An Optimal Auction-Based Routing Scheme for Detecting and Managing Selfish Nodes in Delay-Tolerant Networks

Moirangthem Tiken Singh[1] , N.Hemarjit Singh[2] , Rabinder Kumar Prasad[3] , N K Kaphungkui[4] , Gurumayum Robert Michael[5]

[1,3]Department of Computer Science and Engineering, DUIET, Dibrugarh University, Dibrugarh, India
[2,4,5]Department of Electronic and Communication Engineering, DUIET, Dibrugarh University, Dibrugarh, India
Email: tiken.m@dibru.ac.in[1], nhsingh@dibru.ac.in[2], rkp@dibru.ac.in[3], pipizs.kaps@gmail.com[4], robertmichael@dibru.ac.in[5]

Received: 13.07.2024 Revised: 10.08.2024 Accepted: 28.09.2024

ABSTRACT
Nodes in Delay-Tolerant Networks (DTNs) and other opportunistic networks work collaboratively to ensure efficient message forwarding. The decision of selfish nodes to neither forward nor discard incoming messages had a detrimental effect on the performance of such networks. The focus of this paper was to propose a novel routing scheme for DTNs. This scheme incorporated an optimal auction mechanism which played a crucial role in detecting and managing selfish nodes, ultimately leading to improved efficiency and reliability of the network. Existing detection methods, which encompass neighbor monitoring, acknowledgment, autonomy, reputation, and credit-based approaches, have been found to suffer from drawbacks such as network overhead, trust concerns, and the issue of unreliable data. Within the framework of the proposed auction model, the source node initiated the process by broadcasting a message to its neighboring nodes. This message contained a predefined value, prompting the neighbors to formulate bid strategies that took into account their competence and the costs they would incur for transmitting the bids. The source node made a selection of relay nodes in order to enhance the performance of the network, ensure honesty, and deliver fair rewards. The implementation of this strategy-proof mechanism not only encouraged participants to behave honestly but also effectively deterred any malicious actions and significantly enhanced the overall reliability of the system. Through simulations, it was shown that this method significantly enhanced network performance, detection accuracy, and incentive fairness when compared to the baseline method, ProPhet. In terms of the proposed algorithm, the median delivery ratios varied between approximately 0.6 and 0.7. The median delivery ratios of the ProPhet algorithm ranged from around 0.35 to 0.75.

Keywords: Delay-Tolerant Networks (DTNs), Optimal auction mechanism, Selfish nodes, Routing scheme

1. INTRODUCTION

The primary objective behind the development of Delay-Tolerant Networks (DTNs) [1] is to facilitate effective wireless communication in situations where continuous connectivity or low latency cannot be guaranteed. The main objective behind the design of these networks was to overcome the challenges in a targeted manner. Some common scenarios [2] where these networks are typically found include space exploration [3], which involves the exploration of outer space; disaster recovery, which focuses on providing aid and assistance in the aftermath of natural or man-made disasters [4]; remote sensing, which involves gathering data from a distance using various sensors; and mobile adhoc networks, which are dynamic networks that are formed on the fly without any pre-existing infrastructure [1]. All of these scenarios are characterized by sporadic and opportunistic communication, where communication links may not always be available or reliable. The nature of DTNs dictates that the communication among nodes happens only when they happen to meet, resulting in the formation of dynamic and unpredictable paths for message forwarding [5].

The efficient propagation of messages in DTNs relies heavily on the cooperative behaviour demonstrated by nodes [6]. Each node is responsible for effectively forwarding messages to its neighbouring nodes to facilitate the smooth and efficient flow of data across the entire network. However, the network's overall performance is significantly affected by the existence of selfish nodes that prioritize their data and choose not to forward

messages from other nodes. It is not uncommon to observe selfish behaviours. However, such behaviours are often linked to resource constraints [7], for example, limited battery power, processing capacity, bandwidth, and the varying priorities of individual nodes.

Researchers have put forward a range of strategies to tackle the problem of selfish nodes and identify and minimize their impact. One possible method to exemplify this is by employing neighbour monitoring techniques, such as the Watchdog mechanism [8]. Through the utilization of these techniques, nodes are empowered to actively monitor and evaluate the forwarding of messages by their neighboring nodes, effectively discerning and flagging any nodes that display selfish tendencies. Although this approach has limited effectiveness within specific ranges, it does have the drawback of imposing significant network overhead and necessitating assistance in managing issues like intentional packet dropping. In a different approach, reputation-based mechanisms [9] [10] analyze and distribute trust values to nodes based on their prior behavioral records. Despite the potential benefits, it is essential to acknowledge that these methods come with a hefty resource requirement and can generate apprehensions regarding the manipulation of trust and fairness. Credit-based systems [11], despite their intention to encourage collaboration with the use of virtual currency, ultimately fail due to their failure to recognize the significant implications of energy consumption, particularly in environments where resources are limited.

Despite using different strategies, significant obstacles still hinder the accurate identification and reduction of self-interested nodes, while maintaining optimal network performance. Traditional detection methods often strain the network or overlook the dynamic and unpredictable nature of DTNs. Thus, this paper aims to address several limitations by focusing on the following goals:

1. Develop a new routing scheme: Introduce a novel routing approach to address efficiencyυ issues in network performance.
2. Utilize an optimal auction mechanism: Implement an auction-based model to achieve two keyυ goals:
3. Enhance the accuracy of detecting selfish nodes.
4. Reduce network overhead.
5. Foster collaboration and cooperation: Provide incentives to encourage cooperative behaviorυ among network nodes.
6. Combine detection and incentive strategies: Allow the source node to selectively choose relayυ nodes by integrating detection mechanisms with incentive-based strategies.
7. Minimize the negative impact of selfish nodes: Leverage the auction-based system to mitigateυ the effects of selfish behavior, ensuring fair rewards for cooperative nodes.

The primary objectives of the paper revolve around implementing an optimal auction mechanism, which aims to achieve two key goals: improving the identification of selfish nodes and reducing network overhead. In addition to that, this article also includes incentives that have been specifically designed to promote and encourage collaboration and cooperation among various nodes. By combining detection techniques and incentive mechanisms, the suggested approach enables the source node to have the freedom to selectively decide on relay nodes. Using a model based on auctions, the source node effectively addresses the adverse outcomes that arise when nodes prioritize their own interests over cooperation. This is achieved by the source node actively offering fair incentives to individuals who engage in cooperative behavior.

The remainder of this paper follows this structure: Section 2 offers a comprehensive analysis of various approaches to detecting selfish nodes, classifying them according to their fundamental principles, and discussing their strengths and weaknesses. Section 3 introduces the problem and presents the optimal auction-based routing scheme proposed in this investigation. The results of the simulation are presented in Section 4, which examines how effective the proposed approach is in terms of detection accuracy, network overhead, and overall network performance.

2. LITERATURE REVIEW

The Watchdog mechanism, which involves nodes monitoring the forwarding behaviour of their neighbours, is widely recognized as one of the most effective ways to detect selfish nodes. This mechanism, introduced in [12], tracks whether neighbouring nodes forward messages within a set time. When a node does not forward a message, its fault count increases, and once it surpasses a threshold, the node is labeled as selfish. A variant of the Watchdog, the Collaborative Watchdog Scheme [13], improves upon the original by disseminating information about selfish nodes more rapidly. In [14], the local watchdog detects the selfish node by monitoring transmitted and received packets. The local watchdog informs all nodes about this selfish node,

directly or indirectly. Then, the network isolates the selfish node from the packet transmission. However, watchdog methods struggle with challenges including a limited detection range, network overhead, and the difficulty of identifying misbehaving nodes during fuzzy conflicts or dropped packets because of errors.

An alternative mechanism is a system that relies on acknowledgements. The basis of these methods is that nodes are required to send acknowledgements once they have forwarded data packets. The article [15] states that nodes are obliged to send acknowledgements to the two hops ahead in order to verify message forwarding. Although this method enhances accuracy in detection, it also results in higher network overhead. The authors of [16] present another approach that employs realtime encounter data to track instances of selfish behavior. Despite being effective, these methods often require additional resources due to the frequent need for acknowledgements. Autonomous detection systems rely on historical encounter data to monitor nodes' selfish behavior, using real-time information. For example, the algorithm in [17] uses past encounter data to predict selfishness. Nonetheless, it experiences difficulties due to the unpredictable movements of nodes, potentially resulting in misclassification. An improvement to this method is the RSND algorithm [18], which uses frame analysis and encounter information to enhance detection accuracy. Nonetheless, this strategy disregards the importance of adjusting node behavior based on resource availability, leading to inaccurate assessments.

Reputation-based detection mechanisms assign a dynamic reputation value to each node, which is updated based on its historical forwarding behavior. Nodes with higher reputation values are considered trustworthy, while those with lower values are deemed selfish. For instance, the Core model [19] integrates a reputation system with the Watchdog mechanism to evaluate the trustworthiness of nodes. More recent approaches, such as the one in [20], assess selfishness by monitoring energy usage and contributions of nodes. While reputation-based systems can be effective, they often result in higher network overhead and face challenges related to the subjective nature of reputation values.

In credit-based systems, nodes exchange virtual currency during packet forwarding to incentivize cooperation. Game theory is often integrated into these systems to optimize resource usage and transmission costs. For instance, the scheme in [21] uses a bargaining game to encourage selfish nodes to cooperate by offering virtual currency as compensation.

Similarly, [22] proposes a bargaining game scheme to improve cooperation among nodes. Despite their benefits, credit-based systems often fail to account for energy consumption, which can significantly affect network performance, particularly in resource-constrained environments.

When examining the literature, it becomes evident that the current mechanisms in place possess both strengths and limitations. Although neighbor monitoring-based systems like Watchdog have shown effectiveness, they face difficulties in terms of detection range and overhead. The use of acknowledgment-based schemes has been shown to enhance the reliability of forwarding, however, it does come at the cost of increased overhead. Node mobility can significantly impact the reliability of autonomous detection, making it an unreliable option. However, it is important to note that reputation-based and credit-based approaches, while promising, also bring about their own unique challenges. Among the challenges that need to be addressed, two important ones are the requirement for a robust trust management system and the need to find solutions for concerns related to energy consumption.

This paper, in light of the challenges faced, puts forward a new routing scheme that relies on an optimal auction mechanism [23]. The main focus of this method is to empower source nodes by enabling them to select relay nodes based on selfishness detection. In addition to its other goals, one of the aims of this initiative is to promote cooperation among participants by offering fair incentives Through the use of this approach, the proposed scheme aims to not only enhance network performance but also effectively address the limitations of current mechanisms.

3. The Proposed Method

To address the problem defined in the previous section, this paper proposes a routing scheme for Delay Tolerant Networks (DTNs) using an optimal auction mechanism model. Let be a set representing the neighbors of the source node, encountered in a random order. The source node broadcasts a message with a value to its neighbors .

Any node interested in relaying the message submits a strategy value , where \ represents the bid strategy of node is the node's competency value, and is the transmission cost incurred by node while relaying . The source node then selects one or more relay nodes based on their benefit derived from and assigns them the

message to relay. The valuation for message routing is calculated as where is a cost factor, represents the message length in bytes, and signifies the message's lifetime.
Upon receiving the message from the source, the selected relay node expends effort corresponding to the submitted cost . The nodes that successfully deliver the message to the destination are deemed winners of the relaying auction and receive a reward equal to the corresponding cost. The aim of this auction is represented as the following optimization problem.
Let be a subset of the relay nodes such that . Each relay node submits a valuation to the source. The source node aims to solve the following optimization problem:
where is the battery level of node is the minimum required battery level, is the cache availability of node is the minimum required cache availability, is the selfishness level of node is the maximum allowable selfishness level, is the increment applied to , is the reputation of node , is the decrement applied to is the selfishness level threshold for reputation decrement, is the payment received by node is the base payment amount, represents any additional factor influencing the payment amount, and is a dynamic threshold value used to control the selection of neighbors for message forwarding. The value of depends on the encounter history of the neighbors to ensure an optimal set of neighbors is chosen.
To solve the above optimization problem, we propose a strategy-proof auction model. In this model, when interacting with the source, the relay node submits its information This information is used by the action model to determine the relay nodes for message relaying. Yet, there is unease about the possibility of malicious nodes giving inaccurate information about their type and transmission costs. For example, a node might deceive by exaggerating its type and minimizing transmission costs to obtain more incentives. To guarantee honest behavior from the nodes, we construct the auction mechanism such that the nodes' rewards for their service depend on both their own information and the information of other competing nodes.
In order to ensure truthfulness, the auction model calculates for each submitted by node . When is the minimum benefit among the relay nodes , the benefit for node is given . This benefit is realized solely when node functions as a relay and effectively transmits the message to the destination.
Proposition 1. Submitting truthful type and cost is the only dominant strategy for relay nodes when the source node employs the proposed auction.
Proof: According to the proposed auction model, node with true values is selected only if , and it obtains a benefit such that
(Equation 1)
Equation 1 shows that if other nodes have a lower value than , then has a positive benefit of winning the message relay.
Assuming that node with actual type and cost satisfies , it submits information such that In this case, the actual benefit obtained by node is
(Equation 2)
Equation 2 shows that if other nodes have a higher value than , then has a negative benefit of winning the message relay.
Theorem 1. The proposed auction is a strategy-proof mechanism.
Proof: Based on Proposition 1, truthfully revealing the type and cost is the dominant strategy, confirming the strategy-proof nature of the mechanism.

3.1 Algorithm

This section introduces the algorithm used to simulate and solve the problem defined by the model described in the previous section. It also introduces the performance metrics used to evaluate the performance of the proposed model.
The auction-based routing scheme for Delay Tolerant Networks (DTNs) to solve the defined optimization problem begins by defining the set of neighbors and initializing various parameters, including the cost factor , minimum battery level , minimum cache availability , maximum allowable selfishness level , selfishness level threshold , and a dynamic threshold value . The source node broadcasts a message with a value , calculated as Each neighbor node submits a bid strategy , where represents the competency value of the node and represents the transmission cost. The benefit for each node is then calculated as .

Algorithm 1 Auction-Based Routing Scheme

Require: Set of neighbors $S = \{1, 2, \ldots, n\}$
Require: Parameters: ξ, $B_{\min}$, $C_{\min}$, $\sigma_{\max}$, $\sigma_{\text{threshold}}$, s
Ensure: Optimal relay nodes selection and truthful bidding

Broadcast Message:
$V_m = \xi \times \text{MsgLength}(m) \times \text{MsgTTL}(m)$

Node Bidding:
for each node $i \in S$ **do**
    Node i submits strategy value $\theta_i = (\alpha_i, c_i)$
    Calculate benefit $BV_i = V_m \alpha_i - c_i$
    Append (i, BV_i, θ_i) to bids list
end for

Evaluate Bids:
Sort bids list by BV_i in descending order

Select Relay Nodes:
Initialize $K = []$
Initialize $k = s$
for each (i, BV_i, θ_i) in sorted bids **do**
    if $B_i \geq B_{\min}$ and $C_i \geq C_{\min}$ and $|K| < k$ **then**
        Append (i, BV_i, θ_i) to K
    end if
end for

Adjust Dynamic Threshold:
if encounter history $> \frac{N}{2}$ **then**
    $s = \max(s_{\min}, s - 1)$
else
    $s = \min(s_{\text{initial}}, s + 1)$
end if

return K

The bids are collected and sorted based on the benefit values in descending order. The algorithm then selects the top nodes from the sorted list that meet the battery and cache constraints and . The dynamic threshold is adjusted based on encounter history, where if the encounter history is greater than half the total number of encounters, is decreased; otherwise, it is increased. The pseudocode of the entire process is defined in Algorithm 1.

The optimization problem is then solved to maximize the total benefit from the selected relay nodes, and the selected nodes are assigned the message to relay. For each selected node, if it fails to deliver the message, its selfishness level is increased. If exceeds the threshold , the node's reputation is decremented. Payments are calculated as . Finally, the selected nodes and their payments are returned.

The complexity of the algorithm is dominated by the sorting step, which is . Collecting bids from neighbors is , and selecting relay nodes involves iterating through the sorted list, which is also . The optimization step can vary but is typically . Updating parameters for nodes is , which in the worst case is . Therefore, the overall complexity is .

4. Simulation and Result

4.1 Node Classes

The simulation framework involves the implementation of various node classes to represent different types of nodes in the network. These classes include the , , , and .

The class represents a cooperative node capable of forwarding messages in the network. Each has several attributes such as a unique identifier , competency, transmission cost, cache capacity, battery level, position,

and money. Additionally, it maintains parameters like encounter probability, payment received, successful deliveries, holding time, delivered messages, and reputation. Key methods include calculating deliverability value based on the node's attributes and handling the message delivery process.
The class inherits from the class and represents a node that may exhibit selfish behavior. This class introduces an attribute to quantify the level of selfishness. It overrides the message delivery method to discard packets, reflecting the selfish nature of such nodes. Additional methods include simulating deceptive bidding behavior and adjusting the selfishness level based on the node's current money and reputation.
The class represents a source node that initiates message forwarding. This class has attributes such as a unique identifier , the number of neighbors, a parameter for the maximum number of relay nodes that can be chosen, message value, position, and parameters and for calculating deliverability value. It also includes a base payment for message forwarding and maintains lists for storing relay node values and selected nodes. Key methods include generating unique message identifiers, managing the relay node list, selecting the best relay nodes through an auction process, and handling the payment process after message delivery.
Lastly, the class represents the destination node in the network, characterized primarily by its position. This class is relatively simpler compared to the other node classes, as its primary role is to serve as the endpoint for message delivery
Overall, these node classes provide a comprehensive representation of the different types of nodes in the network, enabling detailed simulation of their interactions and behaviors. To adjust the simulation behavior, the parameters defined in Table 1 are used.

Table 1: Initial Parameters and Their Definitions used in the Simulation

Parameter	Definition
	Maximum number of relay nodes that can be chosen
	Initial threshold value for selecting relay nodes
	Weighting factor for contact ratio in deliverability calculation
	Weighting factor for overall deliverability calculation
	Proportion of selfish nodes in the network
	Factor representing noise in the communication environment
	Probability of packet loss during transmission
	Base payment for message forwarding
	Initial amount of money each node has
	Size of the area in which nodes are positioned
	Total number of nodes in the network
	Maximum range within which nodes can encounter each other
	Value assigned to each message for deliverability calculations

4.2 Performance Metrics

This section defines and discusses the performance metrics used to evaluate the simulation: the delivery ratio and the selfishness level.

4.2.1 Delivery Ratio

The is a critical metric used to assess the effectiveness and reliability of the message delivery system in the network simulation. It is defined as the ratio of the total number of messages successfully received by the

destination nodes to the total number of messages sent by the source nodes. Mathematically, it can be expressed as follows:
A higher delivery ratio indicates better network performance, which means that a larger proportion of messages sent by the source nodes are successfully delivered to the destination nodes. This metric is crucial for understanding the overall reliability and effectiveness of the network, especially in the presence of selfish nodes that may affect the delivery process.

4.2.2 Selfishness Level

The is a measure of the degree to which nodes in the network exhibit selfish behavior. In the simulation, selfish nodes are those that may choose to ignore messages instead of forwarding them, based on their level of selfishness. The selfishness level is initialized to a maximum value and can be adjusted during the simulation based on the node's behavior and interactions. The average level of selfishness of all selfish nodes over time is tracked to analyze its impact on network performance. The average level of selfishness at a given time step is calculated as follows:
where is the number of selfish nodes and is the level of selfishness of the selfish node.
Monitoring the level of selfishness is important to understand how selfish behavior evolves over time and how it influences the delivery ratio and overall network performance. By analyzing these metrics, insights can be gained into the effectiveness of incentive mechanisms and strategies designed to mitigate the impact of selfish nodes.

4.3 Result and Discussion

The simulation framework models and analyzes the behavior of various network nodes, such as cooperative relay nodes, selfish nodes, source nodes, and destination nodes. The behavior of each node type in the network is determined by its specific attributes and methods. The framework utilizes different parameters, including the maximum number of relay nodes , initial threshold for node selection , weighting factors , , and more, to govern the simulation's dynamics. Within a defined area, nodes move and interact with each other based on proximity, using auctions to select the optimal relay nodes for message forwarding. Selfish nodes are made to exhibit deceptive behaviors, affecting the overall network performance. The simulation collects and analyzes results to understand metrics like payment received, successful deliveries, holding times, delivery ratios, and changes in selfishness levels over a specified number of time steps. By using this framework, one can closely study the interactions between nodes and the efficiency of networks across various conditions.

4.3.1 Existing Models

In this simulation analysis, performing various routing algorithms in the presence of malicious nodes was evaluated. The delivery ratio and the delivery cost were the primary metrics used for this evaluation. The delivery ratio (Figure 1) represents the proportion of successfully delivered messages, while the delivery cost (Figure 2) shows the resources spent to achieve successful deliveries. The algorithms considered included Direct, Epidemic [24], PRoPHET [25], SimBet, SimBetTS [26], Bubble [27], SW, and LSFSW [28].

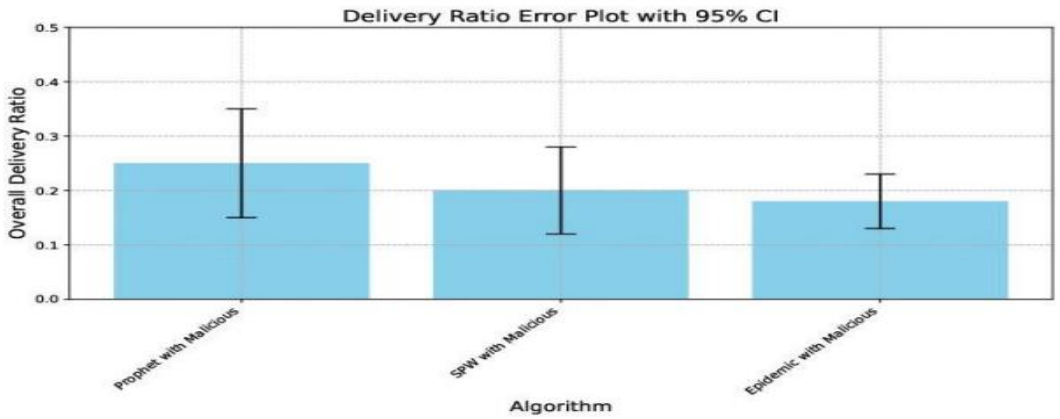

Figure 1. Delivery Ratio Error Plot with 95% CI

Figure 2. Delivery Ratio Comparison between different Algorithms

Among these algorithms, PRoPHET emerged as the most suitable baseline for comparison due to its balanced performance. PRoPHET exhibited a moderate delivery ratio (~0.25) with a reasonable level of variability, indicating consistent performance across different scenarios. Although Epidemic had a slightly lower delivery ratio (~0.18), it incurred the highest delivery cost, which increased linearly with the malicious ratio, making it less cost-efficient. On the other hand, SPW showed a similar delivery ratio (~0.2) to PRoPHET but with narrower variability, suggesting less adaptability in varying network conditions.

PRoPHET's delivery cost was moderate and increased at a manageable rate with the malicious ratio, contrasting sharply with Epidemic's steep cost increase. Compared to other algorithms like SimBet, SimBetTS, Bubble, SW, and LSFSW, PRoPHET maintained a competitive balance between delivery success and resource expenditure. This made PRoPHET a more practical and reliable choice for environments with varying degrees of malicious node presence.

Therefore, based on the simulation results, PRoPHET was justified as the baseline algorithm for comparison. It provides a comprehensive reference point, balancing both delivery ratio and cost, making it a robust standard for evaluating the performance of new or proposed routing algorithms in malicious environments.

4.3.2 Performance Comparison between Proposed Algorithm and ProPhet

The analysis of the delivery ratios (Figure 3) and cost of delivery (Figure 4) for the proposed and ProPhet algorithms across varying selfish ratios and using the parameters defined in Table 2, provides significant insights into their performance

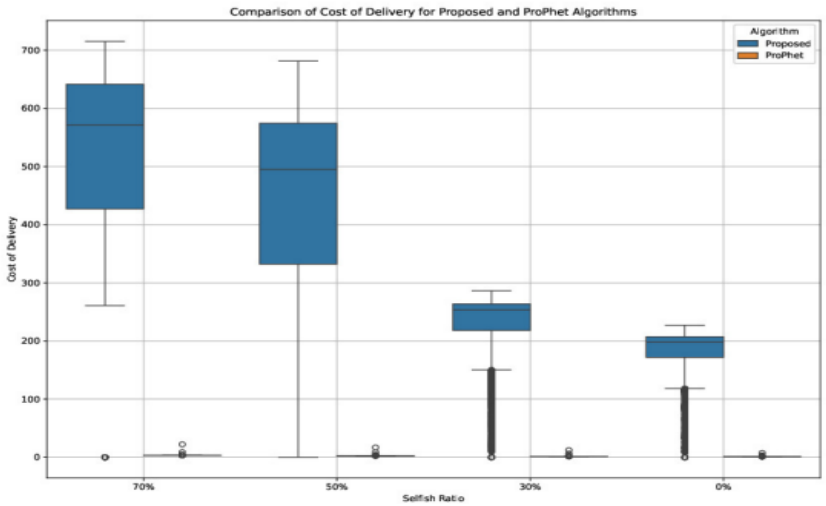

Figure 3: Comparison of delivery ratio between Proposed Algorithm and ProPhet

Table 2: Parameters used in the simulation

The ProPhet algorithm consistently maintains low delivery costs across all selfish ratios, with costs remaining close to zero regardless of the proportion of selfish nodes. In contrast, the proposed

Figure 4. Comparison of Cost of delivery between Proposed Algorithm and ProPhet

algorithm exhibits higher delivery costs, particularly at higher selfish ratios, but these costs decrease as the selfish ratio decreases, indicating an improvement in efficiency as the network becomes less selfish. The higher costs associated with the proposed algorithm can be attributed to the increased number of relay nodes and the behavior of selfish nodes, which drop packets when acting as relay nodes. These selfish nodes cause packets to be repeatedly dropped until they decide to improve their reputation and gain monetary benefits, leading to increased delivery costs.

When examining delivery ratios, the proposed algorithm generally achieves higher delivery ratios compared to ProPhet at higher selfish ratios, with a median delivery ratio of around 0.6 at 70\% selfish ratio, while ProPhet maintains a lower delivery ratio of about 0.4. However, as the selfish ratio decreases, the delivery ratio for the proposed algorithm also diminishes, while the ProPhet algorithm shows a significant increase in delivery ratio, especially at a 0\% selfish ratio, where it reaches around 0.8.

In summary, the ProPhet algorithm demonstrates superior stability and cost-effectiveness, particularly excelling in environments with low or zero selfish ratios. It maintains low delivery costs and improves its delivery ratio as the network becomes more cooperative. On the other hand, the proposed algorithm is more effective in scenarios with a higher presence of selfish nodes, offering better delivery ratios despite higher costs. This makes the proposed algorithm more suitable for networks where maximizing delivery ratios in the presence of selfish behavior is crucial, whereas the ProPhet algorithm is preferable for minimizing costs and achieving stable performance in less selfish or more cooperative network conditions.

To understand how the behavior of selfish nodes changes when controlled by a rational agent, this paper explores the evolution of selfishness levels over simulation time. Figure 5 depicts the average selfishness levels for initial ratios of 70%, 50%, 30%, and 0%. At 70% and 50% initial selfish ratios, the selfishness starts near 1.0, indicating high selfish behavior, and rapidly declines initially. The decline is steeper for the 70% ratio. After the initial drop, the selfishness levels stabilize around 0.6 with minor fluctuations. For the 30% ratio, the initial selfishness is lower and decreases less sharply, stabilizing slightly above 0.5. The 0% ratio remains at 0, as expected, showing no selfish behavior. This analysis shows that higher initial selfish ratios lead to higher initial selfishness, which then declines and stabilizes around 0.5 to 0.6, while the 0% ratio remains unchanged.

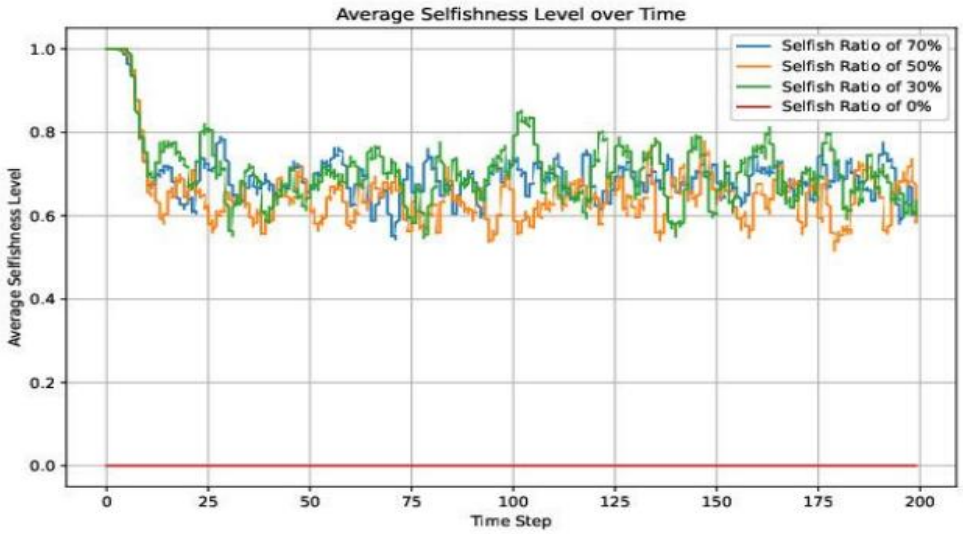

Figure 5. Average Selfishness Level over Time for Different Selfish Ratios

The simulation framework evaluates the behavior of various network nodes, including cooperative and selfish nodes, within a defined area using auctions to select relay nodes for message forwarding. Among the algorithms analyzed (Direct, Epidemic, PRoPHET, SimBet, SimBetTS, Bubble, SW, and LSFSW), PRoPHET served as the baseline due to its balanced performance in delivery ratio and cost. Compared to PRoPHET, the

proposed algorithm showed higher delivery costs, especially at higher selfish ratios, but achieved better delivery ratios under such conditions. PRoPHET maintained low delivery costs and improved delivery ratios in cooperative environments. The selfishness analysis indicated higher initial selfishness levels for higher initial selfish ratios, which declined and stabilized over time. In conclusion, PRoPHET excels in minimizing costs and achieving stable performance in less selfish environments, while the proposed algorithm is more effective in maximizing delivery ratios in the presence of selfish behavior.

5. CONCLUSION

This paper presented an auction-based routing scheme for Delay Tolerant Networks (DTNs) aimed at optimizing the selection of relay nodes under various network conditions. The proposed algorithm dynamically adjusts to the behavior of selfish nodes, ensuring efficient message delivery even in challenging environments. Through simulations, the performance of the proposed algorithm was compared with the widely-used PRoPHET algorithm across different selfishness ratios.

The methodology involved defining the set of neighbors and initializing critical parameters such as cost factor, battery level, cache availability, and selfishness thresholds. The algorithm evaluated bids based on competency values and transmission costs, ensuring the optimal selection of relay nodes. The dynamic threshold adjustment mechanism further refined the relay node selection process by considering encounter histories, thus enhancing adaptability to changing network conditions.

Simulation results demonstrated that the proposed algorithm significantly improves the delivery ratio, particularly in networks with higher selfish ratios, albeit at a higher delivery cost compared to PRoPHET. The proposed algorithm achieved a median delivery ratio of around 0.6 at a 70\% selfish ratio, outperforming PRoPHET's delivery ratio of about 0.4. However, in environments with lower or zero selfish ratios, PRoPHET exhibited superior stability and cost-effectiveness, with delivery ratios reaching around 0.8.

The analysis of selfishness levels over time revealed that higher initial selfish ratios led to a rapid decline and eventual stabilization around moderate selfishness levels. This dynamic adjustment underscores the robustness of the proposed algorithm in mitigating the impact of selfish behavior.

In conclusion, the proposed auction-based routing scheme offers a viable solution for improving message delivery in DTNs, particularly in scenarios with a high presence of selfish nodes. While PRoPHET remains a cost-effective choice for more cooperative networks, the proposed algorithm provides a valuable alternative for maximizing delivery ratios in challenging environments.

Future research could explore several directions to further enhance the proposed routing scheme. One promising approach is the use of machine learning techniques to predict node behavior and optimize bid evaluation and relay selection processes. By integrating machine learning, the algorithm's efficiency and robustness could be significantly improved. Addressing this research direction would allow the proposed routing scheme to be further refined and adapted to meet the evolving demands of DTNs, ensuring efficient and reliable communication in various network environments.

REFERENCES

[1] G. Koukis, K. Safouri and V. Tsaoussidis, "All about Delay-Tolerant Networking (DTN) Contributions to Future Internet," Future Internet, vol. 16, p. 129, 2024.

[2] A. Castillo, C. Juiz and B. Bermejo, "Delay and Disruption Tolerant Networking for Terrestrial and TCP/IP Applications: A Systematic Literature Review," Network, vol. 4, p. 237–259, 2024.

[3] R. Dudukovich, D. Raible, B. Tomko, N. Kortas, E. Schweinsberg, T. Basciano, W. Pohlchuck, J. Deaton, J. Nowakowski and A. Hylton, "Advances in High-rate Delay Tolerant Networking On-board the International Space Station," in IEEE Space Mission Challenges for Information Technology-IEEE Space Computing Conference (IEEE SMC-IT/SCC), 2024.

[4] Z. T. AlAli and S. A. Alabady, "Techniques and methods for managing disasters and critical situations," Natural Hazards, vol. 120, p. 6943–6989, 2024.

[5] S. Prasanna, M. R. Lenka and A. R. Swain, "A Survey on Routing Protocols for Disaster Management," SN Computer Science, vol. 5, p. 216, 2024.

[6] P. R. Makawana, S. Jambukia and P. Trivedi, "Secured Routing Approaches to Mitigate Various Attacks in DTN: A Survey," in International Conference on Smart Computing and Communication, 2024.

[7] G. U. Rehman, M. I. U. Haq, M. Zubair, Z. Mahmood, M. Singh and D. Singh, "Misbehavior of nodes in IoT based vehicular delay tolerant networks VDTNs," Multimedia Tools and Applications, vol. 82, p. 7841–7859, 2023.

[8] M. Preetha and S. Sugitha, "Identifying selfish nodes using mutual neighbor based watchdog mechanism for DTN," in 2016 International Conference on Information Communication and Embedded Systems (ICICES), 2016.
[9] R. Sharma and S. K. Dinkar, "Selfish node detection by modularized deep nmf autoencoder based incentivized reputation scheme," Cybernetics and Systems, vol. 54, p. 1172–1198, 2023.
[10] X. Zhang, H. Deng, Z. Xiong, Y. Liu, Y. Rao, Y. Lyu, Y. Li, D. Hou and Y. Li, "Secure routing strategy based on attribute-based trust access control in social-aware networks," Journal of Signal Processing Systems, p. 1–16, 2024.
[11] A. Sharma, N. Goyal and K. Guleria, "Performance optimization in delay tolerant networks using backtracking algorithm for fully credits distribution to contrast selfish nodes," The Journal of Supercomputing, vol. 77, p. 6036–6055, 2021.
[12] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, New York, NY, USA, 2000.
[13] E. Hernández-Orallo, M. D. S. Olmos, J.-C. Cano, C. T. Calafate and P. Manzoni, "A Fast Model for Evaluating the Detection of Selfish Nodes Using a Collaborative Approach in MANETs," Wireless Personal Communications, vol. 74, pp. 1099-1116, February 2014.
[14] B. V. Sherif and P. Salini, "Detection and Isolation of Selfish Nodes in MANET Using Collaborative Contact-Based Watchdog with Chimp-AODV," Wireless Personal Communications, vol. 128, p. 1373–1390, 2023.
[15] K. Balakrishnan, J. Deng and V. K. Varshney, "TWOACK: preventing selfishness in mobile ad hoc networks," in IEEE Wireless Communications and Networking Conference, 2005, 2005.
[16] K. Liu, J. Deng, P. K. Varshney and K. Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Transactions on Mobile Computing, vol. 6, pp. 536-550, 2007.
[17] G. Bigwood and T. Henderson, "IRONMAN: Using Social Networks to Add Incentives and Reputation to Opportunistic Networks," in 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, 2011.
[18] X. Xiao, Y. Li, X. Kui and A. V. Vasilakos, "Assessing the Influence of Selfishness on the System Performance of Gossip-Based Vehicular Networks," Wireless Networks, vol. 20, pp. 1795-1805, October 2014.
[19] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," in Advanced Communications and Multimedia Security: IFIP TC6 / TC11 Sixth Joint Working Conference on Communications and Multimedia Security September 26–27, 2002, Portorož, Slovenia, B. Jerman-Blažič and T. Klobučar, Eds., Boston, MA: Springer US, 2002, p. 107–121.
[20] M. Fayaz, G. Mehmood, A. Khan, S. Abbas, M. Fayaz and J. Gwak, "Counteracting Selfish Nodes Using Reputation Based System in Mobile Ad Hoc Networks," Electronics, vol. 11, 2022.
[21] O. Nazih, N. Benamar and M. Younis, "An evolutionary bargaining-based approach for incentivized cooperation in opportunistic networks," International Journal of Communication Systems, vol. 33, p. e4377, 2020.
[22] L. Li, Y. Qin and X. Zhong, "A Novel Routing Scheme for Resource-Constraint Opportunistic Networks: A Cooperative Multiplayer Bargaining Game Approach," IEEE Transactions on Vehicular Technology, vol. 65, pp. 6547-6561, 2016.
[23] Y. Chen, A. Hu and J. Zhang, "Optimal auction design with aftermarket Cournot competition," Games and Economic Behavior, vol. 145, p. 54–65, 2024.
[24] A. Vahdat and D. Becker, "Epidemic Routing for Partially-Connected Ad Hoc Networks," 2000.
[25] A. Lindgren, A. Doria and O. Schelén, "Probabilistic Routing in Intermittently Connected Networks," in Service Assurance with Partial and Intermittent Resources, Berlin, 2004.
[26] E. M. Daly and M. Haahr, "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs," IEEE Transactions on Mobile Computing, vol. 8, pp. 606-621, May 2009.
[27] S. Xia, M. Jin, H. Wu and H. Zhou, "Bubble routing: A scalable algorithm with guaranteed delivery in 3D sensor networks," in 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012.
[28] T. Spyropoulos, K. Psounis and C. S. Raghavendra, Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks, 2005.