Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 4 (2023)

Considering Performance Issues in Ad Hoc Networking : A Comprehensive Study

[1]Neeraj Verma, [2]Pro. (Dr.) Awakash Mishra

[1]Research Scholar, Department of Technology
Maharishi university of Information Technology, Lucknow , MUIT, Lucknow , Uttar Pradesh , India -226013
[2]Professor, Department of Computer Science Engineering, School of Engineering and Technology
Maharishi university of Information Technology, Noida
MUIT, Noida, G.B. Nagar, Uttar Pradesh, India -201304

E-mail-Id - [1]vermneeraj@gmail.com
*Co-author E-mail-Id - dean.research@muit.in

Abstract: Ad hoc networks have emerged as a versatile and dynamic communication paradigm with applications spanning from mobile devices and sensor networks to emergency response and military operations. However, their inherent decentralized and self-organizing nature gives rise to a myriad of performance challenges that must be comprehensively addressed to ensure reliable and efficient communication. This paper presents a comprehensive study of performance issues in ad hoc networking, aiming to provide a holistic understanding of the various factors impacting network performance. The study begins by examining the fundamental characteristics of ad hoc networks, highlighting their unique advantages and challenges. We delve into critical performance metrics such as throughput, latency, scalability, and energy efficiency, dissecting the factors that influence each of these metrics in ad hoc environments. The role of routing protocols, MAC layer design, and network topologies in shaping network performance is thoroughly analyzed. Furthermore, this study explores the impact of mobility patterns, traffic models, and interference on ad hoc network performance. It delves into the challenges posed by dynamic network topologies, node failures, and the need for adaptive mechanisms to maintain robust connectivity. Quality of service (QoS) considerations and their implications on performance are also discussed in detail. To provide a comprehensive view, we survey state-of-the-art solutions and techniques proposed in the literature to mitigate performance issues in ad hoc networks. These include adaptive routing algorithms, cross-layer optimization approaches, and novel communication paradigms like cognitive radio networks. Finally, we present a roadmap for future research directions in the field of ad hoc networking performance optimization. The goal is to inspire further investigation and innovation in addressing the evolving challenges faced by ad hoc networks, making them more reliable, efficient, and adaptable for a wide range of applications.
Keywords: Ad Hoc Networking, Performance, MAC layer, Quality of service.

1. Introduction

In the realm of modern communication and networking, ad hoc networks have gained significant prominence due to their ability to provide flexible and spontaneous connectivity in a wide range of scenarios. These networks, often composed of mobile and wireless devices, have found applications in fields as diverse as mobile computing, Internet of Things (IoT), disaster recovery, military operations, and vehicular communication systems. In places where permanent network infrastructure is impracticable or nonexistent, ad hoc networks are a viable alternative because to their decentralised and self-organizing nature. While ad hoc networks offer remarkable advantages in terms of adaptability and rapid deployment, they also present a plethora of performance challenges that must be carefully considered and addressed. These challenges stem from the very nature of ad hoc networks, characterized by dynamic topologies, limited resources, and decentralized decision-making processes. As such, a comprehensive understanding of the performance issues that afflict ad hoc networks is essential to ensure their reliability, efficiency, and suitability for a wide range of applications.

This paper embarks on a journey to explore and dissect the myriad performance issues that confront ad hoc networking, offering a holistic perspective on the complexities and intricacies of this communication

paradigm. We aim to provide researchers, engineers, and practitioners with valuable insights into the challenges and opportunities presented by ad hoc networks, ultimately fostering the development of innovative solutions to enhance their performance and robustness. In this introduction, we set the stage for our comprehensive study by briefly outlining the key characteristics of ad hoc networks and the contexts in which they are deployed. We highlight the fundamental advantages and challenges that define these networks, emphasizing the need for a systematic exploration of performance-related issues. We also provide a glimpse of the structure and objectives of our study, which encompasses an in-depth analysis of critical performance metrics, the role of various network components, and the impact of dynamic environmental factors.

As we delve deeper into the world of ad hoc networking performance, it becomes evident that these networks represent a dynamic and evolving field of research. The challenges they pose are both complex and multifaceted, spanning issues related to throughput, latency, scalability, energy efficiency, and quality of service (QoS), among others. Addressing these challenges necessitates a nuanced understanding of the intricate interplay between network protocols, communication paradigms, and environmental factors. In the subsequent sections of this study, we will undertake a comprehensive examination of these performance issues, dissecting the factors that influence network behavior and exploring state-of-the-art solutions and techniques proposed by the research community. We will also outline a roadmap for future research directions, aiming to inspire further innovation in the field of ad hoc networking performance optimization. The world of ad hoc networking is both captivating and challenging, offering a vast landscape for exploration and improvement. With this comprehensive study, we endeavor to contribute to the collective knowledge and understanding of performance issues in ad hoc networking, ultimately paving the way for more robust, efficient, and adaptable communication systems in an increasingly interconnected world.

1.1 Ad Hoc Networks

In this context, "ad hoc" refers to a network of wirelessly interconnected, relatively power-efficient endpoints. Base stations and other centralised control mechanisms are missing from the networks. This is why node mobility and the formation of new subnetworks are encouraged.

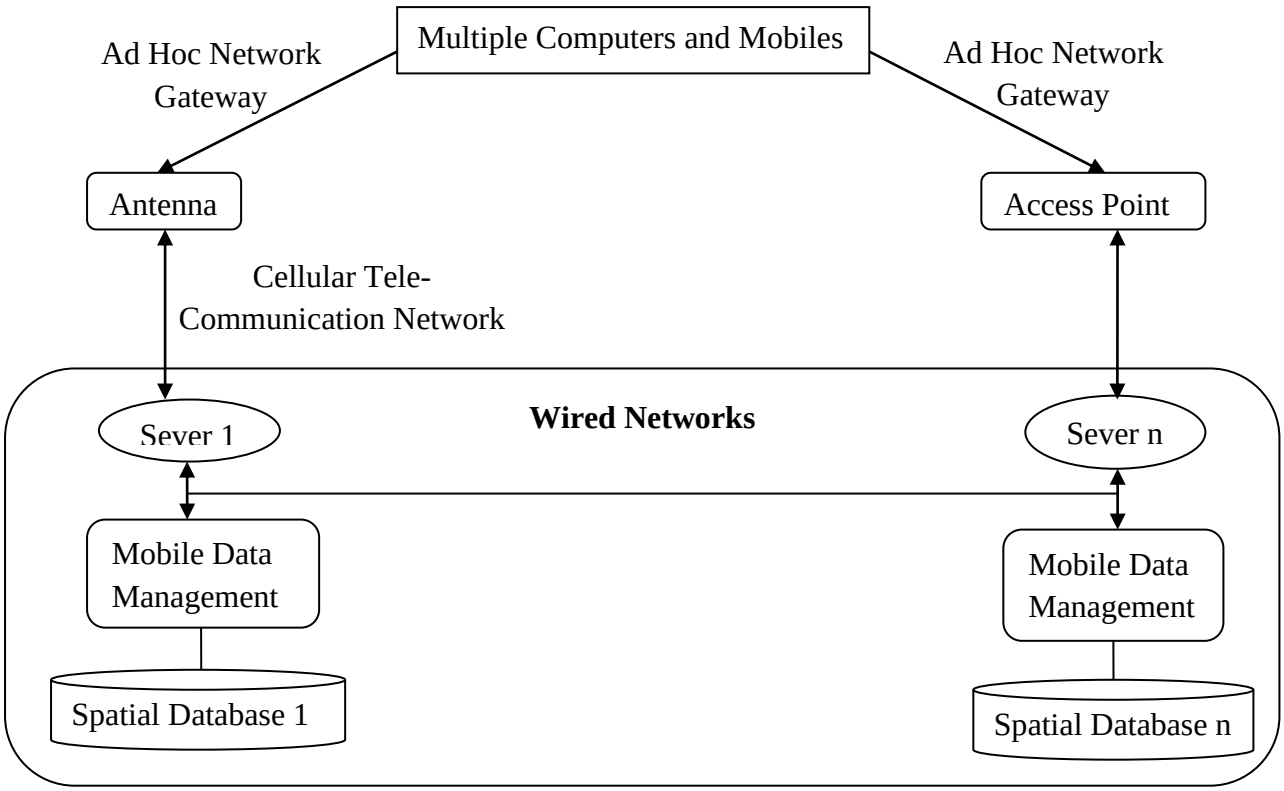

Fig: 1: Ad Hoc Network

These advancements are useful for wireless sensor and vehicular networks, as well as for military communications. Alternative to 4G networks, notably in subterranean transit systems where nodes are located outside the range of

Radio frequency waves. Two major categories of routing protocols exist: reactive and proactive. By using an alternative route when the existing one is underutilised, proactive routing might help keep network nodes linked. Reactive routing also includes determining the optimal route from one node to another. Two nodes can only talk to one another through routing if an entry table isn't present. In a highly dynamic routing system like this network, an ad hoc on-demand distance vector might be created as part of the first transmission. Each node in a

network must know the best route to its destination before transmitting a packet. The paths may remain accessible for as long as is required. The first stage in delivering a message to its intended recipient is for a node to send a signal to its neighbours, requesting advice on the most efficient path to take. Since RREQ has finally arrived, the operation may proceed as planned. A Route Replay message is broadcast along the same route in response to a Route Requirement message from the originating node.

1.2 Threat Categories

Without an entry table, two nodes can only communicate with one another via routing. In a highly dynamic routing system like this network, an ad hoc on-demand distance vector might be created as part of the first transmission. Each node in a network must calculate the best route to its destination before transmitting a packet. The routes may stay open for as long as necessary. The first stage in delivering a message to its intended recipient is for a node to send a signal to its neighbours, requesting advice on the most efficient path to take. Since RREQ has finally arrived, the operation may proceed as planned. In response to a Route Requirement inquiry from a source node, a Route Replay message is sent along the same path. This article focuses on the potential dangers that flawed machine learning techniques, such as indirect model manipulation, might pose in the context of 5G networks. Spoofing, tampering, repudiation, and privilege escalation are just some of the tactics an adversary may employ to back up these classic threats. The primary dangers of ML include:

- **Denial-of-Service (DoS) -** causing congestion, service interruptions, or improper network configuration.
- **Denial-of-Detection (DoD) -** allowing assaults and other threats to take place; preventing ML from issuing alerts in response to incidents.
- **Unfair use or resources (Unf) -** service theft (by sending an attacker to a less-congested area of the network, for instance) or higher victim workloads and/or energy consumption.

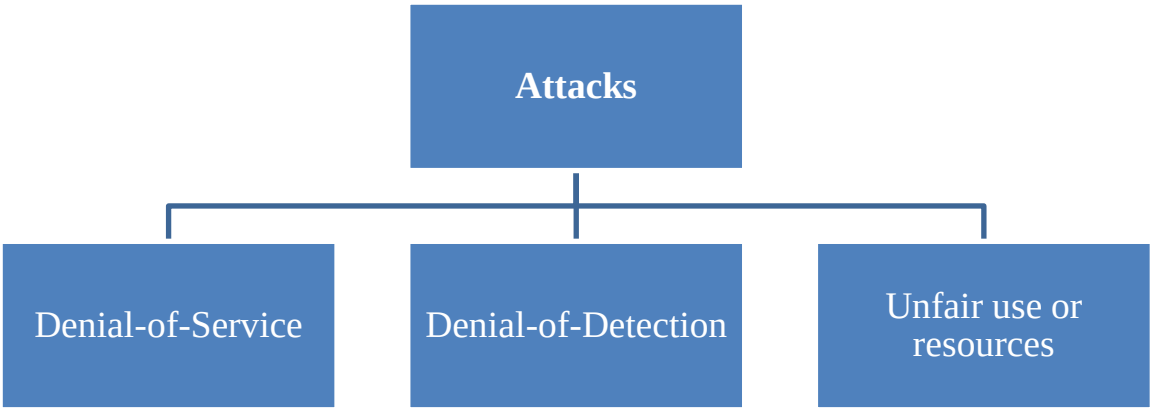

Fig 2: Different type of attacks

1.3 Role of machine learning in attack classification

Since ML relies on ingesting data from the surrounding world, processing it, and then outputting it after receiving feedback and through iterations, the system is inherently insecure. Theoretically, there aren't any

elaborate plans of action that can beat ML. An adversary need just feed false data into a system's learning or operating-system mechanisms to trick them. Information in transit may be spied on, intercepted, or tampered with by an adversary. The infrastructure, data, or models used in ML might be compromised by a threat actor.

1) Attacks Against ML: There are six distinguishing features that may be utilised to classify attacks that are effective in fooling ML. One characteristic of an attack is its impact, which describes how it taints training and corrupts learnt models or how it tampers with learning outcomes to elude detection. The specificity of an attack also determines whether or not it has an influence on the model's efficacy and dependability. Finally, the integrity, availability, or privacy of a target determines the security objective of an adversary. Finally, the frequency parameter indicates whether an attack is a one-and-done event or if it has the potential to happen again. Finally, the knowledge the hostile has about the defenceless system may be described by their degree of skill. The attacker has access to and is able to manipulate the ML system's internals via a white-box attack. In a black-box attack, the attacker is only privy to the system's inputs and outputs. To conclude, the need for false positives or false negatives in an ML model depends on the goal of the test. Attacks against ML procedures may take many forms, and some of them are designed to steal confidential data or models. Such attacks may be launched against hosts where models are being trained or implemented. Theft of confidential company information might occur at any time when it is being sent or stored in the cloud.

2) Inherent Limitations of ML Systems: The effectiveness of ML is dependent on the reliability of the data utilised for the study. In highly variable and complicated contexts, it may be challenging to collect comprehensive and realistic data sets. ML also creates significant maintenance issues in advanced settings. Data from several sources arriving at once might get entangled and generate feedback loops that are difficult to trace. Potential issues include data sources' instability and the complexity of their interconnections. Interdependencies between models and ML-based systems are conceivable, with apparently harmless modifications opening the system up to previously undiscovered hazards. When used with new data, the performance of many learning algorithms is questionable, and the underlying statistical nature of ML makes predictions controversial. This lack of knowledge regarding the origins of mysterious ML raises the possibility that the observed effects are not causally related to the initial issue at hand, but rather are the product of some other, unrelated factor. This sort of mistake is hard to spot since the model could still provide good results.

Features are visible and measurable properties that can be automatically extracted from the data by DL-based ML algorithms. As a result, it is unclear which model attributes were responsible for certain forecasts. This is a serious vulnerability since it makes it more difficult to detect any malicious manipulation of the training data. Knowledgeable experts in recognising patterns are needed to spot this kind of deception. A term, "explain to control," has been created to underline the importance of transparent AI in addressing these concerns.

2. Literature Review

The unpredictable and decentralised nature of ad hoc networks makes them particularly difficult to secure. The need of strong security measures in ad hoc networks cannot be overstated, particularly in light of their use in military operations, disaster recovery, & IoT gadgets. This survey of the relevant literature provides an overview of the most important studies and developments in the area of ad hoc network security.

The work of Muthurajkumar et al. (2017) focuses on the development of efficient, secure, and smart routing protocols for MANETs. Here, we introduce CEESRA, a new cluster-based and energy-efficient secured routing protocol that can effectively identify attackers by using trust ratings on nodes. This approach to routing uses intelligent agents to provide optimal routing alternatives, mitigating the impact of DoS attacks. Experimental findings demonstrate that the proposed trust-based secured routing method enhances security while reducing both energy consumption and routing delay.[1]

To prioritise device connections while decreasing energy usage, Safara et al. (2018) created PriNergy for the IoT. The study suggests a priority-based energy-efficient routing scheme (PriNergy) to cut down on power use. [2]

Femila et al. (2019) suggested a method to maximise data transmission rates in mobile ad hoc networks while minimising energy consumption by nodes in the network. All subsequent communications will use the route with the longest expected lifespan per this approach. Our efforts have resulted in a decrease in routing's

power consumption and an increase in performance. As throughput rises and operating power decreases, efficiency improves. Energy use in regular line and grid line networks might be cut by 45–75 percent if the traditional, shortest-path routing approach was used. By decreasing the network's need for power, the EPAR algorithm makes the system more effective and allows it to run for longer. When applied to Mobile Ad hoc Networks, the EPAR method has the potential to reduce energy usage by as much as 80%.[3]

The energy efficiency of a route-building algorithm for a hybrid ad hoc network was recently evaluated by Kumar Das et al. (2019). We demonstrate an innovative approach to developing routing algorithms for hybrid ad hoc networks by use of geometric programming. GP-EER stands for "Geometric Programming based Energy-Efficient Routing," which is the full meaning of the abbreviation. Its goal is to decrease packet loss and routing overhead, making networks faster and more reliable. [4]

In their research, Anand et al. (2019) Power consumption in MANETs has been lowered thanks to enhancements to the AODV protocol. No fixed infrastructure is required for ad hoc networks, which are made up of mobile nodes that have banded together for communication. Due to its limited resources, MANET can only operate via wireless communication. Given the critical nature of MANET's nonstop connectivity, battery life is of paramount importance. Reducing transmission packet loss has motivated several studies aimed at extending battery life. The process of improving MANETs' battery life is just getting started. In this paper, we provide a method for increasing the packet-transmission capacity and prolonging the operational lifespan of MANET batteries.[5]

Users of wireless Ad hoc networks may now travel securely thanks to the innovative routing strategy developed by Mukeshbhai Desai et al. (2019). First, they look at the foundational research on protecting against sequence number assaults. The evaluation delves further into several facets of the strategy. By pinpointing rogue nodes at different stages of the path-finding process, they also provide a predictable, proactive protection against sequence number assaults. In this case, the AODV routing protocol is modified so that it can serve the purposes of the proposed infrastructure.[6]

Energy-efficient cluster routing utilising fuzzy logic was developed by Balaji et al. (2019) to increase the WSNs' longevity. CRP is the most efficient strategy for conserving energy in a wireless sensor network. Cluster routing protocols (CH) are used to determine who will serve as the cluster head. The data packets then go from one CH to the next until they reach the BS. When choosing a CH, the configuration step is used. Information packets are routed over a network of intermediary nodes. These data packets are destined towards the network's epicentre. In wireless sensor networks, data packets from source sensors go to the network's base station by means of the cluster heads. Fuzzy logic gives more weight to hubs that are also highly reliable. Using type 1 fuzzy logic, CH will be selected as the best possible forwarder. It will show how to reduce network maintenance expenses while increasing their useful lifespan.[7]

You may find some helpful details in Arulkumaran et al.'s (2019) article. In order to detect black hole attacks in mobile ad hoc networks, fuzzy trust analysis might be utilised. The importance of wireless communication technology is emphasised by scenarios requiring links to faraway places, such as natural disasters, military activities, and climate-adaptive strategies. [8]

An in-depth look at how wireless sensor networks might benefit from hierarchical routing solutions that use less power. That which Guleria and company. Abstract: Because of its usefulness in tracking and monitoring in unpopulated or sparsely populated areas, WSNs have gained popularity in recent years. Given the dynamic topology and dispersed nature of WSNs, developing energy-efficient methods for routing data events presents a significant problem. This study primarily aims to find hierarchical routing solutions to issues like network downtime and wasteful energy consumption. This study set out to combine classical and swarm intelligence strategies to see whether it would be possible to create hierarchical algorithms that effectively use energy while re-routing. Both types of routing protocols may benefit from features including low power consumption, centralised data storage, geographic awareness, quality of service, scalability, load balancing, fault tolerance, query-based routing, and multiple paths. Between 2012 and 2017, a comprehensive literature evaluation was conducted on hierarchical energy-efficient routing methods. Academics may utilise the technical advice provided in this overview to design better routing systems. Finally, we speculate on potential future directions for the investigated processes and highlight any knowledge gaps. Diagrammatic Recap: In the body of the article, you could come across [picture not available [9]

Based on NSGA-II, Harrag et al. 2019 provide a novel OLSR self-organized routing scheme for MACS. Recent years have seen a lot of focus on the topic of proactive routing in ad hoc networks. When dealing with a large number of mobile nodes or a big number of load-dependent ad hoc network settings, which are often built intuitively by an experienced expert, the approaches outlined in the literature have drawbacks. In this work, we report our ongoing efforts to automate the process of determining the parameters of the routing protocol by use of a multi-objective genetic algorithm. Under experimental circumstances, the suggested NGSA-II-OLSR performed better than the state-of-the-art OLSR design. The suggested NSGA-II-OLSR enhances performance in terms of PLR (by 8.59% to 33.17%), E2ED (18.17%), and NRL (35.18% to 36.60%) in circumstances where nodes may freely move about. Gains of up to 0.14 percentage points in PLR, 2.34 percentage points in E2ED, 3.47 percentage points in NRL, and 9.94 percentage points in NRL are possible as a result of a highly mobile node. The algorithm's flexibility allows the ad hoc network to rapidly adjust to changing conditions while retaining a high level of flexibility [10]

on order to guarantee delivery on low-power wireless ad hoc networks, Umair Hassan and colleagues (2019) developed a new technique. When devices communicate with one another wirelessly and serve as hosts and routers for one another, they form a wireless ad hoc network. Because they can be established quickly and with little effort, wireless ad hoc networks are rapidly gaining popularity. [11]

Banerjee et al. (2020) studied low-power MANET with a self-organizing topology. In the event that the physical communication network infrastructure fails, a fallback option might be to utilise an infrastructure-free communication network, such as a mobile ad hoc network (MANET). However, MANETs must be flexible in order to function in environments with varying densities of devices, degrees of mobility, and types of energy. The authors of this paper suggest a protocol for distributed, context-aware topology control. The three-algorithm protocol constructs a loop-free, scalable architecture for ad hoc communication by using preferred attachment depending on the energy availability of devices. There are a number of benefits to the suggested approach. It might be utilised in scenarios with a variety of mobile devices and power sources to determine its usefulness. Second, changes to the topology may reduce energy needs. This suggests compatibility with several routing protocols. Thirdly, the protocol may be used with current infrastructure if necessary. No extra software or product recalls are required to deploy this solution for any already available product. The protocol has been successfully tested in a simulated environment, proving that it is possible to coordinate a large number of mobile devices into an ad hoc network with stable communication despite environmental disruptions. [12]

3. Problem Statement

In a comprehensive study on performance issues in ad hoc networking, several key problems and challenges are considered. These problems encompass a wide range of issues that affect the reliability, efficiency, and effectiveness of ad hoc networks. Here are some of the prominent problems that are typically addressed in such a study:

1. **Dynamic Topologies:** Ad hoc networks are characterized by rapidly changing network topologies due to the mobility of nodes. This dynamic nature can lead to frequent link disruptions, packet loss, and challenges in maintaining network connectivity.
2. **Routing and Route Stability:** Finding efficient and stable routes in dynamic ad hoc networks is a significant challenge. Routing protocols need to adapt to changing network conditions, minimize overhead, and ensure timely delivery of data.
3. **Congestion Control:** Congestion may arise as the number of nodes in a network grows or when those resources become scarce. Maintaining high network performance requires the use of efficient congestion management technologies.
4. **Quality of Service (QoS):** Video streaming and real-time data transmission are two examples of applications that need guaranteed QoS. It is a challenging issue to balance these needs with the ever-changing characteristics of ad hoc networks.
5. **Energy Efficiency:** Saving power is especially important with low-capacity gadgets like smartphones & IoT sensors. A major focus is on developing communication protocols and methods that minimise energy use.

6. **Security:** Threats to the security of ad hoc networks include eavesdropping, spoofing, and denial of service attacks. Protecting the privacy, security, and veracity of data and nodes is a major obstacle.
7. **Scalability:** Ad hoc networks should be able to scale to accommodate a varying number of nodes. Maintaining performance as the network size grows is a critical problem.
8. **Interference:** In wireless environments, interference from neighboring networks or devices can degrade performance. Managing interference and coexistence with other networks is a challenge.
9. **Mobility Management:** Handling the movement of nodes within the network while maintaining connectivity and efficient routing is a non-trivial problem.
10. **Resource Allocation:** Efficiently allocating resources such as bandwidth, spectrum, and power among nodes is crucial for optimizing network performance.
11. **Cross-Layer Optimization:** Coordinating different layers of the protocol stack to improve overall network performance is a complex task, as changes in one layer can affect others.
12. **Self-Organization and Autonomy:** Ad hoc networks often operate without centralized control. Ensuring that nodes can self-organize, make autonomous decisions, and still achieve desired performance objectives is challenging.
13. **Adaptation to Network Conditions:** Ad hoc networks must adapt to varying environmental conditions, including weather, interference, and mobility patterns, to maintain optimal performance.
14. **Reliability:** Achieving reliable data transmission in the presence of node failures, link disruptions, and other challenges is a fundamental problem.
15. **Load Balancing:** Distributing network traffic evenly among nodes to prevent bottlenecks and optimize resource utilization is an ongoing challenge.

A comprehensive study on ad hoc networking performance issues explores these and related problems, assesses existing solutions and proposes novel approaches to address them. Researchers aim to provide insights and strategies to enhance the performance and resilience of ad hoc networks in diverse real-world scenarios.

4. Proposed Research Methodology

Proposing a research methodology for a comprehensive study on performance issues in ad hoc networking involves a systematic approach that encompasses data collection, analysis, experimentation, and evaluation. Below is a structured research methodology that can guide such a study:

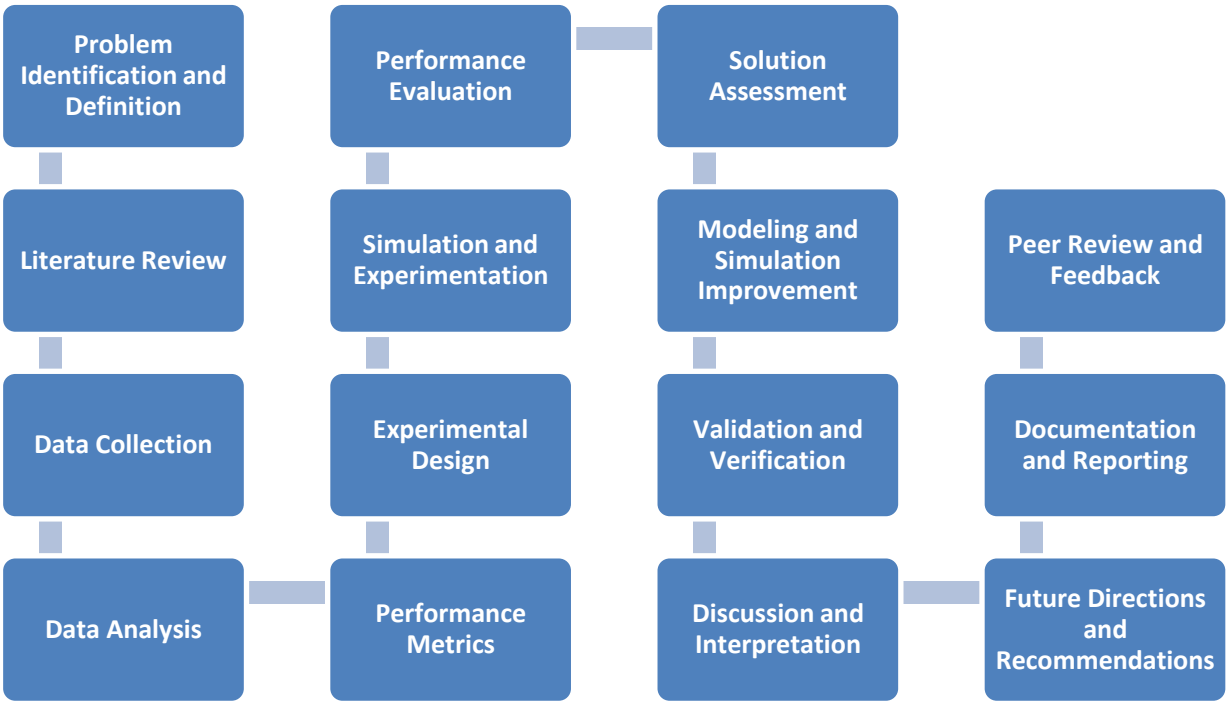

Fig 3: Research Methodology

1. Problem Identification and Definition:

- Clearly define the specific performance issues to be addressed in ad hoc networking.
- Identify the scope and objectives of the study, including the key metrics to be evaluated (e.g., throughput, latency, energy efficiency).

2. Literature Review:

- Perform a comprehensive literature search on the topic of ad hoc networking performance difficulties.
- Identify gaps, challenges, and emerging trends in the field.

3. Data Collection:

- Gather data from relevant sources, including real-world ad hoc network deployments, simulation environments, and testbeds.
- Collect data on network topologies, traffic patterns, mobility models, and other relevant parameters.

4. Experimental Design:

- Design experiments or simulations that replicate the identified performance issues and scenarios.
- Select appropriate tools and simulation platforms or real-world testbeds.

5. Performance Metrics:

- Define the performance metrics that will be used to assess the identified issues. These may include but are not limited to:
  - Throughput
  - Latency
  - Packet loss
  - Energy consumption
  - Quality of service (QoS)
  - Scalability
  - Security parameters

6. Data Analysis:

- Analyze the collected data using statistical techniques and visualization tools.
- Identify patterns, trends, and correlations related to performance issues.

7. Simulation and Experimentation:

- Execute simulations or real-world experiments according to the defined experimental design.
- Record data during experiments, ensuring accuracy and consistency.

8. Performance Evaluation:

- Evaluate the performance of ad hoc networks under various scenarios and conditions.
- Compare results against baseline or reference cases to assess the impact of performance issues.

9. Solution Assessment:

- Investigate and assess existing solutions and strategies proposed in the literature to mitigate performance issues.
- Evaluate their effectiveness in addressing the identified problems.

10. Modeling and Simulation Improvement:

- If applicable, refine simulation models or testbed setups based on the findings and insights from the experiments.

11. Validation and Verification:

- Validate the experimental results by comparing them with theoretical models or analytical predictions where applicable.

12. Discussion and Interpretation:

- Interpret the results in the context of the identified performance issues.
- Discuss the implications and real-world significance of the findings.

13. Future Directions and Recommendations:

- Based on the study's results, provide recommendations for improving performance in ad hoc networking.

- Suggest potential areas for further research and development.

14. Documentation and Reporting:

- Prepare comprehensive research reports or papers detailing the methodology, experimental setup, findings, and conclusions.
- Share the research findings with the scientific community through conferences and publications.

15. Peer Review and Feedback:

- To guarantee the study's validity and rigour, you should: Ask other experts in the area for input and peer review.

This research methodology provides a structured approach to comprehensively investigate and address performance issues in ad hoc networking. It combines theoretical analysis, experimentation, and data-driven insights to contribute to the advancement of knowledge in this domain and to propose practical solutions for improving performance of ad hoc networks.

5. Need of Research

Conducting research to comprehensively study and address performance issues in ad hoc networking is essential for several reasons:

1. **Real-World Applicability:** Critical applications including emergency response, military operations, vehicle communication, and Internet of Things deployments are increasingly relying on ad hoc networks. Understanding and improving their performance is crucial to ensure the reliability and effectiveness of these systems in real-world scenarios.
2. **Complexity of Ad Hoc Networks:** Ad hoc networks exhibit dynamic topologies, varying traffic patterns, and decentralized decision-making. These complexities create unique challenges that demand specialized solutions and optimizations to deliver satisfactory performance.
3. **Quality of Service (QoS) Requirements:** Many applications running on ad hoc networks, including multimedia streaming, telemedicine, and autonomous vehicles, have stringent QoS requirements. Meeting these requirements necessitates a deep understanding of performance issues and effective mitigation strategies.
4. **Resource Optimization:** Efficiently utilizing resources like bandwidth, energy, and spectrum is vital, especially in resource-constrained environments (e.g., IoT devices, wireless sensor networks). Research can lead to resource-efficient protocols and mechanisms.
5. **Security Concerns:** Ad hoc networks are vulnerable to various security threats. Performance research can help in developing solutions that not only improve network performance but also enhance security by mitigating vulnerabilities.
6. **Evolving Technologies:** The field of wireless communication and networking is continually evolving. New technologies and standards, such as 5G and beyond, bring new opportunities and challenges for ad hoc networks. Research ensures that ad hoc networking keeps pace with these developments.
7. **Interdisciplinary Nature:** Ad hoc networking research involves elements from computer science, electrical engineering, wireless communication, and mathematics. A comprehensive study fosters collaboration and cross-pollination of ideas across these disciplines.
8. **Optimizing Existing Solutions:** There is a continuous need to optimize existing protocols and algorithms to make them more efficient, adaptive, and resilient. Performance research identifies areas where improvements can be made.
9. **Benchmarking and Evaluation:** Research provides benchmarking criteria and evaluation methods for comparing different solutions. This is essential for both academia and industry to assess the effectiveness of various approaches.
10. **Standardization and Best Practices:** Research outcomes can contribute to the development of industry standards and best practices for ad hoc networking, ensuring interoperability and consistency in implementations.

11. **Education and Training:** Research findings can be incorporated into educational curricula and training programs, equipping future engineers and researchers with the knowledge and skills needed to address performance issues in ad hoc networking.
12. **Cost Efficiency:** Efficiently designed ad hoc networks can lead to cost savings, especially in scenarios where the deployment of infrastructure-based networks is impractical or costly.

Research dedicated to addressing performance issues in ad hoc networking is indispensable for advancing the field, enhancing the reliability of critical applications, and fostering innovation in communication technologies. It addresses the unique challenges posed by ad hoc networks and contributes to their evolution as robust, efficient, and adaptable communication systems. This comprehensive study sheds light on the multifaceted performance challenges encountered in ad hoc networking and serves as a valuable resource for researchers, engineers, and practitioners seeking to design, deploy, and improve ad hoc networks in diverse real-world scenarios.

6. Future Scope

The future scope for considering performance issues in ad hoc networking is broad and dynamic, with numerous opportunities for further research and development. As technology evolves and the demand for ad hoc networks continues to grow, the following areas hold significant promise for future exploration:

1. **5G and Beyond:** The integration of ad hoc networking principles with 5G and upcoming communication standards presents exciting prospects. Research can focus on optimizing ad hoc networking in 5G networks, exploring new use cases, and leveraging advanced features like network slicing and edge computing.
2. **Autonomous Vehicles and Vehicular Ad Hoc Networks (VANETs):** As autonomous vehicles become more prevalent, VANETs play a critical role in ensuring safe and efficient transportation. Future research can focus on QoS improvements, low-latency communication, and security solutions for VANETs.
3. **IoT and Edge Computing:** The proliferation of IoT devices requires efficient, scalable, and energy-efficient ad hoc networks. Future work may involve designing network protocols and architectures tailored to the unique requirements of IoT and edge computing applications.
4. **Machine Learning and AI:** Integrating machine learning and AI techniques into ad hoc networks for adaptive routing, resource allocation, and interference management offers potential for enhancing performance. Research in this area can explore how AI can optimize various aspects of ad hoc networking.
5. **Blockchain and Security:** Blockchain technology has the potential to enhance security and trust in ad hoc networks. Future research can investigate the integration of blockchain for secure and tamper-proof routing and authentication mechanisms.
6. **Energy-Efficiency and Sustainability:** As environmental concerns grow, research can focus on developing energy-efficient and environmentally sustainable ad hoc networking solutions. This includes energy-aware routing protocols and green communication strategies.
7. **Quantum Communication:** The field of quantum communication holds the promise of ultra-secure communication. Future studies can explore the integration of quantum principles into ad hoc networks for improved security and novel communication paradigms.
8. **Cross-Layer Optimization:** Continued research into cross-layer optimization techniques can lead to more efficient ad hoc networking protocols that consider interactions between different layers of the protocol stack.
9. **Dynamic Spectrum Access:** Research can investigate dynamic spectrum access techniques, including cognitive radio, to better utilize available spectrum resources and mitigate interference in ad hoc networks.
10. **Large-Scale Deployments:** As ad hoc networks are increasingly deployed in large-scale scenarios (e.g., smart cities, disaster recovery), research can focus on scalability challenges, load balancing, and robustness in such environments.

11. **Standardization and Interoperability:** Future efforts can contribute to standardization bodies to ensure interoperability between different ad hoc networking solutions, facilitating seamless communication in heterogeneous environments.
12. **Real-world Testbeds:** Developing and using real-world testbeds that mimic complex ad hoc network scenarios can provide valuable insights and validate research findings under more realistic conditions.
13. **Quantitative Analysis:** More in-depth quantitative analysis, including modeling and mathematical analysis, can provide a deeper understanding of performance issues and their solutions in ad hoc networking.
14. **Educational Initiatives:** The development of educational programs and resources focused on ad hoc networking can help train the next generation of researchers and engineers in this field.
15. **Collaboration with Other Fields:** Interdisciplinary collaboration with fields such as data science, cybersecurity, and transportation engineering can lead to innovative solutions and insights for addressing ad hoc networking performance issues.

In summary, the future scope for research in ad hoc networking performance issues is multifaceted and constantly evolving. Embracing emerging technologies and addressing the evolving needs of modern applications will drive innovation and contribute to the continued growth and relevance of ad hoc networking in diverse domains.

Reference

[1] S. Muthurajkumar, S. Ganapathy, M. Vijayalakshmi, and A. Kannan, "An Intelligent Secured and Energy Efficient Routing Algorithm for MANETs," Wirel. Pers. Commun., vol. 96, no. 2, pp. 1753–1769, 2017, doi: 10.1007/s11277-017-4266-4.

[2] F.Safara, A.Souri, T.Baker, I. A. Ridhawi, and M. Aloqaily, "LJMU Research Online," PriNergy: A Priority-based Energy Efficient Routing Method for IoT Systems Fatemeh," J. Appl. Sport Psychol., vol. 27, no. 2, pp. 2008–2018, 2018.

[3] L. Femila and M. Marsaline Beno, "Optimizing Transmission Power and Energy Efficient Routing Protocol in MANETs," Wirel. Pers. Commun., vol. 106, no. 3, pp. 1041–1056, 2019, doi: 10.1007/s11277-019-06202-7.

[4] S. K. Das and S. Tripathi, "Energy efficient routing formation algorithm for hybrid ad-hoc network: A geometric programming approach," Peer-to-Peer Netw. Appl., vol. 12, no. 1, pp. 102–128, 2019, doi: 10.1007/s12083-018-0643-3.

[5] M. Anand and T. Sasikala, "Efficient energy optimization in mobile ad hoc network (MANET) using better-quality AODV protocol," Cluster Comput., vol. 22, pp. 12681–12687, 2019, doi: 10.1007/s10586-018-1721-2.

[6] A. M. Desai and R. H. Jhaveri, "Secure routing in mobile Ad hoc networks: a predictive approach," Int. J. Inf. Technol., vol. 11, no. 2, pp. 345–356, 2019, doi: 10.1007/s41870-018-0188-y.

[7] S. Balaji, E. Golden Julie, and Y. Harold Robinson, "Development of Fuzzy based Energy Efficient Cluster Routing Protocol to Increase the Lifetime of Wireless Sensor Networks," Mob. Networks Appl., vol. 24, no. 2, pp. 394–406, 2019, doi: 10.1007/s11036-017-0913-y.

[8] G. Arulkumaran and R. K. Gnanamurthy, "Fuzzy Trust Approach for Detecting Black Hole Attack in Mobile Adhoc Network," Mob. Networks Appl., vol. 24, no. 2, pp. 386–393, 2019, doi: 10.1007/s11036-017-0912-z.

[9] K. Guleria and A. K. Verma, "Comprehensive review for energy efficient hierarchical routing protocols on wireless sensor networks," Wirel. Networks, vol. 25, no. 3, pp. 1159–1183, 2019, doi: 10.1007/s11276-018-1696-1.

[10] N. Harrag, A. Refoufi, and A. Harrag, "New NSGA-II-based OLSR self-organized routing protocol for mobile ad hoc networks," J. Ambient Intell. Humaniz. Comput., vol. 10, no. 4, pp. 1339–1359, 2019, doi: 10.1007/s12652-018-0947-4.

[11] M. U. Hassan et al., "Dear-2: An energy-aware routing protocol with guaranteed delivery in wireless ad-hoc networks," EAI/Springer Innov. Commun. Comput., pp. 215–224, 2019, doi: 10.1007/978-3-319-99966-1_20.

[12] I. Banerjee, M. Warnier, and F. M. T. Brazier, "Self-organizing topology for energy-efficient ad-hoc communication networks of mobile devices," Complex Adapt. Syst. Model., vol. 8, no. 1, 2020, doi: 10.1186/s40294-020-00073-7.

[13] N. Usman et al., "An energy efficient routing approach for IoT enabled underwater wsns in smart cities," Sensors (Switzerland), vol. 20, no. 15, pp. 1–29, 2020, doi: 10.3390/s20154116.

[14] U. Mohanakrishnan and B. Ramakrishnan, "MCTRP: An Energy Efficient Tree Routing Protocol for Vehicular Ad Hoc Network Using Genetic Whale Optimization Algorithm," Wirel. Pers. Commun., vol. 110, no. 1, pp. 185–206, 2020, doi: 10.1007/s11277-019-06720-4.

[15] K. Van Nguyen, C. H. Nguyen, P. Le Nguyen, T. Van Do, and I. Chlamtac, "Energy-efficient routing in the proximity of a complicated hole in wireless sensor networks," Wirel. Networks, vol. 27, no. 4, pp. 3073–3089, 2021, doi: 10.1007/s11276-021-02569-3.

[16] S. Amirtharaj, T. Sabapathi, and N. Rathina Prabha, "Cross Layer Approach and ANFIS based Optimized Routing in Wireless Multi-Hop Ad Hoc Networks," Wirel. Pers. Commun., vol. 119, no. 1, pp. 187–209, 2021, doi: 10.1007/s11277-021-08203-x.

[17] S. Venkatasubramanian, A. Suhasini, and C. Vennila, "An Efficient Route Optimization Using Ticket-ID Based Routing Management System (T-ID BRM)," Wirel. Pers. Commun., 2021, doi: 10.1007/s11277-021-08731-6.

[18] A. C. J. Malar, M. Kowsigan, N. Krishnamoorthy, S. Karthick, E. Prabhu, and K. Venkatachalam, "Multi constraints applied energy efficient routing technique based on ant colony optimization used for disaster resilient location detection in mobile ad-hoc network," J. Ambient Intell. Humaniz. Comput., vol. 12, no. 3, pp. 4007–4017, 2021, doi: 10.1007/s12652-020-01767-9.

[19] S. Kalaivanan, "Quality of service (QoS) and priority aware models for energy efficient and demand routing procedure in mobile ad hoc networks," J. Ambient Intell. Humaniz. Comput., vol. 12, no. 3, pp. 4019–4026, 2021, doi: 10.1007/s12652-020-01769-7.

[20] K. Satheshkumar and S. Mangai, "EE-FMDRP: energy efficient-fast message distribution routing protocol for vehicular ad-hoc networks," J. Ambient Intell. Humaniz. Comput., vol. 12, no. 3, pp. 3877–3888, 2021, doi: 10.1007/s12652-020-01730-8.

[21] I. Memon et al., "Energy-efficient fuzzy management system for internet of things connected vehicular ad hoc networks," Electron., vol. 10, no. 9, pp. 1–25, 2021, doi: 10.3390/electronics10091068.

[22] M. Namdev, S. Goyal, and R. Agarwal, "An Optimized Communication Scheme for Energy Efficient and Secure Flying Ad-hoc Network (FANET)," Wirel. Pers. Commun., vol. 120, no. 2, pp. 1291–1312, 2021, doi: 10.1007/s11277-021-08515-y.

[23] N. Boddu, V. Boba, and R. Vatambeti, "A Novel Georouting Potency based Optimum Spider Monkey Approach for Avoiding Congestion in Energy Efficient Mobile Ad-hoc Network," Wirel. Pers. Commun., no. 0123456789, 2021, doi: 10.1007/s11277-021-08571-4.

[24] J. Zheng, C. Li, P. H. J. Chong, and W. Meng, "MONET Special Issue on Towards Future Ad Hoc Networks: Technologies and Applications (II)," Mob. Networks Appl., vol. 27, no. 2, pp. 453–456, 2022, doi: 10.1007/s11036-021-01731-7.

[25] S. Parvathy and B. Gs, "Energy Efficient Management Approach For Wireless Sensor Networks," vol. 2, no. 7, pp. 2201–2205, 2022, doi: 10.48175/IJARSCT-4451.