Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission in Mobile Ad hoc Networks

A Seminar Report Submitted by

Emmanuel Joshy
(4NM20CS069)

UNDER THE GUIDANCE OF

Dr. Rajalaxmi Hegde
Assistant Professor GD III

&

Mr. Akhilraj V. Gadagkar
Assistant Professor GD II

in partial fulfillment of the requirements for the award of the Degree of

Bachelor of Engineering in
Computer Science & Engineering

from

Visvesvaraya Technological University, Belagavi

NITTE EDUCATION TRUST

N.M.A.M. INSTITUTE OF TECHNOLOGY
(An Autonomous Institution affiliated to Visvesvaraya Technological University, Belagavi)
Nitte – 574 110, Karnataka, India

(ISO 9001:2015 Certified), Accredited with 'A' Grade by NAAC
☎: 08258 - 281039 - 281263, Fax: 08258 - 281265

Department of Computer Science and Engineering

September 2023

NITTE
EDUCATION TRUST

N.M.A.M. INSTITUTE OF TECHNOLOGY
(An Autonomous Institution affiliated to Visvesvaraya Technological University, Belagavi)
Nitte – 574 110, Karnataka, India
(ISO 9001:2015 Certified), Accredited with 'A' Grade by NAAC
☎: 08258 - 281039 – 281263, Fax: 08258 – 281265

Department of Computer Science and Engineering
B.E. CSE Program Accredited by NBA, New Delhi from 1-7-2018 to 30-6-2021

CERTIFICATE

Certified that the Seminar entitled

GAME THEORY-BASED STRATEGIC APPROACH TO ENSURE RELIABLE DATA TRANSMISSION IN MOBILE AD HOC NETWORKS

is a bonafide work carried out by

Emmanuel Joshy (4NM20CS069)

in partial fulfilment of the requirements for the award of

Bachelor of Engineering Degree in Computer Science and Engineering
prescribed by
Visvesvaraya Technological University, Belagavi during the year
2023-2024.
It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library.

The seminar report has been approved as it satisfies the academic requirements in respect of the seminar work prescribed for the Bachelor of Engineering Degree.

SEMESTER ASSESSMENT

Name of the Coordinators **Signature with Date**

1. ______________________________

2. ______________________________

ACKNOWLEDGEMENT

The satisfaction that accompanies the completion of any task would be incomplete without the mention of all the people, without whom this endeavor would have been a difficult one to achieve. Their constant blessings, encouragement, guidance and suggestions have been a constant source of inspiration.

First and foremost, my sincere gratitude to my project guide ,**Dr. Rajalaxmi Hegde** and **Akhilraj V. Gadagkar** for their constant guidance throughout the course of this seminar and for the valuable suggestions.
I thank my parents for their unconditional encouragement and support.

I heartily thank our H.O.D, **Dr. Jyothi Shetty**, Department of Computer Science and Engineering, for his guidance and suggestions.

My sincere thanks to our beloved principal, **Dr. Niranjan N Chiplunkar** for giving me an opportunity to carry out this seminar and also sincere thanks for providing all needed facilities.

Finally, thanks to staff members of the Department of Computer Science and Engineering and our friends for their honest opinions and suggestions throughout the course of this seminar.

Emmanuel Joshy

ABSTRACT

The Mobile Ad-Hoc Network (MANET) incorporates a collaborative networking scenario, where dynamic host movement results in frequent topology changes. In MANET, nodes cooperate during route establishment, and the data packet must travel from source to destination through multi-hop intermediate links. The nodes in a MANET can be localized in a restricted zone, where manual intervention to set-up fixed infrastructural support is practically infeasible. However, cooperative packet forwarding and data transmission is quite a common scenario in the context of MANET. Still, due to dynamic topological changes, weak, intermittent links appear within one-hop communication. This leads to a higher possibility of packet drop events and also increases the retransmission scenario, which affects the energy performance of the network. Addressing this issue, the study models a novel and intelligent packet forwarding approach based on the game theory, where trust evaluation in terms of node reputation factor also plays a very vital role.

The approach also enforces an incentive modelling to stimulate the cooperation between mobile nodes during the MANET routing scenario. The system is designed and developed with evolutionary game perspectives to meet the Quality of Services (QoS) requirements. The experimental analysis supports the proposed modelling design aspects. Also, it exhibits that the reputation and trust-based game increases the utility of packet-forwarding strategy with high throughput and negligible network overhead.

TABLE OF CONTENTS

Chapter 1
INTRODUCTION

Mobile Adhoc Networks (MANETs) refer to a special type of wireless ad-hoc network, where nodes are mostly mobile and move independently in any direction with self-organizing capabilities. The key-features of MANET include its dynamic characteristics due to node mobility and also decentralized networking scenarios where the network forms for a temporary interval of time to accomplish a specific task. The term decentralized means that the network formation during the communication scenario does not incur dependency on pre-existing communication infrastructural backbones.

MANET includes a wide range of use-cases, like military communications, disaster management in restricted human areas, etc. The trend of the emphasized research in MANET is mostly concerned about the timely execution of the task with reliable data transmission and reception even if unreliable radio-link is present during the communication scenario. A cooperative event of packet-forwarding is a modern approach to ensure the time-dependent high-throughput curve in MANETs. However, encouraging the other nodes in the MANET environment for packet forwarding for an individual node’s self-interest is a very challenging task. If intermediate nodes are not appropriately chosen during the route-set up and packet forwarding between source to the destination node, then the possibility of intermittent link-breakage between one-hop neighbours increases.

Further, the unreliable communication link also increases the probability of packet drops and retransmission events. This means the utility factor of different packet forwarding strategies will go down and also will affect the energy and throughput performance in MANET eventually. From the security viewpoint also, the cooperative packet forwarding strategies should be robust and flexible enough to deal with every possible route change and also adhere to the communication protocol directions without compromising the QoS and energy parameters.

However, the traditional packet forwarding approaches are shrouded with a set of design limitations and fail to stimulate selfish nodes to cooperate in communication. The prime reasons can be that in MANET, most of the mobile nodes usually operate with limited energy and memory capacity. This makes a node to become self-centered, and that way, it only participates in communication when it brings the node more benefits for its interest than cost. This way, the possibility of the presence of self-centered nodes set amid the other crucial networking components leads to disruption of the overall communication and network performance from both energy and security view-point. Therefore, by addressing the design loopholes in the traditional data forwarding approaches, the proposed study realizes that it is essential to design a mechanism that can effectively encourage a node in packet forwarding even if the transmission happens through unreliable links. This way, a high throughput success rate is envisioned with maximum packet-delivery ratio.

The mechanism jointly incorporates the game mathematical model along with a trust-based reputation evaluation strategy to increase the utility factor of packet forwarding schema. During the packet forwarding instances, trustworthiness of each node is validated and it also enforces cooperative rewards. The attack-resistant security modeling framework is formulated and evaluated with respect to baseline approaches, and the performance metric for validation includes energy, throughput, network burden, and also the rate of successful packet forwarding.

Chapter 2
LITERATURE REVIEW

This section explores the most significant and related literature, which is studied for the investigational analysis purpose. Further, it outlines the research problem that corresponds to the design limitations of the existing system.

Evolutionary game theoretical concept: The experimental analysis shows that the evolutionary game theoretical approach is most popular since through mathematics, it can analyze the strategic interactions among the MANET decentralized nodes, which act as decision-making agents. The authors in introduced a non-cooperative game modelling to defend different attack scenarios in MANETs. The system model incorporated a novel intrusion detection mechanism where actions between a pair of the attacker and regular nodes are considered as a non-cooperative and non-zero game. Authors in also proposed a similar approach to defend against maximum possible lethal security threats in MANET. The study of authors in also directed their research towards cross-layer optimization. For this purpose, it has incorporated a game theory-based approach to improve the communication scenario in vehicular networks. Similarly, authors in also improvised a cooperative game theoretical approach to alleviating the communication performance of MANETs by identifying the misbehaving nodes.

Incentive-based conceptual mechanism: For many years, there have been various research approaches to strengthen the cooperative packet-forwarding policies in MANET where incentive-based mechanisms encouraged self-centered nodes to behave like a normal node and participate in collaborative forwarding schema. In MANET, it is mostly observed that a regular node forwards self-generated data packets as well as of other nodes regardless of its resource utilization factor. On the other hand, a self-centered node or malicious node will tend to drop the data packets to reserve as much resources as possible to accomplish its intended task. This non-cooperative intention, in the long run, affects the communication performance from reliability and efficiency points of view. This incurs a situation where the network becomes susceptible to various forms of lethal attacks. The incentive-based strategies are classified into three major categories, which can be shown in the figure. Virtual currency solutions include tamper-proof hardware, trusted thirty party, etc. Reputation value-based approaches can either be global reputation-based systems or local reputation based systems. Game theory-based solutions find categorization into one-stage game or repeated game.

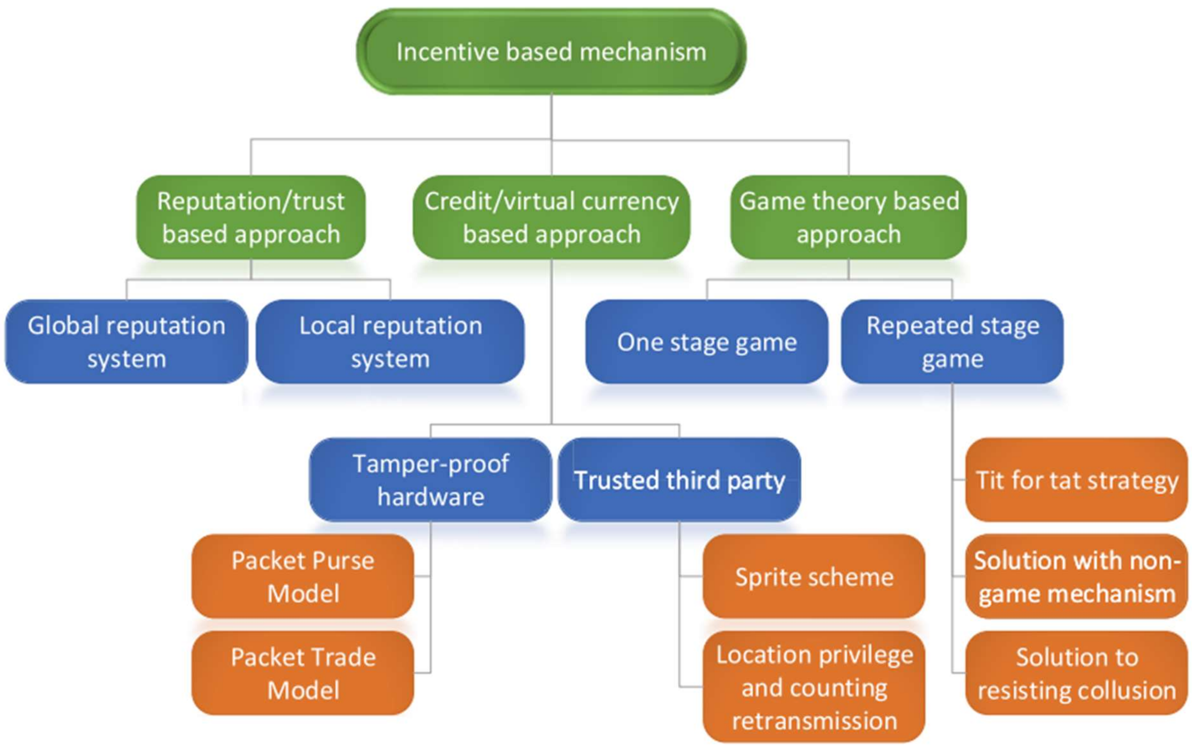


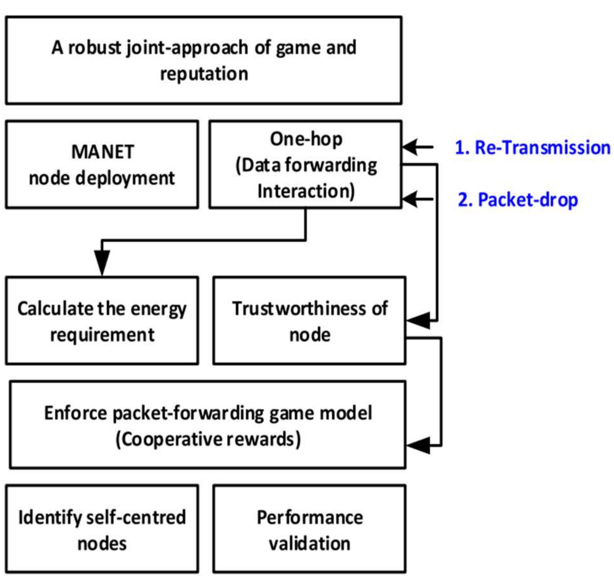
Figure 1 Classification of Incentive-based mechanism.

Chapter 3
PROBLEM DEFINITION

Mobile Ad hoc Networks (MANETs) are characterized by their dynamic and decentralized nature, making them challenging for reliable data transmission and efficient network operation. In these networks, nodes are often self-centered and may not cooperate readily. The problem is exacerbated by the presence of unreliable communication links and limited energy and memory resources in mobile nodes. Thus, the primary problem is to design a strategic approach that leverages game theory principles to incentivize nodes to cooperate in data transmission while considering energy constraints and network reliability in the context of evolving MANETs.

Chapter 4
IMPLEMENTATION

The study in this paper introduces a novel intelligent packet-forwarding strategy based on an evolving game model, which stands out due to its unique design approach. This strategy is formulated analytically and combines two key elements: assessing the likelihood of packet drops and calculating a reward factor based on node reputation. By doing so, the approach effectively identifies self-centered nodes within the MANET and encourages their cooperation in packet forwarding. Additionally, the game formulation is designed to manage and control individual node energy consumption during data transmission. Figure below provides a visual overview of the proposed concept, illustrating its architectural block-based structure.



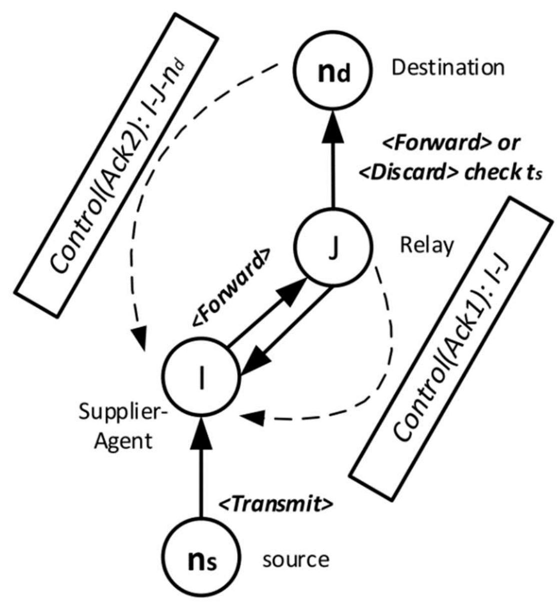


Figure 3 A packet forwarding instance between two nodes < ns, nd >

Figure 2 Block-based architectural overview of the formulated approach.

A. Algorithm:

1. **Input:** n_s, n_d, *Area (A)*, t_s
2. **Output:** *Cooperative msg transmission*
3. **Start**
4. **MANET node deployment with** $\rho(v, e)$
5. $\overrightarrow{m_n}$ **(count)= (400-900)**
6. **Enable mobility-model**
7. **for each time instance** (t_i)
    a. **select the subset of** $\overrightarrow{m_n}$
    b. $< n_s, n_d -> Ex(r_{Table})$
    c. **If**$E(n_r)$ $>$*cut-off*
        i. **Set counter(p) and transmit** *msg* **till** p^{th} **interval**
        ii. **Ensure control** (*Ack1*)**, control** (*Ack2*) **received**
        iii. **Relay(***msg***) transmission success.**
        iv. **Update** r_{Table} **of**SA**(I) and Relay (J)**
    d. **Else if control** (*Ack1*) **not received**
        i. **counter(p) = p** $< t_s$**, p++**
    e. **Else if control** (*Ack2*) **not received**
        i. **relay dropped packet**
        ii. **Update** r_{Table} **of Relay (J)**
    f. **Else**
        i. **End Transmission**
    g. **End**
8. **End**

B.Methodology:

The study focuses on Mobile Ad hoc Networks (MANETs), where self-organizing nodes communicate through intermediate relays, and successful communication depends on cooperative interactions among these nodes.

Cooperative packet forwarding involves an adjacent neighbor (I) helping forward data from the source node (ns) to the nearest intermediate hop (J). J can choose to accept the request, take action (AF) to forward the packet, or act selfishly (AD) and drop the packet. Reputation plays a crucial role, as nodes assisting in forwarding gain rewards, while selfish nodes lose reputation.

Notation (Symbolic)	Description
m_n	Mobile node
t_s	Timestamp for packet re-transmission
n_s	Source node
n_d	Destination node
n_r	Relay node
$'msg'$	Control message
SA	Supplier agent
A_D	Node's action of reject (Declining)
A_F	Node's action of forward (Cooperating)
r_{Table}	Reputation table
t_i	Discrete time interval
d_c	Cost of successful data transmission

Figure 4 Notation Table

The procedure of message forwarding operates within a graph (ρ(v, e)), where pairs of nodes (<SA, nr>) are involved in communication. These pairs are selected for routing and packet forwarding at each time-slot, with one node acting as an intermediate SA and the other as nr.

Node reputation and trustworthiness are evaluated during the packet retransmission process. The system uses a novel threshold mechanism (ts) to limit retransmission and conserve energy.

The system incorporates an evolutionary one-hop packet forwarding game model to encourage cooperation and assess node trustworthiness. The game involves actions like AF for cooperation and AD for selfish behavior.

Pay-off calculations determine node actions based on the probability of each action's gain. Cooperative nodes receive rewards for forwarding packets, which encourages maximum node participation.

Pay-off allocation	I	J	n_d
I	r-pow	r- (I, J)	r- (I, n_d)
J	r- (J, I)	r-pow	r- (J, n_d)
n_d	r- (n_d, I)	r- (n_d, J)	r-pow

The study includes an experimental evaluation comparing the proposed approach with baseline solutions, showing improved packet forwarding performance in terms of energy, throughput, and delay.

The proposed approach offers a balance between energy efficiency and performance in dynamic MANET environments, utilizing reputation tables and introducing the concept of bounded retransmission counts.

The study suggests the potential for machine learning applications to predict node behavior and optimize network performance further.

Cooperative and collaborative reward policies incentivize nodes to select the AF action, ultimately minimizing packet loss rates and improving channel reliability.

The proposed approach is compared to existing solutions, including repeated game, stochastic game, no-cooperation, and bargaining strategies, to validate its performance.

The successful transmission probability for the maximum limit of ts can be computed using :

$$\mu = 1 - (1 - \nu)^\wedge t_s$$

The study also indicated the cost of successful data transmission with dc and that could be computed with respect to the number of packet retransmission count with 1 ≤ p ≤ ts . Here, the dc can be derived using :

$$\sum \Phi_k \{p \mid p \leq t_s\} .g_{pay-off} (I)_k$$
$$= \sum \Phi \{p \mid p \leq t_s\} .g_{pay-off} (J)$$

The pay-off calculation is done depending upon the probability of each node and their respective gain gpay−off. If both I and J opt the AF, then, in that case, the total pay-off can be computed using:

$$d_c = \sum p \times t_s \times \Phi\{p|p \leq t_s\}$$

Chapter 5
RESULTS AND DISCUSSION

The experimental outcomes were obtained through simulations in MATLAB, showcasing the system's achievement of research targets, including reducing network load and efficient energy utilization while maintaining high throughput without delay compromise.

Figure 4 illustrates comparative communication burden outcomes, with the proposed system showing reduced network burden through reputation updating and assessment, efficient utilization of computational and network resources, and bandwidth.

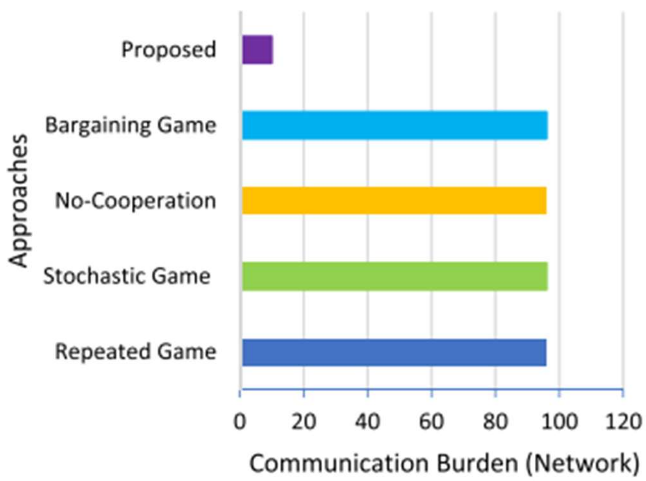


Figure 5 Analysis of network burden in variable traffic condition in Mbps

Figure 5 presents the cost of energy consumption, demonstrating that the proposed approach significantly reduces energy consumption compared to other conventional baseline models, with approximately 50 J of energy consumption.

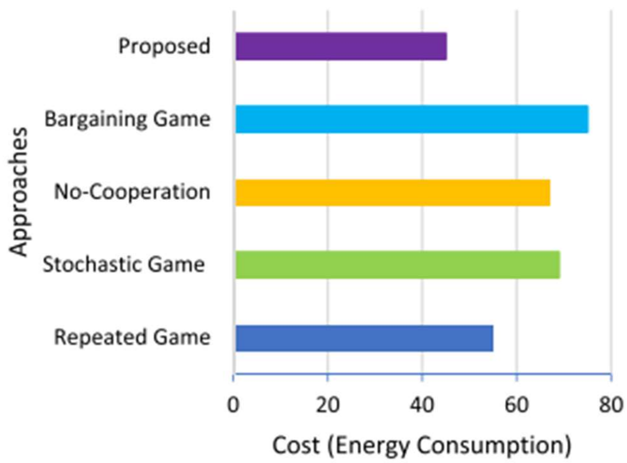


Figure 6 Analysis of cost of energy in Joule (J)

Figure 6 and 7 showcase throughput and rate of packet drops, with the proposed approach achieving approximately 30% improvement in throughput performance and lower packet drop rates compared to existing methods.

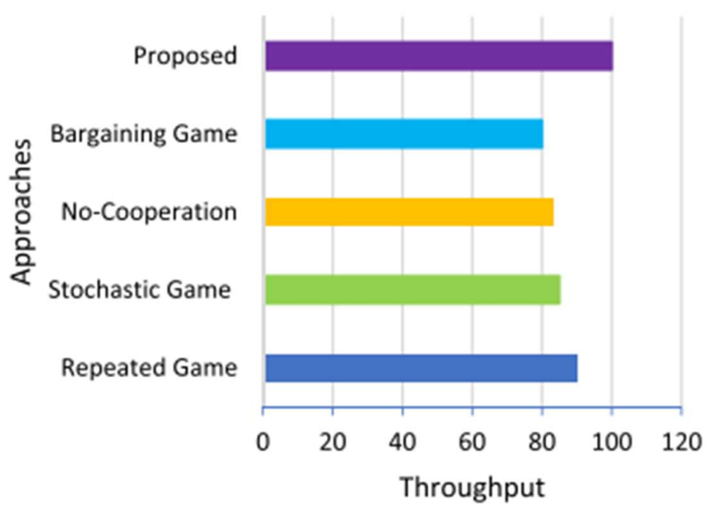


Figure 7 Comparative throughput analysis bits/sec.

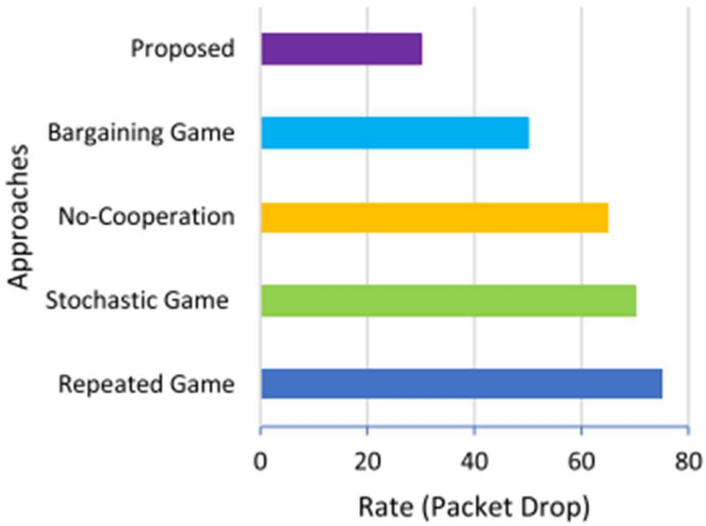


Figure 8 Comparative analysis of the rate of packet drops bits per sec.

Figure 8 indicates the execution time of the proposed algorithm, which is 4 seconds, demonstrating efficient computational and communication performance.

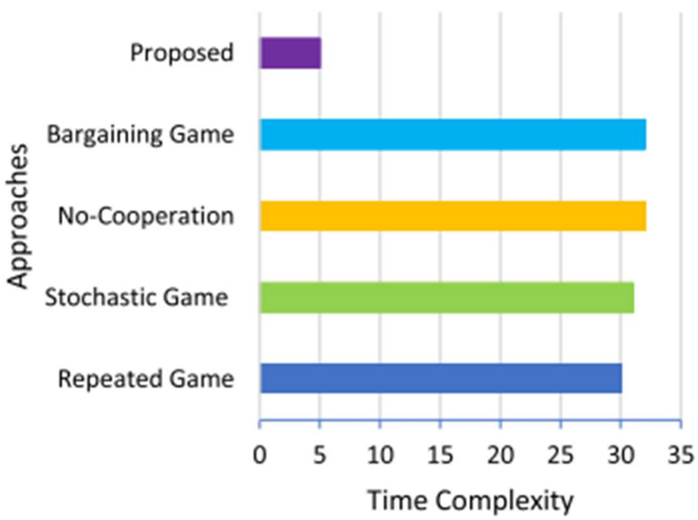


Figure 9 Comparative analysis of time complexity in Sec.

The memory requirement analysis shows that the proposed system consumes only about 7 MB of memory, significantly lower than other approaches, such as the bargaining game model, which consumes around 30 MB.

The study evaluates three crucial factors: upper bound of re-transmission factor, cooperative reward factor, and the probability of successful packet forwarding with a cooperative strategy and 1-hop modeling, all of which contribute to improved network performance.

The proposed system encourages self-centered nodes to participate in packet forwarding, leading to a higher probability of successful packet transmission despite network dynamics.

Network overhead is evaluated and reduced through the cooperative intelligent game mode, which distributes incentives based on collective intelligence, ensuring reliable communication.

The system's game-based solution and cooperative reward strategy incentivize self-centered nodes to relay or forward data packets, contributing to more reliable communication with reduced network overhead.

Chapter 6
CONCLUSION

In conclusion, the paper “Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission in Mobile Ad hoc Networks” emphasizes the importance of maximizing packet forwarding in MANETs, even when dealing with unreliable radio links. It recognizes the challenges posed by resource-constrained, self-configuring mobile nodes in MANETs, where network topology dynamically changes without centralized control. To address these challenges, the study introduces an intelligent packet forwarding approach based on an evolutionary one-hop packet forwarding game model.

REFERENCES

[1] U. I. Khan, R. F. Olanrewaju, F. Anwar, A. R. Najeeb, and M. Yaacob, ‘‘A survey on MANETs: Architecture, evolution, applications, security issues and solutions,’’ Indonesian J. Electr. Eng. Comput. Sci., vol. 12, no. 2, pp. 832–842, 2018, doi: 10.11591/ijeecs.v12.i2.pp832-842.

[2] R. F. Olanrewaju, B. U. I. Khan, F. Anwar, B. R. Pampori, and R. N. Mir, ‘‘MANET security appraisal: Challenges, essentials, attacks, countermeasures & future directions,’’ Int. J. Recent Technol. Eng. (IJRTE), vol. 8, no. 6, pp. 3013–3024, 2020, doi: 10.35940/ijrte.E6537.038620.

[3] G. H. Raghunandan, G. H. Chaithanya, and R. Hajare, ‘‘Independent robust mesh for mobile adhoc networks,’’ in Proc. 4th Int. Conf. Electron. Commun. Syst. (ICECS), Coimbatore, India, Feb. 2017, pp. 125–128, doi: 10.1109/ecs.2017.8067852.

[4] S. Kumar, M. L. Saini, and S. Kumar, ‘‘A survey: Swarm based routing algorithm toward improved quality of service in MANET,’’ Int. J. Manage., Technol. Eng., vol. 8, no. 5, pp. 311–322, 2018.

[5] T. Jamal and S. A. Butt, ‘‘Malicious node analysis in MANETS,’’ Int. J. Inf. Technol., vol. 11, no. 4, pp. 859–867, Dec. 2019, doi: 10.1007/s41870-018-0168-2.

[6] S. Almazyad, ‘‘Reputation-based mechanisms to avoid misbehaving nodes in ad hoc and wireless sensor networks,’’ Neural Comput. Appl., vol. 29, no. 9, pp. 597–607, May 2018, doi: 10.1007/s00521-016-2555-6.

[7] K. Rama Abirami and M. G. Sumithra, ‘‘Preventing the impact of selfish behavior under MANET using neighbor credit value based AODV routing algorithm,’’ Indian Acad. Sci., vol. 43, no. 4, pp. 1–7, Apr. 2018, doi: 10.1007/s12046-018-0803-4.

[8] Bisen and S. Sharma, ‘‘Fuzzy based detection of malicious activity for security assessment of MANET,’’ Nat. Acad. Sci. Lett., vol. 41, no. 1, pp. 23–28, Feb. 2018, doi: 10.1007/s40009-017-0602-1.

[9] T. Seregina, O. Brun, R. El-Azouzi, and B. J. Prabhu, ‘‘On the design of a reward-based incentive mechanism for delay tolerant networks,’’ IEEE Trans. Mobile Comput.,

vol. 16, no. 2, pp. 453–465, Feb. 2017, doi: 10.1109/TMC.2016.2546910.

[10]G. Lau, M. Al-Sabah, M. Jaseemuddin, H. Razavi, and M. Bhuiyan, ‘‘Context-aware RAON middleware for opportunistic network,’’ Pervas. Mobile Comput., vol. 41, pp. 28–45, Oct. 2017, doi: 10.1016/j.pmcj.2017.07.004.

[11]B. U. I. Khan, R. F. Olanrewaju, F. Anwar, and A. Shah, ‘‘Manifestation and mitigation of node misbehaviour in adhoc networks,’’ Wulfenia J., vol. 21, no. 3, pp. 462–470, 2014.

[12]M. Rajesh, ‘‘A review on excellence analysis of relationship spur advance in wireless ad hoc networks,’’ Int. J. Pure Appl. Math., vol. 118, no. 9, pp. 407–412, 2018.