance on protection systems and false accusations). This paper aims to identify the negative impacts of selfish nodes. In this paper, we propose: (1) a classification of selfish behavior at all protocol layers; (2) an analysis of impacts that explains how non- cooperative behavior Ripples into QoS degradation, unfairness, and partitioning; (3) a simple analytical framework that proves nonlinear degradation with hop count and cooperation density; **and (4) a reproducible methodology template for empirical evaluation.**

II. BACKGROUND AND COOPERATION ASSUMPTION

Mobile ad hoc networks (MANETs) are distinguished from traditional wired or fixed wireless networks in several key areas. First, nodes are free to move, associate, and dissociate as desired. Second, links are dynamic and change frequently, making them inherently unreliable. And third, there is no centralized entity to manage any of this, including routing. There are generally three types of routing protocols: reactive (on demand) protocols such as AODV and DSR, proactive protocols like OLSR, and a combination of both, which are referred to as hybrids.

In many models of MANETs, routers are also asked to forward not just data but also other control traffic, such as route requests and replies, hello messages, link-state updates, and route errors. In this sense, the act of forwarding affects not just a particular flow but also affects many routers in their ability to find and maintain routes. To illustrate this, consider a node that does not forward route requests or does not allow others to rebroadcast these requests. In this case, the coverage of route discovery is compromised. Similarly, a node that does not forward route errors causes other routers to continue using outdated routes, resulting in repeated losses.

Selfishness in MANETs has also been a topic of interest since the early days of routing misbehavior and watchdog-based detection schemes, with more recent work focusing on using economic incentives to encourage cooperative behavior. Other more recent work has attempted to quantify the effects of selfishness on network performance, as well as hybrid approaches to routing and detection schemes. In one such work, Shan et al. investigated the effects of energy-based dynamic selfishness in MANETs, showing significant effects on packet losses, delay, and throughput with varying mobility and density.

All these approaches have a common underlying theme: selfishness in a network is not a local problem but a global one, in that it affects the topology of the network by removing routers, increases instability in routes, and in turn can cause a number of other problems, such as repeated route discoveries, wasted resources, congestion, and in the worst cases, partitioning of the network. A good understanding of these adverse effects is a prerequisite to designing solutions to mitigate these problems.

Fig. 1. A multi-hop path disrupted by a selfish forwarding node.

III. TAXONOMY OF SELFISH NODE BEHAVIORS

The selfishness in MANETs manifests at different layers and to different degrees. A more concrete classification is based on the following three criteria: the type of action, the selectivity of the selfish behavior, and the layers affected. The types of actions taken by a selfish node are:

- Refusing to forward the data packets, sometimes even the control packets.
- Selective forwarding of the packets, depending on the source, destination, flow, hop count, etc.
- Injecting delay and jitter by forwarding the packets but after a certain delay to conserve energy.
- Misreporting the routing control information to avoid being selected for packet relaying.
- Resource hoarding by keeping less buffer space for the packets to be forwarded, discarding the packets in a biased manner when the node is congested, and refusing to store the packets for the opportunistic nodes.
- MAC layer selfishness by adjusting the parameters to obtain more channel access time for the node or to lower the cost of cooperation for the node [6].

The selectivity of the selfish behavior is also taken into consideration. The node may cooperate for the packets of the sender but not for the packets to be forwarded. In this case, the node is said to be a free rider. The node may also change the selfish behavior to cooperative and vice versa depending on the energy left in the node. This is called dynamic selfishness. The node is said to be dynamic selfish

if the energy is more.

This is explicitly modeled by Shan et al. [4].

Figure 2 depicts the conceptual sequence from the cause to the effect.

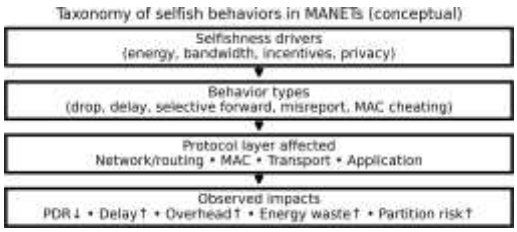

Fig. 2. Conceptual taxonomy and impact chain for selfish behaviors in MANETs.

IV. NEGATIVE EFFECTS

The negative impact of selfish nodes on MANETs comes from a combination of direct effects of forwarding failures and subtle effects of feedback on the control plane. The following sections describe the most significant negative effects of selfish nodes and illustrate their combination.

Packet delivery ratio and reliability. The most immediate impact of selfish nodes is a reduced packet delivery ratio. If a selfish node blocks a critical cut in the connectivity graph of the network, some destinations become unreachable. Even with multiple paths available, the process of routing discovery tends to choose routes that pass through selfish nodes due to local knowledge and decision-making that assume cooperation between nodes. Analysis of selfish nodes' impact on delivery ratio demonstrates that the ratio of delivered packets diminishes with an increasing number of selfish nodes [4].

End-to-end delay and jitter. Latency increases due to selfish nodes because of increased failures of routes that pass through them. Latency increases even further if nodes implement delays before sending packets. Jitter affects real-time traffic such as voice and video most seriously.

Routing overhead and control storms. The loss of packets due to selfish nodes appears as link failures due to mobility. As a result, sources initiate new route discoveries. Reactive routing protocols broadcast new route requests and errors. Selfish nodes that drop routing traffic make the process of route discovery less effective. Excessive broadcasts of route requests and errors constitute routing overhead.

Energy waste and shorter network life. When nodes act selfishly, they save their own energy, but the network wastes more energy in the end. There are repeated discoveries, repeated transmissions, and longer routes for the cooperative nodes, leading to increased radio usage for the cooperative nodes. The hot spot relays run out of power quicker, leading to another round of selfish behavior due to the large number of nodes running out of power.

Fairness and load imbalance. When nodes act selfishly, they impose a greater load on the few cooperative nodes, leading to hotspots where there is increased contention and queueing delays. We can also define fairness in terms of the rate at which each node is used for forwarding, the rate at which each node runs out of power, and Jain's fairness index.

Connectivity degradation and partitioning. When some relay nodes run out of power and leave the network, the density of the cooperative nodes is reduced in the network. If the selfish nodes are clustered together and are in the bridge positions in the network, the entire network can be partitioned into different segments. According to Shan et al. in [4], the partitioning risk is determined by the density, the mobility, and the percentage and type of selfish nodes in the network. Figure 6 shows the conceptual relationship between the selfish percentage, density, and partition risk.

Security and mission risk. Selfish behavior in the network is not necessarily malicious in nature, but the effect it has on the network is like a denial-of-service attack, where the important messages do not get to the destination, the routes become unstable, and the control traffic floods the network. Another issue is that selfish and malicious behavior can go hand in hand in the network. This has led to the formulation of danger theory-based immune systems and intrusion detection systems where the non-cooperative behavior is considered a security threat to the network, as shown in [7], [8].

As seen from the above discussion, selfish behavior in the MANET leads to performance degradation in many ways, which are interconnected to each other in some way. This is further supported in the next section using simple analytical models for these different factors.

Table I: Mapping of Selfish Behaviors to Effects and Metrics

Behavior	Effect	Metrics
Forwarding refusal	PDR↓, reachability loss	PDR, PLR, throughput
Selective forwarding	Biased loss patterns	Per-flow PDR, loss bursts
Control drop	Route discovery failure	RREQ/RERR counts, overhead
Delay injection	Delay/jitter↑	Avg delay, jitter
MAC cheating	Unfair access, collisions	Collision rate, fairness

V. CROSS-LAYER EFFECTS AND ANALYTICAL FRAMEWORK

Cross-layer selfishness is a special case to consider because a selfish action in one layer may cause damage to another layer. For instance, MAC-layer selfishness is present if a node changes its contention strategy for the channel to gain more access or to decrease the cost of cooperative retransmissions. These changes increase the number of collisions and delays for neighboring nodes and appear as an inexplicable decrease in total system throughput. In [6], the authors demonstrate that MAC-layer misbehavior is as harmful as network-layer misbehavior because it contaminates the shared medium and introduces a single point of contention for all the neighboring nodes.

The interaction with the transport and the application layers is another source of complexity. Selfishness may trigger packet loss and jitter, which in turn trigger TCP congestion control and retransmission timeouts, reducing the total system throughput and increasing the average delay. For UDP-based video streams, the jitter and loss also reduce the quality of service. Most importantly, the adaptation mechanisms used by the application to counteract the effects of selfishness, for example, by increasing the sending rate to counteract loss, may further increase congestion, creating a vicious circle.

Finally, energy management may also appear as a form of selfishness. In fact, techniques like duty cycling or sleep schedules may be used to optimize energy consumption. In other words, a negative effect analysis must also consider the distinction between rational energy-saving behaviors and actual misbehavior. Dynamic selfishness models [4] explicitly specify the rule for switching from one state to another and clarify the distinction.

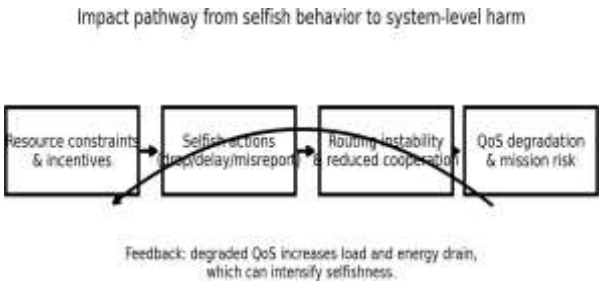

Fig. 3. Impact pathway from selfish behavior to system-level harm.

Analytical models also provide insight into why a small amount of self-centered behavior can lead to a disproportionate amount of damage. Indeed, in a realistic MANET, mobility, interference, and protocol peculiarities are all present, but simple probabilistic models can still show why multi-hop delivery is so sensitive to cooperation.

End-to-end Delivery Probability. We consider a source and destination node connected by a path of h hops. We define p as the proportion of nodes that are selfish. We assume that these selfish nodes will forward a transit packet with a certain probability q (0 <= q <= 1). A simple, but useful, approximation is that each hop in the multi-hop path has a success probability given by (1 - p) + p * q = 1 - p * (1 - q). We then have a simple expression for the end-to-end delivery probability between a source and destination connected by an h-hop path:

$P_{delivery} \approx (1 - p * (1 - q))^h$.

Figure 4 depicts this relationship for a number of different values of q.

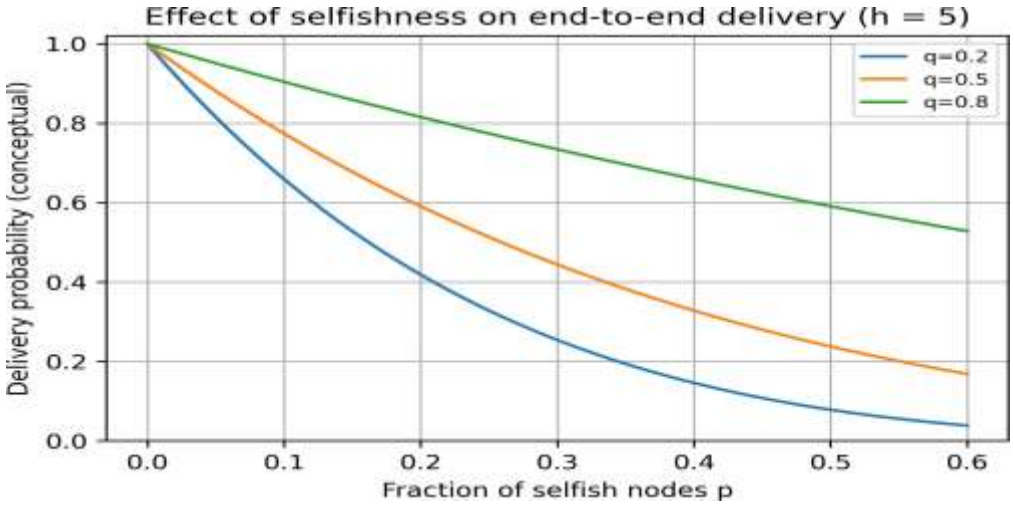

Fig. 4. Conceptual delivery probability vs. selfish-node fraction.

Effective path length and rerouting. When routing through selfish nodes fails, routing protocols may resort to new routes that avoid detected selfish nodes, leading to longer routes that may have more hops. The more hops, the more cumulative loss and delay are incurred. Moreover, more rerouting translates to more control overhead. In this manner, a coupled system emerges where selfish nodes affect delivery, delivery affects routing, and routing drains the very resources that nodes are trying to conserve.

Partition risk. The connectivity of random geometric graphs depends on node density and transmission range. However, selfish nodes reduce effective relay density because they don't forward packets for others. A useful measure of partition risk thus depends on p and inversely on density. Figure 6 depicts a conceptual surface of this idea, showing that transitions can be sharp when cooperative density approaches a percolation threshold.

Interpretation and Limitations. These models are intentionally simple. For example, they don't model spatial clustering of selfish nodes, correlations between nodes, nor protocol-specific tricks like route caching. However, they demonstrate two important truths: first, multi-hop delivery probability drops rapidly with more selfish nodes and more hops, and second, this damage can be exacerbated depending on how routing protocols react to it, e.g., rerouting, retransmissions, and control overheads.

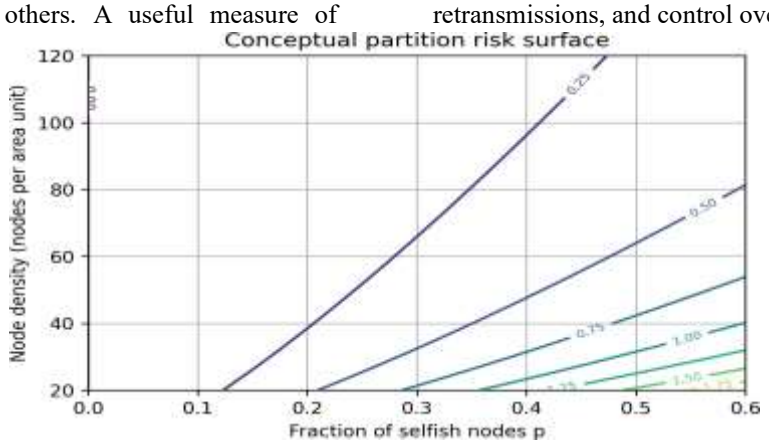

Fig. 6. Conceptual surface of partition risk vs. selfishness and density.

VI. RELATED WORK AND TRENDS

The research literature on selfishness in MANETs follows three lines: quantifying impact, identifying non-cooperation, and providing incentives for cooperation. Some studies quantified the impact of routing misbehavior and introduced watchdog/pathrater concepts to address this issue [1]. However, because these watchdog/pathrater approaches are based on promiscuous listening and are vulnerable to packet collisions or asymmetric links, acknowledgement-based detection approaches such as TWOACK were introduced to detect selfish nodes more reliably [9].

However, reputation-based systems such as CORE and CONFIDANT emphasize social behavior by basing decisions on reputation and observations of other nodes. Selfish nodes are therefore isolated or given lower priority by these systems. However, these systems are plagued by issues such as false accusations and reputation convergence. OCEAN proposed using first-hand observations to reduce trust management complexity. In this system, nodes rely only on their own observations to detect selfish behavior (Bansal & Baker, 2003).

Economic and credit-based systems assume that nodes should pay for service. Buttyan and Hubaux introduced several incentives for cooperation in MANETs. They also proposed several systems that utilize a credit system. The Sprite system introduced a credit system that uses a receipt and a trusted authority. This system prevents selfish nodes from receiving credit for cheated packets. This system recognizes that there are rational reasons for selfish behavior and that networking performance and user utility are related.

Recent research follows these lines of research but incorporates optimization and machine learning. Surveys of detection systems categorize detection systems and emphasize the importance of hybrid systems. Trust-aware clustering and routing protocols are used to identify trustworthy nodes while minimizing overhead. Machine learning approaches are used to differentiate between selfish behavior and packet loss by extracting features from routing statistics, MAC protocol statistics, and other statistics. Security-related research incorporates selfish behavior into intrusion detection systems. This research recognizes that selfish behavior can manifest itself or cause denial-of-service attacks.

Impact studies of selfish behavior demonstrate that selfish behavior causes increased routing overhead and energy consumption. This indicates that system cost should also be used to evaluate selfish behavior detection systems.

VII. METHODOLOGY TEMPLATE

As the manifestation of selfishness is influenced by mobility, density, traffic, and the actual protocol, the experimental scenario must be specified. The following is a flexible template for the study:

Study goals and hypotheses. A basic study could verify the following:

- H1: The more selfish nodes, the lower the packet delivery ratio (PDR).
- H2: The more adverse impact is observed for larger average hop counts.
- H3: Selfish nodes increase the routing overhead more for reactive than for proactive routing.
- H4: Dynamic selfishness based on energy is less detrimental than static selfishness.

Modeling Selfishness. A study must at least implement the following:

- Static selfishness: a node never forwards any packet that is not destined to itself for the entire experiment.
- Dynamic selfishness: a node becomes selfish after its energy falls below a given threshold or when the queue is too long [4].
- Selective selfishness: a node forwards only its own packets or packets from nodes it trusts.
- MAC selfishness (optional): a node manipulates MAC to obtain the channel more often [6].

Protocols and scenarios. Evaluate at least one reactive routing protocol (e.g., AODV or DSR) and one proactive routing protocol (e.g., OLSR) under various mobility models (Random Waypoint, Gauss- Markov, group mobility) and node densities.

Metrics. Identify the basic metrics that should be reported:

PDR and packet loss

End-to-end delay and jitter

Routing overhead: number of control packets or bytes per delivered data packet

Energy per delivered bit and network lifetime: time until X% of nodes run out of energy Fairness: Jain's index for forwarding load or energy depletion

Statistical analysis. Use several random seeds. Provide results as confidence intervals. Avoid over- interpreting results when comparing scenarios: report effect sizes, like percent change over baseline. Avoid over-interpreting results when comparing scenarios: report effect sizes, like percent change over baseline.

Threats to validity. Internal validity threats include unrealistic selfishness models and coding bugs. External validity threats include obstacles in the environment or heterogeneous hardware in deployed networks. Construct validity threats include the choice of metrics that are appropriate for the mission.

Figure 5 shows a workflow template

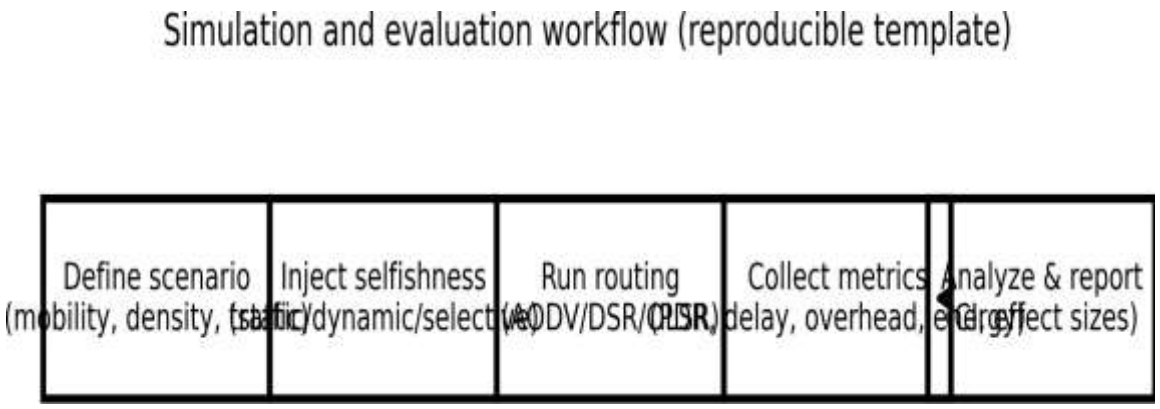

Fig. 5. Simulation and evaluation workflow.

VIII. DISCUSSION, SCENARIOS, AND RECOMMENDATIONS

As a general note, there are a few overarching themes that are clear:

First, selfish behavior causes increased overhead in routing protocols. This is because when there are losses, routing protocols attempt to re-establish routes and re-transmit the messages. However, when there are selfish nodes, this results in an increased number of messages that are ultimately used for nothing, causing an increase in the overall cost at the network level, even if there is an individual benefit at the node level.

Second, the position of the selfish nodes is as critical as their number. Two scenarios with the same number of selfish nodes could have drastically different results depending on their position. This is because, in some cases, the selfish nodes could be in the direction of the most active relays or bridges between clusters. This is why the evaluations should consider different ratios as well as different methods of choosing the nodes.

Third, there are realistic scenarios in which selfish nodes are dynamic. This is because the selfish nodes could be caused by energy constraints or queue overflows. This is realistic because there are devices that tend to fail when there are certain constraints. This also shows that there are intermediate cases that need to be understood to determine whether there is a need for mitigation to avoid any consequences.

Fourth, there are constraints in terms of privacy that need to be considered. This is because there are several detection mechanisms that require the ability to see all the traffic as well as the ability to see all the neighbors. This could be affected by several factors, including encryption, duty cycle, directional antennas, and heterogeneous devices. This could also lead to false accusations, which are also costly in that they could cause several nodes to be taken out of commission.

Finally, there are several applications that are affected in different ways. This is because some networks are used for emergency response, while others are used for IoT. This is why the most significant impact should be determined using utility.

Practical deployments demonstrate the reasons why selfish behavior can be mission-critical to address.

Disaster Response

In a disaster response scenario, first responders use handheld radios or smartphones that create an ad hoc network. Some of the smartphones might choose not to forward packets to save energy for more important voice communication. The worst effects of selfish behavior are the slower delivery of situation reports, lower reachability of command nodes, and increased control traffic that uses precious power.

Tactical Patrol and Reconnaissance

In a tactical mobile ad hoc network, a subset of nodes with high-value tasks might choose not to forward packets to minimize the forwarding overhead and save energy for stealthier operation. If these nodes are placed at bridge positions in the network, selfish behavior can cause the network to fragment into separate squads.

Edge and IoT data collection. In IoT-like MANETs with mobile sensors/drone data collection, a node might not cooperate in relaying data to save its own energy. The negative effect in this case is that there would be incomplete data coverage, which could result in biased data sets.

Design guidelines based on analysis of negative effects:

1) Define mission metrics to assess the impact. In addition to Packet Delivery Ratio, consider delay, jitter, energy per delivered bit, and fairness. The usefulness of a mission might depend on timeliness in addition to reliability.

2) Evaluate the proportion and location of selfish behavior. Randomness might result in an underestimation of impact, especially when compared with the strategic placement of selfish nodes in high centrality locations.

3) Distinguish between legitimate saving behavior and protocol-breaking behavior. Model dynamic behavior in which a node becomes selfish when its energy level crosses a certain threshold and identifies what this threshold is. Compare with benign duty cycle scenarios.

4) Account for costs of mitigating selfish behavior. While detection accuracy is important, consider the overall cost of mitigation (control traffic, energy expenditure, false positives) and whether this reduces partition risk.

5. Use a reproducible methodology. This involves giving details about the simulator version, parameters used, traffic seeds, mobility patterns, and code availability. This is important because selfish behavior is influenced by many factors that are linked together. Although this paper presents negative impacts, mitigation strategies are important because they provide context for why these impacts are important and what they imply. In general, there are five types of defense mechanisms. They are reputation systems such as CORE and CONFIDANT, watchdog and acknowledgment systems such as watchdog/path rater and TWOACK-like systems, incentive systems such as nuggets and Sprite, game theory-based cooperation enforcement mechanisms, and learning-based detection and hybrid security systems. Reputation systems attempt to determine how willing a neighbor is to forward packets and then prefer those with higher reputation [10], [11]. Acknowledgment systems send extra packets to verify that a neighbor is forwarding packets [9]. Incentive systems give rewards for forwarding packets using tokens or micro-payments (Zhong et al., 2003; Buttyan & Hubaux, 2003). Game theory systems use repeated games to design strategies that make cooperation a dominant strategy [15], [16]. Recently, trust-aware routing with optimized clustering and learning-based detection in IoT-MANET scenarios have been proposed [12], [14].

Each method has its own set of costs: monitoring consumes energy, credits have accounting costs, and learning has feature and data acquisition costs. Most importantly, negative effects must be understood to ensure the selection of adequate and proportionate countermeasures to the mission.

IX. LIMITATIONS AND FUTURE WORK

This paper is a general overview and an analytic framework. It is not without limitations: the analytic models used here are simplified and do not fully account for spatial correlations, interference patterns, or specific protocol behaviors. Second, as a general overview, the paper does not present simulation results; rather, it proposes a method and analytic models to follow for empirical analyses. Third, there is a lack of standardization for definitions of selfishness and measurement techniques.

Future work must strive for standardized analytic models for selfishness across simulators and implement reproducible and open-source simulations for the evaluation of detection and incentive mechanisms under realistic mobility patterns and heterogeneous radio behaviors, as well as the joint optimization of detection accuracy and overhead with mission constraints.

X. CONCLUSION

The selfish nodes pose a threat to the very fabric of cooperation in MANETs. The consequences of selfish nodes are not limited to packet drops; they are accompanied by additional consequences of increased end-to-end delays, routing overhead, wasted routing overhead for cooperating nodes, unbalanced traffic distribution, and even partitioning of the MANETs. Because selfish behaviors are, in many cases, rational and can occur in an unpredictable manner, they are difficult to detect, especially because they can be exacerbated by routing protocols that address mobility.

By organizing selfish behaviors into an organized taxonomy, identifying how local selfish behaviors accumulate into system-wide consequences, and providing analytical relationships that demonstrate how system degradation occurs nonlinearly with hop count and cooperative density, this work establishes a strong foundation for rigorous evaluation and design. The methodology template provided within this work establishes a concrete path forward for evaluation studies to measure impacts with various protocols, mobilities, densities, and levels of selfishness. Ultimately, reducing selfish behaviors requires a balanced approach that maximizes cooperation with minimal overhead and no unfair penalty on valid energy conservation behaviors.

REFERENCES

1. Marti et al.'s research paper on mitigating routing misbehavior in MANETs, published at MobiCom 2000 (pages 255-265).
2. Buttyan and Hubaux's research paper on incentivizing cooperation in self-organizing MANETs, published in Mobile Networks and Applications (volume 8, pages 579-592, 2003).
3. Zhong et al.'s research paper on Sprite: a simple, cheat-proof credit-based system for mobile ad hoc networks, published at IEEE INFOCOM 2003.
4. Shan et al.'s research paper on quantitative analysis of energy-cost-driven selfishness in MANETs, published in Sensors (volume 21, issue 3, article 716, 2021; doi:10.3390/s21030716).
5. Vanday Baseri and Fatemidokht's research paper on survey of different methods for detection of selfish nodes in MANETs, published in Journal of Mahani Mathematical Research (volume 11, issue 2, pages 45-59, 2022; doi:10.22103/jmmrc.2022.18626.1180).
6. Kyasanur and Vaidya's research paper on modeling and preventing selfish MAC layer misbehavior in wireless networks, published in IEEE Transactions on Mobile Computing (volume 4, issue 5, pages 502-516, 2005).
7. Jim et al.'s research paper on enhanced security for MANETs using an AIS-based danger theory for detection of selfish nodes, published in Computers & Security (volume 113, article 102538, 2022; doi:10.1016/j.cose.2021.102538).
8. Nirmala Bai et al.'s research paper on design of intrusion detection system using discretion of leading agent and machine learning for efficient MANET

system, published in Scientific Reports (2025; doi:10.1038/s41598-025-89221-8).
9. Here is the text rewritten in a freer, more conversational style, while retaining the same topic and details:
10. Balakrishnan, Deng, and Varshney propose TWOACK as a means to limit selfish behavior in mobile ad hoc networks, published in the proceedings for the IEEE Wireless Communications and Networking Conference in 2005.
11. Michiardi and Molva propose a collaborative reputation system called CORE, meant to enforce cooperation among nodes in mobile ad hoc networks, published in Communications and Multimedia Security (Springer) in 2002, pages 107–121, doi: 10.1007/978-0-387-35612-9_9.
12. Buchegger and Le Boudec evaluate the performance of the CONFIDANT protocol, published in the proceedings for ACM MobiHoc in 2002, doi: 10.1145/513800.513828.
13. Nirmaladevi and Prabha propose a selfish node trust aware approach with optimized clustering for reliable routing in mobile ad hoc networks, published in Measurement: Sensors, vol. 28, article 100680, 2023, doi: 10.1016/j.measen.2023.100680.
14. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00) (pp. 255–265).
15. 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. https://doi.org/10.1007/978-0-387-35612-9_9
16. 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. https://doi.org/10.1038/s41598-025-89221-8
17. Nirmaladevi, K., & Prabha, K. (2023). A selfish node trust aware with optimized clustering for reliable routing protocol in MANET. Measurement: Sensors, 28, 100680. https://doi.org/10.1016/j.measen.2023.100680
18. 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).
19. 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. https://doi.org/10.3390/s21030716
20. 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. https://doi.org/10.22103/jmmrc.2022.18626.1180
21. Varga, A., & Hornig, R. (2008). An overview of the OMNeT++ simulation environment. In Proceedings of the 1st International Conference on Simulation Tools and Techniques (SIMUTools).
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). Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In Proceedings of IEEE INFOCOM 2003.
24. Lupia, A., & Di Rango, F. (2016). A probabilistic energy-efficient approach for monitoring and detecting malicious/selfish nodes in mobile ad-hoc networks. In Proceedings of IEEE Wireless Communications and Networking Conference (WCNC).
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.

APPENDIX

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