ISBN : 978-93-47475-17-7

Ad Hoc Wireless Routing Protocols and Techniques

Editors

Dr.K.Vimala

Dr.K.Sumathi

TeQ Publications
Technology and Expertise in Quality

First Edition: November 2025

Ad Hoc Wireless Routing Protocols and Techniques

(ISBN: 978-93-47475-17-7)

Editors

Dr K.Vimala M.Sc.,M.Phil.,Ph.D.,
Assistant Professor, Department of Computer Science,
SRM Arts and Science College,
Chennai -603 203,Tamilnadu,India.

Dr.K.Sumathi, M.Sc., M.C.A., M.Phil., B.Ed.,Ph.D
Assistant Professor, Department of Computer Application,
K.S. Rangasamy College Of Arts and Science (Autonomous),
Tiruchengode -637 215,Tamilnadu,India.

TeQ Publications
Technology and Expertise in Quality

November 2025

Ad Hoc Wireless Routing Protocols and Techniques

Editors: Dr. K.Vimala , Dr. K.Sumathi
First Edition: November 2025

ISBN: 978-93-47475-17-7

Published by

TeQ Publications
Technology and Expertise in Quality

TeQPublications,India,

(A unit of Extromind Technologies)

#47/27, Mallasamudram, Namakkal,Tamilnadu, India 637503

Website: www.teqpublications.com

E-mail: info@teqpublications.com

PREFACE

The book *"Ad Hoc Wireless Routing Protocols and Techniques"* has been conceived as a comprehensive guide to understanding the evolving world of decentralized, infrastructure-less wireless communication systems. Over the past few decades, the concept of ad hoc networking has moved from experimental military applications to becoming an integral component of modern intelligent communication frameworks such as the Internet of Things (IoT), vehicular networks, unmanned aerial systems, and emerging 6G ecosystems. This transformation has been driven by rapid advancements in mobility, edge intelligence, and autonomous networking — all of which demand adaptable, energy-efficient, and secure routing solutions.

The motivation behind this book stems from the need to consolidate theoretical foundations, routing mechanisms, and emerging research directions within a single structured volume. While a significant body of literature exists on networking and communication systems, few resources provide an integrated view of both the classical and modern perspectives of ad hoc routing, spanning from the earliest distance-vector protocols to AI-assisted and quantum-secure designs. This book aims to bridge that gap by providing readers—be they researchers, engineers, or graduate students—with a deep yet practical understanding of routing paradigms that define today's and tomorrow's wireless connectivity.

The initial chapters (Chapters 1–2) introduce readers to the fundamentals of ad hoc wireless networks and the underlying routing principles that enable dynamic communication in mobile and infrastructure-less environments. These chapters lay the conceptual groundwork necessary to appreciate the complexity and elegance of routing in networks characterized by volatility, decentralization, and resource constraints. Subsequent chapters (Chapters 3–5) delve into the three major classes of routing protocols—proactive, reactive, and hybrid—highlighting their operational mechanisms, design trade-offs, and performance comparisons across diverse environments such as Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs), and Flying Ad Hoc Networks (FANETs). These sections not only explain the theoretical models but also draw connections to real-world applications, including disaster response, military coordination, and smart city communication systems. Chapters 6 and 7 explore specialized routing domains—geographic and energy-efficient routing—where the focus shifts to optimization, sustainability, and context-awareness. While geographic routing leverages spatial intelligence for efficient data dissemination, energy-efficient techniques emphasize extending network lifetime through adaptive power management and resource balancing. Together, they illustrate how routing strategies evolve when constrained by environmental and hardware limitations.

The latter part of the book (Chapters 8–10) addresses advanced and forward-looking themes. Chapter 8 discusses Quality of Service (QoS)-aware routing, ensuring reliable and performance-driven communication, while Chapter 9 focuses

on the pressing challenge of security—examining how trust, cryptography, and AI-driven defense mechanisms can safeguard ad hoc networks from evolving cyber threats. The final chapter, Chapter 10, envisions the future of ad hoc routing, exploring transformative technologies such as AI, blockchain, edge computing, and quantum networking that are redefining the very architecture of wireless communication in the 6G and beyond era.

Each chapter is crafted to be self-contained yet interconnected, allowing readers to explore specific topics or follow the progression from foundational theory to futuristic innovations. The inclusion of detailed keywords, abstracts, and analytical insights ensures that both beginners and advanced readers can navigate through the technical and conceptual depth of the subject with ease.

This book is intended to serve as a reference and inspiration for researchers, academicians, and industry practitioners working in wireless communication, distributed systems, and intelligent networking. It seeks not only to document the state of the art but also to spark new ideas and research directions toward creating networks that are autonomous, adaptive, secure, and sustainable.

I extend my sincere gratitude to the pioneers of ad hoc networking research, whose groundbreaking contributions laid the foundation for this domain, and to the global research community continuously pushing the boundaries of wireless innovation. I am also thankful to my students, collaborators, and peers who provided critical feedback and insights during the development of this work.

It is my hope that *"Ad Hoc Wireless Routing Protocols and Techniques"* will serve as both a learning companion and a research catalyst for those seeking to understand, design, and advance the next generation of wireless ad hoc communication systems.

— Editors

TABLE OF THE CONTENTS

ISBN: 978-93-47475-17-7

Chapter-1

Fundamentals of Ad Hoc Wireless Networks

[1]K.Indhumathi, [2]T.Abirami

[1]Assistant Professor, Department of Computer Applications,
K.S.Rangasamy College of Arts and Science (Autonomous),
Tiruchengode,Tamilnadu, India.

[2]Assistant Professor, Department of Computer Applications,
K.S.Rangasamy College of Arts and Science (Autonomous),
Tiruchengode,Tamilnadu, India.

Abstract: *This chapter introduces the foundational concepts and historical evolution of ad hoc wireless networks, emphasizing their unique characteristics, operational principles, and significance in modern communication systems. Ad hoc wireless networks are infrastructure-less, self-organizing systems where nodes operate both as hosts and routers, enabling multi-hop communication in dynamic topologies. The chapter begins by defining ad hoc networks and distinguishing them from traditional wired and infrastructure-based wireless networks in terms of topology control, scalability, and reliability. It then explores the historical development of ad hoc networking, tracing its origins from early radio communication to modern applications in Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs), Flying Ad Hoc Networks (FANETs), and IoT-based systems. Key technological milestones—such as DARPA's Packet Radio Network (PRNET) and Survivable Radio Network (SURAN) projects, as well as the emergence of routing protocols like DSDV, AODV, and DSR—are discussed in context. The chapter concludes by highlighting how ad hoc networks have become essential in domains such as disaster recovery, military communication, intelligent transportation, UAV coordination, and IoT ecosystems, paving the way for the next generation of decentralized and intelligent wireless communication systems.*

Keywords: *Ad Hoc Wireless Networks; Mobile Ad Hoc Networks (MANETs); Vehicular Ad Hoc Networks (VANETs); Flying Ad Hoc Networks (FANETs); Internet of Things (IoT); Infrastructure-less Communication; Multi-hop Routing; Self-Organization; Packet Radio Network (PRNET); DSDV; AODV; DSR;*

1. Introduction: Ad Hoc Wireless Networks

An ad hoc wireless network is a decentralized type of wireless network in which nodes communicate directly with one another without relying on any pre-existing infrastructure such as routers, access points, or base stations. Each node in this network acts both as a host and as a router, forwarding packets for other nodes. This dual functionality allows data to travel across multiple hops, thereby extending the communication range beyond the direct transmission distance of individual devices.

The fundamental characteristics of ad hoc wireless networks include infrastructure-less operation, meaning they do not depend on any centralized administration or fixed infrastructure. They exhibit self-organization, allowing nodes to join, leave, or move dynamically while the network automatically reconfigures itself. Multi-hop communication enables packets to be relayed through intermediate nodes to reach distant destinations. Due

to node mobility, the network maintains a dynamic topology, where connections change frequently. Additionally, the system operates under decentralized control, with routing and communication decisions distributed among nodes rather than managed by a central authority. These properties make ad hoc wireless networks highly flexible and suitable for environments where traditional network infrastructure is unavailable, damaged, or impractical to deploy.

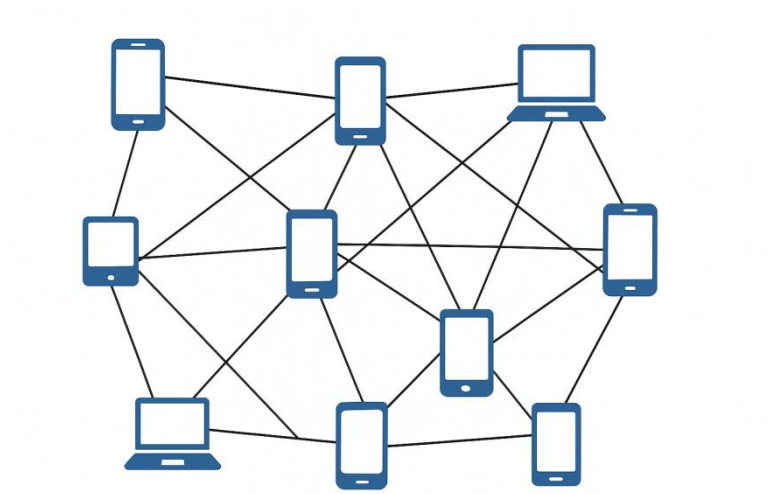


Figure 1: Peer-to-Peer Communication Model Diagram

Key Differences from Traditional Wired and Wireless Networks

Ad hoc wireless networks differ from conventional wired and infrastructure-based wireless networks in several critical aspects:

- **Topology Control:** In traditional wired and infrastructure-based wireless networks, topology is fixed and managed centrally by routers, switches, or base stations. Conversely, in ad hoc networks, the topology is dynamic and continuously changing due to node mobility. Nodes collectively manage routing and network organization without centralized control.
- **Communication Mode:** In wired networks, communication occurs through stable, high-bandwidth physical cables. Infrastructure-based wireless networks such as Wi-Fi or cellular systems depend on base stations or access points for connectivity. However, in ad hoc networks, communication follows a peer-to-peer model, where devices connect directly or through multi-hop paths without any intermediary infrastructure.
- **Scalability:** Traditional networks require physical expansion—adding routers, towers, or access points—to scale up. In contrast, ad hoc networks can scale dynamically as new nodes join or leave the network. However, scalability introduces

challenges such as increased routing overhead and bandwidth consumption, which may impact performance in large deployments.

- **Reliability and Control:** Wired and infrastructure-based networks offer high reliability and centralized management with predefined quality-of-service (QoS) guarantees. On the other hand, ad hoc networks rely on cooperative node behavior, mobility patterns, and available energy resources, which can affect network stability and reliability.

Importance in Modern Communication Systems

Ad hoc wireless networks hold a vital place in contemporary communication systems due to their adaptability, resilience, and rapid deployment capability. They serve as an essential communication backbone in numerous real-world applications:

- ***Disaster Recovery and Emergency Response:*** In natural disasters or war zones where infrastructure is damaged or destroyed, ad hoc networks enable first responders to maintain effective communication and coordination.
- ***Military Operations:*** Mobile ad hoc networks (MANETs) provide secure, infrastructure-free communication among soldiers, vehicles, and drones in dynamic battlefield conditions.
- ***Vehicular Communication (VANETs):*** Vehicles form ad hoc networks to exchange traffic and safety information, enhancing road safety, congestion control, and navigation efficiency.
- ***Internet of Things (IoT) and Smart Devices:*** Wearable sensors, smart home appliances, and industrial IoT devices use ad hoc networking to share data locally and autonomously.
- ***Rural and Remote Connectivity:*** In regions where installing wired or cellular infrastructure is impractical or costly, ad hoc networks offer a feasible alternative for establishing communication links.

In ad hoc wireless networks empower modern communication systems with the ability to function autonomously, flexibly, and reliably in environments where conventional networks cannot operate effectively. Their infrastructure-less, self-organizing nature ensures seamless connectivity in mission-critical and dynamic scenarios, making them indispensable in the era of ubiquitous wireless communication.

1.2 Historical Evolution

The origins of wireless communication trace back to the early 20th century, when Guglielmo Marconi's groundbreaking experiments in radio transmission established the foundation for untethered communication. Initially, wireless systems were developed primarily for broadcasting purposes—such as radio and television—or for point-to-point communication in military and maritime applications. However, the idea of multi-hop wireless communication, where intermediate devices relay data to extend communication range, began to take shape during World War II. Mobile radios deployed in battlefield operations

provided the first real-world example of infrastructure-less networking, demonstrating how communication could continue even in the absence of fixed infrastructure.

By the 1970s, as computer networking gained prominence, researchers started exploring how wireless devices could autonomously form dynamic, peer-to-peer communication systems (Shown: Figure 1) without relying on central nodes or routers. This period marked the intellectual birth of ad hoc networking, introducing the notion that mobile nodes could cooperate to create a self-configuring and infrastructure-free network environment.

Development of Ad Hoc Networking Technologies

The development of ad hoc networking technologies accelerated throughout the 1980s and 1990s, with several pivotal advancements shaping the field. One of the earliest breakthroughs was Packet Radio Networks (PRNET), developed by DARPA in the 1970s. PRNET implemented packet-switched communication using radio channels and served as one of the first experimental prototypes of mobile ad hoc networking, proving its feasibility for military use.

Building on PRNET, DARPA introduced SURAN (Survivable Radio Network) in the 1980s, which brought enhanced robustness, scalability, and adaptive communication protocols suitable for large, mobile, and hostile environments. SURAN's innovations laid the groundwork for reliable mobile networking under unpredictable conditions.

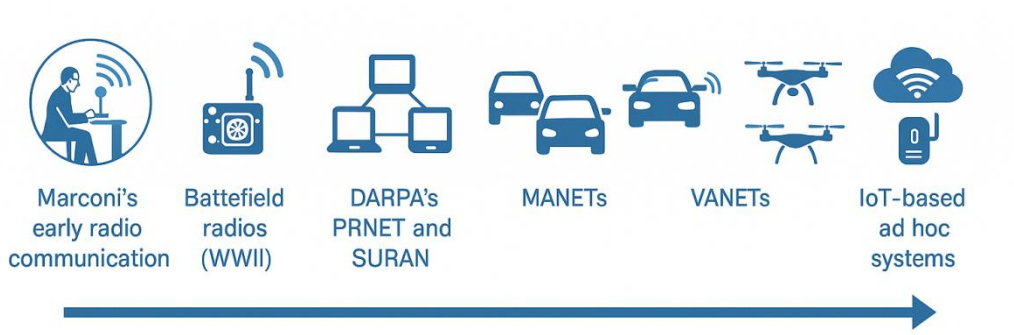


Figure 2: Timeline of Ad Hoc Network Evolution

In the 1990s, the term Mobile Ad Hoc Networks (MANETs) became widely recognized, particularly through the Internet Engineering Task Force (IETF). This era saw the formalization of routing protocols designed specifically for mobile, infrastructure-less networks—such as Destination-Sequenced Distance Vector (DSDV), Ad hoc On-Demand Distance Vector (AODV), and Dynamic Source Routing (DSR). During this period, ad hoc networking research expanded from its military roots into civilian domains, including disaster recovery, vehicular networks, and wireless sensor systems, marking a transition toward broader applications in both public and commercial sectors.

Milestones in MANET, VANET, FANET, and IoT-based Ad Hoc Systems

- **Mobile Ad Hoc Networks (MANETs):** During the 1990s and 2000s, MANETs emerged as the foundation of ad hoc communication systems, featuring key routing protocols like AODV, DSR, and OLSR. The IETF MANET working group led global research and standardization efforts. In the present day, MANETs are applied in disaster response systems, military communications, and community-based mesh networks, where rapid deployment and autonomous operation are essential.
- **Vehicular Ad Hoc Networks (VANETs):** In the early 2000s, researchers began focusing on vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications to improve traffic safety and road efficiency. By the 2010s, VANETs became integral to Intelligent Transportation Systems (ITS) and Dedicated Short-Range Communications (DSRC). Today, they underpin autonomous driving technologies, smart traffic management, and connected car ecosystems, contributing to the evolution of smart mobility.
- **Flying Ad Hoc Networks (FANETs):** With the proliferation of unmanned aerial vehicles (UAVs) in the 2010s, FANETs emerged as specialized ad hoc networks enabling drone-to-drone and drone-to-ground communication. These networks facilitate aerial surveillance, disaster assessment, and real-time environmental monitoring, particularly in regions lacking ground infrastructure. FANETs represent a critical advancement for coordinating autonomous aerial missions and swarm-based UAV operations.
- **IoT-based Ad Hoc Systems:** From the 2010s onward, the Internet of Things (IoT) revolution expanded ad hoc networking to billions of interconnected devices. These include smart sensors, wearables, and industrial machines capable of forming local clusters that communicate autonomously. IoT-enabled ad hoc systems power smart homes, smart cities, healthcare monitoring, and industrial automation by enabling decentralized communication without full reliance on cloud servers. Furthermore, the integration of IoT with 5G and emerging 6G networks, alongside edge computing technologies, has revitalized the relevance of ad hoc networks in modern digital ecosystems, offering high-speed, low-latency, and intelligent connectivity.

From Marconi's early radio experiments and wartime mobile radios to DARPA's packet radio initiatives and the formalization of MANET protocols in the 1990s, ad hoc networking has undergone continuous evolution. Today, it has diversified into multiple specialized domains such as vehicular networks (VANETs), drone-based systems (FANETs), and IoT-driven environments, each addressing unique communication challenges (Figure 2). This progression underscores the growing importance of decentralized, adaptive, and resilient communication systems in an era dominated by mobility, automation, and ubiquitous connectivity.

1.3 Core Characteristics of Ad Hoc Networks

Ad hoc wireless networks possess several defining characteristics that distinguish them from conventional wired and infrastructure-based wireless systems. These unique attributes

enable flexibility, scalability, and resilience, but they also introduce challenges in terms of performance, security, and resource management.

- **Self-organization:** One of the most fundamental features of ad hoc networks is their ability to self-organize. Nodes can automatically detect each other and establish communication links without manual configuration or centralized control. When a new node joins the network, it discovers neighboring nodes and integrates seamlessly into the system. Similarly, if a node leaves or fails, the network dynamically reconfigures itself to maintain connectivity. This property is particularly valuable in scenarios requiring rapid deployment, such as military operations or disaster recovery efforts. The main advantage of self-organization is the ability to establish communication in unpredictable environments, but it also demands intelligent algorithms to manage connectivity efficiently and avoid excessive overhead caused by frequent topology changes.
- **Infrastructure-less Communication:** Unlike traditional wireless systems that rely on fixed infrastructure—such as base stations, routers, or access points—ad hoc networks function entirely without pre-existing infrastructure. Each device operates independently and communicates directly with others within its transmission range. This infrastructure-less nature eliminates dependency on costly or vulnerable equipment, enhancing the network's resilience against single points of failure. For instance, in rural or remote areas where installing cellular towers or fiber networks is impractical, ad hoc networks can provide essential communication services. However, the absence of infrastructure also means that all networking responsibilities, such as routing and coordination, must be managed by the nodes themselves.
- **Multi-hop Routing:** Because individual nodes in an ad hoc network typically have limited radio ranges, communication between distant nodes is achieved through multi-hop routing. Intermediate nodes act as relays, forwarding packets from source to destination, thereby extending the network's coverage area. This allows the formation of large-scale networks without requiring high-power transmissions from any single device. However, multi-hop routing introduces challenges related to route discovery, maintenance, and adaptation to frequent topology changes. Routing protocols such as Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) have been developed to efficiently manage these complexities. While multi-hop communication enhances scalability and connectivity, it also increases routing overhead and latency in highly mobile environments.
- **Dynamic Topology:** The mobility of nodes results in a constantly changing network topology, where links form and break unpredictably. This dynamic nature sets ad hoc networks apart from wired systems, which generally have fixed and stable topologies. The key advantage of dynamic topology is its support for mobile applications, including vehicular ad hoc networks (VANETs) and flying ad hoc networks (FANETs), where nodes such as vehicles or drones are in continuous motion. However, this characteristic presents a major challenge for routing protocols, which must quickly adapt to maintain

reliable communication paths while minimizing control overhead and energy consumption.

- **Decentralized Control:** Ad hoc networks operate without centralized management or coordination. Each node functions both as a host and a router, making independent decisions regarding packet forwarding, resource allocation, and route maintenance. This decentralized control eliminates bottlenecks and enhances fault tolerance, as there is no single point of failure in the network. However, the distributed nature of control also requires cooperative behavior among nodes, which can be difficult to ensure in heterogeneous or untrusted environments. Malicious nodes can exploit this openness by disrupting routing operations or misdirecting traffic, highlighting the need for secure and trust-based routing mechanisms in decentralized systems.

The core characteristics of ad hoc networks—self-organization, infrastructure-less communication, multi-hop routing, dynamic topology, and decentralized control—collectively define their strength as highly adaptive and flexible communication systems. These features enable ad hoc networks to function effectively in dynamic and infrastructure-limited environments. However, they also introduce significant challenges related to scalability, routing efficiency, energy consumption, and security, necessitating continuous research and innovation to optimize their performance in real-world applications.

1.4 Types of Ad Hoc Networks

Ad hoc networks have evolved into various specialized types based on application domains, mobility patterns, and device capabilities. Each type addresses specific operational needs, from mobile communication to sensing and tactical operations (Figure 3). Below is an overview of the major categories of ad hoc networks.

- **Mobile Ad Hoc Networks (MANETs):** A Mobile Ad Hoc Network (MANET) comprises mobile devices such as laptops, smartphones, and tablets that communicate directly without relying on any fixed infrastructure. Each node in a MANET acts as both a host and a router, forwarding data packets for other nodes through multi-hop communication. This self-configuring capability allows MANETs to be rapidly deployed in dynamic environments. MANETs are highly flexible and suitable for scenarios like disaster recovery, temporary events, military operations, and rural wireless access. However, their high mobility often leads to frequent route failures, and limited battery power poses significant challenges to maintaining stable communication.
- **Vehicular Ad Hoc Networks (VANETs):** A Vehicular Ad Hoc Network (VANET) is a specialized form of MANET designed for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. In VANETs, vehicles act as nodes that exchange real-time information to enhance road safety and optimize traffic flow. Key features include high-speed mobility and predictable movement patterns along roads and highways. VANETs support Intelligent Transportation Systems (ITS), collision avoidance, congestion management, and autonomous driving. However, the rapidly

changing topology due to vehicle movement and the demand for ultra-low latency in safety-critical applications make protocol design challenging.

- **Flying Ad Hoc Networks (FANETs):** Flying Ad Hoc Networks (FANETs) consist of Unmanned Aerial Vehicles (UAVs) or drones that communicate in a three-dimensional space. FANETs extend ad hoc networking to aerial environments characterized by high-speed mobility and line-of-sight (LoS) communication. They are used in disaster management, border surveillance, environmental monitoring, and aerial delivery systems. The main challenges include maintaining stable communication links in dynamic 3D environments and managing limited battery life and payload capacity. FANETs represent an emerging area where robust routing and coordination algorithms are crucial for performance optimization.
- **Wireless Sensor Networks (WSNs):** A Wireless Sensor Network (WSN) is composed of numerous small, low-power sensor nodes deployed to monitor and transmit environmental data such as temperature, humidity, or motion. These nodes self-organize into an ad hoc topology to send data to sink nodes or gateways for analysis. WSNs are characterized by resource constraints, low energy consumption, and large-scale deployment. Common applications include environmental monitoring, industrial automation, healthcare, smart homes, and precision agriculture. Key challenges involve achieving energy efficiency, ensuring scalability, and maintaining reliable data transmission despite node failures or harsh conditions.
- **Tactical and Emergency Ad Hoc Networks:** Tactical and Emergency Ad Hoc Networks are designed for mission-critical communication in defense, public safety, and disaster response operations. These networks provide reliable and secure communication in environments where traditional infrastructure is destroyed, unavailable, or compromised. They are characterized by high resilience, robustness, and security-oriented designs. Applications include military battlefield communications, first responder coordination, and post-disaster recovery efforts. Major challenges include ensuring security, fault tolerance, and rapid deployment under unpredictable and often hostile conditions.

The diversity of ad hoc networks—including MANETs for general mobile communication, VANETs for transportation systems, FANETs for aerial applications, WSNs for sensing environments, and tactical/emergency networks for critical operations—demonstrates their adaptability to a wide range of scenarios.

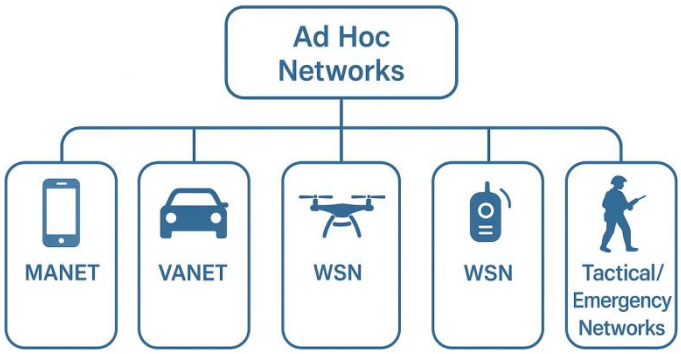


Figure 3: Types of Ad Hoc Networks

Each type presents unique operational requirements and challenges, necessitating tailored routing protocols and optimization strategies to achieve reliable, efficient, and secure communication.

1.5 Applications of Ad Hoc Wireless Networks

Ad hoc wireless networks have become vital in a wide range of domains due to their infrastructure-less, self-organizing, and resilient nature. Their adaptability allows seamless communication in environments where traditional networks are unavailable, expensive, or unsuitable. These networks play a key role in emergency management, defense operations, intelligent transportation, healthcare systems, and industrial automation.

- **Disaster Recovery and Emergency Response:** During natural disasters such as earthquakes, floods, or hurricanes, traditional communication infrastructure is often damaged or completely unavailable. In such situations, ad hoc wireless networks can be quickly deployed to restore communication among rescue teams and affected populations. They enable first responders to coordinate effectively, connect medical personnel, firefighters, and police, and support search-and-rescue operations using drone-based FANETs. The main advantages of using ad hoc networks in disaster response include rapid deployment, resilience against infrastructure failures, and scalability as new nodes join the network.
- **Military and Defense Communications:** Ad hoc networking originated in military applications, where the need for secure, mobile, and infrastructure-free communication is essential. Military units, vehicles, and UAVs can form tactical ad hoc networks that function reliably even in hostile or remote environments. Typical use cases include battlefield communications among soldiers and armored vehicles, real-time surveillance using UAV swarms (FANETs), and secure data exchange without centralized infrastructure. These networks offer high resilience, robust security, and support for mission-critical mobility, ensuring continuous operation in demanding military scenarios.
- **Vehicular Communication and Intelligent Transport Systems:** Vehicular Ad Hoc Networks (VANETs) are a cornerstone of Intelligent Transportation Systems (ITS),

providing the foundation for safer and more efficient roadways. In VANETs, vehicles communicate with one another (V2V) and with roadside infrastructure (V2I) to share real-time data about traffic, road conditions, and potential hazards. Applications include collision avoidance, traffic management, smart parking systems, and navigation assistance. By enabling vehicles to make informed decisions autonomously, VANETs significantly improve road safety, reduce congestion, and support next-generation autonomous driving technologies.

- **Healthcare and Wearable Devices:** In the healthcare domain, ad hoc wireless networks are transforming patient care through wearable medical devices, body area networks (BANs), and mobile health monitoring systems. These networks enable continuous, real-time data transmission from patients to healthcare providers, even in remote or emergency settings. Use cases include patient monitoring for vital signs such as heart rate and glucose levels, ad hoc connectivity in field hospitals, and Wireless Body Area Networks (WBANs) for telemedicine applications. Key advantages include continuous health tracking, immediate alerts for anomalies, and improved patient outcomes through proactive intervention.
- **Industrial IoT and Smart Environments:** The Industrial Internet of Things (IIoT) and smart environments rely heavily on ad hoc networks to support machine-to-machine (M2M) communication, automation, and environmental monitoring. Wireless Sensor Networks (WSNs), a major subclass of ad hoc systems, play a crucial role in enabling smart applications. In smart factories, WSNs interconnect machinery for real-time performance tracking. In agriculture, they monitor soil conditions and optimize irrigation. In smart cities and homes, they manage energy grids, pollution monitoring, and security systems. These networks offer cost efficiency, scalability, and flexibility in environments where installing wired connections is impractical.

The applications of ad hoc wireless networks span across disaster recovery, military operations, intelligent transportation, healthcare, and industrial IoT, highlighting their adaptability and critical importance in modern communication ecosystems. Their ability to deliver reliable, rapid, and flexible connectivity under dynamic and challenging conditions makes them indispensable in both civilian and defense sectors.

1.6 Challenges in Ad Hoc Networking

While ad hoc wireless networks provide exceptional flexibility, scalability, and rapid deployment capabilities, they also face a range of technical and operational challenges. These challenges primarily stem from their infrastructure-less, highly dynamic, and resource-constrained characteristics, which make maintaining efficient, secure, and reliable communication complex.

- **Limited Bandwidth and Spectrum Efficiency:** Ad hoc networks typically function within shared and unlicensed frequency bands, such as the Industrial, Scientific, and Medical (ISM) bands. This shared usage results in bandwidth constraints, as multiple

nodes competing for the same channel can cause signal interference, collisions, and congestion. These issues lead to throughput reduction and degraded network performance, especially in dense or large-scale deployments. To address this, researchers are developing spectrum-aware routing protocols, cognitive radio-based solutions, and adaptive channel allocation strategies that optimize spectrum usage dynamically to enhance efficiency.

- **Node Mobility and Frequent Topology Changes:** One of the defining features of ad hoc networks, particularly Mobile Ad Hoc Networks (MANETs), is the mobility of nodes, which leads to frequent and unpredictable topology changes. As nodes move, communication links may break suddenly, invalidating previously established routes. This results in high control overhead for constant route discovery and maintenance. The consequences include increased latency, packet loss, and unstable connections. To mitigate these effects, solutions such as mobility-aware routing protocols, predictive handoff mechanisms, and clustering-based network management are being explored to enhance route stability and reduce disruptions.
- **Energy Constraints and Battery Limitations:** Most devices in ad hoc networks—such as smartphones, wireless sensors, and UAVs—operate on limited battery power. Since nodes serve dual roles as transmitters and routers, continuous packet forwarding consumes significant energy, especially in dense networks. Uneven energy depletion among nodes can create "network holes," where critical nodes fail and disrupt overall connectivity. This leads to reduced network lifetime and reliability. To address these issues, researchers focus on energy-efficient routing algorithms, duty-cycling mechanisms in WSNs, and energy-harvesting technologies (e.g., solar-powered nodes) that prolong network longevity and balance power consumption.
- **Security Vulnerabilities and Trust Issues:** The decentralized and open nature of ad hoc networks makes them more vulnerable to a variety of security threats. These include eavesdropping, spoofing, blackhole attacks, and denial-of-service (DoS) incidents. Unlike traditional networks, ad hoc systems lack a central authority to manage authentication, making it difficult to ensure trust, integrity, and confidentiality. Such vulnerabilities can compromise data and disrupt network operations. To counter these threats, the adoption of secure routing protocols, trust-based frameworks, blockchain-based authentication, and intrusion detection systems (IDS) has become a critical research direction.
- **Quality of Service (QoS) Requirements:** Ensuring Quality of Service (QoS) in ad hoc networks is especially challenging due to the dynamic topology, variable link quality, and limited resources. Applications such as real-time video streaming, voice communication, and mission-critical IoT operations demand guarantees for bandwidth, latency, jitter, and reliability. However, maintaining these guarantees under mobility and congestion conditions is difficult. As a result, researchers are exploring cross-layer optimization techniques, adaptive QoS-aware routing protocols, and machine learning-based traffic prediction methods to allocate resources intelligently and maintain service quality.

Ad hoc wireless networks face multifaceted challenges including limited bandwidth, node mobility, energy constraints, security vulnerabilities, and QoS management issues. Overcoming these limitations requires innovative protocol design, intelligent cross-layer optimization, and adaptive resource management. Addressing these challenges is essential for ensuring that ad hoc networks evolve into robust, secure, and energy-efficient communication systems capable of meeting the demands of next-generation wireless technologies.

1.7 Advantages and Limitations

Ad hoc wireless networks provide a range of unique advantages that make them highly adaptable for various communication scenarios. Their decentralized, infrastructure-less, and self-organizing nature enables connectivity in environments where conventional networks are impractical. However, these same features introduce several limitations related to efficiency, stability, and security. Understanding both sides is essential for assessing their effectiveness in real-world applications.

Advantages

- **Scalability:** One of the key strengths of ad hoc networks is their inherent scalability. They can easily expand as new nodes join the network without requiring modification or expansion of centralized infrastructure. This dynamic scalability makes ad hoc networks ideal for a wide range of applications — from small-scale personal area networks to large-scale disaster recovery operations or military deployments.
- **Flexibility:** Ad hoc networks are highly flexible, allowing nodes to self-configure and reorganize automatically in response to changing conditions. This flexibility supports operation in diverse and unpredictable environments, including mobile communication, vehicular ad hoc networks (VANETs), UAV swarms (FANETs), and IoT ecosystems. The ability to adapt quickly makes them suitable for both static and mobile applications across civilian, industrial, and defense domains.
- Rapid Deployment a major advantage of ad hoc networks is their capacity for instant deployment without relying on routers, base stations, or other infrastructure components. This enables rapid establishment of communication channels in emergency or temporary situations such as disaster zones, military operations, or large public events. The minimal setup time and self-organizing nature ensure continuity of communication when traditional infrastructure is unavailable or damaged.

Limitations

- **High Overhead** Due to their dynamic topology, ad hoc networks require frequent control messaging to maintain accurate routing information. This continuous

exchange of route updates and management packets generates high overhead, consuming bandwidth that could otherwise be used for data transmission. The result is reduced effective throughput, particularly in dense or large-scale networks where routing updates become more frequent.

- **Unstable Connections** The mobility of nodes leads to frequent link breakages and unstable routes, which affect communication reliability. These disruptions can cause packet loss, increased delays, and inconsistent performance, especially for real-time applications that demand continuous connectivity. Maintaining stable communication under such dynamic conditions remains one of the key challenges in ad hoc networking.
- **Security Concerns** The absence of centralized control in ad hoc networks makes security management more difficult. Authentication, authorization, and trust establishment among nodes are complex, leaving the network vulnerable to malicious attacks such as eavesdropping, spoofing, blackhole, or denial-of-service (DoS) attacks. As nodes rely on mutual trust for routing and data forwarding, securing communication without centralized oversight remains a major research focus.

Ad hoc wireless networks offer scalability, flexibility, and rapid deployment, making them invaluable in situations where infrastructure-based communication is unavailable or impractical. However, these strengths come with trade-offs, including high control overhead, connection instability, and security vulnerabilities. Ongoing research seeks to balance these opposing factors through the development of efficient, adaptive, and secure routing protocols, ensuring that ad hoc networks remain a reliable and resilient communication paradigm for the future.

1.8 Comparison with Traditional Wireless Networks

Ad hoc wireless networks differ significantly from traditional infrastructure-based wireless systems such as Wi-Fi and cellular networks. While both enable wireless communication, their architectural design, control mechanisms, and performance outcomes are fundamentally distinct. The following sections outline the characteristics of each type and highlight the key trade-offs involved.

Infrastructure-Based Networks (Wi-Fi, Cellular)

Infrastructure-based networks rely on centralized management through fixed hardware such as access points (APs) in Wi-Fi or base stations in cellular systems. These central nodes handle coordination, routing, and network maintenance, ensuring smooth and efficient communication. The network topology is stable because devices connect through a fixed infrastructure, which allows predictable and reliable communication paths.

Centralized control enables effective resource optimization — including spectrum allocation, power management, and Quality of Service (QoS) provisioning — leading to high efficiency and reliability. As a result, these networks are ideal for applications that demand guaranteed

connectivity and service-level agreements (SLAs). Examples include home and enterprise Wi-Fi networks, as well as 4G and 5G mobile communication systems.

Ad Hoc Wireless Networks

In contrast, ad hoc wireless networks operate without centralized control. Each node functions autonomously, managing its own routing, communication, and resource allocation. These networks feature a dynamic topology, as nodes can join, leave, or move at any time, leading to frequent route updates and topology changes. Ad hoc networks are self-organizing, forming spontaneously without requiring any pre-existing infrastructure. This flexibility makes them particularly valuable in environments where fixed infrastructure is unavailable or impractical — such as disaster recovery zones, military battlefields, or remote areas. Examples of ad hoc networks include Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs), Flying Ad Hoc Networks (FANETs), and various sensor-based tactical networks.

Key Performance Trade-offs

Aspect	**Infrastructure-Based Networks**	**Ad Hoc Networks**
Control	Centralized (APs/Base Stations)	Decentralized, node-managed
Deployment Speed	Slower, requires infrastructure	Rapid, no infrastructure
Scalability	Limited by infrastructure capacity	High, but with overhead
Reliability	High, predictable connections	Lower, due to mobility and topology changes
Security	Stronger (centralized policies)	Weaker, prone to attacks
Cost	High (infrastructure setup)	Low, no fixed infrastructure
Flexibility	Less flexible, location-bound	Highly flexible, adaptable to environments

Infrastructure-based wireless networks excel in reliability, security, and resource optimization, making them ideal for stable, commercial, and urban communication environments. On the other hand, ad hoc wireless networks offer exceptional flexibility, scalability, and rapid deployment, enabling communication in infrastructure-less or emergency scenarios. However, these advantages come with trade-offs, including higher routing overhead, potential instability, and weaker security mechanisms, which remain key areas of ongoing research and optimization.

1.9. Conclusion

This chapter introduced the fundamental concepts of ad hoc wireless networks, emphasizing their unique role in modern communication systems. We began by defining ad hoc networks and highlighting their core characteristics such as self-organization, infrastructure-less communication, and decentralized control. The historical evolution was traced from early wireless networking concepts to the emergence of MANETs, VANETs, FANETs, WSNs, and IoT-based ad hoc systems. The discussion then explored the different types of ad hoc networks, along with their wide range of applications spanning disaster recovery, military communications, vehicular systems, healthcare, and industrial IoT. We also examined the challenges they face, including limited bandwidth, node mobility, energy constraints, and security vulnerabilities. To balance the discussion, the advantages and limitations of ad hoc networking were compared against traditional infrastructure-based networks, illustrating both their potential and inherent trade-offs. In ad hoc wireless networks are flexible, scalable, and rapidly deployable, making them invaluable for environments where conventional infrastructure is unavailable or impractical. However, their dynamic topology, overhead, and security challenges continue to drive ongoing research.

References

1. Akyildiz, I. F., & Wang, X. (2005). *Wireless mesh networks*. John Wiley & Sons.
2. Basagni, S., Conti, M., Giordano, S., & Stojmenovic, I. (Eds.). (2013). *Mobile ad hoc networking: Cutting edge directions* (2nd ed.). Wiley-IEEE Press.
3. Camp, T., Boleng, J., & Davies, V. (2002). A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing, 2*(5), 483–502. https://doi.org/10.1002/wcm.72
4. Conti, M., & Giordano, S. (2014). Mobile ad hoc networking: Milestones, challenges, and new research directions. *IEEE Communications Magazine, 52*(1), 85–96. https://doi.org/10.1109/MCOM.2014.6710069
5. Corson, S., & Macker, J. (1999). Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations. *RFC 2501*. IETF. https://doi.org/10.17487/RFC2501
6. Gupta, P., & Kumar, P. R. (2000). The capacity of wireless networks. *IEEE Transactions on Information Theory, 46*(2), 388–404. https://doi.org/10.1109/18.825799
7. Joshi, R. C., & Yadav, S. (2013). *Ad hoc mobile wireless networks: Principles, protocols and applications*. Springer.
8. Kaushik, A., & Sharma, A. (2019). Ad hoc networks: Applications, challenges and future trends. *International Journal of Computer Applications, 178*(49), 25–31. https://doi.org/10.5120/ijca2019918774
9. Kumar, S., & Patel, R. B. (2016). Recent developments in routing protocols for mobile ad hoc networks: A survey. *Wireless Personal Communications, 91*(2), 1033–1060. https://doi.org/10.1007/s11277-016-3405-9

10. Li, F., & Wang, Y. (2007). Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular Technology Magazine, 2*(2), 12–22. https://doi.org/10.1109/MVT.2007.912927
11. Perkins, C. E., & Royer, E. M. (1999). Ad-hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications* (pp. 90–100). IEEE. https://doi.org/10.1109/MCSA.1999.749281
12. Royer, E. M., & Toh, C. K. (1999). A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications, 6*(2), 46–55. https://doi.org/10.1109/98.760423
13. Sahni, Y., Cao, J., & Yang, L. T. (2021). Edge mesh: A new paradigm to enable distributed intelligence in Internet of Things. *IEEE Internet of Things Journal, 8*(7), 5146–5156. https://doi.org/10.1109/JIOT.2020.3022320
14. Sakhaee, E., & Jamalipour, A. (2006). The global in-flight Internet. *IEEE Journal on Selected Areas in Communications, 24*(9), 1748–1757. https://doi.org/10.1109/JSAC.2006.879360
15. Sharma, V., Balamurugan, M., & Saini, P. (2020). Flying ad hoc networks (FANETs): A survey. *Computer Science Review, 38*, 100298. https://doi.org/10.1016/j.cosrev.2020.100298
16. Singh, K., & Sharma, N. (2015). Wireless sensor networks: Issues & challenges. *International Journal of Computer Applications, 130*(9), 9–13. https://doi.org/10.5120/ijca2015907039
17. Toh, C. K. (2001). *Ad hoc mobile wireless networks: Protocols and systems*. Prentice Hall.
18. Wu, J., & Lou, W. (2019). Opportunistic and delay-tolerant routing in mobile ad hoc networks. In *Handbook of wireless ad hoc and sensor networks* (pp. 1–23). Springer. https://doi.org/10.1007/978-3-030-12786-2_1
19. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks, 52*(12), 2292–2330. https://doi.org/10.1016/j.comnet.2008.04.002
20. Zhang, Y., & Yan, Y. (2020). Cross-layer design for ad hoc wireless networks: A survey. *IEEE Access, 8*, 125848–125864. https://doi.org/10.1109/ACCESS.2020.3007807

Chapter-2

Routing Fundamentals in Wireless Ad Hoc Systems

[1]S.Vaitheki,[2] T.Ambika,

[1]*Assistant Professor, Department of Computer Science,*
Bon Secours Arts and Science College for Women,
Veppadai,Tamilnadu, India.

[2]*Assistant Professor, Department of Computer Science,*
Bon Secours Arts and Science College for Women,
Veppadai,Tamilnadu, India.

Abstract: *Routing plays a pivotal role in wireless ad hoc networks, enabling efficient data transmission in decentralized and infrastructure-less environments. This chapter explores the fundamental concepts, principles, and challenges underlying routing in ad hoc systems, emphasizing the mechanisms that allow nodes to dynamically discover, maintain, and optimize routes in ever-changing network topologies. Various routing approaches—proactive, reactive, and hybrid—are discussed in detail, highlighting their operational mechanisms, trade-offs, and application suitability. The chapter also delves into essential design considerations such as scalability, adaptability, energy efficiency, and security, which significantly impact protocol performance. Furthermore, routing metrics including hop count, link quality, delay, jitter, packet delivery ratio, and energy consumption are examined as key factors in determining optimal paths. Emerging trends such as AI-assisted routing, cross-layer design, and integration with 5G/6G and edge computing are presented as future directions. Overall, the chapter provides a comprehensive understanding of routing fundamentals, establishing the foundation for exploring specific routing protocols and their real-world applications in subsequent chapters.*

Keywords: *Wireless Ad Hoc Networks, Routing Protocols, Proactive Routing, Reactive Routing, Hybrid Routing, Route Discovery, Route Maintenance, Scalability, Energy Efficiency, Link Quality, QoS Metrics, Delay, Packet Delivery Ratio, Routing Overhead, Network Topology*

2.1 Introduction to Routing in Ad Hoc Networks

Routing is a fundamental process in wireless ad hoc networks, where nodes must communicate without the support of fixed infrastructure such as routers or base stations. Unlike traditional wireless networks that rely on centralized entities for path management, ad hoc systems require nodes to act as both hosts and routers, forwarding packets on behalf of others to enable end-to-end communication. This decentralized nature makes routing one of the most critical and challenging aspects of ad hoc networking (Figure 1).

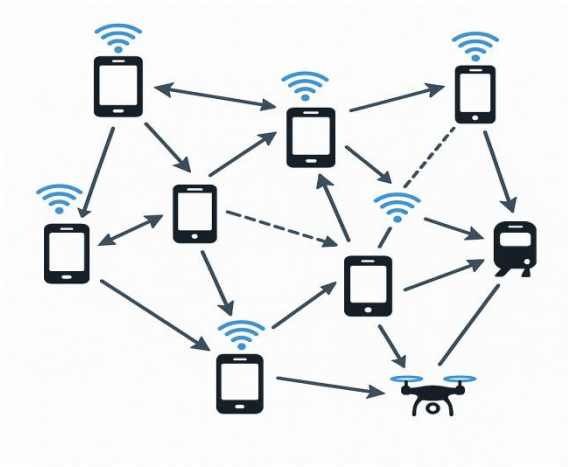


Figure 1: Routing in Wireless Ad Hoc Networks — Overview Diagram

2.1.1 Role of Routing in Decentralized, Infrastructure-less Networks

- In ad hoc networks, routing protocols are responsible for discovering and maintaining communication paths dynamically.
- Each node participates in the routing process, relaying packets to ensure multi-hop communication between distant nodes.
- Efficient routing ensures network connectivity, supports scalability, and allows the network to function in environments where centralized infrastructure is absent (e.g., disaster zones, battlefields, sensor fields).

2.1.2 Key Challenges in Routing Compared to Traditional Networks

Routing in ad hoc networks differs significantly from wired or infrastructure-based wireless systems:

- **Dynamic Topology:** Node mobility leads to frequent route breakages, requiring continuous route updates.
- **Resource Constraints:** Nodes often operate with limited battery power, memory, and processing capacity, making energy-efficient routing essential.
- **Unreliable Links:** Wireless links are prone to interference, fading, and congestion, leading to unstable connections.
- **Scalability Issues:** As the network grows, maintaining updated routing tables and minimizing control overhead becomes complex.
- **Security Concerns:** The absence of centralized control makes routing protocols vulnerable to malicious attacks (e.g., blackhole, wormhole, spoofing).

2.1.3 Metrics for Evaluating Routing Performance

To assess the efficiency and reliability of routing protocols in ad hoc networks, several performance metrics are considered:

- **Latency (End-to-End Delay):** The time taken for a packet to travel from the source to the destination. Lower latency indicates faster route discovery and packet delivery.
- **Throughput:** The total amount of data successfully delivered over the network in a given period. A key indicator of routing efficiency.
- **Energy Efficiency:** Measures how effectively the protocol conserves node battery power during route discovery and maintenance. Essential for sensor and mobile networks.
- **Scalability:** The ability of the routing protocol to maintain performance as the number of nodes or network density increases.

Routing in ad hoc wireless networks is a decentralized, adaptive process that must cope with frequent topology changes, resource limitations, and security risks. Evaluating routing protocols requires analyzing latency, throughput, energy consumption, and scalability to ensure reliable communication in diverse and dynamic environments.

2.2 Basic Principles of Routing

Routing in wireless ad hoc networks is guided by fundamental principles that ensure efficient, reliable, and scalable communication in a decentralized environment. Since there is no fixed infrastructure, each node must actively participate in the discovery, establishment, and maintenance of routes, adapting dynamically to frequent topology changes. These principles govern how nodes interact to form a robust and adaptable communication network despite constraints such as limited bandwidth, energy, and mobility.

2.2.1 Route Discovery and Route Maintenance

The route discovery process involves finding a path between a source and a destination when communication is required. In reactive routing protocols, route discovery is initiated only when a data transmission request arises, thus reducing unnecessary overhead. Conversely, in proactive routing protocols, routes are continuously maintained and updated in routing tables, ensuring immediate data forwarding when needed.

Route maintenance ensures that the selected communication path remains valid and functional during ongoing data transmission. It involves detecting link breakages caused by node mobility, interference, or failures and re-establishing new routes as needed. Efficient route maintenance mechanisms help minimize transmission disruptions, reduce latency, and lower control overhead, thereby improving overall network performance.

2.2.2 Single-Hop vs. Multi-Hop Communication

In **single-hop communication**, data is transmitted directly between two nodes within the same radio range. This method is simple, fast, and energy-efficient but is limited in coverage and scalability, making it suitable only for small or localized networks.

In contrast, **multi-hop communication** extends the communication range by involving intermediate nodes that forward packets from the source to the destination. This approach

enables larger and denser network coverage and ensures connectivity even in fragmented topologies. However, multi-hop transmission introduces additional overhead and latency and may face reliability challenges due to link instability or node mobility.

2.2.3 Reactive vs. Proactive Approaches

Routing protocols in ad hoc networks are generally categorized as **reactive**, **proactive**, or **hybrid** based on how they establish and maintain routes.

Reactive (On-Demand) Routing protocols, such as AODV and DSR, create routes only when communication is required. This approach minimizes control overhead since routes are established as needed. However, it can result in increased initial latency due to the time required for route discovery.

Proactive (Table-Driven) Routing protocols, such as DSDV, continuously maintain up-to-date routing information for all network nodes. While this provides low-latency communication and faster route access, it incurs higher control overhead and greater resource consumption, especially in large or highly dynamic networks.

Hybrid Routing Approaches, such as the Zone Routing Protocol (ZRP), combine the strengths of both reactive and proactive methods. They maintain proactive routing within local zones and use reactive discovery for distant nodes, effectively balancing the trade-offs between latency and overhead.

2.2.4 Loop-Free and Efficient Path Construction

A key objective in routing design is to ensure **loop-free routing**, which prevents data packets from circulating endlessly due to inconsistent or outdated routing information. Techniques such as sequence numbers (used in AODV) or path vector mechanisms are employed to maintain consistent and up-to-date routes.

Equally important is **efficient path selection**, where protocols aim to choose routes that minimize hop count, delay, and energy consumption while maximizing throughput and reliability. Advanced routing designs may incorporate adaptive metrics such as link stability, Quality of Service (QoS) requirements, and node energy levels to optimize overall network performance.

In the basic principles of routing in ad hoc networks revolve around **dynamic path discovery**, **continuous route maintenance**, and **multi-hop communication**. Effective routing strategies must balance the trade-offs between reactive and proactive approaches while ensuring loop-free and efficient path construction. By doing so, ad hoc networks can achieve reliable and scalable communication even in highly dynamic, decentralized, and resource-constrained environments.

2.3 Classification of Routing Protocols

Routing protocols in wireless ad hoc networks are designed to overcome challenges such as dynamic topologies, decentralized control, and limited node resources. Depending on their operational mechanisms, routing protocols are broadly classified into three main categories: proactive (table-driven), reactive (on-demand), and hybrid protocols (Figure 2). Each class presents unique strengths and trade-offs concerning latency, control overhead, scalability, and efficiency.

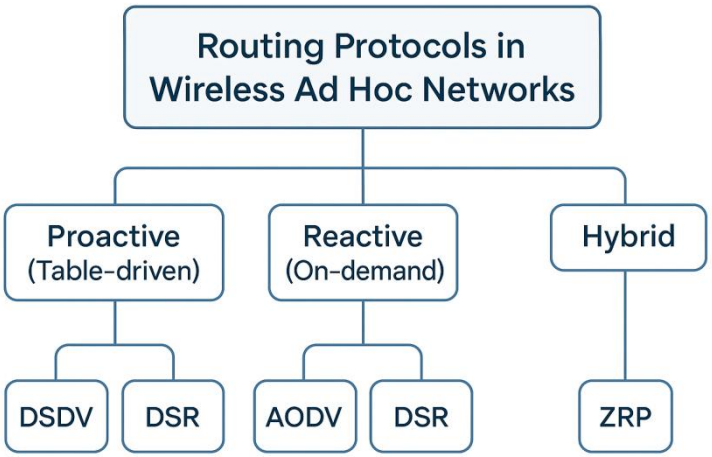


Figure 2: Classification of Routing Protocols in Ad Hoc Networks

2.3.1 Proactive (Table-Driven) Protocols

Proactive or table-driven routing protocols continuously maintain up-to-date routing information to all nodes in the network, even when communication is not required. Each node periodically exchanges control messages to update its routing tables, ensuring that routes are immediately available when data transmission begins.

The main advantages of proactive protocols include low latency and predictable performance in relatively stable environments, as routes are pre-established. However, they also have disadvantages, such as high control overhead due to frequent updates and poor scalability in large or highly mobile networks.

An example of a proactive protocol is the Destination-Sequenced Distance Vector (DSDV) protocol, which employs the Bellman-Ford algorithm enhanced with sequence numbers to prevent routing loops. Although DSDV ensures route consistency and loop-free communication, it generates significant control traffic in networks with frequent topology changes, limiting its efficiency in dynamic scenarios.

2.3.2 Reactive (On-Demand) Protocols

Reactive or on-demand protocols establish routes only when a source node requires communication with a destination node. They operate through two key phases: route discovery and route maintenance. This approach significantly reduces overhead since no periodic updates are exchanged across the network.

The advantages of reactive protocols include reduced control overhead and better scalability in highly dynamic or resource-constrained environments. However, they also exhibit higher initial latency because routes need to be discovered before communication begins. In networks with frequent topology changes, repeated rediscoveries may lead to inefficiencies.

Prominent examples include the Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocols.

- AODV uses sequence numbers to maintain loop-free and up-to-date routes, employing Route Request (RREQ) and Route Reply (RREP) messages during discovery.
- DSR, on the other hand, utilizes source routing, where the complete route is stored in packet headers. This eliminates the need for periodic route advertisements but increases packet overhead due to longer headers.

2.3.3 Hybrid Protocols

Hybrid routing protocols integrate both proactive and reactive features to achieve a balance between overhead and latency. These protocols typically divide the network into zones, where intra-zone routing (within a local area) is proactive, and inter-zone routing (across zones) is reactive. The advantages of hybrid protocols include high efficiency in large-scale networks with moderate mobility, as they reduce control overhead compared to purely proactive protocols while maintaining lower latency than purely reactive ones. However, they introduce greater design complexity, and their performance heavily depends on parameters such as optimal zone size and node mobility.

A well-known hybrid example is the Zone Routing Protocol (ZRP), which applies proactive routing within local neighborhoods and reactive route discovery for distant nodes. This approach effectively balances efficiency, scalability, and adaptability in heterogeneous environments.

In the classification of routing protocols underscores the trade-offs between latency, scalability, control overhead, and adaptability:

- Proactive protocols are best suited for smaller or stable networks where immediate route availability is critical.

- Reactive protocols perform well in highly dynamic or energy-limited environments by minimizing control overhead.
- Hybrid protocols offer a practical compromise, combining the strengths of both approaches to support efficient and scalable communication in diverse network scenarios.

2.4 Essential Design Considerations

The design of routing protocols in wireless ad hoc networks demands special attention to the unique constraints of decentralized, infrastructure-less environments. Unlike traditional fixed networks, ad hoc systems experience frequent topology changes, limited resources, and increased security risks. To ensure efficient and reliable communication, routing strategies must address several essential design considerations, including scalability, adaptability, energy efficiency, bandwidth management, and security.

2.4.1 Scalability in Large, Dense Networks

One of the most significant challenges in ad hoc network design is ensuring scalability as the number of nodes increases. When network size or density grows, maintaining routing tables or performing frequent route discoveries can generate excessive control overhead, leading to degraded network performance.

To achieve scalability, routing protocols must be capable of handling both large-scale and dense networks without overwhelming available bandwidth or computational resources. Effective approaches include hierarchical routing techniques such as clustering or zoning, which reduce global overhead by organizing nodes into manageable subgroups, and geographic or position-based routing, which utilizes node location information to streamline route selection and minimize control traffic.

2.4.2 Adaptability to Node Mobility and Topology Changes

Node mobility introduces continuous topology changes that can lead to route failures, packet loss, and frequent rediscoveries. Therefore, routing mechanisms must be designed to be both robust and adaptive, ensuring uninterrupted communication even under high mobility conditions. To enhance adaptability, several approaches can be employed, such as fast route repair mechanisms that quickly handle broken links, predictive mobility models that forecast node movement to prevent disruptions, and multipath routing schemes that maintain backup routes to ensure communication continuity during link failures.

2.4.3 Energy-Aware Routing and Battery Constraints

Energy efficiency is a critical factor in ad hoc networks, especially when devices operate on limited battery power, as in sensor or handheld nodes. Excessive communication or computation can deplete energy reserves quickly, reducing network lifetime.

To address this challenge, routing protocols must minimize energy consumption while maintaining balanced load distribution across nodes. Techniques such as energy-aware metrics (based on residual battery power or transmission cost), load balancing strategies to prevent overuse of specific nodes, and sleep scheduling or duty cycling in low-power devices are effective methods to enhance energy efficiency and prolong network operation.

2.4.4 Bandwidth Utilization and Congestion Control

Ad hoc networks often operate in bandwidth-limited environments, where collisions, redundant transmissions, and congestion can significantly impact throughput. Efficient bandwidth utilization and congestion control are therefore crucial to maintaining performance in multi-hop communication systems.

Routing protocols should optimize bandwidth use and distribute network traffic effectively. Approaches such as cross-layer optimization between the routing and MAC layers, traffic-aware routing to evenly distribute load, and QoS-aware routing metrics to support multimedia and real-time applications can enhance overall network performance and prevent bottlenecks.

2.4.5 Security-Aware Routing

Security poses a major challenge in ad hoc networks due to their open wireless medium and lack of centralized authority. These networks are susceptible to attacks such as spoofing, blackhole, wormhole, and denial-of-service (DoS) attacks.

To mitigate these threats, routing protocols must incorporate mechanisms for authentication, data integrity, and trust management. Security can be enhanced through trust-based routing frameworks that monitor and evaluate node behavior, lightweight cryptographic techniques such as digital signatures and encryption adapted for low-power environments, and intrusion detection systems (IDS) that identify malicious activities in real time.

In designing effective routing protocols for wireless ad hoc networks requires a careful balance among scalability, adaptability, energy efficiency, bandwidth management, and security. A protocol that fails to address any of these dimensions may suffer from performance degradation, shortened network lifetime, or increased vulnerability to attacks. Consequently, future routing designs should emphasize cross-layer optimization, AI-driven adaptability, and lightweight security mechanisms to meet the complex and evolving demands of large-scale, heterogeneous ad hoc environments.

2.5 Routing Metrics in Ad Hoc Networks

Routing metrics are the foundation for determining optimal paths in wireless ad hoc networks. Unlike traditional wired systems—where bandwidth and reliability are relatively stable—ad hoc networks operate in highly dynamic environments characterized by

fluctuating link qualities, node mobility, and energy limitations. The selection of routing metrics has a profound impact on overall network performance, efficiency, and lifespan. Various metrics have been developed to address these challenges, each focusing on specific performance goals such as minimizing delay, maximizing reliability, or conserving energy.

2.5.1 Hop Count and Path Length

Hop count measures the total number of intermediate nodes (hops) between a source and destination. It is one of the simplest and most widely used metrics, forming the basis of several classical routing protocols such as DSDV and AODV. The primary advantage of using hop count lies in its simplicity—it reduces computational complexity and often minimizes delay in static or lightly loaded networks. However, this metric has notable limitations: it disregards link quality, congestion, and energy constraints. As a result, routes with fewer hops may not necessarily provide reliable or high-quality communication, especially in environments with unstable or noisy wireless links.

2.5.2 Link Quality and Signal Strength

Link quality-based metrics evaluate path reliability by considering wireless channel conditions such as signal-to-noise ratio (SNR), packet loss rate, or expected transmission count (ETX). These parameters provide insight into the stability and performance of communication links. The main advantage of using link quality metrics is their ability to ensure stable, high-throughput connections while reducing retransmissions, thereby saving bandwidth and energy. However, this approach requires continuous monitoring of link conditions, which introduces additional overhead. Moreover, metrics like signal strength may fluctuate rapidly due to interference, node mobility, and channel fading, requiring adaptive and robust measurement mechanisms.

2.5.3 Delay, Jitter, and Packet Delivery Ratio (PDR)

Delay, jitter, and packet delivery ratio (PDR) are critical performance indicators for routing in real-time and Quality of Service (QoS)-sensitive applications.

- Delay refers to the total time taken for a packet to travel from source to destination.
- Jitter measures the variation in delay between packets, which can severely affect time-sensitive services like VoIP or video streaming.
- PDR quantifies the reliability of communication by calculating the ratio of successfully delivered packets to those sent.

These metrics are essential for selecting routes that can meet stringent latency and reliability requirements. Their advantages include suitability for QoS optimization and the ability to improve performance in multimedia or mission-critical systems. However, accurately estimating delay and jitter in a dynamic, multi-hop ad hoc network is complex, requiring frequent updates and synchronization across nodes.

2.5.4 Energy Consumption per Route

Energy-aware routing metrics account for the total energy cost associated with transmitting data along a route. This includes energy consumed during transmission, retransmission, idle listening, and reception. The key advantage of this metric is its ability to extend network lifetime by distributing energy consumption evenly across nodes, thereby avoiding premature battery depletion in specific parts of the network. Nevertheless, energy-efficient routing may introduce longer paths or higher delays if the selected route prioritizes energy conservation over minimal hop count. Moreover, implementing such a metric requires accurate estimation of residual battery levels, which adds to the computational and communication overhead.

2.5.5 QoS-Based Metrics (Priority Traffic, Reliability)

Quality of Service (QoS)-based metrics incorporate application-specific requirements such as minimum bandwidth, maximum delay, and reliability constraints. These metrics are particularly important in heterogeneous networks that support diverse traffic types—ranging from real-time applications to best-effort and mission-critical communications. The main benefit of QoS-based routing lies in its ability to provide differentiated service levels, improving user experience in multimedia and Internet of Things (IoT) environments. However, implementing QoS-based metrics is complex, especially in resource-limited ad hoc systems. Such metrics often require cross-layer coordination between the routing, MAC, and transport layers to manage bandwidth, prioritize packets, and ensure reliable delivery.

Routing metrics define the trade-offs between efficiency, reliability, and resource utilization in ad hoc networks.

- Hop count offers simplicity but ignores link quality.
- Link quality metrics improve reliability but add monitoring overhead.
- Delay, jitter, and PDR are crucial for real-time QoS applications but are complex to maintain dynamically.
- Energy-aware metrics maximize network lifetime but may compromise speed or latency.
- QoS-based metrics enable application-level optimization but increase protocol complexity.

To address these challenges, modern routing protocols increasingly adopt composite or adaptive metrics, combining multiple factors such as link stability, energy level, and delay. This multi-criteria approach provides a balanced trade-off between performance, energy efficiency, and reliability, enabling ad hoc networks to operate effectively in dynamic and resource-constrained environments.

2.6. Performance Challenges in Ad Hoc Routing

Routing in ad hoc wireless networks is inherently more complex than in infrastructure-based systems. The absence of centralized control, combined with node mobility, fluctuating wireless conditions, and limited resources, introduces several performance challenges that significantly impact network stability, efficiency, and security. Understanding these issues is vital for developing routing protocols that can adapt dynamically and maintain reliable communication in unpredictable environments.

2.6.1 Frequent Route Breakages due to Node Mobility

One of the most critical challenges in ad hoc routing is the frequent breaking of routes caused by node mobility. Since nodes are constantly moving, the network topology changes rapidly, making previously established routes invalid within short intervals. This results in increased route discovery frequency, leading to higher latency and greater control overhead. Additionally, broken paths often cause packet losses, thereby reducing the overall packet delivery ratio. To mitigate these issues, predictive mobility models can be used to anticipate link failures before they occur. Multipath routing techniques help maintain alternative backup routes, while local repair mechanisms allow quick restoration of broken links without initiating a full route discovery process.

2.6.2 High Control Overhead in Dynamic Networks

In ad hoc environments, routing protocols—especially proactive and reactive ones—generate significant control traffic to maintain up-to-date routes or discover new ones. In highly dynamic topologies, these control messages can consume considerable bandwidth and energy, reducing the capacity available for actual data transmission. This leads to reduced scalability, particularly in large or dense networks. Strategies to reduce overhead include adaptive update intervals that adjust based on node mobility, hybrid routing schemes that balance proactive and reactive behaviors, and cross-layer optimization to share link-state information efficiently between network layers.

2.6.3 Hidden and Exposed Terminal Problems

The wireless medium introduces two well-known issues that degrade network performance: the hidden terminal and exposed terminal problems. The hidden terminal problem occurs when two nodes that cannot sense each other's transmissions send data simultaneously to a common receiver, leading to packet collisions. Conversely, the exposed terminal problem happens when a node unnecessarily refrains from transmitting because it detects a nearby transmission that would not actually interfere. Both issues lead to low throughput and inefficient bandwidth utilization. Mitigation strategies include implementing RTS/CTS (Request to Send/Clear to Send) mechanisms as defined in IEEE 802.11, using directional antennas to minimize interference, and incorporating MAC-aware routing strategies that avoid congested or interference-prone regions.

2.6.4 Load Balancing Across Nodes

Uneven distribution of routing load is another major challenge in ad hoc networks. Certain nodes may act as primary relays, handling most of the network's traffic, which leads to faster energy depletion and potential network partitioning. Overloaded nodes may also become congestion points, causing increased delays and reduced performance. Effective load balancing ensures that no single node or link becomes a bottleneck. Solutions include energy-aware routing protocols that distribute traffic based on residual battery power, multipath routing to spread the load across multiple routes, and clustering techniques that divide the network into manageable regions for fair workload distribution.

2.6.5 Security Vulnerabilities (Blackhole, Wormhole, Sybil Attacks)

Security remains one of the most pressing concerns in ad hoc routing. The open and decentralized nature of these networks makes them vulnerable to various malicious attacks. Common threats include the blackhole attack, where a malicious node absorbs and drops packets instead of forwarding them; the wormhole attack, where attackers create a false tunnel between distant points to disrupt routing; and the Sybil attack, where a single node assumes multiple fake identities to manipulate routing decisions. Such attacks can lead to severe degradation in trust, confidentiality, and data delivery performance. To counter these threats, secure routing protocols incorporating authentication and encryption are essential. Additionally, trust-based frameworks can monitor node behavior to detect anomalies, while intrusion detection systems (IDS) specifically designed for ad hoc environments can provide real-time attack detection and response.

Ad hoc routing faces multifaceted performance challenges arising from node mobility, high control overhead, wireless interference, uneven load distribution, and security vulnerabilities. While existing proactive, reactive, and hybrid protocols attempt to mitigate these problems, none offer a complete solution under all conditions. Future routing designs must focus on adaptive, energy-efficient, and security-aware strategies capable of maintaining reliability and scalability in highly dynamic, resource-constrained environments.

2.7 Emerging Trends in Ad Hoc Routing

With the rapid evolution of wireless technologies, routing in ad hoc networks is advancing toward more intelligent, adaptive, and resilient paradigms. Traditional routing approaches, which primarily focused on minimizing hop count or delay, are no longer sufficient for modern applications such as autonomous vehicles, IoT ecosystems, smart cities, and tactical communication systems (Figure 3). The next generation of ad hoc routing protocols integrates context-awareness, artificial intelligence, and cross-layer coordination to meet the demands of scalability, reliability, and efficiency in highly dynamic environments.

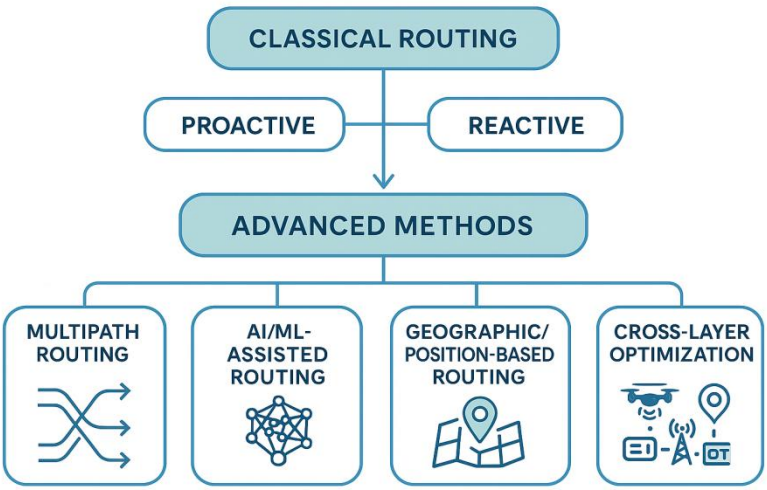


Figure 3: Emerging Trends in Routing: AI, Multipath, and Cross-Layer Approaches

2.7.1 Position-Based and Geographic Routing Protocols

Position-based or geographic routing protocols make routing decisions based on the physical locations of nodes rather than relying solely on topology tables. Nodes use GPS or other localization techniques to identify their geographic positions, allowing data to be forwarded in the direction of the destination. This approach significantly reduces routing table maintenance and overhead, making it suitable for large and dense networks. Notable examples include Greedy Perimeter Stateless Routing (GPSR) and Location-Aided Routing (LAR). These protocols improve scalability and efficiency but may face challenges in environments with poor localization accuracy or obstacles that disrupt direct line-of-sight communication.

2.7.2 Opportunistic and Delay-Tolerant Routing

Opportunistic and delay-tolerant routing strategies are designed for networks with intermittent connectivity or where stable end-to-end paths may not exist. These protocols leverage a store-carry-forward mechanism, allowing nodes to temporarily store data until they encounter another node capable of forwarding it closer to the destination. This concept is particularly useful in delay-tolerant networks (DTNs) such as those found in disaster recovery, deep rural communication, or space-based systems. Examples include Epidemic Routing, Spray and Wait, and PROPHET, which utilize mobility and probabilistic forwarding to ensure eventual data delivery even under harsh conditions.

2.7.3 Multipath Routing for Resilience

Multipath routing enhances network resilience by maintaining multiple alternative paths between the source and destination. Instead of relying on a single route, this approach distributes traffic across several routes, thereby improving fault tolerance, load balancing, and packet delivery ratio. It effectively mitigates the impact of node mobility, link failures, and congestion. Protocols such as Ad hoc On-Demand Multipath Distance Vector (AOMDV) and Multipath DSR (MDSR) exemplify this strategy, offering robust communication for real-time and mission-critical applications. Multipath routing also supports Quality of Service (QoS) by ensuring redundancy and maintaining stable throughput.

2.7.4 AI/ML-Assisted Adaptive Routing

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into routing has revolutionized decision-making in ad hoc networks. These approaches enable protocols to dynamically learn from network behavior and adapt to changes in topology, traffic patterns, and energy levels. Techniques such as reinforcement learning, neural networks, and deep learning help predict link stability, node mobility, and congestion levels. For instance, Q-routing applies reinforcement learning to select optimal paths based on experience, while deep learning models have been used in Vehicular Ad Hoc Networks (VANETs) for predictive route optimization. AI/ML-assisted routing enhances adaptability, reduces latency, and improves the balance between energy efficiency and throughput.

2.7.5 Cross-Layer Routing Strategies (PHY-MAC-Network Integration)

Cross-layer routing breaks the conventional isolation among the physical, MAC, and network layers to allow more integrated and intelligent decision-making. By considering parameters such as link quality, signal interference, and channel conditions from the lower layers, routing protocols can make more informed decisions about path selection and data forwarding. This holistic approach improves overall Quality of Service (QoS), spectrum efficiency, and energy utilization. Examples include cross-layer QoS-aware routing for multimedia traffic and MAC-assisted routing for sensor networks. However, while this integration enhances performance, it also adds design complexity and may challenge protocol modularity.

Emerging trends in ad hoc routing focus on scalability, resilience, and intelligence. Geographic routing simplifies communication in dense topologies, while opportunistic and delay-tolerant routing enables connectivity in intermittently connected networks. Multipath routing enhances reliability and QoS through redundancy, and AI/ML-assisted routing introduces adaptive intelligence for predictive decision-making. Cross-layer integration ensures end-to-end optimization by leveraging insights from multiple network layers. Collectively, these advancements are paving the way for next-generation ad hoc networks capable of supporting IoT infrastructures, 5G/6G systems, UAV swarms, and mission-critical communication environments that demand adaptability, efficiency, and robustness.

2.8 Comparative Analysis of Routing Strategies

Routing strategies in ad hoc networks can be broadly categorized into **table-based (proactive)**, **on-demand (reactive)**, and **hybrid** approaches. Each of these strategies offers unique advantages and trade-offs depending on network conditions, mobility, and resource constraints. The selection of a suitable strategy is crucial for optimizing performance across various domains such as Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs), Flying Ad Hoc Networks (FANETs), and Wireless Sensor Networks (WSNs). A detailed comparative analysis helps in understanding their operational mechanisms, benefits, limitations, and deployment suitability.

2.8.1 Table-Based (Proactive) Routing

In table-based or proactive routing, each node maintains continuously updated routing tables through the periodic exchange of control messages. This ensures that routes to all nodes are readily available at any time, providing low-latency communication. The main advantages of proactive routing are immediate route availability and predictable performance in stable network conditions. However, this approach generates high control overhead, especially in large or highly mobile networks where frequent topology changes occur. Such overhead consumes bandwidth and energy, reducing network efficiency and scalability. Proactive routing is therefore most effective in static or low-mobility environments, such as small MANETs or WSNs. Prominent examples include Destination-Sequenced Distance Vector (DSDV) and Optimized Link State Routing (OLSR) protocols.

2.8.2 On-Demand (Reactive) Routing

On-demand or reactive routing protocols create routes only when they are required for data transmission. Instead of maintaining routing tables for all nodes, a route discovery process is initiated through Route Request (RREQ) and Route Reply (RREP) messages when communication is needed. This significantly reduces control overhead, making reactive protocols more efficient in dynamic and resource-constrained environments. However, the initial route discovery introduces latency, which may affect time-sensitive applications. Additionally, frequent route breakages due to high mobility can degrade performance. Reactive routing is ideal for high-mobility scenarios such as MANETs, VANETs, and FANETs, where topological changes occur frequently. Well-known examples include Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR).

2.8.3 Hybrid Routing

Hybrid routing protocols combine the strengths of both proactive and reactive approaches. Typically, they maintain proactive routing information within a local zone, while employing reactive routing for nodes beyond that zone. This design achieves a balance between low latency for nearby communication and reduced overhead for distant transmissions. The adaptability of hybrid protocols makes them suitable for large-scale and heterogeneous networks. However, they are more complex to configure, as their performance depends on parameters such as the optimal zone radius and node density. Hybrid routing performs effectively in large MANETs, tactical military networks, and IoT-based ad hoc systems. Common examples include the Zone Routing Protocol (ZRP) and Hybrid Wireless Mesh Protocol (HWMP).

2.8.4 Trade-offs in Routing Strategies

The following trade-offs highlight how proactive, reactive, and hybrid routing differ across key performance metrics:

Aspect	Table-Based (Proactive)	On-Demand (Reactive)	Hybrid
Latency	Very low (routes always available)	Higher (due to route discovery)	Moderate (depends on intra-/inter-zone)
Control Overhead	High (continuous updates)	Low (only when needed)	Medium (zonal optimization)
Energy Efficiency	Low (due to frequent updates)	Higher (reduced control messages)	Balanced (optimized for conditions)
Scalability	Limited	Better in dynamic, smaller networks	Good for large-scale heterogeneous networks
Suitability	Stable MANETs, small WSNs	High-mobility MANETs, VANETs, FANETs	Large MANETs, tactical/IoT networks

This comparison demonstrates that no single approach is universally superior—each offers advantages under specific network conditions and design goals.

2.8.5 Suitability for Different Application Domains

Different ad hoc network types have distinct requirements, and routing strategy suitability varies accordingly. In MANETs (Mobile Ad Hoc Networks), reactive and hybrid approaches dominate due to frequent topology changes. VANETs (Vehicular Ad Hoc Networks) favor reactive routing (such as AODV or DSR) and geographic-based methods to cope with high mobility. In FANETs (Flying Ad Hoc Networks), hybrid and geographic routing strategies are preferred to handle three-dimensional mobility and rapid link fluctuations. Conversely, WSNs (Wireless Sensor Networks) benefit from proactive or energy-aware hybrid protocols, as they are generally static and resource-limited.

Proactive routing protocols excel in stable, small-scale networks by providing instant route access but suffer from excessive overhead in dynamic environments. Reactive protocols are more suitable for high-mobility scenarios, offering reduced overhead but at the cost of higher latency. Hybrid protocols present a balanced solution, effectively combining responsiveness and scalability for large, heterogeneous ad hoc systems. Ultimately, the choice of routing strategy should align with factors such as application domain, node mobility, network density, energy constraints, and Quality of Service (QoS) requirements to ensure optimal performance.

2.9 Case Studies and Real-World Applications

The practical significance of ad hoc routing protocols becomes most evident when applied to real-world scenarios. Various domains—ranging from disaster recovery and intelligent transportation systems (ITS) to UAV swarms and industrial IoT—demand specialized routing solutions that can address their unique performance, scalability, and reliability challenges. The following case studies illustrate how different routing protocols are implemented and optimized for diverse operational environments.

2.9.1 AODV in Disaster Recovery Networks

In post-disaster environments such as earthquakes, floods, or hurricanes, traditional communication infrastructure is often destroyed or rendered inoperative. In such cases, the Ad hoc On-Demand Distance Vector (AODV) routing protocol proves highly effective due to its reactive nature, establishing routes only when required. This minimizes control overhead and conserves bandwidth in resource-limited conditions.

AODV's main advantages include quick deployment without the need for centralized infrastructure and dynamic route adaptation as rescue teams and emergency vehicles move within the affected area. However, the frequent movement of nodes can lead to route breakages, resulting in higher latency and packet loss. Additionally, the protocol can be vulnerable to security threats like blackhole and wormhole attacks in hostile conditions. Despite these challenges, AODV has been effectively used in emergency response frameworks deployed by organizations such as the Red Cross and FEMA, enabling robust communication among first responders in disaster-stricken zones.

2.9.2 VANET Routing for Intelligent Transport Systems (ITS)

Vehicular Ad Hoc Networks (VANETs) form the foundation of intelligent transport systems, facilitating vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. These networks enable a wide range of applications, including real-time traffic monitoring, collision avoidance, emergency alerts, and infotainment services.

Routing protocols in VANETs must cope with high mobility, rapid topology changes, and urban interference. Commonly used protocols include GPSR (Greedy Perimeter Stateless Routing), which relies on geographic forwarding, and AODV or DSR variants adapted for

vehicular environments. The advantages of VANET routing include low-latency message dissemination for safety-critical operations and improved traffic flow through adaptive routing decisions. However, challenges such as urban canyon effects and frequent link failures due to high vehicle speeds remain significant obstacles.

Real-world VANET implementations are central to connected vehicle trials in Europe, Japan, and the United States, supporting initiatives like cooperative driving, smart highways, and automated transport systems.

2.9.3 FANET Routing in UAV Swarms

Flying Ad Hoc Networks (FANETs) consist of unmanned aerial vehicles (UAVs) that communicate autonomously to execute collaborative missions, including aerial surveillance, search-and-rescue, and precision agriculture. FANET routing faces unique challenges such as 3D mobility, rapid topology fluctuations, and intermittent connectivity due to aerial dynamics.

Routing in FANETs often relies on optimized variants of OLSR and AODV or geographic routing protocols that utilize UAV positions and predicted trajectories. These methods enhance swarm coordination and fault tolerance, ensuring reliable communication during mission-critical operations. Advantages include multipath routing for resilience and swarm intelligence for coordinated task execution. The primary challenges are topology fragmentation and energy constraints, as UAVs typically have limited battery capacity.

FANET-based communication has been deployed in applications such as border surveillance, disaster response, wildfire monitoring, and military reconnaissance, highlighting its potential in dynamic aerial environments.

2.9.4 WSN Routing for Industrial IoT

Wireless Sensor Networks (WSNs) serve as a critical component of the Industrial Internet of Things (IIoT), enabling data-driven operations in smart manufacturing, environmental sensing, and predictive maintenance. In these environments, routing must prioritize energy efficiency, scalability, and reliable data transmission.

Two widely adopted protocols in this domain are LEACH (Low-Energy Adaptive Clustering Hierarchy) and RPL (Routing Protocol for Low Power and Lossy Networks). LEACH employs cluster-based routing to reduce communication overhead and balance energy consumption among sensor nodes, while RPL supports hierarchical data delivery optimized for large-scale IoT deployments.

The main advantages of WSN routing include extended network lifetime, high scalability, and robust performance under varying conditions. However, challenges such as limited node energy, low processing capability, and interference in industrial environments can

hinder performance. Real-world applications of WSN routing include smart factories, oil and gas monitoring, and precision agriculture, forming the backbone of modern Industry 4.0 systems.

These case studies underscore the **diversity and adaptability** of ad hoc routing protocols across multiple domains:

- **AODV** supports **rapid and infrastructure-free deployment** in disaster recovery networks.
- **VANET routing** enhances **road safety and intelligent mobility** in smart transportation systems.
- **FANET routing** empowers **UAV swarms** to perform coordinated missions in challenging aerial environments.
- **WSN routing** enables **energy-efficient communication** in large-scale industrial IoT networks.

Each application domain presents unique **mobility, scalability, and security challenges**, emphasizing that there is **no one-size-fits-all solution**. Instead, routing strategies must be carefully tailored to the operational context, ensuring optimal performance, reliability, and resilience in real-world ad hoc network deployments.

2.10. Conclusion

This chapter introduced the fundamentals of routing in wireless ad hoc networks, emphasizing its critical role in enabling communication within decentralized, infrastructure-less environments. The discussion began with the basic principles of routing, including route discovery, maintenance, and the importance of efficient path construction in dynamic topologies. Routing protocols were broadly classified into proactive, reactive, and hybrid approaches, each offering distinct advantages and limitations. Proactive methods provide low-latency communication at the cost of high control overhead, reactive protocols reduce overhead but incur route discovery delays, while hybrid approaches seek to balance these trade-offs. The chapter also highlighted essential design considerations such as scalability, energy efficiency, adaptability to mobility, and security awareness. Various routing metrics—including hop count, link quality, delay, jitter, and energy consumption—were examined to illustrate how protocol performance is measured. Key performance challenges such as frequent route breakages, high control overhead, hidden/exposed terminal problems, and security vulnerabilities were discussed in depth. Furthermore, emerging trends like AI/ML-driven routing, geographic and opportunistic approaches, multipath resilience, and cross-layer design were introduced as pathways toward addressing these challenges. A comparative analysis of routing strategies demonstrated the trade-offs between latency, scalability, energy efficiency, and reliability, showing that no single approach is universally optimal. Real-world case studies—including AODV in disaster recovery, VANET routing in intelligent transport systems, FANET routing in UAV swarms, and WSN routing in industrial IoT—underscored the practical relevance of these protocols across diverse domains. Routing in ad hoc networks involves balancing multiple trade-offs

between performance, overhead, adaptability, and security. These fundamentals form the foundation for the more detailed exploration of specific routing families. The next chapter will focus on Proactive Routing Protocols in Ad Hoc Networks, examining table-driven approaches such as DSDV and OLSR in detail.

References

1. Arafat, M. Y., & Moh, S. (2019). Routing protocols for wireless sensor networks in smart grid environments: A survey. *IEEE Access, 7*, 38597–38620. https://doi.org/10.1109/ACCESS.2019.2904890
2. Boukerche, A., Turgut, B., Aydin, N., Ahmad, M. Z., Bölöni, L., & Turgut, D. (2020). Routing protocols in ad hoc networks: A survey. *Computer Networks, 172*, 107145. https://doi.org/10.1016/j.comnet.2020.107145
3. Chouhan, S. S., Sharma, R., & Singh, P. K. (2021). Energy-aware multipath routing protocols for MANETs: A survey and future directions. *Journal of Network and Computer Applications, 177*, 102938. https://doi.org/10.1016/j.jnca.2021.102938
4. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546. https://doi.org/10.1016/j.future.2017.07.060
5. Darabkh, K. A., Hassan, M. A., & El-Yabroudi, M. Z. (2019). Energy-aware and load-balancing multipath routing protocol for MANETs. *Ad Hoc Networks, 84*, 149–169. https://doi.org/10.1016/j.adhoc.2018.10.016
6. Gurung, S., & Chauhan, S. (2020). Trust-based secure routing in MANET using fuzzy logic. *Wireless Networks, 26*(3), 2011–2028. https://doi.org/10.1007/s11276-019-02147-8
7. Hassan, R., Hossain, M. S., Alshamrani, S. S., & Fortino, G. (2021). Machine learning for routing in vehicular ad hoc networks: A comprehensive survey. *Computer Communications, 172*, 33–56. https://doi.org/10.1016/j.comcom.2021.02.012
8. Kaur, K., Garg, S., Ahmed, S. H., & Rodrigues, J. J. P. C. (2019). Edge computing in the Industrial Internet of Things environment: Software-defined-networks-based edge-cloud interplay. *IEEE Communications Magazine, 56*(2), 44–51. https://doi.org/10.1109/MCOM.2018.1700642
9. Khan, M. A., Abbas, F., & Ghafoor, K. (2019). Position-based routing protocols for vehicular ad hoc networks: A survey. *Vehicular Communications, 13*, 66–79. https://doi.org/10.1016/j.vehcom.2018.05.004
10. Koutsiamanis, R. A., Passarella, A., & Conti, M. (2018). Opportunistic networking protocols for IoT: A survey. *IEEE Communications Surveys & Tutorials, 20*(2), 1322–1346. https://doi.org/10.1109/COMST.2018.2788763
11. Kumar, V., Kumar, R., & Rodrigues, J. J. P. C. (2020). Intelligent and energy-efficient routing for wireless sensor networks: Machine learning approach. *Computer Communications, 150*, 324–341. https://doi.org/10.1016/j.comcom.2019.11.030

12. Lin, Y. D., Chen, Y. C., & Lai, Y. C. (2020). Cross-layer routing design in mobile ad hoc networks. *Ad Hoc Networks, 100*, 102079. https://doi.org/10.1016/j.adhoc.2019.102079
13. Liu, C., Li, Y., & Guo, S. (2021). AI-assisted routing in UAV ad hoc networks: A survey. *IEEE Communications Surveys & Tutorials, 23*(4), 2669–2709. https://doi.org/10.1109/COMST.2021.3102721
14. Mehmood, A., Khan, M. N. A., & Shafiq, O. (2020). Secure routing in wireless sensor networks: A machine learning perspective. *Future Generation Computer Systems, 108*, 1102–1115. https://doi.org/10.1016/j.future.2020.03.024
15. Miao, F., Han, Z., & Zhang, H. (2019). Distributed energy-efficient multipath routing in MANETs using game theory. *IEEE Transactions on Mobile Computing, 18*(12), 2749–2762. https://doi.org/10.1109/TMC.2018.2889045
16. Oubbati, O. S., Chaib, N., Lakas, A., & Lorenz, P. (2019). A survey on position-based routing protocols for flying ad hoc networks (FANETs). *Vehicular Communications, 13*, 1–13. https://doi.org/10.1016/j.vehcom.2018.09.004
17. Qureshi, K. N., Din, S., & Jeon, G. (2020). Adaptive load-aware routing protocols for IoT-based ad hoc networks. *Journal of Network and Computer Applications, 160*, 102631. https://doi.org/10.1016/j.jnca.2020.102631
18. Roy, S., Misra, S., & Obaidat, M. S. (2019). Blockchain for secure routing in MANETs: A distributed trust management approach. *IEEE Internet of Things Journal, 6*(3), 4689–4697. https://doi.org/10.1109/JIOT.2018.2876152
19. Sairam, A., & Kumar, M. (2021). Quality of service-aware routing in mobile ad hoc networks: A survey. *Wireless Personal Communications, 117*(3), 1725–1746. https://doi.org/10.1007/s11277-020-07730-8
20. Sharma, S., & Ghose, M. K. (2021). Secure and energy-efficient hybrid routing for heterogeneous ad hoc networks. *Ad Hoc Networks, 115*, 102453. https://doi.org/10.1016/j.adhoc.2021.102453

Chapter-3

Proactive Routing Protocols: Design and Applications

[1]S.Sasipriya, [2]D.Jeevitha, [3]M.Dharshini

[1,] Assistant Professor,
Department of Computer Applications,
K.S.Rangasamy College of Arts and Science (Autonomous),
Tiruchengode,Tamilnadu, India.

[2,3]Assistant Professor,
Department of Computer Applications,
K.S.Rangasamy College of Arts and Science (Autonomous),
Tiruchengode,Tamilnadu, India.

Abstract: *This chapter explores proactive routing protocols—also known as table-driven routing—which form a foundational approach to routing in ad hoc wireless networks. Unlike reactive methods that initiate route discovery only when data transmission is required, proactive protocols maintain continuous and up-to-date routing tables through periodic information exchanges among network nodes. The chapter begins with an introduction to the core principles and operational mechanisms of proactive routing, followed by a detailed examination of key protocols such as Destination-Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR), Wireless Routing Protocol (WRP), and Global State Routing (GSR). It discusses the design considerations, including trade-offs between update frequency, bandwidth utilization, and energy efficiency, as well as the importance of maintaining loop-free, consistent, and low-latency routes. The chapter also evaluates performance metrics such as routing overhead, packet delivery ratio, and scalability in dense networks. Comparative analyses highlight the suitability of proactive routing for various environments like MANETs, VANETs, FANETs, and WSNs, emphasizing applications in military communication, disaster recovery, healthcare, and smart cities. Finally, the chapter explores current trends and enhancements, including AI-driven predictive routing, energy-aware algorithms, and 5G/6G integration, along with case studies that demonstrate real-world implementations of proactive routing protocols.*

Keywords: *Proactive Routing, Table-Driven Protocols, DSDV, OLSR, WRP, GSR, Ad Hoc Networks, MANET, VANET, FANET, WSN, Low Latency, Routing Overhead, Energy Efficiency, Scalability, Periodic Updates, Loop-Free Routing, Edge Computing, AI-Based Routing, 5G/6G Networks.*

3.1 Introduction to Proactive Routing

Proactive routing also referred to as **table-driven routing**, represents one of the fundamental approaches to route management in ad hoc wireless networks. In this paradigm, each node maintains up-to-date routing tables containing the best-known paths to all other nodes in the network. These tables are refreshed periodically through the exchange of control messages, ensuring that routes remain valid even before they are required for data

transmission. Unlike reactive routing, which establishes routes only when needed, proactive routing ensures that network-wide route information is always available, thereby minimizing latency during data transfer (Figure 1).

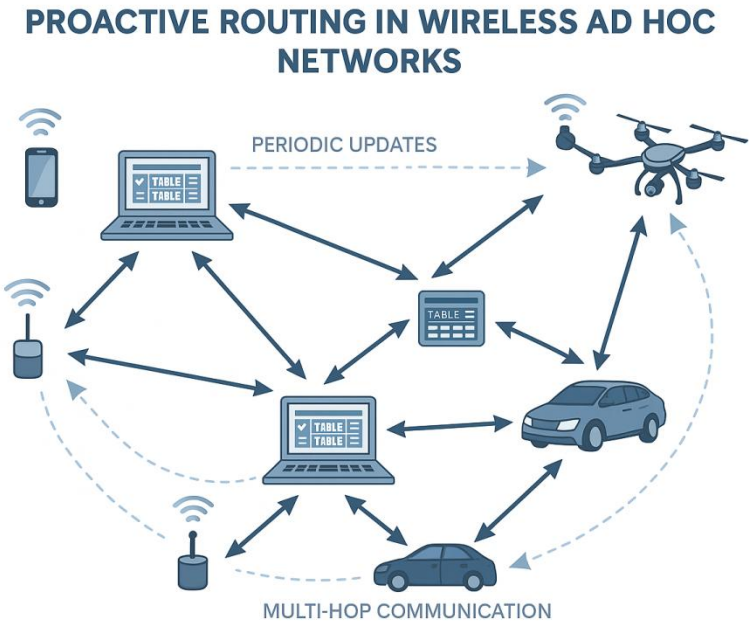


Figure 1: Architecture and Operation of Proactive Routing Protocols

Proactive routing protocols establish and maintain a global knowledge of network topology by continuously disseminating routing information throughout the network. Each node stores one or more routing tables that are updated at regular intervals or whenever significant topology changes occur. This ensures that when a packet needs to be forwarded, a valid and up-to-date route is already available without delay.

The key principle of proactive routing is to maintain fresh routes at all times. This is achieved through the periodic exchange of routing updates across all nodes in the network. Some of the most prominent examples of proactive routing protocols include the Destination-Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR), and the Wireless Routing Protocol (WRP). These protocols differ in their methods of table maintenance and control overhead, but they share the same fundamental goal of keeping the routing information continuously updated.

Role of Periodic Route Updates in Maintaining Global Topology Knowledge

Periodic route updates play a crucial role in ensuring that all nodes in the network maintain a synchronized and consistent view of the overall topology.

- **Topology Awareness:** Every node possesses near real-time knowledge of all reachable destinations, allowing seamless communication even in dynamic environments.

- **Low Latency:** Since routes are pre-computed, packets can be forwarded immediately without initiating a route discovery process.
- **Consistency:** Mechanisms such as sequence numbers and update intervals help prevent routing loops and maintain accuracy across routing tables.
- **Resilience:** Even in the presence of node mobility or link failures, periodic updates quickly propagate the changes across the network, ensuring continued connectivity and reliability.

This constant dissemination of control messages forms the backbone of proactive routing and is what differentiates it from reactive or hybrid schemes.

Strengths and Weaknesses Compared to Reactive and Hybrid Protocols

Aspect	Proactive (Table-driven)	Reactive (On-demand)	Hybrid
Route Availability	Always available (pre-computed)	Discovered when needed	Available within local zones
Latency	Very low (immediate forwarding)	Higher (due to discovery delay)	Moderate
Control Overhead	High (due to periodic updates, even when unused)	Lower (updates only when needed)	Balanced
Scalability	Limited; overhead grows with network size	Better scalability	High scalability
Energy Efficiency	Lower; constant updates consume more power	Higher; fewer updates required	Balanced
Best Suited For	Low-latency, stable environments	Highly dynamic, traffic-driven networks	Large and heterogeneous systems

Strengths of Proactive Routing

Proactive routing ensures **minimal latency** for data delivery, as routes are readily available when needed. It provides **consistent and loop-free paths**, guaranteeing reliability in communication. This makes it ideal for **time-critical applications**, such as military networks, healthcare systems, and industrial monitoring, where communication delay must be minimized.

Weaknesses of Proactive Routing

Despite its advantages, proactive routing also faces several limitations. It introduces **high routing overhead** due to continuous table updates, even when there is little or no data transmission. This limits its scalability in **large or highly mobile networks**, where frequent topology changes can cause excessive control traffic. Additionally, **energy consumption is**

higher, making it less suitable for **battery-powered or resource-constrained devices** such as wireless sensors or IoT nodes.

Proactive routing protocols are best suited for scenarios that prioritize **low latency and consistent connectivity** over energy efficiency and scalability. Their deterministic nature makes them dependable in stable or moderately mobile environments, serving as a foundation for mission-critical and delay-sensitive applications.

3.2 Working Mechanism of Proactive Protocols

Proactive routing protocols operate through the continuous exchange of routing information, ensuring that every node in an ad hoc wireless network maintains a consistently updated view of the network topology. Unlike reactive protocols, which discover routes only when required, proactive approaches keep route information current at all times, allowing data packets to be transmitted without delay. The functioning of these protocols revolves around key mechanisms such as routing table construction, periodic updates, the use of sequence numbers and timers, route maintenance strategies, and efficient handling of topology changes and link failures.

3.2.1 Routing Table Construction and Update Mechanisms

When a node first joins the network, it initializes a routing table containing destination addresses, next-hop nodes, and routing metrics such as hop count and link quality. This table serves as the foundation for all routing decisions. Each node periodically broadcasts its routing information to its neighboring nodes, enabling the propagation of routing data across the entire network and allowing every node to build a comprehensive and synchronized view of the network topology.

To optimize efficiency, many protocols—such as Destination-Sequenced Distance Vector (DSDV)—support incremental updates, where only the changed parts of the routing table are transmitted instead of the full table. This reduces bandwidth consumption and control message overhead. Typical routing table entries include the destination node ID, the next hop, the path cost metric, and a sequence number to ensure that the most recent and valid route is used for packet forwarding.

3.2.2 Use of Sequence Numbers, Timers, and Periodic Broadcasts

Sequence numbers play a crucial role in maintaining route freshness and preventing routing loops. Each destination node assigns monotonically increasing sequence numbers to its routes, ensuring that nodes always select the path with the highest sequence number, indicating the most recent information.

Timers are employed to regulate the periodic broadcasting of routing information and to remove stale entries from routing tables. If a route remains unused or unacknowledged for a

specific duration, it is automatically marked as expired to prevent incorrect forwarding decisions.

Periodic broadcasts ensure that all nodes maintain an up-to-date network view; however, this approach introduces significant control overhead in large or highly mobile networks. To reduce redundancy, optimized protocols like Optimized Link State Routing (OLSR) utilize **Multipoint Relays (MPRs)**, where only selected nodes are responsible for rebroadcasting updates. This drastically cuts down on unnecessary transmissions while maintaining efficient network-wide dissemination.

3.2.3 Route Maintenance Strategies

Proactive routing protocols maintain routes even when they are not immediately needed, ensuring that paths are always available for data transmission. This **proactive maintenance** minimizes delay but increases bandwidth and energy consumption due to continuous updates.

To ensure consistency, routing loops are avoided through mechanisms such as sequence numbering and link-state validation. Nodes periodically verify the reachability of their neighbors using "hello" messages or acknowledgment signals. When inconsistencies or broken links are detected, routing tables are refreshed through periodic updates or triggered messages, restoring accurate network topology information.

This approach guarantees rapid route recovery and minimizes packet loss, though it may lead to increased control overhead in highly dynamic environments.

3.2.4 Handling Topology Changes and Link Failures

Mobility is a defining characteristic of ad hoc networks, and frequent topology changes can disrupt established routes. Proactive protocols address this challenge through rapid dissemination of updated routing information. When a link breaks, protocols such as DSDV immediately initiate a **triggered update**, broadcasting new information throughout the network to re-establish valid routes and reduce packet loss.

Some proactive protocols also maintain **multiple alternative paths** to destinations, enabling quick rerouting when primary links fail. Entries corresponding to unreachable nodes are marked as **invalid** until new information is received, helping prevent routing errors. However, this robustness comes at the cost of higher signaling overhead and energy consumption, especially under conditions of high mobility or dense node deployment. Despite these challenges, proactive routing remains valuable for networks that prioritize low-latency communication and consistent topology awareness.

The working mechanism of proactive routing protocols revolves around continuous routing table updates, sequence number management, and rapid dissemination of topology changes

to maintain a coherent and consistent network view. This ensures **low-latency route availability** and **high reliability**, making proactive routing suitable for time-sensitive applications. However, these benefits are offset by **increased control overhead** and **higher energy consumption**, particularly in large or highly dynamic ad hoc networks.

3.3 Advantages and Limitations of Proactive Routing

Proactive routing protocols provide several key benefits that make them advantageous in certain ad hoc network environments, while their inherent drawbacks limit their efficiency in others. These protocols maintain up-to-date routing tables through periodic exchanges, ensuring immediate route availability but at the cost of high control overhead. Understanding their advantages, limitations, and trade-offs helps in determining where they are most effectively deployed.

3.3.1 Advantages of Proactive Routing

One of the most significant advantages of proactive routing protocols is **low-latency data delivery**. Since routes are precomputed and continuously updated, packets can be forwarded immediately without waiting for a route discovery phase. This feature is particularly beneficial for **real-time or delay-sensitive applications** such as Voice over IP (VoIP), live video streaming, and mission-critical communications like military or emergency operations.

Another major benefit is **predictable performance**. Because routing decisions are made using regularly refreshed global topology information, proactive protocols ensure consistent and stable packet forwarding. This predictability makes them well-suited for low-mobility or moderately dynamic networks, where the overall topology does not fluctuate rapidly.

Proactive protocols also demonstrate **robustness in steady or static networks**. In environments such as industrial wireless sensor networks, where node positions remain fixed or change infrequently, proactive routing provides reliable long-term connectivity. The periodic updates not only maintain accurate topology information but also facilitate rapid detection and correction of link failures, enhancing overall reliability and uptime.

3.3.2 Limitations of Proactive Routing

Despite their advantages, proactive routing protocols face several key challenges. The most prominent limitation is **high control overhead**. Because these protocols rely on periodic broadcasting of routing information, bandwidth is consumed even during periods of low or no data transmission. In large or highly mobile networks, this can lead to network congestion and wasted communication resources.

Another limitation involves **scalability challenges**. As the number of nodes increases, both the routing table size and update frequency expand, placing significant strain on network resources. Maintaining an updated global view of topology in massive or dense networks

becomes computationally intensive and inefficient, making proactive protocols less suitable for large-scale ad hoc deployments.

A third drawback is **wasted resources in low-traffic scenarios**. Even when routes are not used, proactive protocols continue to consume energy and bandwidth to maintain them. This inefficiency can be detrimental in energy-constrained systems such as **Wireless Sensor Networks (WSNs)** or battery-operated IoT devices, where prolonging network lifetime is a critical goal.

3.3.3 Trade-offs Between Energy Efficiency and Latency

Proactive routing protocols inherently involve a trade-off between energy efficiency and latency. Continuous periodic updates require significant energy expenditure, which reduces node and network lifetime. However, the advantage is that routes are always available, minimizing end-to-end delay during data transmission.

The balance between these two factors depends on the application's priorities. In delay-sensitive applications, such as military communications or disaster recovery systems, minimizing latency takes precedence, and the extra energy cost is considered acceptable. Conversely, in energy-limited networks—like IoT or sensor-based systems—where conserving battery life is paramount, the high overhead of proactive routing makes reactive or hybrid approaches more practical.

Proactive routing protocols offer fast, reliable, and predictable communication by maintaining precomputed routes, which ensures minimal latency and consistent performance. However, these benefits come at the expense of high control overhead, limited scalability, and increased energy consumption. The decision to use proactive routing depends largely on the specific requirements of the application—particularly the balance between latency sensitivity and energy efficiency. For stable and latency-critical networks, proactive protocols remain a strong choice, while dynamic or resource-constrained environments may benefit more from reactive or hybrid alternatives.

3.4 Key Proactive Routing Protocols

Proactive routing protocols rely on periodic updates to maintain a consistent and up-to-date view of the network topology. These protocols aim to ensure that routes to all possible destinations are available at any given time, minimizing the need for route discovery delays. Several well-established protocols exemplify different design philosophies, each offering distinct advantages and limitations. Figure 2, This section examines four major proactive routing protocols widely discussed in ad hoc network research and implementations: Destination-Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR), Wireless Routing Protocol (WRP), and Global State Routing (GSR).

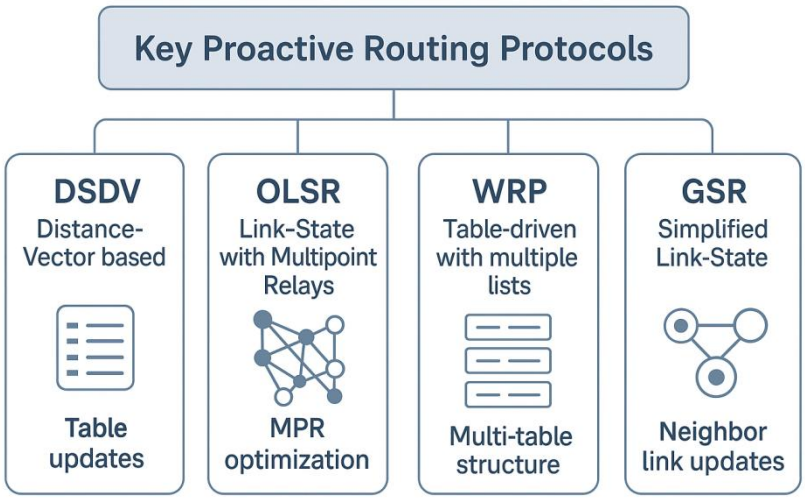


Figure 2: Classification and Mechanisms of Proactive Routing Protocols

4.1 Destination-Sequenced Distance Vector (DSDV)

The Destination-Sequenced Distance Vector (DSDV) protocol is based on the Bellman-Ford distance vector algorithm, where each node maintains a routing table containing the next hop and hop count to every possible destination. DSDV introduces sequence numbers, generated by destination nodes, to prevent routing loops and ensure the freshness of routing information. The protocol operates through periodic broadcasts of routing tables to neighboring nodes. When minor topology changes occur, only incremental updates are sent, while full dumps are used for significant changes.

DSDV's strengths include providing loop-free routes, maintaining a consistent global topology, and offering simplicity in small to medium-sized networks. However, it suffers from high control overhead due to frequent updates, poor scalability in large or dynamic networks, and resource wastage in maintaining routes that may not be immediately used.

3.4.2 Optimized Link State Routing (OLSR)

The Optimized Link State Routing (OLSR) protocol is a proactive link-state routing mechanism designed to reduce the flooding overhead of traditional link-state methods. It introduces the innovative concept of Multipoint Relays (MPRs)—selected nodes that are solely responsible for forwarding control messages. This reduces redundant retransmissions and significantly improves efficiency.

OLSR operates by exchanging HELLO messages to discover neighboring nodes and select MPRs. Topology Control (TC) messages are then disseminated through these MPRs to update the network topology. OLSR's advantages include better scalability, faster route computation, and efficient operation in dense networks. However, it still incurs some control overhead due to periodic HELLO and TC exchanges, and its performance may degrade in sparse or highly mobile scenarios.

3.4.3 Wireless Routing Protocol (WRP)

The Wireless Routing Protocol (WRP) is a table-driven approach that ensures loop-free routing by maintaining multiple tables, including the distance table, routing table, link-cost table, and message retransmission list. It employs a path-finding mechanism in which updates are triggered by link changes rather than periodic intervals. Each node exchanges update messages with neighbors and uses message retransmission lists to guarantee reliable delivery of control information.

WRP achieves fast convergence and maintains highly accurate routes, making it suitable for networks requiring reliability. However, it imposes high storage and processing demands due to multiple routing tables and larger control messages. Consequently, WRP is less practical for large-scale or highly dynamic networks where overhead and complexity can become significant.

3.4.4 Global State Routing (GSR)

The Global State Routing (GSR) protocol is a simplified link-state-based approach designed for wireless ad hoc networks. It maintains connectivity and distance information without requiring full flooding of link-state updates. Each node exchanges link-state information only with its neighbors, which significantly reduces control message overhead while still ensuring a coherent global network view.

GSR's periodic updates help maintain network consistency, making it more bandwidth-efficient than traditional link-state protocols. It also offers better scalability with moderate complexity. However, it still experiences periodic overhead, and its performance depends on the update frequency and node mobility. In highly dynamic topologies, maintaining accurate global state information becomes challenging.

Protocol	Core Idea	Strengths	Limitations	Best Use Cases
DSDV	Distance-vector with sequence numbers	Loop-free, consistent routes, simple design	High overhead, poor scalability	Small/medium ad hoc networks
OLSR	Link-state with MPR optimization	Scalable, reduced flooding, good in dense networks	Overhead in sparse/high-mobility scenarios	VANETs, dense MANETs
WRP	Multiple tables for loop-free	Fast convergence, accurate routes	High memory & processing	Stable networks requiring

	routing		demand	reliability
GSR	Simplified link-state with neighbor updates	Bandwidth-efficient, scalable	Overhead in dynamic topologies	Moderate-size WSNs, IoT deployments

3.5 Design Considerations in Proactive Routing

Designing effective **proactive (table-driven) routing protocols** involves achieving a delicate balance between maintaining accurate, up-to-date routing information and minimizing the consumption of limited network resources. Since proactive protocols rely on periodic updates and a global view of network topology, their efficiency depends on how well they manage control message frequency, mobility adaptation, loop prevention, and energy conservation. Several key design considerations must be addressed to optimize their performance in dynamic and resource-constrained ad hoc environments.

3.5.1 Frequency of Periodic Updates vs. Bandwidth Utilization

One of the most critical design challenges in proactive routing is managing the frequency of routing updates. Frequent updates ensure that topology information remains current, minimizing stale routes and improving packet delivery accuracy. However, such updates significantly increase control overhead, consuming valuable bandwidth and processing power. On the other hand, infrequent updates reduce overhead but risk outdated routes, leading to packet loss and transmission delays. Therefore, the design goal is to determine an optimal update interval that balances accuracy and efficiency based on factors such as network size, density, and node mobility.

3.5.2 Handling Node Mobility and Dynamic Topologies

Ad hoc networks are inherently dynamic, with nodes frequently moving, joining, or leaving the network. These mobility patterns cause constant topology changes that must be efficiently managed. Effective proactive protocols incorporate adaptive update intervals that increase during high-mobility periods to maintain accurate routing information, while localized update mechanisms are used to avoid unnecessary global flooding of control messages. These strategies enhance the robustness of the protocol under dynamic conditions while reducing unnecessary bandwidth consumption.

3.5.3 Ensuring Loop-Free and Consistent Routes

Maintaining loop-free and consistent routes is essential for the stability and reliability of proactive routing protocols. Routing loops can waste network resources, cause packet duplication, and increase latency. To prevent these issues, mechanisms such as sequence numbers (as used in DSDV) are employed to verify the freshness of routing information and prevent outdated routes from being used. Additionally, path validation mechanisms help

detect and eliminate routing inconsistencies. These design elements ensure reliable data delivery and contribute to the overall integrity of network communication.

3.5.4 Balancing Routing Overhead with Network Performance

Another major consideration in proactive routing is the trade-off between control overhead and network performance. Since each node maintains routing tables for all possible destinations, excessive control message exchanges can overload the network. To mitigate this, various strategies are employed, such as selective flooding techniques like Multipoint Relays (MPRs) in OLSR, incremental updates instead of full table dumps, and hierarchical routing to reduce table size and control message volume. These mechanisms help achieve an optimal balance between responsiveness and resource efficiency, enabling proactive protocols to function effectively across different network conditions.

3.5.5 Energy Consumption Challenges

Energy efficiency is a crucial design parameter, especially for battery-powered nodes in mobile or sensor networks. Frequent broadcasts and continuous listening for updates can rapidly drain energy, reducing the operational lifetime of the network. To address this, proactive protocols may implement energy-aware routing strategies that minimize redundant transmissions and use duty-cycling techniques to reduce power consumption during low-traffic periods. By managing energy more efficiently, these protocols can extend network lifespan and ensure sustainable performance, particularly in Wireless Sensor Networks (WSNs) and mobile devices.

Designing proactive routing protocols involves optimizing update frequency, scalability, loop prevention, and energy efficiency to ensure consistent performance under diverse network conditions. A well-designed proactive routing protocol dynamically adapts to varying mobility levels, traffic patterns, and resource constraints while minimizing unnecessary control overhead. By balancing accuracy, responsiveness, and resource utilization, proactive routing can deliver reliable and energy-efficient communication across different types of ad hoc networks.

3.6 Performance Metrics for Proactive Protocols

The performance of proactive routing protocols in ad hoc networks is assessed using a set of quantitative metrics that measure their efficiency, reliability, and scalability. Because these protocols rely on continuous, table-driven updates, their performance can be significantly influenced by network parameters such as node mobility, network density, and traffic load. The following metrics are commonly used to evaluate how well proactive protocols perform under various network conditions.

3.6.1 Routing Overhead

Routing overhead refers to the proportion of control packets, such as routing updates and broadcasts, relative to the total network traffic. It is one of the most critical factors determining the efficiency of proactive routing protocols. High routing overhead consumes available bandwidth, leaving less capacity for actual data transmission. This issue becomes more pronounced in dense or highly mobile networks, where frequent updates are required to maintain accurate routing tables. For instance, OLSR reduces control message overhead through the use of Multipoint Relays (MPRs) that limit redundant broadcasts, while DSDV tends to generate excessive updates in larger networks, resulting in higher overhead.

3.6.2 End-to-End Latency

End-to-end latency measures the average time taken for a data packet to travel from the source node to the destination node. In proactive routing, this metric generally exhibits low values because routes are precomputed and readily available in each node's routing table. This allows for immediate packet forwarding without the need for route discovery, as seen in reactive approaches. However, latency may increase if stale routing information is used before new updates have propagated through the network. Low latency makes proactive protocols highly suitable for delay-sensitive applications such as VoIP, real-time communication, and video streaming.

3.6.3 Packet Delivery Ratio (PDR)

The Packet Delivery Ratio (PDR) is the ratio of successfully delivered data packets to the total number of packets sent by the source node. It is a key indicator of the reliability and effectiveness of a routing protocol. A high PDR reflects stable and dependable communication, even when network topology changes frequently. In proactive protocols, regular routing updates generally help maintain a high PDR by ensuring that valid routes are available. However, excessive control traffic may cause network congestion, leading to packet losses. Maintaining a strong PDR is crucial for mission-critical applications where reliability and data consistency are paramount.

3.6.4 Energy Efficiency

Energy efficiency quantifies the amount of energy consumed per successfully delivered data packet. Since proactive routing protocols depend on frequent control broadcasts and periodic table updates, they tend to consume more power compared to reactive protocols. This issue is particularly concerning for battery-powered devices and wireless sensor networks (WSNs), where energy resources are limited. To mitigate this, energy-aware proactive routing mechanisms have been proposed, which aim to reduce redundant transmissions and adjust update intervals dynamically. Improved energy efficiency extends the operational lifetime of the network and enhances overall sustainability.

3.6.5 Scalability in Dense Networks

Scalability reflects the ability of a routing protocol to maintain acceptable performance as the number of nodes and network density increase. In large-scale ad hoc networks, maintaining complete global topology information leads to exponential growth in routing table size and control message frequency. As a result, proactive protocols often experience scalability

limitations. Among these, OLSR performs relatively better in dense networks due to its MPR optimization, which reduces redundant transmissions. In contrast, DSDV may struggle under similar conditions. To enhance scalability, researchers have introduced hierarchical and cluster-based routing structures, which help limit the propagation of control messages to localized regions.

Evaluating the performance of proactive routing protocols involves analyzing five critical metrics: routing overhead, end-to-end latency, packet delivery ratio, energy efficiency, and scalability. While proactive protocols offer significant advantages in terms of low-latency route availability and predictable performance, they often face challenges in terms of control overhead and energy consumption, particularly in large-scale or highly dynamic networks. Achieving an optimal balance among these performance metrics is essential for deploying efficient and sustainable proactive routing solutions in modern ad hoc and wireless environments.

3.7 Comparative Analysis of Proactive Protocols

This section provides a comparative evaluation of four major proactive (table-driven) routing protocols — DSDV, OLSR, WRP, and GSR — across essential performance parameters. It highlights their strengths, limitations, and suitability for different types of ad hoc networks, including MANETs, VANETs, FANETs, and WSNs, while also discussing the key trade-offs among latency, control overhead, scalability, and energy efficiency.

Quick Protocol Profiles

DSDV (Destination-Sequenced Distance Vector):

DSDV is based on the distance-vector routing approach, enhanced with sequence numbers to ensure loop-free and fresh routes. It uses both periodic and incremental updates to maintain network-wide consistency. The protocol's simplicity makes it efficient in smaller networks, but its reliance on frequent updates causes high control overhead in larger or highly dynamic environments.

OLSR (Optimized Link State Routing):

OLSR adopts a link-state approach optimized for wireless networks. Its key innovation is the use of Multipoint Relays (MPRs), which reduce redundant broadcasts during flooding. This optimization makes OLSR well-suited for dense topologies, as it achieves faster convergence with less overhead compared to traditional link-state protocols.

WRP (Wireless Routing Protocol):

WRP is a table-driven protocol that maintains multiple tables — including distance, link-cost, and retransmission lists — to guarantee loop-free routing and fast convergence. It achieves high accuracy and reliability but requires substantial memory and processing power, making it more suitable for networks where nodes can handle the computational load.

GSR (Global State Routing):

GSR is a simplified link-state-style protocol designed to reduce flooding overhead by exchanging link-state information only with neighboring nodes. It maintains global connectivity with lower bandwidth usage, making it more bandwidth-efficient than traditional link-state methods, though it still depends on periodic updates and may struggle in highly mobile scenarios.

Comparative Analysis Across Key Metrics

In proactive routing, each protocol demonstrates a unique balance of performance characteristics. **DSDV** offers low latency but high overhead, **OLSR** achieves scalability through MPRs, **WRP** ensures rapid convergence at a computational cost, and **GSR** focuses on bandwidth efficiency.

- **Latency:** All four protocols provide low latency since routes are precomputed. WRP exhibits the lowest latency due to its fast convergence mechanisms.
- **Control Overhead:** DSDV and WRP incur higher overhead due to frequent and detailed updates, while OLSR minimizes overhead using MPRs. GSR performs moderately well by reducing redundant flooding.
- **Convergence Speed:** WRP converges the fastest, followed by OLSR, while DSDV and GSR show moderate convergence rates.
- **Energy Efficiency:** OLSR is relatively energy-efficient in dense networks, whereas DSDV and WRP consume more power due to frequent updates and processing demands.
- **Scalability:** OLSR and GSR scale better than DSDV and WRP, though their performance still depends on mobility levels and update frequency.
- **Loop Prevention:** All four protocols implement mechanisms such as sequence numbers or link-state validation to maintain loop-free routes.

Suitability by Application Domain

Mobile Ad Hoc Networks (MANETs):

- *DSDV* is suitable for **small or low-mobility MANETs** where simplicity and low latency are required.
- *OLSR* performs better in **moderately dense MANETs** due to reduced flooding and efficient route calculation.
- *WRP* is effective in environments where **fast consistency** is crucial, provided nodes have adequate processing resources.
- *GSR* works well for **medium-scale networks**, balancing bandwidth efficiency with moderate update needs.

Vehicular Ad Hoc Networks (VANETs):

- *OLSR* outperforms DSDV in dense urban VANETs because MPRs prevent broadcast storms.
- However, high-speed mobility in VANETs challenges all table-driven protocols, often making them less efficient than reactive or hybrid approaches.

Flying Ad Hoc Networks (FANETs):

- Proactive protocols generally struggle in FANETs due to 3D high mobility.
- *OLSR* can be adapted with optimized MPR selection, but **geographic or hybrid routing** methods are typically more effective.

Wireless Sensor Networks (WSNs) / Industrial IoT:

- *DSDV* and *GSR* are applicable for **static or semi-static sensor networks** where immediate route availability is valuable.
- *OLSR* can support **dense sensor deployments**, but its periodic control messages consume significant energy.
- For **battery-constrained networks**, **energy-aware**, **cluster-based**, or **probabilistic** routing variants offer better efficiency.

Trade-offs — Summary and Guidance

- **Latency vs. Overhead:** Proactive protocols ensure **low latency** since routes are precomputed, but this benefit incurs continuous **control overhead**. They are ideal for **real-time, low-latency applications** such as tactical or mission-critical systems with stable topologies.
- **Overhead vs. Scalability:** As network size increases, **control overhead** grows proportionally. **OLSR** mitigates this through MPR optimization, while **DSDV** and **WRP** face scalability challenges. For **large-scale networks**, hybrid or reactive protocols are typically more suitable.
- **Energy Efficiency vs. Responsiveness:** Frequent updates drain energy resources, reducing network lifetime in energy-sensitive applications. To balance energy efficiency and responsiveness, **energy-aware proactive protocols**, **duty cycling**, or **adaptive update intervals** are recommended.
- **Complexity vs. Robustness:** Protocols like **WRP** achieve **robustness** and **fast convergence**, but with higher **memory and processing demands**. They are preferable in environments where nodes have sufficient computational capacity and reliability is critical.

Proactive routing protocols excel at delivering **immediate route availability** and **minimal latency**, making them highly effective for **delay-sensitive applications** in **small to medium**,

stable, or **dense** networks. However, their **continuous control overhead**, **scalability challenges**, and **energy demands** limit their applicability in large, dynamic, or energy-constrained environments. Therefore, protocol selection should align with the **network's mobility profile**, **node resources**, and **performance priorities**. In many modern applications, **hybrid** or **cross-layer proactive-geographic** designs offer a more practical and balanced approach to achieving efficient ad hoc communication.

3.8 Applications of Proactive Routing Protocols

Proactive routing protocols play a crucial role in various ad hoc network environments that require low-latency communication and continuous route availability. Because these protocols are table-driven, each node maintains updated routes to all other nodes in the network at all times. This characteristic makes proactive routing especially suitable for applications that depend on real-time responsiveness, predictable performance, and reliable connectivity, such as military systems, disaster recovery, vehicular networks, IoT, and healthcare monitoring.

3.8.1 Military and Tactical Networks

Military and tactical communication systems often operate in highly dynamic, infrastructure-less environments where rapid deployment and secure coordination are critical. In these mission-critical networks, proactive routing protocols such as **WRP** and **OLSR** are preferred due to their ability to provide instantaneous route availability without waiting for on-demand route discovery. This ensures quick communication setup and reliable data transmission, which are vital for command control, situational awareness, and live video or sensor data sharing in the battlefield. However, a potential drawback is the high control overhead, which can affect performance in environments with extreme node mobility.

3.8.2 Disaster Recovery and Emergency Response

In post-disaster scenarios, where conventional communication infrastructure like cellular towers or wired networks is damaged or destroyed, proactive routing protocols enable rapid establishment of temporary ad hoc networks. These networks facilitate communication among rescue teams, drones, and mobile command centers. **DSDV** and **OLSR** are often employed for field communication among emergency responders, providing immediate route availability that supports real-time coordination, survivor tracking, and map updates. The primary advantage of proactive routing in such environments is its reliability and low-latency performance during time-critical rescue operations.

3.8.3 Vehicular Ad Hoc Networks (VANETs)

Vehicular Ad Hoc Networks (VANETs) allow vehicles to communicate directly with each other (V2V) and with roadside infrastructure (V2I). In urban settings with high vehicle density, **OLSR** proves particularly useful because its **Multipoint Relay (MPR)** mechanism

minimizes redundant broadcasting and enhances scalability. Proactive routing ensures that routes are readily available, supporting real-time applications like traffic management, collision avoidance, and cooperative driving. However, the rapid topology changes caused by high-speed mobility in VANETs may still challenge the periodic update mechanisms of proactive protocols.

3.8.4 Internet of Things (IoT) and Wireless Sensor Networks (WSNs)

In the Internet of Things (IoT) and Wireless Sensor Network (WSN) domains, nodes often exhibit low mobility and continuous communication requirements. Proactive routing protocols, such as **DSDV** and **OLSR**, are well-suited to such environments because they maintain persistent connectivity and allow efficient data forwarding without the overhead of frequent route discovery. These protocols support real-time monitoring, industrial automation, and environmental sensing. However, since proactive protocols involve regular control message exchanges, they can consume significant energy. Therefore, energy-aware enhancements or clustering techniques are often employed to extend network lifetime, particularly in battery-powered sensor networks.

3.8.5 Healthcare and Wearable Networks

Proactive routing protocols are increasingly applied in **healthcare and wearable body area networks (BANs)**, where continuous, low-latency communication is essential for patient monitoring. In applications such as remote health tracking, emergency telemetry, and hospital wireless systems, proactive routing ensures real-time data exchange between sensors, monitoring hubs, and healthcare servers. **OLSR-based frameworks** are often used for their reliability and minimal delay in transmitting vital patient data. This improves responsiveness, minimizes packet loss, and enhances patient safety during critical health monitoring.

Proactive routing protocols are ideally suited for applications that require stable, predictable, and low-latency communication. Despite their relatively higher control overhead, their ability to provide instant route availability and maintain robust performance in moderate mobility environments makes them particularly valuable in domains such as **military operations, disaster management, vehicular networks, IoT/WSNs, and healthcare systems**. With appropriate optimizations for energy and scalability, proactive routing continues to play a key role in real-time, mission-critical ad hoc network deployments.

3.9 Current Trends and Enhancements in Proactive Routing

Proactive routing protocols have undergone significant evolution beyond their traditional table-driven designs to meet the complex requirements of modern **Mobile Ad Hoc Networks (MANETs)**, **Vehicular Ad Hoc Networks (VANETs)**, **Unmanned Aerial Vehicle (UAV)** systems, and **Internet of Things (IoT)** ecosystems. Modern research emphasizes

improving scalability, energy efficiency, security, and adaptability to cope with increasingly dynamic and heterogeneous environments. Figure 3, this section explores the major trends and technological enhancements driving the next generation of proactive routing mechanisms.

3.9.1 Integration with 5G/6G and Edge Computing

With the emergence of **5G** and the evolution toward **6G** networks, the focus has shifted to achieving ultra-low latency, massive device connectivity, and intelligent edge-based communication. Proactive routing protocols are being integrated with **edge-assisted MANET architectures**, where local edge nodes maintain partial or global network awareness to optimize routing decisions. This integration reduces control overhead by enabling **localized route management** and enhances **real-time responsiveness** in dense or mission-critical networks. For example, **hybrid proactive frameworks leveraging Mobile Edge Computing (MEC)** have demonstrated improved handoff efficiency and data routing performance in vehicular and UAV systems. The synergy between proactive routing and edge computing ensures faster data delivery and higher reliability in next-generation wireless environments.

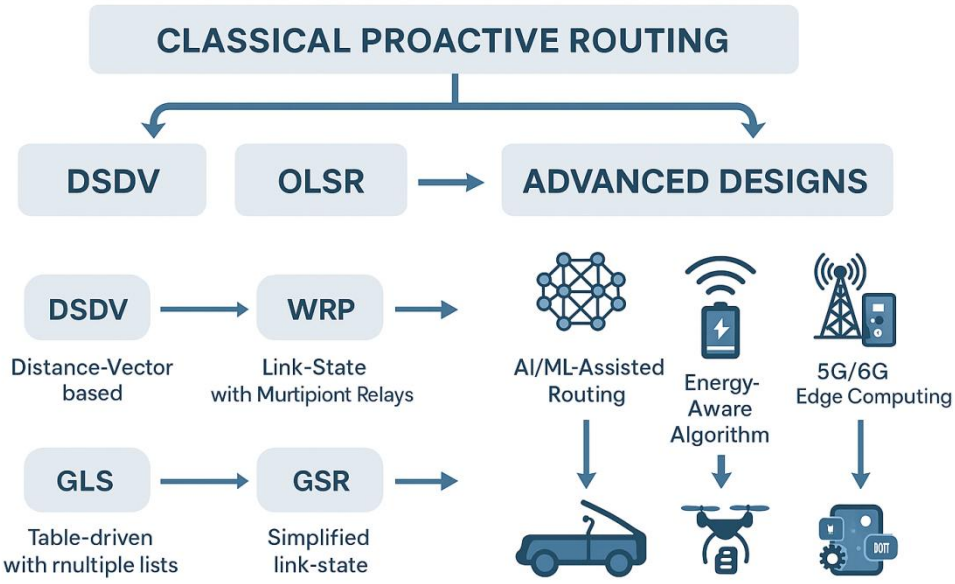


Figure 3: Evolution and Emerging Trends in Proactive Routing

3.9.2 Cross-Layer Optimization for Reduced Overhead

Traditional proactive routing protocols operate independently at the **network layer**, without considering real-time information from other protocol layers. **Cross-layer optimization** addresses this limitation by enabling interaction among different layers such as the **MAC**, **physical**, and **application** layers. Through this integration, proactive routing protocols can

dynamically adjust **routing table update intervals** based on real-time link quality, signal strength, and congestion levels. This approach minimizes redundant broadcast messages and improves **energy and bandwidth utilization**. For instance, cross-layer optimized versions of **OLSR** adapt their update frequencies according to channel conditions, resulting in significantly reduced overhead in high-mobility or congested environments. Such adaptive mechanisms make proactive routing more efficient and resilient in diverse operating conditions.

3.9.3 Machine Learning and AI-Based Enhancements

The integration of **Artificial Intelligence (AI)** and **Machine Learning (ML)** into proactive routing has revolutionized how networks predict and respond to dynamic changes. AI-based proactive routing protocols analyze historical data, mobility patterns, and network conditions to **anticipate route failures** before they occur. Techniques such as **Reinforcement Learning (RL)** optimize route selection by continuously learning from past transmission outcomes, while **Deep Learning (DL)** models predict node mobility and topology variations to proactively maintain stable routes. These intelligent enhancements significantly improve route stability, minimize packet loss, and enhance throughput, particularly in **VANETs** and **UAV networks**, where rapid topology shifts are common. By enabling predictive and adaptive routing, AI-powered proactive protocols make networks more autonomous and context-aware.

3.9.4 Energy-Aware Proactive Routing Protocols

Energy efficiency remains a central challenge in proactive routing, especially for **battery-powered** and **sensor-based** devices. To address this, modern enhancements incorporate **energy metrics**—such as residual battery power and estimated link lifetime—into routing decisions. Adaptive update mechanisms reduce broadcast frequency when network topology remains stable, thereby conserving energy without compromising connectivity. Examples include **EOLSR (Energy-Optimized Link State Routing)**, which adjusts Multipoint Relay (MPR) selection based on node energy levels, and **EE-DSDV (Energy-Efficient DSDV)**, which minimizes routing updates during low-mobility periods. These energy-aware innovations extend overall **network lifetime** while maintaining the proactive protocol's advantage of low-latency communication, making them particularly suitable for **IoT** and **Wireless Sensor Networks (WSNs)**.

3.9.5 Security-Aware Proactive Routing Mechanisms

Due to their decentralized and open nature, ad hoc networks are highly vulnerable to attacks such as **blackhole**, **wormhole**, and **routing table poisoning**. As a result, security enhancements have become an integral part of proactive routing protocol design. Modern approaches embed **cryptographic authentication**, **intrusion detection systems (IDS)**, and **trust-based models** directly within the routing layer. These mechanisms verify node

credibility, ensure message integrity, and mitigate malicious activities. For instance, **Secure OLSR (SOLSR)** employs digital signatures to validate routing update integrity, while **Trust-Enhanced DSDV** introduces weighted trust factors that influence routing table decisions. These improvements significantly strengthen data integrity, node authentication, and overall network resilience against both internal and external threats.

Contemporary advancements in proactive routing protocols focus on integrating emerging technologies such as **5G/6G**, **edge computing**, **machine learning**, and **energy-aware** mechanisms, while embedding robust **security frameworks**. These innovations aim to create **intelligent, adaptive, and context-aware routing architectures** capable of supporting the scalability, responsiveness, and reliability required by next-generation **ad hoc**, **vehicular**, and **IoT networks**. As a result, proactive routing is evolving from static, table-driven systems into dynamic, learning-enabled frameworks that align with the performance and efficiency demands of future wireless communication ecosystems.

3.11 Conclusion

This chapter explored the fundamental concepts, design principles, and practical implementations of proactive (table-driven) routing protocols in wireless ad hoc networks. Proactive routing maintains continuous, updated routing information across all participating nodes, enabling low-latency data transmission and predictable performance — key advantages in time-sensitive applications. The discussion began with an overview of the working mechanisms behind proactive protocols, including routing table construction, periodic updates, and sequence-number management for loop-free communication. Key protocols such as DSDV, OLSR, WRP, and GSR were analyzed in terms of their operational methodologies, advantages, and limitations. Comparative evaluations highlighted the trade-offs among latency, control overhead, energy consumption, and scalability, illustrating that while proactive routing ensures rapid data delivery, it can incur high overhead in highly dynamic or large-scale networks. The chapter also presented real-world applications and case studies, demonstrating how proactive routing supports domains such as military communication, vehicular networks, wireless sensor networks, and UAV swarms. Additionally, emerging trends such as AI/ML-based predictive routing, energy-aware enhancements, and integration with 5G/6G and edge computing were discussed, showcasing the ongoing evolution of proactive routing paradigms. In conclusion, proactive routing protocols are best suited for networks requiring consistent, low-latency communication and predictable topology behavior, such as tactical, vehicular, and IoT environments. While they face scalability and energy challenges, their structured design and reliability make them a foundational component in ad hoc networking research and deployment.

References

1. Alotaibi, E., & Mukherjee, B. (2020). A survey on routing algorithms for wireless ad-hoc and mesh networks. *Computer Networks, 172*, 107145. https://doi.org/10.1016/j.comnet.2020.107145
2. Arulkumaran, K., & Rajesh, S. (2022). Performance analysis of proactive routing protocols in MANET under varying mobility models. *Wireless Personal Communications, 126*(1), 493–512. https://doi.org/10.1007/s11277-022-09734-4
3. Bakhshi, T., & Hamid, Z. (2023). Machine learning-based proactive routing in mobile ad hoc networks: A review and open issues. *Ad Hoc Networks, 145*, 103063. https://doi.org/10.1016/j.adhoc.2023.103063
4. Barabasz, A., & Niewiadomska-Szynkiewicz, E. (2019). Energy-aware OLSR routing in ad hoc networks. *Journal of Network and Computer Applications, 136*, 28–38. https://doi.org/10.1016/j.jnca.2019.03.009
5. Chandra, R., & Kumar, P. (2021). Comparative study of DSDV, WRP, and OLSR protocols for MANETs. *International Journal of Wireless and Mobile Computing, 20*(2), 143–154.
6. Chouikhi, S., & Abdellaoui, M. (2020). Secure proactive routing in MANETs using trust-based mechanisms. *Wireless Networks, 26*(7), 5403–5418. https://doi.org/10.1007/s11276-020-02349-2
7. Dinesh, K., & Sharma, N. (2018). Enhancing scalability in OLSR-based mobile ad hoc networks through clustering. *Procedia Computer Science, 132*, 1051–1060. https://doi.org/10.1016/j.procs.2018.05.122
8. Gupta, V., & Singh, R. (2024). Cross-layer optimization for energy-efficient proactive routing in IoT-based ad hoc systems. *IEEE Internet of Things Journal, 11*(3), 4150–4162. https://doi.org/10.1109/JIOT.2024.3345101
9. Hassan, M. A., & Khan, S. (2019). OLSR optimization in VANETs using multipoint relay selection enhancement. *IEEE Access, 7*, 142306–142319. https://doi.org/10.1109/ACCESS.2019.2943654
10. Jha, P., & Verma, R. (2022). Proactive routing for UAV-based FANETs: Performance evaluation of DSDV and OLSR. *Ad Hoc Networks, 132*, 102926. https://doi.org/10.1016/j.adhoc.2022.102926
11. Kaur, G., & Bansal, A. (2023). AI-driven proactive routing for dynamic ad hoc networks. *Wireless Communications and Mobile Computing, 2023*, 1–13. https://doi.org/10.1155/2023/6674015
12. Li, H., & Zhang, X. (2021). Edge-assisted proactive routing protocol for hybrid 5G ad hoc environments. *IEEE Transactions on Mobile Computing, 20*(9), 2915–2928. https://doi.org/10.1109/TMC.2020.3019211
13. Mahajan, R., & Pathak, A. (2020). A study on the performance of proactive and reactive routing in smart city WSNs. *International Journal of Communication Systems, 33*(15), e4562. https://doi.org/10.1002/dac.4562

14. Malik, S., & Kaur, R. (2019). Comparative evaluation of OLSR and DSDV in healthcare ad hoc networks. *Journal of Ambient Intelligence and Humanized Computing, 10*(12), 4951–4963.
15. Nguyen, T. H., & Kim, J. (2023). Deep learning-assisted OLSR for reliable vehicular ad hoc networks. *Sensors, 23*(11), 4961. https://doi.org/10.3390/s23114961
16. Pandey, A., & Kumar, D. (2021). Energy-efficient DSDV routing for IoT-enabled MANETs. *Sustainable Computing: Informatics and Systems, 30*, 100528. https://doi.org/10.1016/j.suscom.2021.100528
17. Rahman, M. M., & Kabir, M. H. (2020). Security-aware proactive routing for MANETs against blackhole and wormhole attacks. *Wireless Networks, 26*(8), 6041–6053. https://doi.org/10.1007/s11276-020-02464-0
18. Sharma, D., & Patel, P. (2022). Comparative analysis of proactive routing protocols in high-mobility VANETs. *Mobile Networks and Applications, 27*(4), 1345–1359. https://doi.org/10.1007/s11036-022-01953-3
19. Singh, N., & Kumar, V. (2024). A survey on energy-aware and QoS-enhanced proactive routing in ad hoc networks. *Computer Communications, 224*, 35–48. https://doi.org/10.1016/j.comcom.2024.02.015
20. Zhang, L., & Chen, Y. (2018). Hybrid enhancements for proactive routing in large-scale ad hoc networks. *Ad Hoc Networks, 78*, 90–101. https://doi.org/10.1016/j.adhoc.2018.06.009

Chapter-4

Reactive Routing Protocols — On-Demand Approaches

[1]M.Jothilakshmi, [2]D.P.Savithri

[1]Assistant Professor,
Department of Computer Science,
K.S.Rangasamy College of Arts and Science(Autonomous),
Tiruchengode,Tamilnadu, India.

[2]Assistant Professor,
Department of Computer Science,
K.S.Rangasamy College of Arts and Science(Autonomous),
Tiruchengode,Tamilnadu, India.

Abstract: *Reactive routing protocols, also known as on-demand routing protocols, play a crucial role in ad hoc wireless networks by establishing communication paths only when they are needed. Unlike proactive protocols that continuously maintain routing tables, reactive protocols initiate route discovery and maintenance processes dynamically, thereby reducing control overhead and conserving network resources. This chapter explores the operational principles, mechanisms, and key protocols within this class, including Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Temporally Ordered Routing Algorithm (TORA). The discussion highlights the route discovery and maintenance procedures, comparative performance analysis, and optimization strategies that enhance scalability, energy efficiency, and reliability. Furthermore, the chapter examines security challenges, real-world applications, and emerging trends such as AI-driven adaptive routing and integration with 5G/6G infrastructures. By the end of this chapter, readers will gain a comprehensive understanding of the strengths, limitations, and evolving landscape of reactive routing in modern ad hoc networks.*

Keywords: *Ad hoc networks; Reactive routing; On-demand protocols; AODV; DSR; TORA; Route discovery; Route maintenance; Wireless communication; Mobility management; Energy efficiency; Cross-layer optimization; Secure routing; AI-driven routing; MANET; VANET; Edge computing; 5G/6G integration; Network scalability; Dynamic topology.*

4.1 Introduction

Routing in ad hoc wireless networks plays a vital role in ensuring reliable data transmission between mobile nodes that operate without any fixed infrastructure. In such decentralized environments, nodes communicate over dynamically changing topologies, making routing one of the most challenging yet essential functions. Since nodes act both as hosts and routers, each device participates in route discovery and maintenance, which demands efficient algorithms capable of adapting to frequent topology changes, limited bandwidth, and constrained energy resources. Routing protocols in ad hoc networks are generally classified into three categories — proactive (table-driven), reactive (on-demand), and hybrid.

- ***Proactive protocols*** such as DSDV and OLSR maintain up-to-date routing tables by periodically exchanging control messages, ensuring that routes are always available when needed.
- ***Reactive protocols***, including AODV and DSR, establish routes only when a communication request arises, reducing control overhead in dynamic networks.
- ***Hybrid protocols***, like ZRP, combine features of both approaches to balance efficiency and responsiveness.

This chapter focuses specifically on reactive or on-demand routing protocols, which are designed to initiate route discovery only when data transmission is required. Unlike proactive approaches, reactive protocols do not maintain complete routing information continuously, thereby conserving bandwidth and power. The key motivation for adopting on-demand routing lies in its efficiency in highly dynamic and resource-constrained environments such as MANETs, VANETs, and FANETs. In these networks, where node mobility and topology fluctuations are frequent, maintaining up-to-date routing tables can be costly and impractical. Reactive routing minimizes unnecessary control traffic and energy consumption while offering adaptability to changing network conditions, making it an ideal choice for mobile and ad hoc communication systems.

4.2 Fundamental Concepts of Reactive Routing

Reactive routing, also known as on-demand routing, operates on the principle of establishing routes only when they are required by a source node for data transmission. Unlike proactive routing protocols that maintain continuous updates of the entire network topology, reactive protocols initiate a route discovery process dynamically, which minimizes unnecessary control overhead and conserves network resources.

The working mechanism of reactive routing consists of two key phases — route discovery and route maintenance.

- ***Route Discovery:*** When a source node needs to communicate with a destination and has no existing route, it broadcasts a route request (RREQ) throughout the network. Intermediate nodes forward this request until it reaches the destination or a node with a valid route to the destination. Once a path is established, a route reply (RREP) is sent back to the source, enabling data transmission.
- ***Route Maintenance:*** During communication, links may break due to node mobility or signal loss. When a link failure occurs, the node detecting the break sends a route error (RERR) message to affected nodes, prompting a new route discovery if communication needs to continue.

In comparison to proactive routing protocols, which continuously maintain routing tables for all possible destinations, reactive protocols significantly reduce control message overhead and energy consumption. However, they may introduce initial latency during route discovery, which can affect real-time or delay-sensitive applications. Reactive routing offers several advantages, including scalability, reduced bandwidth usage, and adaptability

to frequent topology changes. Nonetheless, it faces limitations such as increased latency during route establishment and potential flooding issues caused by widespread RREQ broadcasts in dense networks.

These protocols are widely used in Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs), and disaster recovery systems, where infrastructure is unavailable, and network conditions change rapidly. The design goals of reactive routing protocols focus on achieving scalability, low control overhead, high adaptability, and robustness. By optimizing route discovery and maintenance mechanisms, reactive routing provides a balance between performance efficiency and resource conservation, making it a cornerstone of modern ad hoc network design.

4.3 Route Discovery Mechanisms

The route discovery mechanism is a fundamental process in reactive routing protocols, responsible for establishing communication paths between source and destination nodes on demand. This process ensures that routes are created only when needed, thereby conserving bandwidth and energy—two critical resources in ad hoc wireless networks.

The route discovery process typically begins when a source node has data to send but lacks an active route to the desired destination. It initiates a Route Request (RREQ) message, which is broadcast to neighboring nodes. Each intermediate node that receives the RREQ checks whether it is the destination or if it already has a valid route to the destination in its route cache. If neither condition is met, the node rebroadcasts the RREQ, allowing it to propagate through the network. When the RREQ eventually reaches the destination (or an intermediate node with a valid route), a Route Reply (RREP) message is generated and sent back along the reverse path established by the RREQ propagation. This backward tracing ensures that a path is formed between the source and destination without requiring global topology knowledge.

Flooding and controlled broadcasting play a key role in this process. While flooding allows the RREQ to reach all nodes, it can cause redundant transmissions and network congestion. To mitigate this, controlled broadcasting techniques such as sequence numbers, time-to-live (TTL) fields, or probabilistic forwarding are used to prevent duplicate message dissemination and reduce overhead.

Another essential concept in route discovery is reverse path setup and route caching. During the RREQ propagation, each node temporarily records the address of the node from which it received the RREQ. This forms a reverse path back to the source, which is used for forwarding the RREP. Route caching further optimizes performance by storing known routes for future use, minimizing the need for repeated route discoveries and lowering latency.

To further enhance efficiency, several optimization techniques have been developed to reduce broadcast overhead, including expanding ring search (ERS), query localization, and neighbor connectivity analysis. These strategies ensure that only the most relevant nodes participate in route discovery, significantly improving scalability and performance in dense networks.

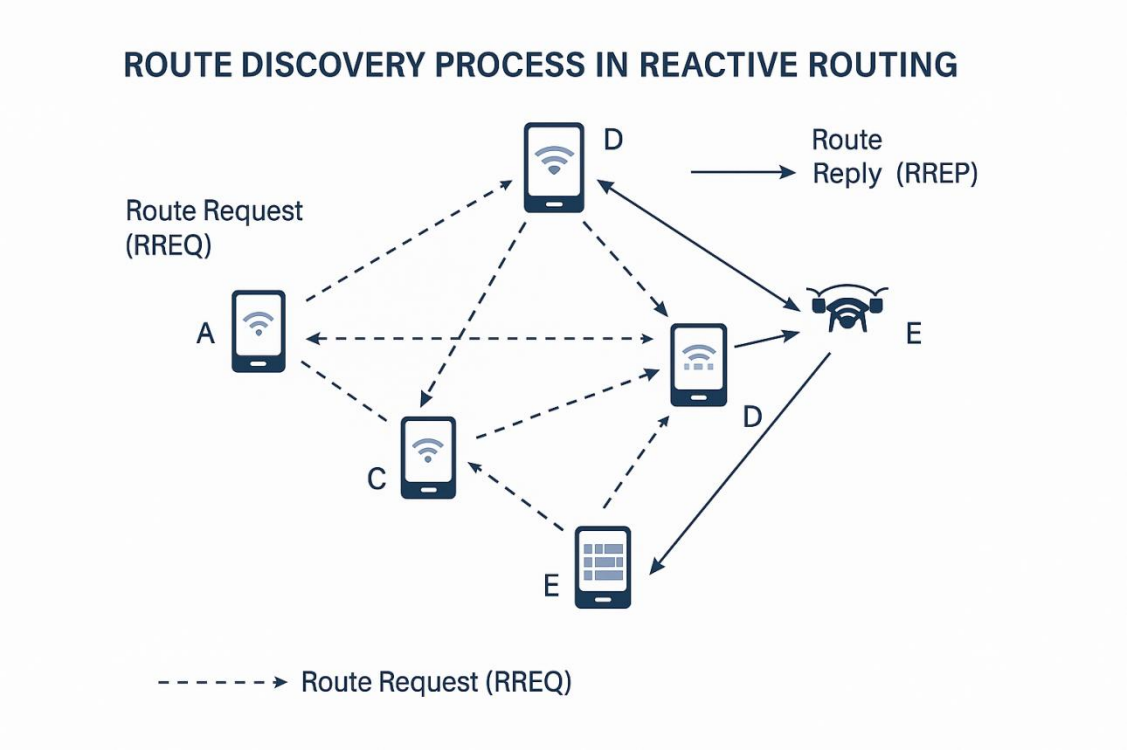


Figure 1: Route Discovery Process in Reactive Routing Protocols (AODV/DSR)

Illustrative Example: Figure 1, Consider a scenario where node A wants to send data to node F, but no existing route is available. Node A broadcasts an RREQ to its neighbors (B, C, and D). Node B forwards it to E, and C forwards it to F. When node F receives the RREQ, it generates an RREP that travels back along the reverse path (F → C → A), establishing a valid communication route. If the link between C and F later breaks, a new RREQ will be initiated, and an alternative route may be established via another path such as A → B → E → F.

The route discovery mechanism in reactive routing protocols enables dynamic path establishment with minimal overhead, using intelligent broadcasting, caching, and optimization techniques. These mechanisms ensure efficient communication even in highly dynamic and infrastructure-less environments.

4.4 Route Maintenance Techniques

In reactive routing protocols, route maintenance ensures the continued reliability and accuracy of communication paths once they are established. Since ad hoc wireless networks are characterized by frequent topology changes and node mobility, maintaining valid routes

is as crucial as discovering them. Route maintenance mechanisms help detect link failures, repair broken paths, and prevent the use of stale or invalid routes.

One of the primary tools used in route maintenance is the Route Error (RERR) message. When an intermediate node detects a link failure—often through missing acknowledgments or link-layer feedback—it generates an RERR message and sends it back to the source node. This notification allows all nodes along the affected path to update or delete the broken route entries from their routing tables. For example, if node C in the path A–B–C–D detects that the link to D has failed, it issues an RERR that propagates back toward A, ensuring that outdated routes are removed to prevent packet loss.

To address link failures, reactive protocols employ two main strategies: local route repair and global rediscovery. In local route repair, an intermediate node attempts to find a new path to the destination without involving the source node. This approach reduces latency and control overhead, particularly when the failure occurs near the destination. However, if the repair attempt fails or no nearby alternate path exists, the protocol falls back on global route rediscovery, where the source node initiates a new route discovery process. This balance between local repair and global rediscovery ensures efficient recovery with minimal disruption.

Sequence numbers play a vital role in loop prevention and route validation. They help nodes determine the freshness of routing information, ensuring that only the most recent and accurate routes are used. A higher sequence number indicates a more recent route, preventing routing loops and ensuring data packets always follow the most efficient path.

To maintain route freshness, protocols implement timeout mechanisms. Each route entry is assigned a lifetime; if unused for a certain duration, it expires automatically. This prevents stale routes from being reused and ensures that routing tables remain current and efficient. Timeouts are especially important in high-mobility networks, where route validity changes rapidly.

Finally, reactive routing protocols must balance responsiveness and overhead. While frequent route checks improve responsiveness to topology changes, they also increase control message overhead and energy consumption. Effective protocols strike a balance by adapting maintenance frequency based on network dynamics, node mobility, and traffic patterns.

Route maintenance in reactive routing protocols involves detecting link failures, repairing or rediscovering routes, managing sequence numbers for freshness and loop prevention, and optimizing responsiveness while minimizing overhead. These mechanisms collectively ensure that ad hoc networks remain reliable and efficient even under highly dynamic and unpredictable conditions.

4.5 Key Reactive Routing Protocols

Reactive routing protocols, also known as on-demand routing protocols, establish communication paths only when required by a source node. Unlike proactive protocols that maintain constant route updates, reactive approaches minimize control overhead and are well-suited for highly dynamic ad hoc environments. Among these, the Ad hoc On-Demand Distance Vector (AODV) protocol stands as one of the most widely studied and implemented on-demand routing methods.

4.5.1 Ad hoc On-Demand Distance Vector (AODV)

Core Principles and Operation

The AODV protocol is designed to enable dynamic, self-starting, and loop-free routing among mobile nodes in ad hoc networks. It combines the on-demand route discovery of reactive protocols with distance vector principles, allowing nodes to maintain routing information only for active destinations. Routes are created when needed and maintained as long as they are in use, which helps conserve bandwidth and memory resources.

Each node in AODV maintains a routing table that stores next-hop information for active routes. When a node needs to communicate with another node but lacks a route to it, AODV initiates a route discovery process using control messages.

Route Discovery and Maintenance Steps

The route discovery process begins when a source node broadcasts a Route Request (RREQ) message throughout the network. Each intermediate node that receives the RREQ records the address of the node from which it was received, creating a reverse path back to the source. If an intermediate node knows a valid route to the destination or if the destination node itself receives the RREQ, it generates a Route Reply (RREP) message. The RREP travels along the reverse path to the source, establishing a forward route.

Once established, data packets are sent along this path until it becomes invalid. During data transmission, if a link break occurs, the detecting node sends a Route Error (RERR) message to inform upstream nodes of the broken link. Depending on the location of the failure, either local route repair or global route rediscovery is initiated to re-establish connectivity.

Sequence Numbers and Loop-Free Operation

A distinguishing feature of AODV is its use of destination sequence numbers to ensure loop-free and fresh routes. Each destination node maintains and increments its sequence number whenever a significant topology change occurs. When nodes receive multiple route advertisements, they select the one with the highest sequence number, indicating the most recent route. This mechanism prevents the use of outdated paths and ensures that routing information remains consistent across the network.

Performance Characteristics and Limitations

AODV offers several advantages, including low control overhead in low-traffic or low-mobility scenarios, efficient route establishment, and scalability to moderate network sizes. Its ability to discover routes on demand makes it energy-efficient compared to proactive routing protocols that continuously exchange updates.

However, AODV also faces limitations. Route discovery latency can increase when initiating new connections, particularly in large networks. Frequent broadcasting of RREQ messages may cause network congestion in dense environments. Moreover, link failures in high-mobility networks trigger repeated rediscoveries, leading to higher delays and packet loss.

Enhancements and Variants (e.g., EAODV, MAODV)

Several extensions to AODV have been proposed to overcome its limitations and adapt it to specific application domains:

- EAODV (Enhanced AODV): Focuses on improving energy efficiency by selecting routes that minimize overall power consumption, thus extending network lifetime.
- MAODV (Multicast AODV): Extends AODV to support multicast communication, allowing efficient group data transmission in scenarios like conferencing or collaborative missions.
- AODV-SEC and SAODV: Introduce security enhancements through cryptographic mechanisms to defend against routing attacks such as spoofing and blackhole attacks.
- AODV-LL (Link Layer Feedback): Improves responsiveness by detecting link breakages quickly through link-layer notifications rather than waiting for upper-layer timeouts.

In summary, AODV remains a cornerstone of reactive routing due to its simplicity, adaptability, and efficient on-demand route establishment. Despite its challenges in scalability and delay sensitivity, continuous enhancements and hybrid adaptations have solidified AODV's role as a foundational protocol for mobile ad hoc networks (MANETs), vehicular networks (VANETs), and emerging IoT-based systems.

4.5.2 Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) protocol is a prominent reactive routing protocol specifically designed for multi-hop wireless ad hoc networks. It enables nodes to discover and maintain routes dynamically without relying on periodic routing advertisements. DSR operates using the principle of source routing, where the entire path to the destination is explicitly included in the packet header. This feature gives DSR a high level of flexibility and adaptability in rapidly changing topologies typical of mobile ad hoc networks (MANETs).

Concept of Source Routing and Route Caching

In DSR, the source node determines the complete route to the destination before sending a data packet. This route is then stored in the packet header, allowing intermediate nodes to forward packets without maintaining up-to-date routing tables. This source routing mechanism eliminates the need for periodic routing updates, reducing control overhead and conserving bandwidth.

Additionally, DSR employs route caching, where each node stores routes that it learns through direct communication or overhearing other transmissions. When a source node needs a route to a destination, it first checks its cache. If a valid route is found, it is used immediately, avoiding a new route discovery process. Route caching significantly improves efficiency, especially in stable or moderately mobile networks, by reducing the frequency of route discovery operations.

Route Discovery and Maintenance Process

The DSR protocol operates through two core mechanisms: Route Discovery and Route Maintenance.

- Route Discovery: When a source node lacks a route to the desired destination, it initiates a Route Request (RREQ) message that is broadcast to neighboring nodes. Each node appends its own address to the RREQ before forwarding it. Once the RREQ reaches the destination or an intermediate node with a cached route to the destination, a Route Reply (RREP) message is generated. The RREP is sent back to the source using the reverse path, allowing the source to record the discovered route.
- Route Maintenance: DSR uses Route Error (RERR) messages to detect and respond to link failures. When a node identifies a broken link during data transmission, it sends an RERR message to the source, which then removes the invalid route from its cache. The source may attempt an alternative cached route or initiate a new route discovery if necessary.

This mechanism ensures continuous communication despite frequent topology changes and mobility in the network.

Header Overhead Issues and Caching Efficiency

While source routing simplifies route management, it also introduces header overhead, as the entire route (all intermediate node addresses) must be included in each packet. This overhead can become significant in networks with long multi-hop paths, consuming additional bandwidth and energy.

Moreover, stale cache entries may lead to routing errors if nodes rely on outdated paths. To mitigate this, DSR incorporates cache timeout mechanisms and route validation processes to

maintain cache accuracy. Optimized cache management strategies, such as path shortening and selective cache replacement, further enhance performance and reliability.

Performance Trade-offs and Optimizations

DSR performs exceptionally well in networks with low to moderate mobility, where routes remain valid for longer durations. Its lack of periodic control messages makes it energy-efficient and suitable for battery-powered devices. However, in high-mobility or large-scale networks, DSR's performance may degrade due to increased route discovery latency and header overhead.

Several optimizations have been proposed to improve DSR's efficiency:

- ***Adaptive Cache Management:*** Limits the size of route caches and removes stale routes promptly.
- ***Link-Layer Feedback Integration:*** Reduces route maintenance delay by leveraging lower-layer feedback to detect link breakages faster.
- ***Hierarchical DSR:*** Organizes nodes into clusters to minimize broadcast storms during route discovery.
- ***Hybrid DSR-AODV Models*:** Combine DSR's caching efficiency with AODV's scalable route discovery mechanisms.

Dynamic Source Routing (DSR) provides a robust and flexible framework for on-demand routing in ad hoc networks. Its source routing and caching mechanisms make it particularly effective in networks with moderate mobility and limited node density. Although header overhead and stale cache issues present challenges, various optimization techniques have made DSR a foundational routing protocol and a benchmark for evaluating newer ad hoc routing strategies.

4.5.3 Temporally Ordered Routing Algorithm (TORA)

The Temporally Ordered Routing Algorithm (TORA) is a reactive (on-demand) routing protocol designed specifically for highly dynamic and large-scale ad hoc wireless networks. It aims to provide efficient, loop-free, and adaptive routing through localized control messages, minimizing network-wide communication overhead. TORA's unique feature is its reliance on link reversal and Directed Acyclic Graph (DAG)-based routing, which enables rapid route reconfiguration following link failures — a critical capability in mobile environments.

Principle of Link Reversal Routing

At the core of TORA lies the link reversal principle, a mechanism that ensures continuous and loop-free routing. When a node detects a broken link to its downstream neighbor (i.e., a

link toward the destination), it reacts locally by reversing the direction of the affected link to maintain a valid route structure.

This adaptive behavior allows nodes to reestablish routes without triggering a network-wide route discovery, thereby containing the impact of topology changes within a limited area. The link reversal process follows a temporal ordering mechanism, meaning that each update is time-stamped to preserve the chronological order of link reversals. This ensures loop-free operation even in complex, rapidly changing topologies.

Concept of Directed Acyclic Graph (DAG) Formation

TORA organizes routing paths using a Directed Acyclic Graph (DAG) rooted at the destination node. Each node in the network is assigned a height metric, which represents its logical distance from the destination.

- Downstream links are those directed toward nodes with a lower height value.
- Upstream links point toward nodes with a higher height value.

When data packets are sent, they always flow "downhill" toward the destination along downstream links. If a link failure occurs, the affected node increases its height value, effectively reversing the link direction to reestablish the DAG structure. This hierarchical approach allows multiple valid routes to coexist, improving reliability and load distribution across the network.

Route Maintenance and Multiple Path Support

TORA's route maintenance mechanism is designed to handle link breakages locally and efficiently. When a node loses its downstream link (indicating a broken path), it performs a localized re-heighting operation rather than initiating a global route discovery. Neighboring nodes adjust their heights in response, and a new DAG is reconstructed dynamically.

One of TORA's distinguishing features is its support for multiple paths. Unlike single-path routing protocols such as AODV or DSR, TORA maintains several alternative downstream routes simultaneously. This multipath capability enhances fault tolerance, load balancing, and data delivery reliability. If no alternate path exists and the network becomes partitioned, TORA invokes a route erasure procedure to clear invalid routes and prevent routing loops. This ensures that only valid paths remain active, maintaining the consistency of the routing state.

Strengths and Weaknesses in Highly Dynamic Environments

Strengths:

- Highly adaptive and localized operation: TORA minimizes control overhead by restricting route updates to localized regions affected by topology changes.

- Multipath routing: Ensures high reliability and fault tolerance, suitable for dynamic networks such as MANETs and UAV swarms.
- Loop-free routing: The use of temporal ordering and DAG structure guarantees loop-free data transmission.
- Scalability: Performs well in large networks where frequent mobility causes constant topology changes.

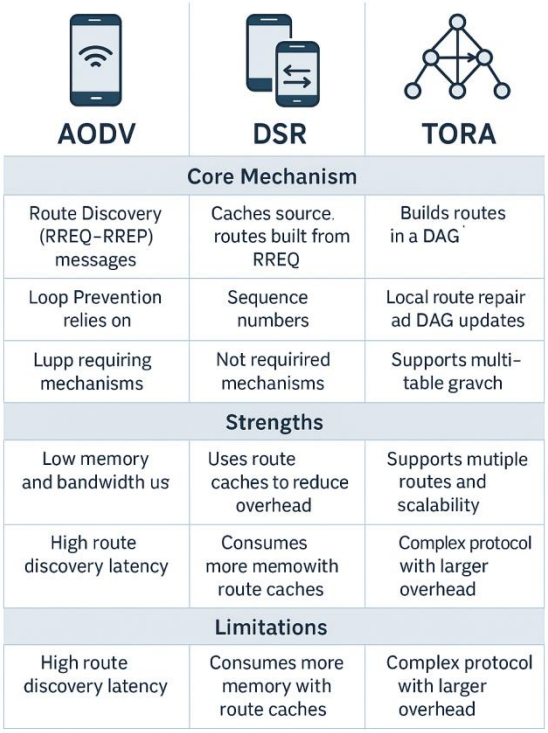
Weaknesses:

- Complexity in implementation: The DAG maintenance and temporal ordering mechanisms increase algorithmic complexity.
- Control message overhead in dense networks: Although localized, frequent link reversals can generate substantial control traffic under high mobility.
- Dependence on synchronized clocks: TORA relies on accurate time synchronization among nodes to maintain temporal order, which can be challenging in decentralized networks.
- Inefficiency in small or static networks: In low-mobility scenarios, simpler protocols like AODV or DSR often outperform TORA in terms of efficiency.

The Temporally Ordered Routing Algorithm (TORA) represents an advanced and adaptive routing solution tailored for highly dynamic and large-scale ad hoc environments. Its link reversal and DAG-based mechanisms provide robustness and scalability unmatched by many other reactive protocols. However, the protocol's complexity, synchronization requirements, and potential control overhead can limit its practicality in smaller or less dynamic networks. Despite these challenges, TORA remains an influential model for designing resilient, distributed, and adaptive routing algorithms in modern mobile ad hoc systems.

4.6 Comparative Analysis of Reactive Protocols

Reactive routing protocols, also known as on-demand protocols, establish routes only when required by a source node. Among the most studied reactive protocols in ad hoc wireless networks are AODV (Ad hoc On-Demand Distance Vector), DSR (Dynamic Source Routing), and TORA (Temporally Ordered Routing Algorithm). Each of these protocols adopts different strategies for route discovery, maintenance, and optimization.



AODV	DSR	TORA
Core Mechanism		
Route Discovery (RREQ-RREP) messages	Caches source. routes built from RREQ	Builds routes in a DAG
Loop Prevention relies on	Sequence numbers	Local route repair ad DAG updates
Lupp requiring mechanisms	Not requirired mechanisms	Supports multi-table gravch
Strengths		
Low memory and bandwidth us	Uses route caches to reduce overhead	Supports mutiple routes and scalability
High route discovery latency	Consumes more memowith route caches	Complex protocol with larger overhead
Limitations		
High route discovery latency	Consumes more memory with route caches	Complex protocol with larger overhead

Figure 2: Comparison of Major Reactive Routing Protocols: AODV, DSR, and TORA

Figure 2, this section presents a detailed comparative analysis based on performance metrics, strengths and weaknesses, and suitability for various application scenarios, followed by a summary table highlighting their key differences.

Performance Metrics

Reactive protocols are typically evaluated using several core performance parameters:

- Latency: Measures the time taken for data to reach the destination after being sent from the source. Lower latency is crucial for real-time and mission-critical applications.
- Throughput: Represents the successful data transmission rate over the network. Higher throughput indicates more efficient use of network resources.
- Packet Delivery Ratio (PDR): The ratio of packets successfully delivered to those sent. It reflects the reliability and robustness of the routing protocol under varying conditions such as node mobility and congestion.
- Control Overhead: Quantifies the amount of routing-related control traffic (e.g., RREQ, RREP, RERR messages) relative to the total data transmitted. Protocols with excessive control overhead may experience reduced efficiency, especially in dense networks.

Each reactive protocol balances these metrics differently, depending on its design focus — such as scalability, adaptability, or reliability.

Strengths and Weaknesses Comparison (AODV vs. DSR vs. TORA)

1. AODV (Ad hoc On-Demand Distance Vector):
    - Strengths:
        - Maintains loop-free routes using sequence numbers.
        - Scales well in large, dynamic networks.
        - Efficient route maintenance through localized RERR messages.
    - Weaknesses:
        - High control overhead during frequent topology changes.
        - Delay in route discovery when no cached path exists.
        - Performance degradation in high-mobility scenarios due to frequent route breaks.
2. DSR (Dynamic Source Routing):
    - Strengths:
        - No periodic updates, minimizing control overhead in static or moderately mobile networks.
        - Route caching reduces route discovery frequency.
        - Multiple cached routes improve resilience against link failures.
    - Weaknesses:
        - Source routing increases header overhead, reducing efficiency in large networks.
        - Cache staleness may lead to routing errors.
        - Scalability issues in dense networks due to long route headers.
3. TORA (Temporally Ordered Routing Algorithm):
    - Strengths:
        - Highly adaptive and scalable in large, mobile networks.
        - Multiple path support enhances fault tolerance.
        - Localized route repair reduces global broadcast overhead.
    - Weaknesses:
        - Complex implementation with dependency on synchronized clocks.
        - Control message bursts under frequent topology changes.
        - Inefficient for small or low-mobility networks.

Suitability Across Application Scenarios

- Low-Mobility, Small Networks: DSR performs best due to minimal control overhead and effective use of route caching. Suitable for sensor or static IoT networks.
- Moderate Mobility, Medium to Large Networks: AODV is preferable as it maintains balanced performance with loop-free routing and efficient route maintenance

mechanisms. Ideal for vehicular ad hoc networks (VANETs) and mobile communication groups.

- High-Mobility, Large-Scale Networks: TORA excels in rapidly changing environments such as UAV swarms, battlefield communications, or disaster management scenarios, where frequent topology changes demand adaptive and localized route repair mechanisms.

Table 1: Comparison of Reactive Routing Protocols

Feature / Metric	AODV	DSR	TORA
Routing Mechanism	Distance vector	Source routing	Link reversal (DAG-based)
Route Discovery	On-demand using RREQ/RREP	Source-based, with route caching	On-demand DAG formation
Route Maintenance	Local repair, RERR messages	Cache update and route salvage	Localized link reversal
Loop Prevention	Sequence numbers	Source-defined path	Temporal ordering
Multiple Path Support	Limited	Yes (cached)	Yes (inherent feature)
Control Overhead	Moderate	Low (in static) / High (in dynamic)	High (in dense networks)
Scalability	Good	Moderate	Excellent
Adaptability to Mobility	Moderate	Low to moderate	High
Energy Efficiency	Average	High in static networks	Moderate
Implementation Complexity	Medium	Low	High
Best Suited For	MANETs, VANETs	Small IoT or sensor networks	UAV swarms, military, large dynamic systems

Reactive routing protocols such as AODV, DSR, and TORA form the backbone of on-demand communication in ad hoc networks. Each protocol offers distinct trade-offs between control overhead, adaptability, and scalability. AODV balances efficiency and scalability, DSR minimizes control traffic through caching but struggles with scalability, and TORA provides robust adaptability for highly mobile environments at the cost of complexity. Selecting the optimal protocol depends on specific application requirements, including network size, node mobility, energy constraints, and QoS expectations. Together, these protocols exemplify the evolution of on-demand routing strategies for modern decentralized wireless networks.

4.7 Performance Optimization Strategies

Reactive routing protocols, while efficient in dynamically changing environments, face inherent challenges such as high route discovery latency, excessive control overhead, and limited energy efficiency. To improve their performance, several optimization strategies have been developed to enhance scalability, adaptability, and reliability. These strategies focus on optimizing route discovery and maintenance, conserving node energy, and incorporating intelligent decision-making mechanisms.

Reducing Route Discovery Latency

One of the major drawbacks of reactive routing is the delay introduced during the route discovery phase, as routes are established only when needed. Several methods can be employed to minimize this latency:

- Expanding Ring Search (ERS): Limits the scope of route request (RREQ) flooding by gradually increasing the Time-To-Live (TTL) value, reducing unnecessary broadcasts.
- Cached Route Utilization: Nodes maintain a cache of recently used routes, allowing faster route retrieval without initiating a new discovery process.
- Preemptive Route Discovery: Anticipates link failures using signal strength or mobility patterns and establishes backup routes before the existing one breaks.

By integrating these methods, reactive protocols can significantly reduce end-to-end delay and improve response time in time-sensitive applications such as vehicular networks or disaster response systems.

Enhancing Energy Efficiency and Scalability

Energy efficiency is critical in ad hoc networks, where nodes often operate on battery power. Optimizations in this area aim to reduce redundant transmissions and balance energy consumption:

- Energy-Aware Routing: Prioritizes paths with nodes that have sufficient residual energy, extending overall network lifetime.
- Load Balancing: Distributes routing responsibilities evenly among nodes to avoid premature energy depletion of specific nodes.
- Hierarchical or Cluster-Based Routing: Organizes nodes into clusters, reducing control message overhead and improving scalability in large networks.
- Sleep Scheduling and Duty Cycling: Allows nodes to enter low-power states when idle, minimizing energy wastage in sensor or IoT networks.

These strategies ensure that energy resources are conserved without compromising connectivity or routing efficiency.

Adaptive Broadcasting and Caching Schemes

Broadcasting is essential in route discovery but can lead to congestion and collisions if not controlled. Adaptive broadcasting mechanisms help manage this challenge:

- Probabilistic Broadcasting: Instead of blind flooding, nodes rebroadcast RREQs based on a calculated probability, reducing redundant messages.
- Neighbor-Aware Broadcasting: Utilizes knowledge of neighboring nodes to decide when and how to forward route requests efficiently.
- Intelligent Caching: Updates cached routes dynamically based on usage frequency and validity, preventing stale route utilization.

By fine-tuning broadcasting and caching techniques, reactive routing protocols can improve throughput, reduce control overhead, and enhance overall scalability.

Cross-Layer Optimization and Mobility Prediction Techniques

Traditional routing protocols follow a strict layered architecture (e.g., OSI model), which limits the exchange of information across layers. Cross-layer optimization breaks this limitation by enabling collaboration between different protocol layers:

- Physical Layer Feedback: Signal strength and link quality indicators help routing protocols predict link breakages.
- MAC Layer Coordination: Adaptive transmission scheduling and contention management minimize packet collisions.
- Mobility Prediction: Predictive algorithms estimate node movement patterns to select stable and long-lasting routes.

For instance, combining mobility prediction with link-quality estimation helps select routes that remain stable for longer durations, reducing route maintenance frequency and improving network reliability.

Use of AI/ML for Intelligent Route Selection

The integration of Artificial Intelligence (AI) and Machine Learning (ML) has revolutionized routing optimization in ad hoc networks. These techniques enhance decision-making and adaptability under varying network conditions:

- Reinforcement Learning (RL): Allows nodes to learn optimal routing decisions through continuous interaction with the environment.
- Supervised and Unsupervised Learning: Used for traffic classification, anomaly detection, and adaptive congestion control.
- Federated Learning (FL): Enables distributed model training across nodes without centralized data storage, preserving privacy while enhancing intelligence.

- Predictive Analytics: Forecasts link failures, mobility trends, and energy consumption to preemptively adjust routes.

Performance optimization in reactive routing protocols is essential to overcome inherent limitations like latency, control overhead, and energy inefficiency. Techniques such as adaptive broadcasting, intelligent caching, cross-layer coordination, and AI/ML-based route prediction contribute to creating highly responsive and efficient ad hoc networks. These optimizations not only improve protocol performance but also ensure the scalability and sustainability of reactive routing in emerging domains such as IoT, 5G/6G communication, and intelligent edge networks.

4.8 Security Considerations in On-Demand Routing

Security is a critical concern in reactive routing protocols, as their decentralized, dynamic, and infrastructure-less nature makes them vulnerable to various network attacks. Unlike traditional networks with centralized control, ad hoc networks rely on the cooperation of all nodes, creating opportunities for malicious actors to disrupt routing operations. This section discusses common vulnerabilities, security enhancement mechanisms, notable secure protocol variants, and the trade-offs between security and performance.

Common Vulnerabilities: Blackhole, Wormhole, and Flooding Attacks

Reactive routing protocols such as AODV and DSR depend on route discovery mechanisms that are easily exploited if proper authentication and verification are lacking. Some of the most prominent attacks include:

- ***Blackhole Attack:*** A malicious node falsely claims to have the shortest route to the destination during route discovery. Once it attracts data packets, it drops them instead of forwarding, leading to packet loss and denial of service.
- ***Wormhole Attack:*** Two colluding attackers establish a private high-speed link (a "wormhole") between distant parts of the network. They replay or tunnel routing messages, disrupting the normal route discovery process and misleading nodes into choosing incorrect or suboptimal paths.
- ***Flooding Attack:*** Malicious nodes generate excessive Route Request (RREQ) or Route Reply (RREP) messages, overwhelming the network with control packets. This depletes bandwidth and node energy, leading to denial-of-service (DoS) conditions.

These attacks can degrade performance metrics such as packet delivery ratio, throughput, and network lifetime, posing severe challenges in mission-critical applications like military or disaster recovery networks.

Trust-Based and Cryptographic Enhancements for Reactive Routing

To counteract security threats, researchers have proposed trust-based and cryptographic mechanisms that enhance the reliability of on-demand routing protocols.

- Trust-Based Mechanisms: Each node maintains a trust score for its neighbors based on past interactions, successful packet forwarding, and observed behavior. Nodes with low trust values are avoided in route selection.
    - *Example:* Trust-based AODV (TAODV) and reputation-based DSR variants use cooperative monitoring to isolate malicious nodes.
- Cryptographic Techniques: Employ digital signatures, hash chains, and encryption to verify message integrity and node authenticity.
    - *Symmetric Cryptography* (e.g., AES, HMAC) is efficient but requires secure key management.
    - *Asymmetric Cryptography* (e.g., RSA, ECC) offers stronger security but incurs higher computational overhead.

These mechanisms ensure confidentiality, integrity, and authenticity of routing messages, reducing the likelihood of spoofing and message tampering.

Secure Versions of Reactive Protocols

Several secure variants of traditional reactive routing protocols have been developed to address security vulnerabilities while maintaining efficiency:

- Secure AODV (SAODV): Extends AODV by using digital signatures to authenticate non-mutable fields and hash chains to protect mutable hop-count values. This prevents attackers from altering routing information.
- Secure Routing Protocol (SRP): Introduces end-to-end authentication between communicating nodes using shared keys. Intermediate nodes cannot modify route requests or replies without detection, enhancing data integrity.
- Ariadne: A secure version of DSR that relies on TESLA (Timed Efficient Stream Loss-tolerant Authentication) for broadcast authentication and MAC-based verification to ensure lightweight security suitable for MANETs.

Each of these protocols strengthens security at different layers but may also introduce extra processing time and bandwidth usage.

Balancing Security and Performance Overhead

Security enhancements, while essential, often come with trade-offs that can affect the overall efficiency of reactive routing protocols:

- Increased Control Overhead: Cryptographic operations and additional authentication fields increase packet size, consuming more bandwidth and energy.

- Higher Latency: Verification processes and secure route establishment add delay during route discovery and maintenance.
- Energy Consumption: Encryption and decryption tasks require computational power, reducing the lifetime of battery-operated nodes.

To balance security and performance, adaptive mechanisms are employed—such as lightweight cryptography, selective authentication, and context-aware security levels that adjust protection based on application sensitivity or threat level. For example, military ad hoc networks may use full cryptographic security despite higher overhead, while IoT-based ad hoc systems may prefer lightweight, trust-based solutions to conserve resources.

Security in on-demand routing protocols is a complex yet crucial aspect of ad hoc network design. Common attacks such as blackhole, wormhole, and flooding exploit the openness of reactive routing mechanisms, necessitating robust protection through trust management and cryptographic techniques. Secure variants like SAODV, SRP, and Ariadne have significantly improved resilience against malicious behavior. However, a key challenge remains in balancing security strength with network performance, ensuring that reactive protocols can remain both secure and efficient in highly dynamic, resource-constrained environments.

4.9 Applications of Reactive Routing Protocols

Reactive routing protocols have become an essential component in mobile ad hoc networks (MANETs) and their derivatives, owing to their on-demand nature, low routing overhead, and adaptability to dynamic environments. These protocols establish routes only when required, making them highly efficient in scenarios where network topology changes frequently. Their application spans across a variety of real-world domains such as military operations, vehicular networks, disaster management, and unmanned systems. This section explores these key applications in detail.

Tactical and Military Communication Networks

Reactive routing protocols play a pivotal role in tactical and battlefield communications, where the network environment is highly mobile, decentralized, and infrastructure-less. Military networks demand secure, robust, and adaptive routing to ensure real-time information exchange among soldiers, vehicles, and command centers.

- Use Case: Coordination of troops, surveillance drones, and armored vehicles in combat zones.
- Protocol Suitability:
    - AODV is preferred for its quick route discovery and minimal control overhead.
    - DSR supports multi-hop communication with route caching, suitable for small tactical units.

    - TORA excels in dynamic environments with its rapid link-reversal mechanism.
- Advantages:
    - On-demand route setup reduces unnecessary transmissions, conserving energy.
    - Multi-path support ensures resilience against node failures or attacks.

In such mission-critical systems, secure extensions like SAODV or Ariadne are often integrated to protect sensitive data from interception or manipulation.

Vehicular Ad Hoc Networks (VANETs)

In Vehicular Ad Hoc Networks, vehicles communicate with each other (V2V) and with roadside units (V2I) to enhance traffic safety, route planning, and infotainment services. The high mobility of vehicles creates a rapidly changing network topology—conditions under which reactive routing protocols can perform efficiently due to their on-demand and flexible route establishment.

- Use Case: Vehicle collision avoidance, traffic congestion alerts, and smart highway coordination.
- Protocol Suitability:
    - AODV is widely used due to its scalability and quick adaptation to frequent topology changes.
    - TORA is effective in urban mobility scenarios because of its ability to maintain multiple routes and adapt to disconnections.
- Advantages:
    - Reduces routing overhead in highly mobile environments.
    - Adapts dynamically to real-time traffic patterns and vehicle density.

In VANETs, cross-layer enhancements combining AODV with GPS-based mobility prediction further optimize route stability and minimize packet loss.

Disaster Relief and Emergency Response Systems

During natural disasters such as earthquakes, floods, or hurricanes, traditional communication infrastructure is often damaged or unavailable. Reactive routing protocols enable instant ad hoc network formation among emergency responders, medical units, and coordination centers.

- Use Case: Rapid deployment of communication networks among rescue teams in affected zones.
- Protocol Suitability:
    - DSR is beneficial for small-scale operations with limited nodes due to its route caching feature.
    - AODV offers efficient connectivity in larger, more dynamic networks.

    - TORA is valuable in maintaining robust connections in partially mobile emergency networks.
- Advantages:
    - Quick establishment of communication links without pre-existing infrastructure.
    - Flexibility in node movement, essential for field mobility and coordination.

Such networks can integrate with satellite links or cellular backhauls to form hybrid architectures, ensuring sustained connectivity even in isolated regions.

Wireless Sensor and UAV Networks

In Wireless Sensor Networks (WSNs) and Unmanned Aerial Vehicle (UAV) networks, reactive routing protocols support data collection, monitoring, and coordination in applications like environmental sensing, agriculture, and surveillance.

- Use Case: UAV swarms communicating in real time for disaster assessment or crop monitoring.
- Protocol Suitability:
    - AODV provides energy-efficient and reliable routing in sensor clusters.
    - DSR leverages cached routes to reduce control message overhead.
    - TORA supports mobility among UAV nodes with minimal reconfiguration delay.
- Advantages:
    - Reduces communication overhead by initiating routes only when needed.
    - Adaptable to intermittent connectivity and node mobility common in UAV operations.

Additionally, AI-driven route selection integrated with reactive routing improves flight path optimization and autonomous coordination among UAVs, enhancing mission reliability.

Reactive routing protocols continue to prove indispensable across diverse domains where real-time communication, adaptability, and resilience are paramount. Their ability to self-organize, minimize control overhead, and respond dynamically to topology changes makes them a foundational technology for modern ad hoc and autonomous networking systems.

4.10 Future Trends in Reactive Routing

Reactive routing protocols continue to evolve to meet the growing demands of next-generation wireless networks, intelligent mobility, and autonomous communication systems. As emerging technologies such as 5G/6G, edge computing, and AI-based decision-making mature, reactive routing is expected to become more adaptive, energy-efficient, and

application-aware. This section explores key future trends that are shaping the next phase of on-demand routing evolution.

Integration with 5G/6G and Edge Computing

The convergence of reactive routing protocols with 5G and 6G communication architectures is set to revolutionize ad hoc networking performance. Next-generation wireless systems provide ultra-low latency, massive connectivity, and high data throughput, which are essential for time-sensitive and mission-critical applications.

- Edge computing enhances reactive routing by offloading route computation and data processing tasks from mobile nodes to nearby edge servers, minimizing latency and conserving energy.
- In vehicular, UAV, and IoT-based ad hoc networks, edge-assisted reactive routing ensures real-time path computation and context-aware communication.
- For example, an edge-enabled AODV variant could leverage edge intelligence to predict link stability or node movement, improving route reliability.

The integration of 5G/6G with reactive routing thus enables ultra-responsive, high-capacity, and context-aware communication for large-scale, heterogeneous ad hoc networks.

AI-Driven Adaptive Route Management

Artificial Intelligence (AI) and Machine Learning (ML) are becoming central to the next generation of adaptive reactive routing. Traditional reactive protocols rely on static route discovery mechanisms that may not perform efficiently in high-mobility or energy-constrained environments. AI-based enhancements address these challenges through prediction, optimization, and self-learning.

- Reinforcement Learning (RL) can optimize routing paths dynamically by learning from network performance feedback.
- Deep Neural Networks (DNNs) can predict node mobility, congestion, or link failures, reducing the need for frequent route discoveries.
- Federated Learning (FL) allows distributed nodes to collaboratively improve routing intelligence without sharing sensitive data, supporting privacy-preserving optimization.

These intelligent routing mechanisms help achieve adaptive, energy-efficient, and reliable communication suited for smart cities, autonomous vehicles, and UAV networks.

Energy Harvesting and Green Routing Designs

Sustainability and energy efficiency are major concerns in ad hoc and sensor-based networks, particularly in remote or battery-dependent environments.

Future reactive routing research emphasizes green routing strategies that minimize energy waste while maintaining high performance.

- Energy-aware AODV and DSR variants integrate metrics like residual battery power, transmission cost, and harvesting potential into route selection.
- Energy harvesting nodes, capable of utilizing solar, kinetic, or RF energy, enable longer network lifetimes and self-sustaining communication systems.
- Protocols are also being enhanced to balance energy consumption across nodes, preventing premature network partitioning.

Green reactive routing aligns with global sustainability goals, particularly in environmental monitoring, rural IoT deployments, and disaster management networks.

Hybrid Reactive-Proactive Routing Evolution

As ad hoc networks become more complex and diverse, purely reactive or proactive approaches often fall short of meeting all application needs. The future points toward hybrid routing protocols that combine the on-demand efficiency of reactive mechanisms with the readiness of proactive approaches.

- Hybrid designs dynamically switch between proactive and reactive modes based on network size, mobility, and traffic load.
- For example, Zone Routing Protocol (ZRP) maintains proactive routing within local zones and uses reactive discovery for distant nodes.
- AI-assisted hybrid routing could further optimize this balance, ensuring low latency during mobility while minimizing control overhead.

This evolution will result in self-optimizing, scalable, and context-aware routing architectures suited for 6G-enabled IoT, vehicular, and aerial networks.

The future of reactive routing is moving toward intelligent, sustainable, and integrated designs that can adapt seamlessly to the demands of next-generation wireless ecosystems. By combining AI-driven adaptability, 5G/6G connectivity, energy-aware design, and hybrid protocol frameworks, reactive routing will evolve into a resilient and context-optimized communication paradigm. These advancements will be critical in supporting emerging domains such as autonomous systems, metaverse communications, and massive IoT deployments—where real-time responsiveness, scalability, and efficiency are non-negotiable.

4.11 Conclusion

This chapter explored the fundamental concepts, mechanisms, and advancements of reactive routing protocols in ad hoc wireless networks. Unlike proactive protocols that maintain

continuous route updates, reactive (on-demand) routing establishes routes only when needed, minimizing unnecessary control overhead in dynamic and resource-constrained environments. The discussion began with the principles of route discovery and maintenance, detailing processes such as Route Request (RREQ), Route Reply (RREP), and Route Error (RERR) message handling.

Key reactive routing protocols — AODV (Ad hoc On-Demand Distance Vector), DSR (Dynamic Source Routing), and TORA (Temporally Ordered Routing Algorithm) — were analyzed in depth, highlighting their operational characteristics, design philosophies, and performance trade-offs. Comparative analysis showed how AODV ensures loop-free routing using sequence numbers, DSR emphasizes source routing and caching efficiency, and TORA excels in highly dynamic environments through link-reversal techniques.

The chapter also examined performance metrics such as latency, throughput, and control overhead, providing insights into the strengths and weaknesses of each protocol across varying mobility levels and network sizes. Optimization strategies like AI-driven routing, cross-layer design, and energy-efficient broadcasting were discussed as key methods to enhance scalability, reliability, and adaptability. Furthermore, security considerations were addressed through techniques such as trust-based routing, cryptographic authentication, and secure protocol variants like SAODV and Ariadne.

Applications of reactive routing span a wide range — from tactical military networks and vehicular communication systems (VANETs) to disaster recovery and IoT-enabled sensor networks. Emerging trends indicate integration with 5G/6G infrastructures, AI-based adaptive routing, and energy-harvesting mechanisms, paving the way for intelligent, sustainable, and hybrid routing architectures.

In reactive routing protocols remain vital for dynamic, decentralized, and rapidly changing environments, where adaptability and responsiveness are crucial. The next chapter transitions to Hybrid Routing Protocols, which aim to combine the proactive approach's stability with the reactive model's efficiency, achieving a balanced and context-aware routing strategy for future ad hoc network applications.

References

1. Perkins, C. E., & Royer, E. M. (1999). Ad hoc On-Demand Distance Vector (AODV) routing. *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 90–100.
2. Perkins, C. E., Belding-Royer, E. M., & Das, S. R. (2003). Ad hoc On-Demand Distance Vector (AODV) Routing. *RFC 3561, IETF MANET Working Group.*
3. Johnson, D. B., Maltz, D. A., & Hu, Y. C. (2004). The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. *RFC 4728, IETF MANET Working Group.*
4. Park, V. D., & Corson, M. S. (2001). Temporally Ordered Routing Algorithm (TORA) version 1: Functional specification. *IETF Internet Draft, MANET Working Group.*

5. Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y. C., & Jetcheva, J. (1998). A performance comparison of multi-hop wireless ad hoc network routing protocols. *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98)*, 85–97.
6. Marina, M. K., & Das, S. R. (2002). On-demand multipath distance vector routing in ad hoc networks. *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, 14–23.
7. Chakeres, I. D., & Perkins, C. E. (2008). Dynamic MANET On-demand (DYMO) routing. *Internet-Draft, IETF MANET Working Group*.
8. Hu, Y. C., Johnson, D. B., & Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks, 1*(1), 175–192.
9. Zapata, M. G., & Asokan, N. (2002). Securing ad hoc routing protocols. *Proceedings of the 1st ACM Workshop on Wireless Security (WiSe'02)*, 1–10.
10. Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., & Jamalipour, A. (2007). A survey of routing attacks in mobile ad hoc networks. *IEEE Wireless Communications, 14*(5), 85–91.
11. Tarique, M., Tepe, K. E., Adibi, S., & Erfani, S. (2009). Survey of multipath routing protocols for mobile ad hoc networks. *Journal of Network and Computer Applications, 32*(6), 1125–1143.
12. Alsharif, M. H., & Nordin, R. (2013). Energy-efficient AODV routing protocol for MANETs. *Journal of Communications, 8*(3), 158–167.
13. Sethi, M., & Singh, M. (2015). Energy-aware enhancements in AODV routing for MANETs. *Wireless Personal Communications, 83*(2), 979–992.
14. Karthikeyan, N., & Karthik, R. (2017). Performance analysis of on-demand routing protocols under varying mobility models in MANET. *Wireless Networks, 23*(7), 2121–2134.
15. Singh, R., & Chauhan, D. S. (2018). Enhanced secure AODV for mitigating blackhole and wormhole attacks. *International Journal of Communication Systems, 31*(3), e3476.
16. Raj, R., & Ganesan, R. (2020). Machine learning-based adaptive route selection in AODV for MANETs. *Computer Networks, 180*, 107376.
17. Bansal, D., & Sharma, S. (2021). A comparative analysis of DSR and AODV routing protocols in dynamic ad hoc environments. *International Journal of Wireless and Mobile Computing, 20*(4), 329–338.
18. Ahmed, M. A., & Lee, K. (2022). AI-driven route optimization in reactive routing for VANETs. *IEEE Access, 10*, 78245–78256.
19. Chhabra, S., & Singh, G. (2023). Secure and energy-aware reactive routing for UAV ad hoc networks. *Ad Hoc Networks, 139*, 103082.
20. Li, H., & Zhang, Z. (2024). Deep reinforcement learning-based route discovery and maintenance in MANETs. *IEEE Transactions on Mobile Computing, 23*(2), 511–524.

ISBN: 978-93-47475-17-7

Chapter-5

Hybrid Routing Protocols: Balancing Proactive and Reactive Strategies

[1]P.Myvizhi,[2] V.S.Harini, [3]R.Janani

[1]Assistant Professor,
Department of Computer Applications,
K.S.Rangasamy College of Arts and Science(Autonomous),
Tiruchengode,Tamilnadu, India.

[2,3]Assistant Professor,
Department of Computer Applications,
K.S.Rangasamy College of Arts and Science(Autonomous),
Tiruchengode,Tamilnadu, India.

Abstract: *Hybrid routing protocols represent an advanced evolution in ad hoc network routing, designed to balance the strengths and mitigate the weaknesses of both proactive and reactive approaches. While proactive routing ensures low-latency access to nearby routes through periodic updates, reactive routing minimizes overhead by discovering routes only when needed. Hybrid protocols integrate these paradigms to achieve scalability, adaptability, and efficiency in dynamic network environments. By combining localized proactive maintenance with on-demand global route discovery, hybrid routing protocols offer a flexible framework suitable for diverse scenarios such as mobile ad hoc networks (MANETs), vehicular networks (VANETs), and large-scale Internet of Things (IoT) systems. Their core objective is to provide reliable, energy-efficient, and low-delay communication while dynamically adjusting to network topology changes and node mobility patterns.*

Keywords: *Hybrid routing, zone-based routing, scalability, dynamic topology, Zone Routing Protocol (ZRP), Scalable Hybrid Adaptive Routing Protocol (SHARP), hybrid MANETs, hierarchical routing, mobility management, adaptive routing strategies.*

5.1. Introduction

Routing in ad hoc wireless networks presents unique challenges due to their decentralized architecture, dynamic topology, and limited resources such as bandwidth and energy. Traditional routing protocols are generally classified into two categories — proactive and reactive — each with distinct advantages and limitations. Proactive routing protocols continuously maintain updated routing tables, enabling quick data transmission but at the cost of high control overhead, especially in highly mobile networks. On the other hand, reactive routing protocols establish routes only when needed, reducing overhead but introducing route discovery delays that can hinder time-sensitive applications.

To overcome these challenges, hybrid routing protocols have emerged as a balanced approach that combines the strengths of both proactive and reactive strategies. These protocols aim to achieve low latency and efficient route maintenance while minimizing control message overhead. Typically, they maintain proactive routing information within a local zone and rely on reactive mechanisms for distant nodes, thus optimizing performance based on network conditions and mobility patterns.

The integration of proactive and reactive elements makes hybrid routing protocols well-suited for large-scale, heterogeneous, and highly dynamic networks such as Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs), and Wireless Sensor Networks (WSNs). This chapter explores the fundamental design principles of hybrid routing, analyzes key protocols, compares their performance characteristics, and discusses future trends and challenges in achieving scalability, adaptability, and robustness in ad hoc environments.

5.2 Fundamentals of Hybrid Routing

The fundamental principle of hybrid routing lies in its ability to combine the strengths of proactive (table-driven) and reactive (on-demand) mechanisms to achieve efficient and scalable routing in ad hoc wireless networks. In hybrid routing, the network is typically divided into zones or hierarchies where proactive routing is used within local regions to maintain up-to-date route information, while reactive routing is employed for communication between distant nodes. This dual approach enables hybrid protocols to dynamically adapt to varying network conditions such as node mobility, density, and traffic load.

Hybrid routing protocols exhibit adaptive behavior by adjusting their routing strategy based on real-time network parameters. For instance, in low-mobility or small-scale environments, the proactive component can dominate to ensure minimal delay, whereas in large or highly mobile networks, the reactive component becomes more active to reduce unnecessary control overhead. This adaptability allows hybrid protocols to maintain an optimal balance between latency, bandwidth efficiency, and scalability.

A core concept in hybrid routing is the use of hierarchical or zone-based design architectures. Nodes are organized into local clusters or zones, where intra-zone communication relies on proactive updates for quick route access, while inter-zone communication triggers on-demand route discovery. This hierarchical structure reduces the global routing overhead while ensuring rapid response within localized regions.

Overall, hybrid routing protocols aim to balance the trade-offs among control overhead, end-to-end latency, and scalability. By intelligently integrating proactive and reactive operations, these protocols provide robust and efficient routing performance across diverse

ad hoc networking scenarios, making them particularly suitable for large, dynamic, and heterogeneous networks.

5.3 Architectural Components of Hybrid Routing Protocols

The architecture of hybrid routing protocols is designed to seamlessly integrate both proactive and reactive routing mechanisms, ensuring efficient communication across varying network conditions. These protocols typically organize the network into zones or hierarchical structures, where each component plays a specific role in optimizing routing efficiency, minimizing overhead, and improving scalability.

Intra-zone routing forms the proactive part of hybrid routing protocols, responsible for managing communication within a node's local zone. Each node maintains up-to-date routing information about its nearby neighbors through periodic updates. This proactive mechanism ensures low-latency communication within the local region, as routes to nearby nodes are immediately available without the need for on-demand discovery. Examples include table-driven approaches similar to those used in DSDV or OLSR, adapted for zone-based operation.

Inter-zone routing, on the other hand, handles communication with nodes located outside the local zone using reactive or on-demand techniques. When a node needs to communicate with a distant node beyond its proactive zone, it initiates a route discovery process similar to AODV or DSR. This helps reduce unnecessary control message flooding across the entire network and ensures that long-distance communications occur efficiently only when needed.

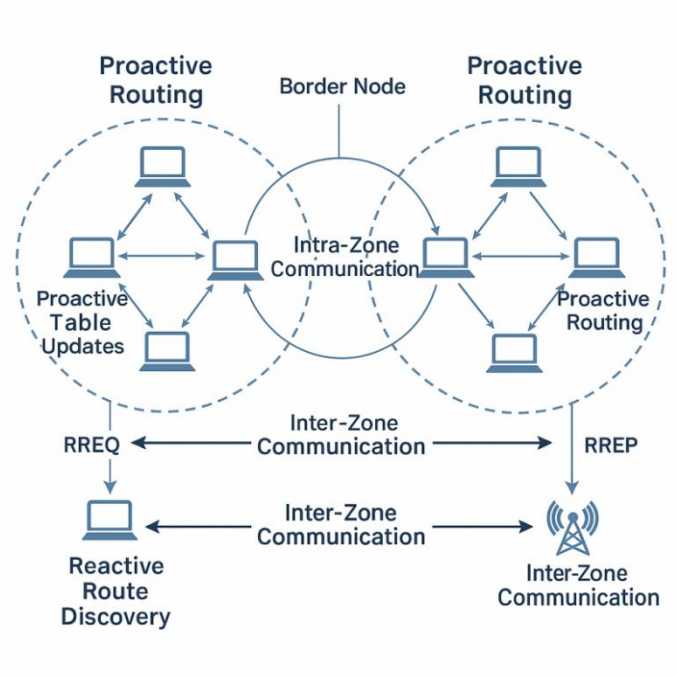


Figure 1: Hybrid Routing Architecture: Integration of Proactive and Reactive Mechanisms

A key design parameter in hybrid routing is the zone radius, which defines the size or number of hops included in each node's proactive region. The selection of this radius significantly impacts network performance. A smaller radius reduces the proactive overhead but increases reactive route discovery frequency, while a larger radius ensures faster intra-zone communication at the cost of higher maintenance overhead. Hence, adaptive zone radius adjustment based on network mobility and density is often employed to optimize overall efficiency.

Control message management is another crucial architectural component. Hybrid protocols must balance the frequency of proactive updates and reactive discoveries to minimize bandwidth consumption and maintain up-to-date routes. Efficient mechanisms such as selective broadcasting, caching, and adaptive update intervals help achieve this balance, preventing excessive network congestion.

The architectural design of hybrid routing protocols—encompassing proactive intra-zone communication, reactive inter-zone routing, adaptive zone radius selection, and intelligent control message management—enables these protocols to deliver high scalability, reduced delay, and balanced routing efficiency in complex and dynamic ad hoc environments.

5.4 Core Hybrid Routing Protocols

Hybrid routing protocols are designed to combine the strengths of both proactive and reactive routing methods, ensuring efficient communication in networks with varying mobility and scalability demands. Among the most well-known hybrid routing protocols are the Zone Routing Protocol (ZRP), Zone-Based Hierarchical Link State Routing (ZHLS), and the Scalable Hybrid Adaptive Routing Protocol (SHARP). Each of these protocols adopts a unique strategy to balance proactive and on-demand routing processes.

5.4.1 Zone Routing Protocol (ZRP)

The Zone Routing Protocol (ZRP) is one of the earliest and most influential hybrid routing models, designed to minimize routing overhead while ensuring low-latency communication. Its operation is based on dividing the network into overlapping zones, each defined by a specific hop radius from a given node. Within each zone, routing is managed proactively, while communication between zones occurs reactively.

ZRP integrates two key sub-protocols:

- **Intra-zone Routing Protocol (IARP):** Handles local communication within a node's zone using proactive routing updates. This ensures immediate route availability for nearby nodes.

- **Inter-zone Routing Protocol (IERP):** Manages communication with nodes outside the local zone using an on-demand route discovery process. This limits flooding to border nodes rather than the entire network.

The concept of bordercasting is central to ZRP's efficiency. Instead of broadcasting route requests to all nodes, ZRP sends them only to border nodes of the originating zone, which then forward the requests to adjacent zones. This significantly reduces broadcast overhead. Another critical parameter is the zone radius, which determines the size of each node's proactive region. Adjusting the zone radius helps tune performance — smaller zones reduce overhead, while larger zones minimize reactive route discoveries.

Strengths: ZRP achieves a balance between low-latency access to local routes and reduced control overhead for distant communication. **Weaknesses:** Its performance depends heavily on optimal zone radius selection and may degrade in highly mobile or dense networks due to frequent topology updates.

5.4.2 Zone-Based Hierarchical Link State Routing (ZHLS)

The Zone-Based Hierarchical Link State Routing (ZHLS) protocol extends the zone-based concept by incorporating a hierarchical structure that enhances scalability in large mobile ad hoc networks (MANETs). In ZHLS, the network is divided into zones, each with a unique zone identifier and an addressing mechanism that supports hierarchical routing.

Within each zone, nodes maintain intra-zone topology information through proactive link-state updates, while inter-zone communication relies on zone-level topology management. This hierarchical organization allows ZHLS to maintain efficient routing tables and reduce the amount of global information each node must store. Route discovery in ZHLS involves first determining the destination zone and then finding the specific node within that zone, reducing the search space compared to flat routing. Link-state updates are disseminated at both node and zone levels, ensuring accurate topology representation with lower control traffic than purely proactive approaches. ZHLS is particularly suitable for large-scale MANETs and networks with moderate mobility, where hierarchical organization improves efficiency. However, it requires zone-level coordination, which may introduce additional complexity in highly dynamic environments.

Strengths: High scalability, reduced global overhead, and efficient route discovery. **Weaknesses:** Overhead in maintaining hierarchical structures and potential delays in inter-zone communication.

5.4.3 Scalable Hybrid Adaptive Routing Protocol (SHARP)

The Scalable Hybrid Adaptive Routing Protocol (SHARP) introduces adaptability as a key feature, dynamically adjusting the balance between proactive and reactive behavior based on network conditions such as node density, mobility, and traffic load. Unlike static hybrid protocols, SHARP can modify its routing strategy in real time to optimize performance.

SHARP maintains proactive routes for frequently communicating or nearby nodes, while distant or less active routes are discovered reactively on demand. This adaptive behavior minimizes unnecessary control traffic during low mobility and ensures quick route availability during high traffic or mobility conditions. A notable feature of SHARP is its Quality of Service (QoS) support, which allows it to prioritize delay-sensitive applications by adjusting routing parameters and thresholds dynamically. Additionally, SHARP incorporates energy-aware mechanisms to distribute load evenly among nodes and prevent early depletion of critical nodes, enhancing overall network lifetime.

Strengths: Dynamic adaptability, QoS support, and energy-efficient operation. **Weaknesses:** Complexity in managing adaptive thresholds and potential instability under rapidly changing conditions.

The ZRP, ZHLS, and SHARP protocols represent key milestones in hybrid routing research. While ZRP focuses on zone-based flexibility, ZHLS emphasizes hierarchical scalability, and SHARP introduces intelligent adaptability. Together, these protocols demonstrate how hybrid routing effectively balances proactive and reactive strategies to achieve efficient, scalable, and resilient communication in ad hoc wireless networks.

5.5 Performance Evaluation and Comparison

Evaluating the performance of hybrid routing protocols is essential to understand their operational efficiency and suitability for different network environments. Since hybrid protocols aim to balance the proactive and reactive paradigms, their effectiveness is measured based on multiple quantitative and qualitative parameters, including throughput, end-to-end delay, control overhead, scalability, and adaptability under various mobility and density conditions.

5.5.1 Key Performance Metrics

- **Throughput:** Refers to the successful data delivery rate across the network. A higher throughput indicates efficient route discovery, reduced packet loss, and better utilization of available bandwidth. Hybrid protocols like SHARP typically achieve higher throughput under dynamic conditions due to their adaptive behavior.
- **End-to-End Delay:** Measures the time taken for a packet to travel from source to destination. Low latency is a sign of rapid route availability and efficient routing. ZRP generally provides low delay for local communication due to its proactive intra-zone routing.
- **Control Overhead:** Represents the amount of control traffic (e.g., routing updates, route requests) generated by the protocol. Reducing this overhead conserves bandwidth and energy. ZHLS and ZRP minimize global flooding by confining updates within zones or hierarchies.

- **Scalability:** Assesses the protocol's ability to maintain performance as network size grows. ZHLS demonstrates excellent scalability because of its hierarchical routing design, while SHARP scales well due to adaptive control mechanisms.
- **Packet Delivery Ratio (PDR):** The ratio of successfully delivered packets to those sent by sources. A high PDR reflects routing stability and reliability, which SHARP often achieves in mixed-mobility networks.
- **Energy Efficiency:** Evaluates the overall power consumption of routing operations. Protocols that limit unnecessary control messages, such as SHARP's adaptive approach, contribute to prolonged node and network lifetime.

5.5.2 Comparative Evaluation of ZRP, ZHLS, and SHARP

Each hybrid protocol performs differently based on topology dynamics, node density, and network size. The following comparative analysis highlights their relative strengths and trade-offs:

Parameter	ZRP	ZHLS	SHARP	Traditional Protocols (AODV, OLSR)
Routing Type	Zone-based hybrid	Hierarchical hybrid	Adaptive hybrid	Reactive (AODV) / Proactive (OLSR)
Routing Structure	Overlapping zones	Zone-based hierarchy	Adaptive proactive-reactive balance	Flat topology
Throughput	Moderate to high	High in large networks	Very high under dynamic loads	Variable; depends on topology
End-to-End Delay	Low for local zones	Moderate	Low to moderate (adaptive)	High (AODV) / Low (OLSR)
Control Overhead	Moderate	Low to moderate	Adaptive (minimal under light load)	High in large networks
Scalability	Good (zone radius tuning)	Excellent	Excellent	Poor to moderate
Energy Efficiency	Moderate	Good	High (load balancing)	Low
Mobility Tolerance	Moderate	Moderate	High	Low (AODV) / Moderate (OLSR)
QoS Support	Limited	Limited	Supported	Minimal
Complexity	Moderate	High	High	Low to moderate

5.5.3 Suitability for Different Network Scenarios

- **Low Mobility, Small Network:** *ZRP* performs efficiently, as proactive updates within small zones minimize delay.

- **Large-Scale, Hierarchical Networks:** *ZHLS* is preferred due to its structured, scalable routing that reduces control overhead.
- **Highly Dynamic, Dense Environments:** *SHARP* excels by adapting its routing mode based on real-time mobility and traffic patterns, maintaining stable throughput and low delay.
- **Energy-Constrained or Heterogeneous Networks:** *SHARP* provides better energy conservation through adaptive control and load balancing mechanisms.

Hybrid routing protocols outperform purely proactive or reactive schemes by offering a balanced trade-off between routing overhead, latency, and scalability.

- ZRP achieves efficiency through zone-based local routing and limited reactive flooding.
- ZHLS ensures scalability through hierarchical organization and efficient inter-zone communication.
- SHARP advances hybrid routing with adaptability, QoS support, and energy awareness, making it suitable for future 5G-enabled MANETs and IoT environments.

Hybrid protocols represent a robust evolution in ad hoc network routing—combining the best of both worlds to achieve resilience, adaptability, and high performance under diverse conditions.

5.6 Optimization and Enhancement Techniques

Hybrid routing protocols aim to balance the benefits of proactive and reactive routing; however, their performance can still be improved through advanced optimization and enhancement mechanisms. As ad hoc networks evolve—particularly in the contexts of 5G/6G, IoT, UAV swarms, and edge computing—hybrid protocols must become more adaptive, intelligent, and resource-efficient. This section explores various techniques that enhance the scalability, reliability, and energy efficiency of hybrid routing systems.

5.6.1 Dynamic Zone Resizing for Mobility Adaptation

One of the most effective strategies in hybrid routing—especially for protocols like ZRP (Zone Routing Protocol)—is dynamic zone resizing.

- Concept: The zone radius (defining how far proactive routing extends) can be adjusted in real time based on node mobility, density, and traffic load.
- Mechanism:
  - When mobility is low, zones are expanded to reduce reactive route discovery.
  - When mobility is high, zones are contracted to limit frequent updates.
- Advantages:
  - Balances proactive overhead and reactive latency.

    - Enhances adaptability to dynamic topologies.
    - Improves packet delivery and reduces control message flooding.
- Example: In vehicular ad hoc networks (VANETs), adaptive zone radius tuning helps maintain stable routing during varying vehicle speeds and densities.

5.6.2 Cross-Layer and AI/ML-Based Hybrid Optimization

Traditional hybrid routing protocols often operate independently of other layers in the network stack, which can lead to suboptimal decisions. Cross-layer optimization and AI/ML-driven routing intelligence address this gap.

- Cross-Layer Design:
    - Integrates physical, MAC, and network layer information (e.g., signal strength, link stability, queue length) to make more informed routing decisions.
    - Enables route selection based on both link quality and traffic conditions, not just hop count.
    - Improves throughput and energy efficiency under fluctuating network conditions.
- AI/ML Techniques:
    - Reinforcement Learning (RL): Enables nodes to learn optimal routing policies dynamically by rewarding stable and energy-efficient paths.
    - Neural Networks & Decision Trees: Predict link failures and node mobility to proactively adjust routing strategies.
    - Clustering Algorithms (e.g., K-Means): Support adaptive zone formation and resource allocation.
- Outcomes:
    - Reduces routing overhead and packet loss.
    - Improves adaptability to unpredictable topology changes.
    - Enables predictive and autonomous route management.

5.6.3 Energy-Aware and Congestion-Controlled Hybrid Routing

Energy efficiency remains a critical challenge in mobile ad hoc networks (MANETs), sensor networks, and UAV systems. Hybrid protocols can integrate energy-aware and congestion-control techniques to ensure network longevity and balanced load distribution.

- Energy-Aware Mechanisms:
    - Nodes monitor their residual energy and participate in routing based on energy thresholds.
    - Routing algorithms prioritize nodes with higher energy reserves to prevent early depletion of critical nodes.
    - Techniques such as multi-path routing and load distribution reduce the energy burden on any single node.
- Congestion Control:

  - Dynamic route switching based on buffer occupancy or packet delay metrics.
  - Integration with traffic-aware MAC protocols to prevent bottlenecks.
  - Use of feedback-based control loops to detect congestion early and reroute traffic accordingly.
- Benefits:
  - Prolonged network lifetime.
  - Stable data transmission under high traffic load.
  - Reduced packet loss due to adaptive congestion avoidance.

5.6.4 Integration with SDN and Edge Computing for Adaptive Control

Emerging paradigms such as Software-Defined Networking (SDN) and Edge Computing are transforming how hybrid routing protocols can be managed and optimized.

- SDN-Based Hybrid Routing:
  - SDN introduces a centralized or semi-centralized control plane that can oversee distributed MANET operations.
  - Controllers collect network state data and dynamically adjust hybrid routing parameters (e.g., zone radius, route selection policies).
  - Enables global optimization while maintaining local autonomy.
- Edge Computing Integration:
  - Edge nodes perform localized computation and caching to assist in real-time route management.
  - Facilitates faster decision-making, reduces latency, and offloads computation from resource-limited mobile nodes.
  - Particularly useful in IoT environments, vehicular networks, and UAV clusters.
- Advantages:
  - Enhanced global visibility and network coordination.
  - Reduced routing delay through edge-assisted route computation.
  - Greater scalability and interoperability with modern network architectures.

Optimization and enhancement techniques transform hybrid routing protocols from static designs into adaptive, intelligent, and efficient systems.
Key takeaways include:

Dynamic zone resizing enables real-time adaptation to topology changes.

- Cross-layer design and AI/ML integration empower predictive and context-aware routing.
- Energy and congestion management ensure sustainability and reliability in dense networks.

- SDN and edge computing integration bring centralized intelligence and scalability to decentralized MANETs.

These advancements position hybrid routing protocols as essential enablers for next-generation mobile networks, ensuring seamless communication in heterogeneous, high-mobility, and energy-sensitive environments.

5.7 Security Considerations in Hybrid Routing

Hybrid routing protocols, while offering a balanced approach between proactive and reactive routing, remain vulnerable to various security threats due to the decentralized and dynamic nature of ad hoc wireless networks. Ensuring secure and trustworthy communication is critical, especially in applications such as military operations, emergency response, and vehicular networks, where data integrity and availability are paramount. This section explores the major threats faced by hybrid routing protocols, the design of secure hybrid frameworks, and the trade-offs between security, efficiency, and scalability.

5.7.1 Potential Threats in Hybrid Routing

Hybrid routing protocols, by combining proactive and reactive mechanisms, inherit vulnerabilities from both paradigms. Key security threats include:

- **Spoofing Attacks:** Malicious nodes impersonate legitimate ones by falsifying their network identities or IP addresses. This can lead to false routing updates, traffic misdirection, or network partitioning.
- **Blackhole Attacks: A** malicious node advertises itself as having the shortest or best route to a destination. Once data packets are routed through it, the attacker drops or modifies them, leading to severe packet loss.
- **Wormhole Attacks:** Two colluding nodes create a low-latency tunnel between distant points in the network. This tunnel distorts routing information, misguiding nodes to choose non-optimal or malicious paths.
- **Denial of Service (DoS) Attacks:** Attackers flood the network with excessive route requests or control messages, overwhelming routing tables and consuming bandwidth and energy resources. In hybrid protocols, such attacks can disrupt both intra-zone proactive updates and inter-zone reactive discoveries, causing widespread instability.
- **Routing Table Poisoning:** Malicious nodes inject false route information into proactive routing zones, corrupting the routing tables of nearby nodes and leading to incorrect path selections.

These threats not only degrade performance but also compromise confidentiality, integrity, and availability—the core pillars of network security.

5.7.2 Secure Hybrid Routing Frameworks

To counteract these challenges, researchers have proposed secure hybrid routing protocols that integrate authentication, trust management, and cryptographic mechanisms.

- **Secure Zone Routing Protocol (SZRP):** An enhanced version of ZRP that employs cryptographic authentication for both intra-zone and inter-zone communications.
    - Uses digital signatures or hash-based message authentication codes (HMACs) to verify the integrity of route requests (RREQ) and replies (RREP).
    - Prevents spoofing and tampering of control messages.
    - Limits participation of untrusted nodes through a local trust evaluation mechanism.
- **Hybrid Trust-Based Routing Models:** These frameworks use trust scores to evaluate the reliability of neighboring nodes.
    - Nodes monitor packet forwarding behavior and assign reputation values.
    - High-trust nodes are preferred during route formation, minimizing the risk of routing through malicious entities.
    - Can be combined with blockchain-based authentication for immutable trust record maintenance.
- **Lightweight Secure Hybrid Protocols**: Designed for resource-constrained environments such as IoT or sensor networks.
    - Employ symmetric key cryptography and energy-efficient encryption algorithms to reduce computational burden.
    - Integrate with AI-driven intrusion detection systems (IDS) for anomaly recognition and automated mitigation.

Example – Secure SHARP Variants: Enhanced versions of SHARP (Scalable Hybrid Adaptive Routing Protocol) incorporate dynamic key exchange and QoS-aware secure routing, ensuring robust communication under varying network loads and attack intensities.

5.7.3 Balancing Security with Efficiency and Scalability

While strong security mechanisms are essential, they must be balanced with the performance needs of hybrid networks, which often operate under limited bandwidth, energy, and processing power. The key challenge lies in achieving this security-performance equilibrium.

- **Efficiency Considerations:**
    - Excessive cryptographic operations increase control overhead and routing delay.
    - Secure frameworks must use lightweight authentication methods such as elliptic curve cryptography (ECC) or identity-based cryptosystems.

    - Selective security application—e.g., encrypting only inter-zone communications—can minimize computational load.
- **Scalability Factors:**
    - As network size increases, maintaining global trust records or frequent key exchanges becomes expensive.
    - Cluster-based security management and distributed key distribution can ensure scalable operation.
    - Integration with edge computing allows offloading of complex security computations to nearby edge nodes, maintaining performance for end devices.
- **Adaptability and Autonomy:**
    - Secure hybrid protocols should adapt dynamically to network conditions—activating higher security levels only under attack detection.
    - Machine learning-based adaptive security models can identify attack patterns and automatically adjust security intensity.

Security remains a pivotal factor in the reliability and adoption of hybrid routing protocols. Major takeaways include:

- Hybrid networks face combined threats from both proactive and reactive domains, including spoofing, blackhole, and wormhole attacks.
- Frameworks such as SZRP and trust-based hybrid models integrate authentication, encryption, and trust evaluation to enhance resilience.
- The future of secure hybrid routing lies in adaptive, intelligent, and lightweight mechanisms that harmonize security with energy efficiency and scalability.

As hybrid routing continues to underpin advanced communication systems—from vehicular networks to autonomous UAV swarms—embedding robust yet efficient security frameworks will be fundamental to sustaining trustworthy and high-performance network operations.

5.8 Applications of Hybrid Routing Protocols

Hybrid routing protocols play a crucial role in modern wireless communication systems by providing a balanced approach between proactive and reactive routing mechanisms. This adaptability makes them suitable for a wide range of applications that require both efficient local communication and on-demand global connectivity. The following sections discuss major domains where hybrid routing protocols have demonstrated significant utility.

5.8.1 Smart City and IoT Ecosystems

In smart cities and large-scale Internet of Things (IoT) deployments, numerous interconnected devices—such as sensors, actuators, and controllers—exchange data to support applications like traffic management, environmental monitoring, and energy

optimization. Hybrid routing protocols are ideal for these networks because they efficiently handle dense local communication and sporadic long-distance data transmission.

- Advantages:
  - Proactive intra-zone routing ensures continuous communication among nearby IoT nodes with minimal delay.
  - Reactive inter-zone routing reduces control overhead by initiating route discovery only when distant communication is needed.
  - Dynamic adaptability allows routing to adjust to changing network loads and topology variations.
- Examples:
  - ZRP-based IoT frameworks have been implemented in smart lighting systems, where nodes maintain local routes for nearby lamps while discovering remote paths only when required.
  - In environmental sensor networks, hybrid routing enhances energy efficiency and scalability, enabling real-time data collection over large geographic areas.

5.8.2 Military and Tactical Networks

Military and tactical communication systems demand reliable, secure, and delay-tolerant routing mechanisms in highly dynamic and infrastructure-less environments. Hybrid routing protocols address these needs effectively by providing robust connectivity and resilience under mobility.

- Advantages:
  - Zone-based design supports localized, proactive communication within platoons or teams, while inter-unit communication occurs reactively to save bandwidth.
  - Fast route recovery mechanisms ensure communication continuity during movement or combat operations.
  - Integration with secure hybrid routing frameworks (e.g., Secure Zone Routing Protocol, SZRP) enhances protection against interception and spoofing attacks.
- Applications:
  - Battlefield networks, where soldiers and vehicles communicate autonomously using hybrid MANET structures.
  - Disaster relief and emergency military operations, enabling coordination among drones, ground units, and command centers even without pre-existing infrastructure.

5.8.3 Vehicular Ad Hoc Networks (VANETs)

In vehicular networks, hybrid routing protocols are particularly effective in balancing low-latency local communication (among nearby vehicles) and on-demand long-distance routing (to remote nodes or infrastructure). Given the high mobility and dynamic topology of VANETs, a purely proactive or reactive approach alone is often insufficient.

- Advantages:
  - Proactive routing enables real-time data sharing among vehicles within the same zone (e.g., for collision avoidance or traffic signaling).
  - Reactive routing supports long-range information dissemination (e.g., road condition updates or emergency messages).
  - Scalability and adaptability allow hybrid protocols to handle fluctuating vehicle densities in urban and highway environments.
- Use Cases:
  - Smart traffic management systems, where hybrid routing aids in adaptive routing of data between vehicles and roadside units (RSUs).
  - Autonomous vehicle coordination, ensuring robust communication during high-speed movements and dynamic clustering scenarios.

5.8.4 UAV Swarms and Heterogeneous Wireless Networks

Hybrid routing is also highly applicable in Unmanned Aerial Vehicle (UAV) swarms and heterogeneous wireless systems that combine various communication technologies such as Wi-Fi, LTE, and satellite links. These environments require protocols capable of maintaining real-time coordination while adapting to frequent topology changes.

- Advantages:
  - Proactive intra-swarm routing ensures continuous and low-latency communication between nearby UAVs during missions.
  - Reactive inter-swarm routing activates when UAVs need to communicate with distant ground stations or other networks.
  - Dynamic zone resizing allows the routing system to adjust to UAV density and mobility, optimizing performance and energy usage.
- Applications:
  - Search and rescue missions, where UAVs form dynamic communication zones for coordination and data relay.
  - Agricultural and environmental monitoring, leveraging hybrid routing for distributed data collection and real-time control.
  - Heterogeneous network integration, where hybrid routing connects UAVs, terrestrial nodes, and satellite systems to form a unified communication architecture.

Hybrid routing protocols have become a cornerstone of next-generation wireless networks, bridging the gap between proactive stability and reactive flexibility. Their adaptive and

scalable nature enables seamless operation in diverse domains—ranging from smart city IoT ecosystems and military communications to vehicular networks and UAV swarms. By intelligently balancing control overhead, delay, and energy consumption, these protocols ensure reliable connectivity in dynamic, large-scale, and mission-critical environments. As emerging technologies such as 5G/6G, AI-driven networking, and edge computing continue to evolve, hybrid routing protocols are expected to play an even more central role in building intelligent, autonomous, and resilient communication infrastructures.

5.9 Future Trends and Research Directions

As wireless communication systems evolve toward greater intelligence, scalability, and energy efficiency, hybrid routing protocols are expected to play a central role in next-generation ad hoc networks. Their ability to dynamically balance proactive and reactive routing makes them adaptable to complex and heterogeneous communication environments. The following emerging trends and research directions outline how hybrid routing is being enhanced to meet future networking challenges.

5.9.1 AI-Driven Self-Learning Hybrid Routing Mechanisms

Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing hybrid routing by enabling self-learning and context-aware decision-making. Traditional routing protocols rely on static thresholds or pre-defined configurations, which may not perform optimally under varying network conditions. AI-driven hybrid routing introduces adaptive intelligence that allows protocols to learn from network behavior and adjust routing parameters in real time.

- Approaches:
  - Reinforcement Learning (RL): Enables nodes to learn optimal routing strategies through feedback mechanisms based on delay, energy, and link quality.
  - Deep Learning Models: Used for predicting node mobility, link stability, and congestion to improve zone radius selection and routing decisions.
  - Federated Learning: Allows distributed AI training across nodes while preserving data privacy, enhancing scalability and robustness.
- Benefits:
  - Improved adaptability to changing mobility and topology conditions.
  - Reduced control overhead through intelligent route prediction.
  - Enhanced network lifetime via optimized energy utilization.

5.9.2 Integration with 5G/6G and Satellite Communication Systems

The convergence of ad hoc networks with 5G, 6G, and satellite systems represents a significant step toward building global, seamless, and high-performance communication

architectures. Hybrid routing protocols will be instrumental in managing communication between terrestrial, aerial, and space-based nodes.

- Key Trends:
  - 5G/6G Edge Integration: Hybrid routing will leverage Multi-Access Edge Computing (MEC) for offloading computation and improving real-time performance in dense IoT or vehicular networks.
  - Non-Terrestrial Networks (NTNs): The integration of Low Earth Orbit (LEO) satellites with MANETs and UAV swarms will extend connectivity to remote and disaster-prone regions.
  - Network Slicing and QoS-Aware Hybrid Routing: 6G architectures will enable dynamic routing decisions based on service types, latency requirements, and energy constraints.
- Outcomes:
  - Global connectivity with consistent quality of service (QoS).
  - Reduced latency and energy consumption through intelligent multi-domain routing.
  - Enhanced resilience for critical applications like emergency response and defense communications.

5.9.3 Energy Harvesting and Green Routing Adaptations

As energy efficiency becomes a major concern in large-scale and resource-constrained networks, energy harvesting and green routing techniques are gaining traction in hybrid routing research. Future hybrid protocols will integrate energy-awareness and harvesting mechanisms to extend network longevity without compromising performance.

- Research Directions:
  - Solar, wind, and kinetic energy harvesting nodes that adapt routing decisions based on available energy reserves.
  - Energy-aware zone resizing, allowing low-power nodes to reduce proactive participation while maintaining connectivity through reactive means.
  - Eco-routing frameworks that minimize control packet transmissions and idle listening to reduce carbon footprint and battery consumption.
- Expected Benefits:
  - Prolonged network lifetime and reduced maintenance costs.
  - Sustainable operation in remote, off-grid, or battlefield environments.
  - Alignment with global green communication initiatives.

5.9.4 Hybrid Protocols for Multi-Layer and Multi-Domain Ad Hoc Environments

Future networks will operate across multiple layers and domains, involving terrestrial, aerial, maritime, and space components. Hybrid routing protocols must evolve to manage communication across heterogeneous domains while maintaining consistency, reliability, and scalability.

- Trends:
    - Multi-Layer Integration: Seamless coordination among UAVs, ground vehicles, underwater sensors, and satellites through hierarchical hybrid routing.
    - Cognitive and Context-Aware Protocols: Utilizing environmental and situational awareness (e.g., node density, channel quality) to dynamically adjust routing strategies.
    - Software-Defined Networking (SDN) and Network Function Virtualization (NFV): Centralized control planes managing distributed hybrid routing for improved global optimization.
- Potential Applications:
    - Smart transportation systems combining terrestrial VANETs and aerial FANETs.
    - Disaster recovery architectures integrating ground, air, and satellite layers.
    - Autonomous maritime and space exploration networks.

The future of hybrid routing protocols lies in intelligence, integration, and sustainability. By incorporating AI-driven self-learning mechanisms, 5G/6G and satellite integration, energy-aware adaptations, and multi-domain interoperability, hybrid routing will become the backbone of next-generation ubiquitous communication systems. These advancements will enable networks that are not only self-organizing and resilient but also capable of real-time adaptation to complex and heterogeneous operating environments, setting the stage for fully autonomous, scalable, and green wireless ecosystems.

5.10 Conclusion

Hybrid routing protocols represent a balanced evolution of ad hoc network routing strategies, merging the proactive and reactive paradigms to achieve optimized performance in dynamic and large-scale environments. This chapter provided a comprehensive overview of the principles, architectures, and advancements that define hybrid routing in Mobile Ad Hoc Networks (MANETs) and their extensions into heterogeneous systems.

Hybrid routing protocols combine the strengths of proactive routing—which ensures immediate route availability within localized zones—with the reactive approach, which discovers routes on-demand beyond those zones. This dual strategy reduces control overhead while maintaining low latency and scalability. Key hybrid protocols such as Zone Routing Protocol (ZRP), Zone-Based Hierarchical Link State (ZHLS), and Sharp Hybrid Adaptive Routing Protocol (SHARP) demonstrate how adaptive zone formation and hierarchical control can enhance performance in dynamic topologies. These protocols were analyzed in terms of design structure, routing process, and adaptability under varying network densities and mobility levels.

When compared to purely proactive or reactive routing mechanisms, hybrid routing protocols offer a scalable and adaptive compromise.

- Proactive protocols maintain continuous route tables but suffer from high control overhead in large networks.
- Reactive protocols minimize control load but introduce delays during route discovery.

  Hybrid routing effectively merges these advantages by limiting proactive operations to local zones while using reactive discovery for distant nodes, thereby achieving balance between responsiveness and efficiency. Performance evaluations have shown that hybrid approaches outperform traditional models in scenarios with moderate to high node mobility and variable density distributions.

A recurring theme across hybrid routing research is the emphasis on scalability and adaptability. Dynamic zone resizing, AI/ML-based optimization, and energy-aware routing mechanisms enable hybrid protocols to efficiently manage complex and evolving topologies. Additionally, security considerations such as trust-based frameworks and secure hybrid models (e.g., SZRP) address common vulnerabilities like spoofing and blackhole attacks. These innovations ensure that hybrid routing remains robust, secure, and efficient, even in mission-critical and high-mobility applications like UAV networks, smart cities, and military operations.

References

1. Haas, Z. J., & Pearlman, M. R. (2001). The Zone Routing Protocol (ZRP) for Ad Hoc Networks. *Internet Draft, IETF MANET Working Group.*
2. Haas, Z. J., Pearlman, M. R., & Samar, P. (2002). The Zone Routing Protocol (ZRP) for Ad Hoc Networks. *IETF Internet Draft*, draft-ietf-manet-zone-zrp-04.
3. Pearlman, M. R., & Haas, Z. J. (1999). Determining the optimal configuration for the Zone Routing Protocol. *IEEE Journal on Selected Areas in Communications, 17*(8), 1395–1414.
4. Joa-Ng, M., & Lu, I.-T. (1999). A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications, 17*(8), 1415–1425.
5. Jiang, M., Li, J., & Tay, Y. C. (1999). Cluster Based Routing Protocol (CBRP) Functional Specification. *IETF Internet Draft*.
6. Ahn, C. W., & Lee, H. (2003). An adaptive hybrid routing protocol considering node mobility for mobile ad hoc networks. *IEICE Transactions on Communications, E86-B*(10), 3103–3111.
7. Ramasubramanian, V., Haas, Z. J., & Sirer, E. G. (2003). SHARP: A hybrid adaptive routing protocol for mobile ad hoc networks. *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'03)*, 303–314.

8. Wang, J., Chen, J., & Niu, Y. (2016). A hybrid routing algorithm based on zone routing and clustering for MANET. *International Journal of Distributed Sensor Networks, 12*(5), 1–11.
9. Al-Gabri, M., & Abdullah, A. H. (2013). Hybrid routing protocols for mobile ad hoc networks: A comparative study. *Journal of Theoretical and Applied Information Technology, 48*(1), 1–8.
10. Perkins, C. E., & Royer, E. M. (1999). Ad hoc On-Demand Distance Vector (AODV) Routing. *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 90–100.
11. Johnson, D. B., Maltz, D. A., & Hu, Y. C. (2004). The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. *RFC 4728, IETF MANET Working Group.*
12. Marina, M. K., & Das, S. R. (2002). On-demand multipath distance vector routing in ad hoc networks. *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, 14–23.
13. Li, H., & Zhang, Z. (2018). Machine learning-based adaptive hybrid routing protocol for MANETs. *Wireless Networks, 24*(8), 2879–2891.
14. Gupta, S., & Misra, S. (2017). Energy-efficient hybrid routing in mobile ad hoc networks: A distributed learning approach. *Ad Hoc Networks, 63*, 24–35.
15. Sharma, P., & Ghose, M. K. (2015). Hybrid routing scheme for energy-efficient and scalable MANETs. *International Journal of Computer Networks and Communications, 7*(2), 35–49.
16. Niyogi, S., & Panda, M. (2020). Secure hybrid routing protocol for MANETs using trust and cryptography. *International Journal of Information Security Science, 9*(3), 48–59.
17. Singh, R., & Chauhan, D. S. (2019). A review of hybrid routing protocols in mobile ad hoc networks. *Wireless Personal Communications, 108*(1), 345–369.
18. Zhu, Y., Lin, C., & Li, Y. (2021). AI-assisted adaptive routing for next-generation ad hoc and vehicular networks. *IEEE Access, 9*, 43788–43800.
19. Kumar, N., & Misra, S. (2022). Hybrid routing and resource optimization in 5G-based ad hoc networks. *IEEE Transactions on Network and Service Management, 19*(2), 221–232.
20. Chhabra, S., & Singh, G. (2023). Edge-enabled hybrid routing for IoT and UAV networks. *Computer Networks, 229*, 109751.

Chapter-6
Geographic and Location-Aided Routing Techniques

P.Balamurugan

Assistant Professor,
Department of Computer Applications,
K.S.Rangasamy College of Arts and Science(Autonomous),
Tiruchengode,Tamilnadu,India.

Abstract: *Geographic and Location-Aided Routing (LAR) techniques represent a vital advancement in the design of efficient communication protocols for mobile ad hoc networks (MANETs), wireless sensor networks (WSNs), and vehicular ad hoc networks (VANETs). Unlike traditional topology-based routing schemes, geographic routing leverages the physical positions of nodes—obtained through GPS or other localization systems—to make intelligent forwarding decisions. This position-aware approach significantly reduces routing overhead, improves scalability, and enhances adaptability in highly dynamic network environments. This chapter explores the fundamental concepts, architectures, and classifications of geographic routing protocols, emphasizing greedy forwarding and location-aided mechanisms. Detailed discussions on key protocols such as GPSR, LAR, DREAM, and GeoTORA illustrate how geographic information enhances performance in terms of efficiency, energy conservation, and delivery reliability. The chapter further examines location service management, security and privacy challenges, and performance evaluation metrics. Finally, it highlights emerging trends such as AI-driven mobility prediction, 3D geographic routing, and blockchain-assisted location verification, offering a forward-looking perspective on the evolution of location-based communication paradigms.*

Keywords: *Geographic Routing; Location-Aided Routing (LAR); Greedy Forwarding; GPSR; DREAM; GeoTORA; MANET; WSN; VANET; Location Services; Mobility Prediction; Energy Efficiency; QoS; Privacy-Preserving Routing; Position-Based Forwarding; Hybrid Routing; Edge Computing; Secure Localization; Geographic Information Systems (GIS); Blockchain-Assisted Routing.*

6.1 Introduction

In mobile ad hoc networks (MANETs), routing plays a crucial role in determining how data packets are transmitted across dynamically changing network topologies. Traditional routing protocols rely heavily on maintaining topological information through periodic control messages and route discovery mechanisms. However, as the number of nodes increases and node mobility becomes more unpredictable, these topology-based approaches face challenges in scalability, latency, and routing overhead. To address these issues, Geographic and Location-Aided Routing (LAR) techniques have emerged as a promising alternative, leveraging the physical position of nodes to optimize route selection and data forwarding.

Overview of Geographic Routing Principles

Geographic routing, also referred to as position-based routing, uses the geographical coordinates of nodes to guide the forwarding process. Each node determines its own position using a localization system such as Global Positioning System (GPS), Received Signal Strength Indicator (RSSI), or other sensor-based localization techniques. Instead of relying on established end-to-end paths, packets are forwarded toward the destination based on its last known location. Intermediate nodes use the positional information of their neighbors to make localized, stateless forwarding decisions, minimizing the need for maintaining complex routing tables. This spatially aware routing reduces communication overhead and improves scalability, particularly in large and highly mobile networks.

Importance of Location Awareness in Ad Hoc Networks

Location awareness introduces a spatial dimension to routing decisions, enabling more efficient utilization of network resources. By knowing the position of nodes, a routing protocol can determine the most suitable next-hop that brings the packet closer to its destination, avoiding unnecessary flooding or redundant transmissions. This approach significantly reduces control message exchange and improves energy efficiency, which is critical in resource-constrained networks such as WSNs and IoT environments. Furthermore, location information supports context-aware services, such as geofencing, spatial clustering, and mobility prediction, which enhance routing accuracy and reliability. In vehicular ad hoc networks (VANETs), for instance, position-based routing allows for real-time data dissemination along predictable road topologies.

Comparison with Topology-Based Routing Approaches

Unlike topology-based protocols—which depend on link-state or distance-vector information—geographic routing does not require maintaining complete network topology or path information. Traditional proactive protocols (e.g., OLSR, DSDV) maintain continuous route updates, leading to high control overhead, while reactive protocols (e.g., AODV, DSR) initiate route discovery only when needed, often causing initial latency. Geographic routing, in contrast, eliminates the need for route discovery phases by using instantaneous positional knowledge, thus achieving lower latency and faster adaptation to node mobility. However, its performance heavily depends on accurate and timely location information. Position errors or localization inaccuracies can degrade routing efficiency, leading to suboptimal path selection or packet loss.

Motivation for Using Position Information in Routing Decisions

The motivation behind integrating geographic information into routing lies in achieving high scalability, reduced overhead, and improved robustness in dynamic networks. By making forwarding decisions locally and independently, geographic routing protocols minimize dependency on global network knowledge. They inherently adapt to topological changes caused by node mobility without requiring costly route rediscovery procedures. Moreover, position-based routing is particularly effective in dense or large-scale networks, where maintaining complete topology information becomes impractical. As networks evolve

toward supporting autonomous systems, unmanned aerial vehicles (UAVs), and Internet of Things (IoT) applications, the ability to make intelligent, context-aware routing decisions based on spatial data becomes increasingly essential.

6.2 Fundamentals of Geographic and Location-Aided Routing

Geographic and Location-Aided Routing (LAR) techniques operate on the fundamental concept of utilizing positional information of nodes to guide packet forwarding decisions. Unlike traditional routing approaches that depend on the maintenance of routing tables and network topology, geographic routing mechanisms leverage spatial coordinates of nodes—either absolute (such as GPS-based) or relative (computed using local measurements)—to determine the most efficient path toward the destination. This paradigm enhances scalability, reduces control overhead, and improves performance in dynamic or large-scale ad hoc networks such as MANETs, VANETs, and WSNs.

Concept of Geographic Routing

At its core, geographic routing (also known as position-based routing) assumes that each node in the network is aware of its own geographic position and that of its immediate neighbors. The destination node's location is typically obtained through a location service that provides either the exact or last known coordinates of the node. When a source node wishes to send data, it attaches the destination's geographic coordinates to the packet header. Intermediate nodes forward the packet to the neighbor that is geographically closer to the destination, following a greedy forwarding strategy (Figure 1).

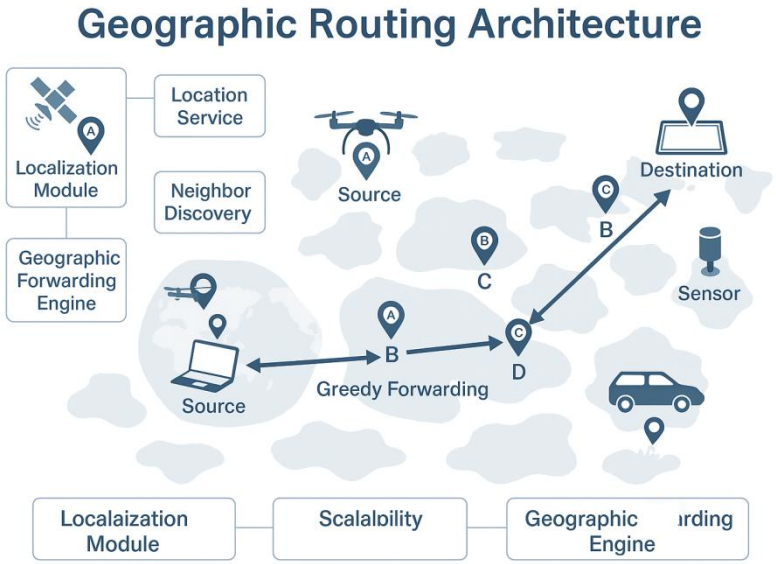


Figure 1: Geographic Routing Architecture and Greedy Forwarding in Ad Hoc Networks

If a local minimum is encountered—where no neighbor is closer to the destination—the protocol may switch to an alternative recovery mode, such as perimeter routing or face traversal. By making forwarding decisions based solely on local information, geographic routing avoids the need for route establishment and maintenance, offering high adaptability in environments with frequent topological changes.

Role of GPS and Other Positioning Systems

The accuracy of geographic routing largely depends on the underlying positioning technology used to determine node locations. The Global Positioning System (GPS) is the most widely used method for obtaining precise spatial coordinates, providing global coverage and high positional accuracy. However, GPS may not function effectively in indoor, underwater, or obstructed environments, where alternative localization methods become necessary.

Other techniques include:

- Received Signal Strength Indicator (RSSI): Estimates distance based on signal attenuation.
- Angle of Arrival (AoA): Determines position by measuring the angle at which signals are received.
- Time of Arrival (ToA) and Time Difference of Arrival (TDoA): Calculate location based on propagation time of signals.
- Hybrid Localization Systems: Combine GPS with inertial sensors, Wi-Fi triangulation, or Bluetooth beacons for improved accuracy.

The integration of such systems ensures that nodes maintain accurate and timely location data, which is crucial for reliable geographic routing decisions.

Location Information Dissemination Techniques

Efficient dissemination of location information is critical to ensure that nodes possess up-to-date positional data about their neighbors and destinations. Location dissemination techniques can be categorized as follows:

- **Periodic Broadcasting:** Nodes periodically exchange "hello" messages containing their current coordinates. While simple, this method may consume considerable bandwidth and energy in dense networks.
- **Event-Driven Updates:** Nodes transmit location updates only when significant movement or positional change is detected, optimizing energy efficiency.
- **Hierarchical Dissemination:** In large-scale networks, nodes are grouped into clusters or grids, and location information is distributed through a hierarchical structure to reduce flooding overhead.
- **Query-Based Dissemination:** A source node queries specific location servers or directories to obtain the destination's current or last known position before initiating communication.

Effective dissemination ensures routing accuracy, minimizes stale information, and enhances protocol scalability.

Position-Based Forwarding vs. Topology-Based Forwarding

Position-based forwarding fundamentally differs from topology-based forwarding in how routing decisions are made and maintained.

Aspect	Position-Based Forwarding	Topology-Based Forwarding
Routing Basis	Geographic coordinates of nodes	Network topology and link states
Route Discovery	Not required; forwarding is local	Required (proactive or reactive)
State Maintenance	Stateless or localized	Requires global or partial topology state
Adaptability	High, due to dynamic local decisions	Limited in high-mobility networks
Overhead	Low control message overhead	Higher due to periodic updates
Scalability	Highly scalable for large networks	Degrades as network size increases

Position-based routing offers superior scalability and adaptability, especially in networks with frequent topology changes. However, it depends heavily on accurate and timely location data; inaccuracies in position estimation can lead to packet misdirection or delivery failure.

Metrics: Distance, Direction, and Geographic Proximity

Geographic routing decisions rely on specific spatial metrics that guide packet forwarding:

- Distance Metric: Nodes calculate the Euclidean distance between themselves and the destination. The next hop is typically the neighbor closest to the destination, minimizing transmission hops.
- Direction (Angular) Metric: Some protocols select the next-hop node based on the smallest angular deviation from the line connecting the source and destination, optimizing directional consistency.
- Geographic Proximity Metric: Combines distance and direction parameters to select the node that ensures minimal transmission cost while maintaining progress toward the destination.
- Hybrid Metrics: In advanced routing schemes, additional factors such as residual energy, link reliability, or node density may be incorporated into the geographic decision process.

These metrics collectively ensure efficient and reliable forwarding by balancing path optimality, energy efficiency, and routing robustness.

In essence, the fundamentals of geographic and location-aided routing revolve around leveraging spatial information to enable decentralized, efficient, and scalable data delivery. Through accurate localization, effective information dissemination, and intelligent use of distance and direction metrics, these protocols overcome the limitations of traditional topology-based schemes and lay the foundation for advanced mobility-aware communication systems.

6.3 Architecture of Location-Aided Routing Systems

The architecture of a location-aided routing system is designed to efficiently utilize positional information to guide the process of data transmission in mobile ad hoc networks (MANETs), wireless sensor networks (WSNs), and vehicular networks (VANETs). Unlike

topology-based architectures that rely on maintaining global network knowledge, location-aided systems emphasize localized decision-making, allowing nodes to forward packets based on spatial and directional awareness. The architectural design typically consists of several core components—namely, the location service module, neighbor discovery mechanism, geographic forwarding engine, and location database management system—that work collaboratively to ensure efficient, adaptive, and scalable routing in highly dynamic environments.

Components of a Location-Aware Routing System

A location-aware routing system integrates multiple functional modules that collectively enable geographic routing decisions. These include:

1. Localization and Positioning Module: Determines the node's own geographic coordinates using GPS or alternative localization techniques.
2. Location Service Module: Manages the acquisition and dissemination of destination position information.
3. Neighbor Discovery Mechanism: Identifies and maintains an updated list of neighboring nodes within communication range.
4. Geographic Forwarding Engine: Selects the optimal next-hop node based on distance, direction, and proximity metrics.
5. Location Database and Maintenance Subsystem: Stores, updates, and validates positional data of nodes to ensure routing accuracy.
6. Security and Synchronization Layer: (optional) Ensures integrity, confidentiality, and temporal consistency of location information.

These interconnected components form the backbone of a reliable and efficient geographic routing architecture, allowing nodes to operate autonomously with minimal network overhead.

Location Service Module

The location service module plays a central role in enabling source nodes to obtain the geographic coordinates of destination nodes before initiating data transmission. It can be implemented as either a distributed or hierarchical service.

- In distributed location services (DLS), every node maintains partial information about other nodes and collaboratively responds to location queries.
- In hierarchical location services (HLS), the network area is divided into grids or zones, and higher-level nodes (cluster heads or servers) maintain the positional data for nodes within their region.

Some well-known mechanisms include the Grid Location Service (GLS), Hierarchical Location Service (HLS), and Quorum-based Location Service (QLS).

The efficiency of a location service depends on factors such as update frequency, query delay, storage overhead, and location accuracy. An optimal service minimizes control traffic while ensuring that nodes can retrieve accurate positional data even in rapidly changing network conditions.

ISBN: 978-93-47475-17-7

Neighbor Discovery Mechanism

The neighbor discovery mechanism allows each node to identify nearby nodes that lie within its transmission range. This process typically relies on periodic "hello" messages or beacon signals containing the node's current coordinates, ID, and timestamp.

Upon receiving these beacons, nodes update their neighbor tables, which serve as a local view of the network topology within proximity. Efficient neighbor discovery ensures that nodes possess accurate and timely information about potential next-hop candidates.

Several strategies exist to enhance the efficiency of this module:

- Adaptive Beaconing: Adjusts the beaconing rate based on node mobility or network density.
- Passive Listening: Reduces overhead by inferring neighbor presence from data packet receptions rather than active beacons.
- Energy-Aware Discovery: Minimizes power consumption by controlling the frequency of beacon transmissions.

Accurate neighbor discovery is essential for maintaining robust connectivity and avoiding packet drops due to stale or outdated neighbor information.

Geographic Forwarding Engine

The geographic forwarding engine is the decision-making unit responsible for selecting the next-hop node to which a packet should be forwarded. This module employs various geometric and spatial algorithms to determine the most efficient route toward the destination.

Key forwarding strategies include:

- Greedy Forwarding: Chooses the neighbor closest to the destination's geographic position.
- Directional Forwarding: Selects the neighbor with the smallest angular deviation from the source-destination line.
- Perimeter or Face Routing: Used as a recovery mechanism when greedy forwarding fails (i.e., in local minima scenarios).

Advanced forwarding engines may integrate multi-metric decision models, considering factors such as residual energy, link stability, signal quality, or node velocity in addition to geographic distance. To further improve robustness, hybrid mechanisms may switch dynamically between greedy and recovery modes based on network conditions.

Location Database and Maintenance

A location database is a critical repository that stores both the node's own position and the location information of other nodes obtained through location services or neighbor discovery. The maintenance of this database involves periodic updates, synchronization, and validation to prevent the use of stale or incorrect location data.

Key functions include:

- Update Management: Refreshing entries when new positional data are received or when nodes move beyond predefined thresholds.
- Data Aging and Expiration: Removing outdated information after a specific time interval to maintain accuracy.

- Consistency Verification: Cross-verifying location data received from multiple sources to avoid duplication or malicious entries.

A well-designed location database ensures timely and accurate routing decisions, minimizing route errors and retransmissions.

Challenges in Dynamic Network Topologies

Implementing location-aided routing in highly dynamic and mobile networks introduces several challenges:

- Localization Errors: Inaccurate or delayed position estimates can lead to inefficient routing and packet loss.
- Frequent Topology Changes: High node mobility may cause rapid neighbor turnover, making it difficult to maintain accurate location data.
- Beacon Overhead: Periodic beaconing increases bandwidth consumption and energy usage, especially in dense networks.
- Scalability Constraints: In large-scale deployments, location service queries and updates can become bottlenecks if not efficiently managed.
- Security and Privacy Concerns: Location information may be susceptible to spoofing, tampering, or unauthorized tracking.
- Synchronization Issues: Time delays in acquiring or propagating location data can lead to inconsistency across nodes.

Addressing these challenges requires adaptive mechanisms that balance accuracy, scalability, and efficiency, ensuring reliable geographic routing even under high mobility and variable environmental conditions.

The architecture of a location-aided routing system integrates a cohesive set of modules that enable position-based decision-making while minimizing control overhead. Through effective cooperation between location services, neighbor discovery, and forwarding engines, these systems achieve scalable and efficient data dissemination. However, maintaining performance in dynamic, mobile, and error-prone environments remains a key research challenge, motivating the exploration of hybrid, AI-assisted, and energy-aware geographic routing architectures.

6.4 Geographic Routing Protocol Classifications

Geographic routing protocols can be categorized based on several design aspects, including their forwarding strategy, use of location information, and target network environment. Each classification highlights distinct operational philosophies and optimization goals, addressing challenges such as node mobility, energy constraints, and scalability. This section provides a structured overview of these classifications, emphasizing how different strategies utilize positional data to achieve efficient and adaptive communication.

6.4.1 Classification Based on Forwarding Strategy

The forwarding strategy determines how a node selects the next-hop for packet transmission using geographic information. The main categories include greedy forwarding protocols, restricted directional flooding, and hierarchical or cluster-based geographic routing.

(a) Greedy Forwarding Protocols

Greedy forwarding is the most fundamental and widely used geographic routing strategy. In this approach, each node forwards a packet to the neighbor that is geographically closest to the destination, thus minimizing the remaining distance with every hop.

- Working Principle:
  Each node uses local neighbor position data to select the next-hop node with minimum Euclidean distance to the destination. If no neighbor is closer than the current node, the protocol triggers a recovery mechanism (e.g., perimeter routing).
- Advantages:
  - Stateless routing; minimal control overhead
  - Scalable and suitable for dense networks
  - Fast packet forwarding with reduced delay
- Limitations:
  - May fail in local minima scenarios (dead ends)
  - Performance degrades with inaccurate position data
- Representative Protocols:
  - Greedy Perimeter Stateless Routing (GPSR)
  - Most Forward within Radius (MFR)
  - Compass Routing (DIR)
  - Greedy Other Adaptive Face Routing (GOAFR)

Greedy forwarding is efficient for networks where node density is sufficient to maintain continuous connectivity between the source and destination.

(b) Restricted Directional Flooding (RDF)

In restricted directional flooding, packets are forwarded within a confined directional region toward the destination, rather than to all neighbors. This controlled broadcasting approach ensures that data dissemination is focused on the likely path to the target, reducing network overhead.

- Working Principle: The source defines a forwarding zone based on geometric parameters such as angle, distance, or expected trajectory of the destination. Only nodes located within this zone are eligible to forward packets.
- Advantages:
  - Reduces flooding overhead compared to blind broadcasting
  - Enhances reliability in sparse networks where greedy forwarding may fail
  - Provides robustness against node failures and mobility
- Limitations:
  - Increased latency due to multi-path propagation
  - Requires precise calculation of the forwarding region

- Representative Protocols:
    - Location-Aided Routing (LAR) Scheme 1 and 2
    - Directional Location-Aided Routing (DLAR)
    - Spatially Aware Packet Routing (SAPR)

Restricted directional flooding is particularly effective in high-mobility or sparse environments, such as vehicular and UAV networks, where maintaining continuous neighbor connectivity is difficult.

(c) Hierarchical and Cluster-Based Geographic Routing

In hierarchical or cluster-based geographic routing, the network is divided into multiple zones, clusters, or grids, each managed by a local leader or cluster head responsible for intra- and inter-cluster communication.

- Working Principle: Nodes within a cluster communicate through their local cluster head, which maintains positional data and forwards packets to other clusters using geographic awareness.
- Advantages:
    - Improves scalability and reduces network congestion
    - Supports energy-efficient operation, suitable for large-scale WSNs
    - Enhances load balancing and localized fault tolerance
- Limitations:
    - Cluster head nodes may experience high energy consumption
    - Requires periodic re-clustering in dynamic environments
- Representative Protocols:
    - Zone-Based Hierarchical Link State (ZHLS)
    - Grid Location Service (GLS)
    - Hierarchical Geographic Multicast Routing (HGMR)
    - Cluster-Based Energy-Efficient Location Routing (CEELR)

Hierarchical geographic routing is widely adopted in sensor and IoT networks, where energy conservation and scalability are major design concerns.

6.4.2 Classification Based on Location Information Usage

Geographic routing protocols also differ based on how extensively they use location information in the routing process. Two main categories can be identified: fully location-based and partial or probabilistic location-based protocols.

(a) Fully Location-Based Protocols

In fully location-based routing, both the source node and all intermediate nodes use exact geographic coordinates for making forwarding decisions. Every node must possess accurate positional information of its neighbors and the destination.

- Characteristics:
    - Requires precise and frequent localization updates
    - Highly efficient in dense, stable networks with low localization error

- Advantages:
  - High packet delivery ratio
  - Minimal route discovery delay
  - Supports fast decision-making through local computation
- Limitations:
  - High dependency on GPS or localization systems
  - Sensitive to localization inaccuracies and synchronization delays
- Examples: GPSR, GOAFR, DREAM

(*b) Partial or Probabilistic Location-Based Protocols*

In contrast, partial or probabilistic location-based protocols use estimated or inferred positional information rather than exact coordinates. These schemes are designed to reduce overhead associated with continuous location updates, making them more energy-efficient and resilient to localization errors.

- Working Principle: Nodes estimate the probable region of the destination or use motion prediction models to infer its position. Forwarding decisions are made using probabilistic confidence levels rather than deterministic coordinates.
- Advantages:
  - Lower energy consumption
  - Tolerant to location inaccuracy
  - Reduced dependency on GPS and beacons
- Limitations:
  - Increased routing uncertainty
  - Potentially higher delay or suboptimal paths
- Examples:
  - Probabilistic Location-Aided Routing (PLAR)
  - Energy-Aware Probabilistic Geographic Routing (EAPGR)
  - Mobility Prediction-Based Geographic Routing (MPGR)

Such protocols are particularly useful in resource-constrained sensor networks and environments with limited localization infrastructure.

6.4.3 Classification Based on Network Type

Geographic routing strategies are often customized according to the specific characteristics of the underlying network.

The following categories reflect adaptations of geographic routing across different ad hoc and wireless environments.

(a) MANETs (Mobile Ad Hoc Networks)

In MANETs, nodes are mobile and operate without fixed infrastructure. Geographic routing protocols like GPSR, LAR, and DREAM are designed to handle frequent topology changes and mobility while maintaining scalability and low routing overhead.

- Key focus: Mobility adaptation and robustness
- Challenges: Location accuracy and beacon overhead

(b) VANETs (Vehicular Ad Hoc Networks)

In VANETs, vehicles act as nodes moving at high speeds along predictable paths (roads). Geographic routing leverages map-based and trajectory-aware forwarding to enhance communication reliability.

- Representative protocols: Geographic Source Routing (GSR), Greedy Perimeter Coordinator Routing (GPCR), GPSR+AGF
- Key focus: Real-time routing, delay minimization, and predictive mobility models

(c) WSNs (Wireless Sensor Networks)

In WSNs, nodes are energy-constrained and typically static or slowly moving. Geographic routing protocols in this domain focus on energy efficiency, load balancing, and localized data aggregation.

- Representative protocols: Geographic Adaptive Fidelity (GAF), Geographic Energy-Aware Routing (GEAR), Energy Efficient Geographic Routing (EEGR)
- Key focus: Minimizing energy consumption and extending network lifetime

(d) UAV Networks (Unmanned Aerial Vehicle Networks)

UAV networks consist of highly mobile nodes operating in three-dimensional (3D) space. Geographic routing in these networks must account for dynamic topology, altitude variation, and 3D spatial awareness.

- Representative protocols: 3D-GPSR, Aerial Position-Based Routing (APBR), GeoUAV-R
- Key focus: 3D mobility handling, adaptive link prediction, and latency reduction

Geographic routing protocols demonstrate remarkable diversity, evolving to address the specific demands of different environments and operational constraints. Whether based on greedy forwarding, directional flooding, or hierarchical organization, each classification reflects a unique balance between efficiency, reliability, and complexity. The choice of strategy depends largely on factors such as node density, localization accuracy, mobility patterns, and energy availability—making the classification of these protocols essential to understanding their design trade-offs and application suitability.

6.5 Greedy Forwarding Techniques

Geographic routing protocols often employ greedy forwarding as a fundamental mechanism to deliver packets toward the destination using minimal control overhead. Unlike traditional topology-based routing, greedy forwarding relies solely on positional information of the current node, its neighbors, and the destination to determine the next hop. This stateless and localized decision-making paradigm enables scalability, efficiency, and adaptability, especially in highly dynamic ad hoc environments such as MANETs, VANETs, and UAV networks.

6.5.1 Principle of Greedy Forwarding

The core principle of greedy forwarding is straightforward: each intermediate node forwards the packet to a neighbor that is geographically closer to the destination than itself. This process continues iteratively until the packet reaches the destination or a node where no closer neighbor exists (a condition known as a *local maximum*). The greedy strategy

assumes that progress can always be made based on location coordinates, without the need for maintaining end-to-end paths or routing tables.

In most implementations, nodes periodically exchange beacon messages containing their positions to build a local neighbor table. When a packet arrives, the node compares the positions of its neighbors and selects the one that maximizes geographic advancement toward the destination. This simple yet effective mechanism greatly reduces routing overhead, as route maintenance and discovery procedures are not required.

6.5.2 Next-Hop Selection Criteria

In greedy forwarding, the choice of the next-hop node is critical for ensuring both routing efficiency and reliability. Several selection criteria are employed depending on the network context and routing objective:

- Closest to Destination: The most common criterion, where the neighbor closest to the destination in Euclidean distance is selected. This approach guarantees the greatest immediate progress toward the target.
- Least Angular Deviation: Some protocols consider the *angular deviation* between the line connecting the current node to the destination and the line connecting the current node to each neighbor. The neighbor with the smallest deviation angle is chosen to maintain a direct trajectory toward the destination, reducing unnecessary detours.
- Most Forward within Radius (MFR): In this criterion, the neighbor located farthest along the direction of the destination within the transmission range is selected. It ensures maximum progress per hop and minimizes the total number of hops, improving energy efficiency.

These criteria can also be combined or adapted dynamically to suit specific network conditions, such as node density or mobility patterns.

6.5.3 Advantages and Limitations

Advantages:

- Low Overhead: Greedy forwarding does not require route discovery or maintenance, significantly reducing control message exchange.
- Scalability: The localized nature of decision-making allows it to scale efficiently in large or dense networks.
- Adaptability: It quickly adapts to changes in topology since each decision is made independently using current neighbor information.
- Energy Efficiency: Fewer control messages and shorter routing paths contribute to reduced power consumption.

Limitations:

- Local Maximum Problem: When a node cannot find any neighbor closer to the destination, the packet becomes “stuck.” This requires additional mechanisms like perimeter or face routing to recover.
- Dependence on Accurate Location Data: Position inaccuracies (due to GPS errors or localization delays) can lead to suboptimal routing or packet loss.
- Sparse Network Challenges: In networks with low node density, greedy forwarding may fail frequently due to the absence of suitable next-hop nodes.

6.5.4 Example Protocols

Several geographic routing protocols employ or extend greedy forwarding mechanisms to achieve optimal packet delivery performance:

- Greedy Perimeter Stateless Routing (GPSR): GPSR is one of the most widely recognized geographic routing protocols. It uses greedy forwarding as the primary mode of operation and switches to perimeter mode when encountering a local maximum. The protocol leverages planar graph traversal (using the right-hand rule) to route around voids and resume greedy forwarding once a closer node is found. GPSR's stateless nature and localized decision-making make it suitable for highly mobile environments like MANETs and VANETs.
- Greedy Other Adaptive Face Routing (GOAFR): GOAFR combines greedy forwarding with adaptive face routing to ensure delivery even in the presence of obstacles or voids. It dynamically adjusts the search area and balances between greedy advancement and route detouring, improving routing efficiency and delivery ratio. GOAFR is particularly effective in irregular or sparse topologies.
- Compass Routing and Most Forward within Radius (MFR): In Compass Routing, the node forwards the packet to the neighbor that makes the smallest angle with the direct line to the destination, optimizing trajectory precision. The MFR algorithm, on the other hand, selects the neighbor offering the maximum projected progress toward the destination within the transmission radius. Both methods aim to minimize route length while maintaining directional consistency.

Greedy forwarding remains a foundational approach in geographic routing due to its simplicity, scalability, and effectiveness in reducing routing overhead. However, its limitations in handling void regions and dependence on precise location information have led to the development of hybrid techniques such as perimeter, adaptive, and hierarchical routing, which extend greedy principles to improve reliability and robustness.

6.6 Location-Aided Routing (LAR) Protocols

The Location-Aided Routing (LAR) protocol represents a significant advancement in the design of efficient routing mechanisms for mobile ad hoc networks (MANETs). It utilizes location information obtained through systems such as the Global Positioning System (GPS) to limit the scope of route discovery processes, thereby reducing control overhead and improving scalability. By integrating spatial awareness into the routing process, LAR achieves a balance between proactive topology maintenance and reactive route discovery, minimizing unnecessary broadcasting and conserving network resources.

6.6.1 Concept and Working of LAR

Traditional on-demand routing protocols like AODV or DSR initiate network-wide flooding of route request (RREQ) messages during route discovery, which can lead to excessive bandwidth consumption and congestion, particularly in dense networks. The key innovation of LAR is the introduction of location awareness to confine the route request

propagation to a limited geographic region, rather than broadcasting across the entire network.

In LAR, when a source node needs to communicate with a destination, it estimates the possible location of the destination based on its last known coordinates and movement characteristics (e.g., velocity and direction). Using this estimate, the protocol defines two key regions—the expected zone and the request zone—to optimize the flooding process (Figure 2).

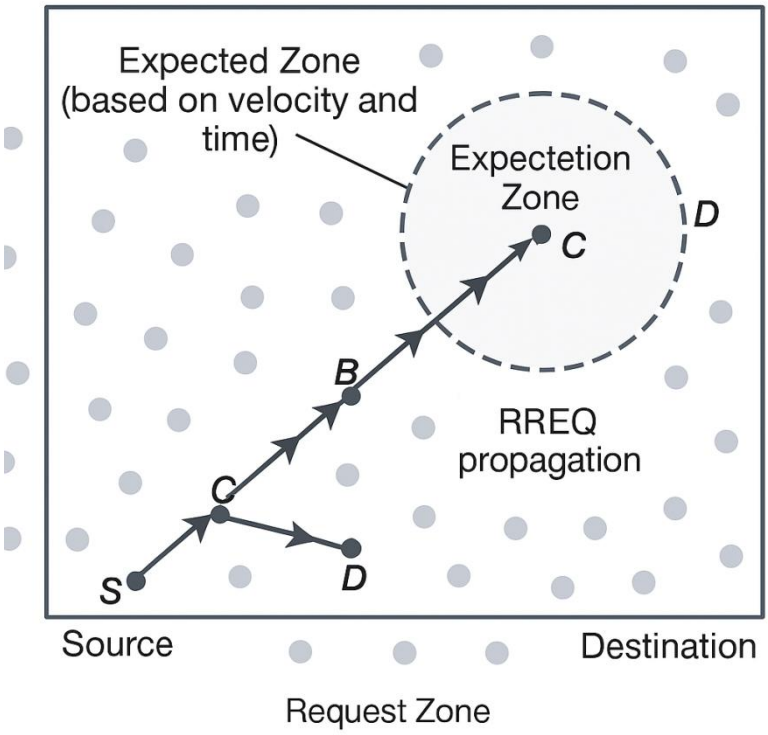


Figure 2: Expected Zone and Request Zone in Location-Aided Routing (LAR)

Packets are only forwarded by nodes that fall within the request zone, significantly reducing redundant transmissions and improving energy efficiency while maintaining high packet delivery ratios.

6.6.2 Expected Zone and Request Zone Mechanisms

- Expected Zone: The expected zone represents the region where the destination node is most likely to be located at the time of route discovery. It is calculated using the destination's last known position (xd,yd), the time elapsed since that position was recorded, and the node's estimated velocity v.
  The expected zone can be visualized as a circle centered at the last known position, with a radius proportional to v×Δt, where Δt is the time elapsed since the last update.
- Request Zone: To further restrict flooding, a request zone is defined as the smallest rectangle (or bounded area) that includes both the source node and the expected zone of the destination. Only nodes inside this request zone are allowed to forward the RREQ packets. Nodes outside this zone simply discard them.

This spatial limitation minimizes routing overhead while ensuring that the RREQ reaches the destination or nodes likely to have valid route information.

The combination of these two mechanisms ensures localized route discovery, making LAR particularly effective in large-scale or highly mobile ad hoc networks.

6.6.3 LAR Scheme 1 and Scheme 2

Two major variants of the LAR protocol—Scheme 1 and Scheme 2—differ in how they define the request zone and manage RREQ propagation:

- LAR Scheme 1: In this scheme, the request zone is explicitly defined using the destination's expected zone and the source node's position. Each node determines whether it lies within the request zone based on its own coordinates before forwarding RREQs.
  This mechanism effectively reduces the number of control packets by preventing nodes outside the request zone from participating in the route discovery process.
- LAR Scheme 2: Scheme 2 further simplifies the forwarding rule by using distance-based criteria instead of geometric boundaries. A node forwards a route request only if it is closer to the destination than the node from which it received the request. This incremental forwarding approach leads to even lower overhead in dense networks but may slightly increase the probability of missing the optimal route in sparse environments.

Both schemes rely on accurate and timely location updates to ensure that the defined zones effectively encompass the destination's position. Errors in location estimation can degrade performance, leading to route discovery failures or longer paths.

6.6.4 Performance Metrics and Evaluation

Performance evaluation of LAR protocols typically considers several key metrics:

- Packet Delivery Ratio (PDR): Measures the success rate of data packet delivery from source to destination. LAR maintains high PDR by reducing collisions caused by unnecessary flooding.
- Routing Overhead: Indicates the ratio of control packets to successfully delivered data packets. LAR significantly reduces overhead compared to traditional reactive protocols.
- Average End-to-End Delay: Represents the time taken for a packet to reach its destination. LAR minimizes delay by limiting route discovery to a smaller geographic region.
- Route Discovery Latency: Measures the time required to establish a valid route. LAR generally achieves lower latency than AODV or DSR due to spatially constrained flooding.

Simulation studies often show that LAR performs better in terms of energy efficiency, bandwidth utilization, and scalability, especially in networks with moderate mobility and predictable movement patterns.

6.6.5 Energy Efficiency and Route Discovery Latency

Energy efficiency in LAR arises from its selective broadcasting approach, which conserves battery power by limiting participation in route discovery. Since only nodes within the request zone handle RREQs, the total number of transmissions decreases significantly, extending the lifetime of energy-constrained devices, such as those in sensor or IoT networks.

Additionally, the reduction in flooding area directly lowers route discovery latency, as fewer nodes are involved in processing and forwarding control messages. This results in faster route establishment and reduced channel contention. However, when mobility patterns are highly unpredictable or location information becomes outdated, performance may degrade due to inaccurate expected zone estimation.

The Location-Aided Routing (LAR) protocol exemplifies the effectiveness of integrating location information into reactive routing paradigms. Through its expected zone and request zone concepts, LAR minimizes control overhead, improves energy efficiency, and achieves faster route discovery compared to traditional flooding-based methods. Variants such as LAR Scheme 1 and Scheme 2 demonstrate adaptability across different network densities and mobility conditions, making LAR a foundational model for modern location-aware routing frameworks in MANETs, VANETs, and emerging UAV networks.

6.7 Hybrid Geographic Routing Approaches

Hybrid geographic routing approaches integrate the strengths of position-based routing with topology-aware mechanisms to improve reliability, scalability, and adaptability in dynamic network environments. By combining geographic information with conventional routing techniques, these protocols aim to mitigate the limitations of purely greedy or purely topology-based strategies, such as local minima, route instability, and excessive control overhead.

6.7.1 Combining Geographic and Topology-Based Mechanisms

Hybrid protocols exploit geographic knowledge for localized forwarding decisions while utilizing topology-based information to maintain route continuity and robustness. This combination allows nodes to:

- Forward packets using position-based heuristics when neighbor information is sufficient.
- Switch to topology-based routing (e.g., reactive path discovery or link-state information) in regions where greedy forwarding fails, such as sparse networks or void areas.
- Dynamically adapt to network changes, including node mobility, link failures, and varying node density.

The hybrid approach balances efficiency, reliability, and robustness, leveraging the scalability and stateless benefits of geographic routing while retaining the global path awareness of topology-based protocols.

6.7.2 Adaptive Switching Based on Node Mobility or Density

A key feature of hybrid geographic routing is adaptive switching, where the protocol selects the most suitable routing mode based on local network conditions:

- Node Mobility:
  - High mobility may favor geographic forwarding, as maintaining up-to-date topology information becomes costly.
  - In stable regions, topology-based routing may be employed to leverage pre-established paths and reduce packet loss.
- Node Density:
  - In dense networks, greedy forwarding or localized geographic decisions work efficiently due to abundant next-hop candidates.
  - In sparse networks, topology-based strategies or recovery mechanisms help overcome network voids and ensure end-to-end connectivity.
- Hybrid Decision Metrics:
  - Some protocols consider additional factors such as residual energy, link reliability, and transmission delay to determine the routing strategy dynamically.
  - Adaptive mechanisms reduce overall control overhead and improve network longevity without compromising packet delivery reliability.

6.7.3 Example Protocols

Several hybrid geographic routing protocols have been proposed to address the challenges of mobility, sparse connectivity, and energy efficiency:

(a) DREAM (Distance Routing Effect Algorithm for Mobility)

- Concept: DREAM is a predictive geographic routing protocol that uses motion history and velocity vectors to estimate node positions over time.
- Hybrid Aspect: It combines greedy forwarding with predictive updates from topology-aware mechanisms to maintain accurate neighbor information.
- Advantages: Efficient in highly mobile networks, low overhead, and capable of adjusting routing decisions dynamically based on node movement.

(b) GeoTORA (Geographic Temporally-Ordered Routing Algorithm)

- Concept: GeoTORA extends the classical TORA (Temporally-Ordered Routing Algorithm) by incorporating geographic information to guide route discovery.
- Hybrid Aspect: Uses TORA's link-reversal and topology maintenance principles in combination with geographic positioning for localized forwarding.
- Advantages: Supports loop-free multipath routing, efficient recovery from link failures, and reduced control message overhead in dynamic topologies.

(c) GLAR (Geographic Location-Aided Routing)

- Concept: GLAR enhances location-aided routing by using geographic coordinates to define forwarding zones and restrict route discovery.
- Hybrid Aspect: Integrates topology-awareness for nodes at the boundaries of forwarding zones to handle connectivity gaps and improve reliability.

- Advantages: Reduces flooding overhead, improves delivery ratio in sparse networks, and adapts effectively to node mobility.

Hybrid geographic routing approaches represent a balanced solution for modern ad hoc networks, where neither purely geographic nor purely topology-based methods are sufficient. By dynamically integrating position information with topology knowledge, hybrid protocols improve routing reliability, scalability, and adaptability across varying node densities and mobility scenarios. Protocols such as DREAM, GeoTORA, and GLAR exemplify these principles, demonstrating how hybrid mechanisms can optimize packet delivery, energy consumption, and route discovery efficiency while addressing the limitations of conventional routing paradigms.

6.8 Geographic Routing with Mobility Prediction

In highly dynamic networks, particularly vehicular ad hoc networks (VANETs) and UAV networks, node mobility significantly affects routing performance. Traditional geographic routing protocols, which rely on current location information, often suffer from packet loss, suboptimal paths, or local minima when nodes move rapidly. Mobility prediction-based geographic routing addresses these challenges by estimating the future positions of nodes and incorporating this knowledge into forwarding decisions.

6.8.1 Predictive Location Models for Moving Nodes

Predictive location models aim to forecast the probable position of a mobile node over a short time horizon, reducing the impact of high-speed mobility on routing. These models use:

- **Linear Motion Models:** Assume nodes move at a constant velocity and direction. The future position (x′,y′) can be calculated as:

$$x' = x + v_x . \Delta t$$
$$y' = y + v_y . \Delta t$$

  Where, v_x and v_y are velocity components and Δ_t is the prediction interval.
- **Acceleration-Based Models:** Incorporate acceleration and changes in velocity to improve prediction accuracy for nodes undergoing frequent speed or direction changes.
- **Pattern-Based Models:** Use historical mobility patterns or route knowledge (e.g., road maps in VANETs) to predict future positions probabilistically.

Accurate predictive models allow forwarding nodes to select next hops based not only on current positions but also on anticipated positions, minimizing packet misrouting.

6.8.2 Mobility Pattern-Based Forwarding

Mobility prediction enables pattern-based forwarding, where packets are forwarded to nodes expected to remain in the forwarding path long enough to deliver the data. Key techniques include:

- Trajectory-Aware Forwarding: Selects neighbors whose predicted trajectories align closely with the source-destination path.

- Velocity-Constrained Forwarding: Considers relative speed between nodes; nodes moving away from the destination are deprioritized.
- Predictive Greedy Forwarding: Combines traditional greedy forwarding with predicted positions, enhancing packet delivery success in sparse or high-speed networks.

By anticipating node movements, mobility-aware forwarding reduces the likelihood of route breaks, packet drops, and loop formation.

6.8.3 Application in Vehicular Ad Hoc Networks (VANETs)

VANETs exemplify environments where mobility prediction is essential due to:

- High Node Speeds: Vehicles often travel at tens to hundreds of kilometers per hour, causing frequent topology changes.
- Predictable Mobility Patterns: Vehicles typically follow road maps, lanes, and traffic rules, allowing route prediction with reasonable accuracy.
- Safety-Critical Applications: Low-latency delivery of messages (e.g., accident warnings) requires proactive routing decisions.

Protocols such as Predictive GPSR (P-GPSR) and Mobility Prediction-Based Geographic Routing (MPGR) leverage vehicle speed, direction, and road map information to improve packet delivery and reduce forwarding delays in VANETs.

6.8.4 Handling High-Speed Mobility and Position Inaccuracy

While mobility prediction enhances routing, it must account for prediction errors and position inaccuracy due to GPS limitations, environmental interference, or abrupt motion changes. Strategies to mitigate these challenges include:

- Adaptive Prediction Intervals: Adjusting the prediction horizon based on node speed and mobility variability to minimize errors.
- Confidence-Based Forwarding: Assigning weights or confidence values to predicted positions and choosing neighbors with the highest likelihood of staying within the forwarding path.
- Hybrid Forwarding Mechanisms: Combining predicted positions with reactive recovery methods (e.g., perimeter routing) to handle unanticipated route breaks.
- Error Correction Techniques: Incorporating feedback mechanisms to refine prediction models using actual observed positions.

These methods collectively ensure that geographic routing with mobility prediction remains robust even in high-speed, uncertain environments.

Geographic routing with mobility prediction enhances traditional position-based routing by incorporating temporal and movement-aware intelligence into forwarding decisions. By forecasting node positions, these protocols improve packet delivery ratio, reduce route failure events, and minimize latency in highly dynamic networks such as VANETs and UAV networks. However, their effectiveness depends on the accuracy of prediction models and mechanisms to handle position inaccuracy, motivating ongoing research into hybrid and AI-assisted mobility-aware routing solutions.

6.9 Location Service Management

Efficient location service management is critical for the operation of geographic and location-aided routing protocols. Location services provide nodes with the necessary positional information of other nodes in the network, enabling accurate and timely routing decisions. The design of location service mechanisms must balance accuracy, scalability, latency, and control overhead, particularly in mobile and resource-constrained environments such as MANETs, VANETs, and UAV networks.

6.9.1 Location Discovery and Update Mechanisms

Location discovery involves determining the current geographic coordinates of a node, while location updates ensure that this information remains current within the network. Common techniques include:

- **Periodic Updates:** Nodes broadcast their positions at regular intervals to neighbors or location servers. While simple, this method can generate significant overhead in dense networks.
- **Event-Driven Updates:** Position information is transmitted only when a node moves beyond a predefined threshold distance or changes its trajectory. This approach conserves bandwidth and energy.
- **Query-Based Discovery:** Source nodes initiate a request for the destination's position when needed. This reduces unnecessary updates but may introduce query latency.
- **Hybrid Approaches:** Combine periodic, event-driven, and query-based updates to optimize both accuracy and resource utilization.

Efficient discovery and update mechanisms are essential to maintain low route discovery latency, high packet delivery ratios, and minimized energy consumption.

6.9.2 Distributed vs. Centralized Location Services

Location services can be categorized based on their architectural deployment:

- Centralized Location Services: A dedicated node or a set of central servers maintains the position information of all nodes. While this ensures consistent and easily accessible data, it suffers from single points of failure, scalability issues, and potential bottlenecks in large networks.
- Distributed Location Services: Position information is stored and managed across multiple nodes, often using hashing or partitioning schemes. Distributed approaches enhance scalability and fault tolerance, as no single node is critical to network operation.

  Examples of distributed schemes include Distributed Hash Table (DHT)-based location services and quorum-based approaches.

Distributed architectures are generally preferred in large-scale or highly mobile networks, where centralized solutions may be impractical.

6.9.3 Grid-Based and Hierarchical Location Services

Several advanced location service architectures have been proposed to improve efficiency, scalability, and accuracy:

- **Grid-Based Location Services (GLS):** The network area is divided into logical grids, with each grid maintaining position information for nodes within its boundaries.

Nodes can locate the destination by querying a sequence of grids leading to the target. GLS reduces routing overhead and localizes updates within relevant areas.

- **Hierarchical Location Services (HLS):** Nodes are organized into zones or clusters, with higher-level nodes (cluster heads) maintaining positional information for all nodes in their region. Queries for node positions propagate through the hierarchical structure, limiting flooding and reducing control traffic. HLS is particularly suitable for large-scale networks with high node density.

Both approaches aim to minimize overhead while ensuring that location information is accessible and timely, supporting efficient geographic routing decisions.

6.9.4 Location Accuracy and Synchronization Issues

The effectiveness of location-aided routing heavily depends on the accuracy and freshness of location information. Challenges include:

- Localization Errors: GPS inaccuracies, multipath effects, and sensor limitations can introduce errors in position estimates, leading to suboptimal routing or packet loss.
- Mobility-Induced Inaccuracy: High node mobility can render previously recorded positions obsolete, especially in sparse or high-speed networks like VANETs.
- Synchronization Issues: Time delays in location updates or beacon transmissions can cause inconsistencies among neighboring nodes, affecting next-hop selection and increasing the risk of routing loops or packet misdelivery.

Strategies to mitigate these issues include:

- Incorporating mobility prediction to estimate future positions.
- Using confidence intervals or error bounds when forwarding decisions are made.
- Employing adaptive update intervals based on node speed and network dynamics.

Maintaining accurate, synchronized location information is essential for the reliability and efficiency of geographic and location-aided routing protocols.

Location service management forms the backbone of geographic routing by providing timely and accurate positional information. Effective management involves robust discovery and update mechanisms, a choice between distributed and centralized architectures, and the use of grid-based or hierarchical structures to optimize scalability and overhead. Ensuring location accuracy and synchronization is critical for minimizing packet loss, route failures, and energy consumption, especially in highly dynamic or large-scale ad hoc networks.

6.10 Energy-Efficient and QoS-Aware Geographic Routing

Energy efficiency and Quality of Service (QoS) are critical design objectives in modern ad hoc and wireless sensor networks. Geographic routing protocols, while inherently efficient due to their localized forwarding decisions, must address the trade-offs between energy conservation, routing accuracy, and QoS requirements such as delay, throughput, and reliability. In large-scale and mobile environments—such as MANETs, WSNs, and VANETs—achieving a balance between energy consumption and performance guarantees is essential for sustaining long-term network operation and application-level quality.

6.10.1 Trade-Offs Between Energy Consumption and Routing Accuracy

Geographic routing protocols reduce control overhead by eliminating global topology maintenance; however, frequent position updates, beacon exchanges, and retransmissions caused by inaccurate location data can increase energy expenditure.

- **Energy–Accuracy Dilemma:** Maintaining precise location information requires frequent beaconing and updates, leading to higher energy consumption. Conversely, reducing update frequency conserves energy but degrades routing accuracy, causing suboptimal next-hop selection or packet loss.
- **Adaptive Energy Management:** Energy-efficient routing strategies dynamically adjust beacon intervals based on mobility rate, residual energy, or traffic load. Nodes with low energy may reduce their participation in forwarding decisions or delegate tasks to more energy-abundant neighbors.
- **Sleep Scheduling and Duty Cycling:** In sensor-based geographic networks, nodes alternate between active and sleep states while maintaining coverage through geographic clustering or wake-up radio mechanisms, thereby extending network lifetime.

Achieving an optimal trade-off requires adaptive mechanisms that intelligently balance energy saving with routing precision, ensuring sustainable and reliable communication.

6.10.2 Load Balancing in Dense Geographic Networks

In dense networks, nodes near the geographic center or in frequently used paths may deplete energy faster due to repeated forwarding, leading to energy holes and connectivity loss.

Load balancing techniques help distribute traffic evenly across the network:

- **Energy-Aware Next-Hop Selection:** Nodes select the next hop not only based on distance to the destination but also on residual energy and traffic load, ensuring equitable energy consumption among nodes.
- **Geographic Load Balancing:** Forwarding zones or paths are adjusted dynamically to reroute packets through less congested areas, improving both energy distribution and network longevity.
- **Cluster-Based Load Control:** In hierarchical networks, cluster heads aggregate data and manage forwarding tasks to reduce redundant transmissions. Cluster rotation mechanisms ensure that no single node is overburdened.

Effective load balancing enhances both energy efficiency and network stability, particularly in IoT and WSN applications where node replacement is impractical.

6.10.3 Delay and Throughput Optimization

Delay and throughput are key QoS parameters affected by routing efficiency, link stability, and node mobility. Geographic routing protocols can optimize these parameters through spatial and temporal awareness:

- Delay Minimization: Predictive geographic routing and mobility-aware forwarding help reduce end-to-end delay by anticipating node movement and selecting stable next hops.

Priority-based packet scheduling can further minimize latency for delay-sensitive applications (e.g., real-time tracking or VANET safety alerts).

- Throughput Maximization: Multi-path geographic routing improves throughput by distributing data flows over multiple disjoint paths, preventing congestion and increasing overall bandwidth utilization. Adaptive transmission power control and interference-aware forwarding enhance link quality and minimize packet collisions.

Protocols integrating cross-layer optimization (between routing and MAC layers) have shown significant improvement in throughput and delay performance under varying mobility and traffic conditions.

6.10.4 Quality of Service (QoS) Enhancements

QoS-aware geographic routing protocols extend traditional models by incorporating service differentiation and performance guarantees for diverse applications. Key mechanisms include:

- **QoS Metrics Integration:** Next-hop decisions consider not just distance or energy, but also link stability, signal strength, delay constraints, and bandwidth availability.
- **Priority-Aware Forwarding:** Packets are classified into priority levels (e.g., emergency, multimedia, or best-effort traffic). High-priority packets are routed through paths offering minimal latency and higher reliability.
- **Geographic QoS Frameworks:** Protocols such as QGRP (QoS-Geographic Routing Protocol) and E-GR (Energy-efficient Geographic Routing) integrate energy-aware and delay-sensitive mechanisms to maintain consistent service quality.
- **Context-Aware Adaptation:** QoS parameters are dynamically adjusted based on real-time conditions such as congestion level, node speed, and network topology changes. This adaptability ensures reliable delivery for applications ranging from vehicular networks to environmental monitoring systems.

Energy-efficient and QoS-aware geographic routing represents the next evolution in spatially informed network design. Through adaptive trade-off management, load balancing, and QoS-driven optimization, these protocols address the limitations of traditional position-based routing. They enable longer network lifetimes, faster data delivery, and better reliability, making them suitable for emerging applications such as IoT systems, VANETs, and mission-critical mobile networks. The ongoing integration of machine learning and cross-layer intelligence promises even greater adaptability in achieving optimal energy–QoS balance in future geographic routing paradigms.

6.11 Conclusion

This chapter presented an in-depth exploration of geographic and location-aided routing techniques, which utilize spatial information to enhance the efficiency and scalability of ad hoc networks. Beginning with the fundamentals of position-based communication, the discussion highlighted how the integration of geographic coordinates—often obtained through GPS or other localization systems—enables intelligent, localized forwarding

decisions that significantly reduce routing overhead compared to traditional topology-based approaches. The chapter systematically examined the architectural components of location-aware systems, including location services, neighbor discovery mechanisms, and geographic forwarding engines, which collectively form the foundation for efficient route determination and maintenance. Various protocol classifications were analyzed, encompassing greedy forwarding, hierarchical geographic routing, and hybrid schemes that integrate topology awareness with positional data. Through detailed discussions of representative protocols such as GPSR, GOAFR, LAR, DREAM, and GeoTORA, readers gained insights into the diverse strategies employed for optimizing path selection, route recovery, and mobility adaptation. Emphasis was placed on the role of mobility prediction, location service management, and energy-aware design, which are crucial for achieving reliability in dynamic and resource-constrained environments such as MANETs, WSNs, VANETs, and UAV networks.

A key takeaway from this chapter is the balance between energy efficiency, routing accuracy, and Quality of Service (QoS). Geographic routing protocols, by leveraging real-time positional awareness, can dynamically adapt to changing topology conditions, minimizing delay and improving throughput. Moreover, integrating QoS-aware and energy-optimized mechanisms ensures long-term network sustainability and robust data delivery performance. In summary, geographic and location-aided routing offers a scalable and adaptive approach to wireless communication, capable of addressing the challenges of mobility, density, and resource limitation. As ad hoc networks evolve toward intelligent and self-organizing architectures, these techniques serve as a foundation for the next generation of QoS- and energy-efficient routing protocols.

References

1. Basagni, S., Conti, M., Giordano, S., & Stojmenovic, I. (Eds.). (2013). *Mobile Ad Hoc Networking: Cutting Edge Directions* (2nd ed.). Wiley-IEEE Press.
2. Bose, P., Morin, P., Stojmenovic, I., & Urrutia, J. (2001). Routing with guaranteed delivery in ad hoc wireless networks. *Wireless Networks, 7*(6), 609–616. https://doi.org/10.1023/A:1012319418150
3. Camp, T., Boleng, J., & Davies, V. (2002). A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing, 2*(5), 483–502. https://doi.org/10.1002/wcm.72
4. Clausen, T., & Jacquet, P. (2003). *Optimized Link State Routing Protocol (OLSR)*. IETF RFC 3626.
5. Ko, Y.-B., & Vaidya, N. H. (2000). Location-Aided Routing (LAR) in mobile ad hoc networks. *Wireless Networks, 6*(4), 307–321. https://doi.org/10.1023/A:1019106118419
6. Karp, B., & Kung, H. T. (2000, August). GPSR: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom 2000)* (pp. 243–254). ACM.
7. Li, J., Jannotti, J., De Couto, D. S. J., Karger, D. R., & Morris, R. (2000, August). A scalable location service for geographic ad hoc routing. In *Proceedings of the 6th*

Annual International Conference on Mobile Computing and Networking (MobiCom 2000) (pp. 120–130). ACM.

8. Mauve, M., Widmer, J., & Hartenstein, H. (2001). A survey on position-based routing in mobile ad hoc networks. *IEEE Network, 15*(6), 30–39. https://doi.org/10.1109/65.967595
9. Kuhn, F., Wattenhofer, R., Zhang, Y., & Zollinger, A. (2003, September). Geometric ad-hoc routing: Of theory and practice. In *Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing (PODC 2003)* (pp. 63–72). ACM.
10. Seada, K., Helmy, A., & Helmy, A. (2004). Geographic protocols in sensor networks. *University of Southern California Technical Report*.
11. Stojmenovic, I. (2002). Position-based routing in ad hoc networks. *IEEE Communications Magazine, 40*(7), 128–134. https://doi.org/10.1109/MCOM.2002.1018018
12. Stojmenovic, I., & Lin, X. (2001). Power-aware localized routing in wireless networks. *IEEE Transactions on Parallel and Distributed Systems, 12*(11), 1122–1133. https://doi.org/10.1109/71.969123
13. Royer, E. M., & Toh, C.-K. (1999). A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications, 6*(2), 46–55. https://doi.org/10.1109/98.760423
14. Naumov, V., & Gross, T. R. (2007). Connectivity-aware routing (CAR) in vehicular ad hoc networks. *IEEE INFOCOM 2007*, 1919–1927. https://doi.org/10.1109/INFCOM.2007.198
15. Lochert, C., Mauve, M., Füssler, H., & Hartenstein, H. (2005). Geographic routing in city scenarios. *ACM SIGMOBILE Mobile Computing and Communications Review, 9*(1), 69–72. https://doi.org/10.1145/1055959.1055970
16. Chen, Y., Liu, W., & Wang, S. (2018). Energy-efficient geographic routing based on mobility prediction in MANETs. *Ad Hoc Networks, 75–76*, 100–111. https://doi.org/10.1016/j.adhoc.2018.04.005
17. Li, Y., & Wang, J. (2019). QoS-aware geographic routing for wireless sensor networks. *IEEE Access, 7*, 96325–96337. https://doi.org/10.1109/ACCESS.2019.2928462
18. Raza, S., & Khan, M. A. (2020). Energy-aware hybrid geographic routing for IoT-enabled ad hoc networks. *IEEE Internet of Things Journal, 7*(12), 11658–11670. https://doi.org/10.1109/JIOT.2020.2993943
19. Zheng, H., Wu, Q., & Sun, G. (2021). Deep learning-assisted geographic routing in vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems, 22*(7), 4023–4035. https://doi.org/10.1109/TITS.2020.3010157
20. Sharma, A., & Singh, S. (2022). Blockchain-based secure geographic routing for 5G-enabled ad hoc networks. *IEEE Transactions on Network and Service Management, 19*(2), 1547–1561. https://doi.org/10.1109/TNSM.2021.3128994

Chapter -7

Energy-Efficient Routing Protocols for Ad Hoc Networks

[1]S. Bharathi, [2]Dr. D. Maruthanayagam

[1]Research Scholar, PG and Research Department of Computer Science,
Sri Vijay Vidyalaya College of Arts & Science,
Dharmapuri, Tamilnadu, India.

[2]Dean cum Professor, PG and Research Department of Computer Science,
Sri Vijay Vidyalaya College of Arts & Science,
Dharmapuri, Tamilnadu, India.

Abstract: *Energy efficiency has emerged as one of the most critical challenges in the design and operation of ad hoc networks, where nodes rely on limited battery power and operate in highly dynamic environments. As network lifetime directly depends on power management, the development of energy-efficient routing protocols is essential for sustaining communication performance and minimizing resource depletion. This chapter presents a comprehensive exploration of energy-aware routing mechanisms that aim to optimize network lifetime, reduce transmission costs, and balance energy consumption among participating nodes. The chapter begins by outlining the fundamentals of energy consumption models and the underlying factors influencing power utilization in wireless communication. It then categorizes energy-efficient routing protocols based on routing strategies (proactive, reactive, hybrid), optimization objectives (minimum energy, load-balanced, lifetime-maximizing), and network architecture (flat, clustered, hierarchical). Representative protocols such as E-AODV, FEA-DSDV, LEACH, HEED, GEAR, and MTPR are analyzed in terms of design principles, operational mechanisms, and trade-offs between energy savings and performance metrics such as delay, throughput, and reliability. Special emphasis is placed on cross-layer optimization, multi-path cooperation, and energy harvesting techniques, which enhance adaptability under diverse network conditions. Furthermore, the chapter discusses QoS-constrained, security-aware, and AI-driven energy routing frameworks that align with the demands of emerging IoT, 5G, and vehicular networks. Through systematic classification and analytical insights, this chapter provides readers with a holistic understanding of how energy-efficient routing protocols contribute to the longevity, scalability, and resilience of ad hoc wireless networks.*

Keywords: *Energy Efficiency; Energy-Aware Routing; Power Optimization; Network Lifetime; Ad Hoc Networks; Proactive and Reactive Routing; Cluster-Based Routing; Hierarchical Energy Management; Load Balancing; Cross-Layer Design; Multi-Path Routing; Cooperative Communication; Geographic Energy Routing; Energy Harvesting; QoS-Constrained Routing; Secure Energy-Aware Routing*

7.1 Introduction

Energy efficiency plays a pivotal role in the design and performance of wireless ad hoc networks, where nodes typically rely on limited battery power to perform communication, computation, and control functions. Unlike traditional wired or infrastructure-based wireless systems, ad hoc networks operate in a decentralized and dynamic environment, where each node functions as both a host and a router. Consequently, the overall network lifetime and stability are strongly influenced by how effectively energy resources are managed and conserved throughout the routing process.

Overview of Energy Efficiency in Wireless Ad Hoc Networks

Energy efficiency in ad hoc networks refers to the ability of routing protocols and communication mechanisms to minimize power consumption without compromising performance metrics such as throughput, delay, or packet delivery ratio. Since nodes are typically deployed in scenarios where recharging or replacing batteries is impractical—such as battlefields, disaster recovery zones, and remote sensing applications—energy management becomes a fundamental design consideration. Efficient routing ensures that energy expenditure during packet transmission, reception, and control overhead is kept minimal while maintaining robust network connectivity.

Importance of Power Conservation in Mobile Nodes

Mobile nodes in ad hoc networks perform dual roles as end systems and intermediate routers, forwarding packets for other nodes. This multi-hop communication paradigm leads to uneven energy consumption across nodes, where heavily loaded or centrally positioned nodes may deplete their energy faster than others, potentially fragmenting the network. Power conservation strategies—such as sleep scheduling, transmission power control, and load balancing—are therefore essential to extend the operational lifetime of both individual nodes and the entire network. The ultimate goal is to ensure sustainable connectivity and balanced energy utilization across all participants.

Relationship between Energy Consumption and Network Lifetime

The network lifetime is directly proportional to how energy resources are utilized and distributed among nodes. High energy consumption in certain routes can create energy holes, leading to disconnections or degraded performance. Consequently, routing decisions must account for the residual energy of nodes, communication distance, and traffic intensity to avoid premature node failures. By optimizing these factors, energy-efficient routing protocols aim to maximize lifetime, minimize control overhead, and maintain quality of service (QoS) in dynamic environments.

Challenges: Node Mobility, Limited Battery, and Dynamic Topology

Designing energy-efficient routing protocols is complicated by several inherent challenges in ad hoc networks.

- **Node Mobility:** Frequent movement of nodes leads to changing topologies, broken links, and the need for continuous route rediscovery—all of which increase energy expenditure.
- **Limited Battery Resources:** Nodes typically operate on constrained power supplies, making it vital to reduce unnecessary retransmissions and idle energy consumption.
- **Dynamic Topology and Scalability:** As the number of nodes increases, maintaining energy efficiency while ensuring routing accuracy and low latency becomes increasingly difficult.

Addressing these challenges requires **adaptive, distributed, and context-aware routing mechanisms** that can adjust to environmental and mobility variations without excessive energy cost.

Comparison of Energy-Aware vs. Traditional Routing Approaches

Traditional routing protocols, such as AODV, DSR, and OLSR, primarily focus on finding the shortest or fastest path between nodes, often disregarding energy constraints. In contrast, energy-aware routing protocols incorporate parameters like residual node energy, transmission cost, and energy balance into their path selection criteria. While traditional schemes may achieve lower latency or higher throughput initially, they can lead to uneven energy depletion and shorter network lifespans. Energy-efficient routing approaches, on the other hand, strike a balance between performance and sustainability, ensuring prolonged network operation even under mobility and load fluctuations.

In essence, energy efficiency is not merely an optimization goal but a survival requirement for wireless ad hoc networks. By integrating energy-awareness into routing strategies, networks can achieve longer operational lifetimes, higher reliability, and reduced maintenance costs. The subsequent sections of this chapter explore the fundamentals, classifications, and advanced mechanisms of energy-efficient routing protocols, providing insight into both classical and emerging energy optimization techniques for next-generation ad hoc networks.

7.2 Fundamentals of Energy Consumption in Ad Hoc Networks

Energy consumption is a central factor that determines the performance, sustainability, and operational lifetime of wireless ad hoc networks. Since each node in an ad hoc network is powered by a finite energy source, typically a battery, understanding how energy is consumed during different operational states is crucial for designing efficient routing and communication mechanisms. This section explores the fundamental components of energy usage, the power models for wireless communication, the impact of routing overhead, and the trade-offs that influence network performance metrics.

Components of Energy Usage: Transmission, Reception, Idle, and Sleep Modes

The total energy consumption of a mobile node can be classified into four major operational states (Figure 1):

- **Transmission Mode:** Energy is consumed when a node transmits packets over the wireless medium. The power required depends on factors such as transmission distance, signal strength, modulation scheme, and interference levels. Longer transmission ranges demand higher power, making routing decisions that minimize hop distance critical for energy efficiency.
- **Reception Mode:** During packet reception, nodes consume energy to decode incoming signals. Although the energy cost per packet is generally lower than in transmission, nodes that frequently act as intermediate routers may experience significant cumulative energy depletion.

- **Idle Mode:** In this mode, a node's radio remains active, listening to the channel for potential transmissions. Idle listening is a **major source of energy wastage**, as nodes consume nearly the same power as in reception mode without performing useful work. Efficient MAC-layer protocols and sleep scheduling can mitigate this issue.
- **Sleep Mode:** To conserve power, nodes can enter a low-energy sleep state when inactive. However, frequent transitions between active and sleep states introduce latency and synchronization challenges. Optimal scheduling is necessary to balance energy saving with communication responsiveness.

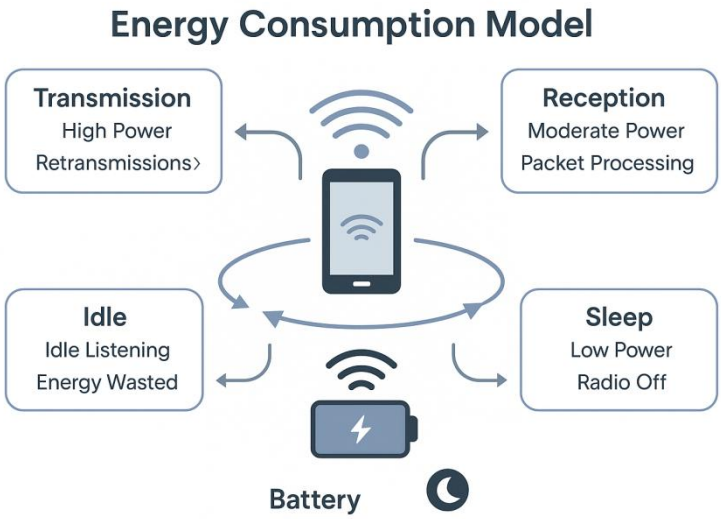


Figure 1: Energy Consumption Components in Mobile Ad Hoc Networks

Power Models for Wireless Communication

Energy consumption in wireless communication is typically modeled using radio energy dissipation models, which quantify the power required to transmit and receive data based on transmission distance and hardware characteristics. A common model expresses the energy consumed to transmit a k-bit packet over a distance d as:

$$E_{TX}(k,d) = E_{elec} \times k + E_{amp} \times k \times d^{n}$$

Where:

- E_{elec}: Energy consumed by electronic circuitry per bit
- E_{amp}: Energy required by the transmitter amplifier per bit per distance unit
- n: Path-loss exponent (typically 2–4 depending on the environment)

Similarly, the energy consumed to receive a k-bit message is:

$$E_{RX}(k) = E_{elec} \times k$$

These models highlight the importance of **short-distance, multi-hop transmission** and **power-controlled routing**, as transmission energy grows exponentially with distance.

Impact of Routing Overhead and Retransmissions on Energy Depletion

Routing protocols incur control overhead through mechanisms such as route discovery, maintenance, and link updates. Frequent broadcasting of control packets in dynamic topologies consumes additional energy, especially in reactive protocols like AODV or DSR. Moreover, unreliable wireless links and node mobility often result in packet losses, necessitating retransmissions. Each retransmission not only consumes energy but also increases congestion and delay, leading to further energy inefficiency. Therefore, minimizing routing overhead and retransmission frequency is vital for prolonging network lifetime.

Trade-offs Between Energy Efficiency, Delay, and Throughput

Designing energy-efficient routing involves balancing competing performance objectives:

- **Energy vs. Delay:** Reducing transmission power or using energy-saving sleep schedules may increase end-to-end delay.
- **Energy vs. Throughput:** Limiting retransmissions or using fewer active routes can save energy but may reduce network throughput.
- **Energy vs. Reliability:** Aggressive energy conservation can compromise link stability, increasing packet loss and route failures.

Thus, optimal energy-aware routing protocols strive to **minimize total energy consumption** while maintaining acceptable **Quality of Service (QoS)** in terms of delay, packet delivery, and throughput.

Metrics for Energy Performance Evaluation (E2ED, NLT, NDE, etc.)

To quantitatively assess the energy performance of routing protocols, several evaluation metrics are employed:

- **Energy per Packet (E2ED):** Measures the average energy consumed to successfully deliver a packet from source to destination.
- **Network Lifetime (NLT):** Represents the duration until the first node exhausts its energy or the network becomes partitioned. It is a key metric for overall sustainability.
- **Node Density Energy (NDE):** Evaluates how energy consumption is distributed among nodes relative to their density, ensuring balanced load and fairness.
- **Energy Consumption per Bit (ECB):** Indicates the energy required to transmit a single bit of data successfully.
- **Residual Energy Ratio (RER):** Reflects the average remaining energy of all nodes over time, showing how evenly the energy burden is shared.

These metrics help researchers and engineers compare different routing approaches in terms of both **efficiency and fairness**, guiding the development of protocols that extend network longevity while ensuring stable communication.

Understanding the fundamentals of energy consumption in ad hoc networks provides the foundation for designing efficient routing protocols. By analyzing energy usage across various operational states, modeling transmission power requirements, and evaluating trade-offs between energy efficiency and QoS, researchers can develop adaptive, context-aware mechanisms that prolong network lifetime. The next section explores the **classification of energy-efficient routing protocols**, highlighting diverse strategies for optimizing energy utilization in dynamic mobile environments.

7.3 Design Goals and Principles of Energy-Efficient Routing

Energy-efficient routing in ad hoc networks focuses on optimizing communication processes to extend the operational lifetime of mobile nodes and the overall network. Since each node acts as both a host and a router, its energy consumption directly impacts connectivity, throughput, and network resilience. This section explores the core design goals and guiding principles that form the foundation for developing energy-aware routing protocols, emphasizing balanced energy consumption, adaptive power control, and cross-layer optimization.

Prolonging Network Lifetime through Balanced Energy Consumption

The primary goal of energy-efficient routing is to maximize network lifetime — defined as the duration until critical nodes deplete their energy or network partitioning occurs. Traditional routing algorithms tend to overuse certain nodes (e.g., those near the center or with high connectivity), leading to **energy holes** and early link failures.

Energy-efficient protocols aim to balance this load by:

- Distributing routing tasks among multiple nodes.
- Avoiding repeated use of the same paths.
- Dynamically rotating forwarding roles to prevent overburdening any single node.

Approaches such as **minimum total transmission power routing** and **maximum residual energy-based next-hop selection** help maintain a uniform energy consumption pattern across the network, ensuring longer connectivity and robustness.

Minimizing Control Overhead and Retransmission Costs

In ad hoc networks, **control messages**—used for route discovery, maintenance, and topology updates—consume significant energy. Moreover, **retransmissions** due to collisions, congestion, or mobility-induced link breakages further increase energy expenditure.

Energy-efficient routing protocols therefore strive to:

- Reduce the frequency of **route discovery floods** through caching, clustering, or selective broadcasting.
- Employ **localized repair mechanisms** instead of full route rediscovery.
- Integrate **link quality estimation** to minimize retransmissions caused by unstable links.

By minimizing control overhead and retransmission rates, these protocols not only conserve energy but also improve packet delivery ratios and reduce latency.

Adaptive Transmission Power Control

Adaptive transmission power control (TPC) is a key principle for conserving energy during communication. Instead of using fixed transmission power, nodes dynamically adjust their signal strength based on:

- Distance to the next-hop node,
- Link quality or signal-to-noise ratio (SNR),
- Interference level in the communication channel.

Reducing transmission power lowers energy consumption and mitigates interference, enabling higher spatial reuse of the wireless channel. However, excessively low power can cause frequent link breakages, requiring a careful **balance between connectivity and conservation**. Hybrid TPC algorithms that adaptively scale power according to mobility or traffic conditions are widely employed in modern ad hoc routing designs.

Reducing Redundant Forwarding and Collision Losses

Uncontrolled broadcasting in dense networks can lead to **redundant packet forwarding**, known as the **broadcast storm problem**, resulting in wasted energy and increased collisions. Energy-efficient routing protocols address this by:

- Using **probabilistic forwarding** or **selective relaying** mechanisms.
- Employing **geographic and directional routing** to restrict forwarding to nodes within a specific area.
- Implementing **MAC-layer collision avoidance** and **sleep scheduling** to reduce contention.

By minimizing redundant transmissions and collision-induced losses, these strategies help preserve node energy and enhance network throughput efficiency.

Role of Cross-Layer Optimization in Energy-Efficient Design

Traditional network architectures separate protocol layers, but this separation can hinder energy optimization. **Cross-layer design** allows different layers (MAC, network, and physical) to share information, enabling adaptive and context-aware routing decisions.
Examples of cross-layer energy optimizations include:

- Adjusting **transmission power** at the physical layer based on **routing layer feedback** about link reliability.
- Using **MAC-layer scheduling** to coordinate node sleep cycles with **routing layer activity**.
- Employing **application-layer traffic patterns** to predict and preempt energy hotspots.

This holistic approach ensures that energy efficiency is maintained across the entire communication stack, leading to a more integrated and intelligent routing framework.

Designing energy-efficient routing protocols requires balancing multiple, often conflicting objectives — extending network lifetime, minimizing overhead, maintaining connectivity, and ensuring quality of service. Key design principles such as balanced energy utilization, adaptive power control, and cross-layer cooperation play crucial roles in achieving these

goals. By embedding these principles into protocol design, ad hoc networks can achieve sustainable, scalable, and energy-conscious communication even under highly dynamic and resource-constrained conditions.

7.4 Classification of Energy-Efficient Routing Protocols

Energy-efficient routing protocols in ad hoc networks can be categorized according to their routing strategies, optimization objectives, and the protocol layer at which energy conservation mechanisms are implemented. Each category reflects a distinct design philosophy for managing power consumption while maintaining reliable and scalable communication among mobile nodes. This section classifies these protocols from three key perspectives: **routing strategy**, **network layer focus**, and **optimization objectives (Figure 2)**.

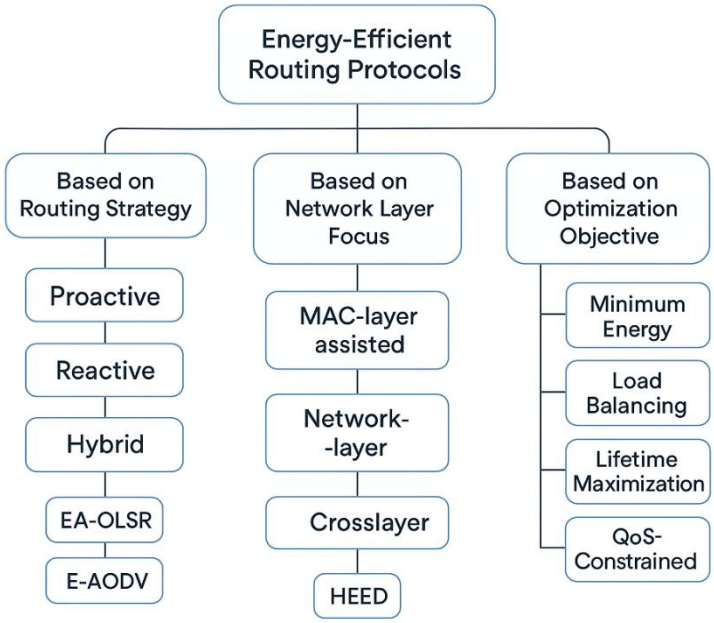


Figure 2: Taxonomy of Energy-Efficient Routing Protocols in Ad Hoc Network

7.4.1 Based on Routing Strategy

Energy-efficient routing protocols can be broadly divided into **proactive**, **reactive**, and **hybrid** approaches, depending on how routes are established and maintained.

(a) Proactive (Table-Driven) Protocols

Proactive protocols maintain up-to-date routing information for all network nodes by periodically exchanging routing tables. Energy-efficient variants of these protocols focus on **reducing the frequency and size of control message exchanges** to conserve energy. Examples include:

- **Energy-Aware Optimized Link State Routing (EA-OLSR)** – minimizes link update intervals based on node energy levels.

- **Power Efficient DSDV –** employs selective updates to lower control overhead.

Although proactive methods offer **low latency**, their periodic updates can lead to **higher idle energy consumption**, making them suitable for **low-mobility, energy-stable environments**.

(b) Reactive (On-Demand) Protocols

Reactive protocols discover routes **only when required**, thereby minimizing unnecessary energy usage. They focus on **reducing route discovery overhead** and **avoiding redundant retransmissions**. Examples include:

- **Minimum Energy Dynamic Source Routing (MEDSR) –** uses power control during route discovery to find energy-minimizing paths.
- **Energy-Aware AODV (EA-AODV) –** integrates residual energy and link stability into route selection.

Reactive protocols are typically **more energy-efficient** in highly dynamic environments, but route discovery delays can affect QoS in real-time applications.

(c) Hybrid Energy-Efficient Protocols

Hybrid routing protocols combine the advantages of proactive and reactive schemes. They employ **proactive routing within clusters or zones** and **reactive routing between them**, thereby optimizing energy and scalability. Examples include:

- **Zone-Based Energy-Aware Routing (ZBEAR)**
- **Hybrid Energy-Efficient Distributed Routing (HEED)**

These protocols adapt to **network size, mobility, and node energy** conditions, making them ideal for heterogeneous and large-scale ad hoc deployments.

7.4.2 Based on Network Layer Focus

Energy efficiency can be achieved by optimizing operations at various layers of the network stack. Depending on where energy-aware mechanisms are implemented, protocols can be classified as MAC-layer assisted**,** network-layer optimized**, or** cross-layer coordinated**.**

(a) MAC-Layer Assisted Energy Optimization

At the MAC layer, energy savings are achieved by reducing idle listening, collisions, and retransmissions. Mechanisms such as sleep scheduling, adaptive contention window adjustment, and low-power listening contribute to significant power conservation. Protocols like S-MAC (Sensor-MAC) and T-MAC (Timeout-MAC) exemplify this approach by introducing duty-cycling and contention-based energy optimization.

(b) Network-Layer Routing Energy Reduction

Network-layer routing focuses on selecting **energy-efficient paths** based on transmission cost, residual energy, and hop count. For instance:

- **Minimum Total Transmission Power Routing (MTPR)** chooses routes that minimize cumulative transmission power.
- **Max-Min Battery Capacity Routing (MMBCR)** prioritizes nodes with higher residual energy to prevent early depletion.

Such strategies directly influence **route selection policies** to extend both node and network lifetime.

(c) Cross-Layer Energy Coordination

Cross-layer energy-efficient designs integrate information across protocol layers—such as link quality, node energy state, and mobility metrics—to optimize routing decisions dynamically. Protocols like CL-EEAODV (Cross-Layer Energy-Efficient AODV) demonstrate this by adjusting transmission power based on both physical-layer SNR and MAC-layer link utilization. This holistic view enables more context-aware and adaptive routing performance.

7.4.3 Based on Optimization Objective

Energy-efficient routing protocols may also be distinguished by their primary optimization objectives, depending on whether the goal is to minimize energy use, balance load, extend lifetime, or maintain QoS constraints.

(a) Minimum Energy Routing

These protocols aim to minimize the total energy consumed per data delivery by selecting the path with the lowest cumulative transmission cost. However, such strategies may overuse certain nodes, leading to unbalanced energy depletion. Examples include MTPR and PARO (Power-Aware Routing Optimization).

(b) Load-Balanced Energy Routing

To prevent energy exhaustion of critical nodes, load-balanced protocols distribute forwarding responsibilities evenly across the network. Conditional Max-Min Battery Capacity Routing (CMMBCR) and Load-Balanced Energy Aware Routing (LBEAR) exemplify this approach by dynamically rerouting traffic through underutilized nodes.

(c) Lifetime-Maximizing Routing

Here, the primary focus is on maximizing network lifetime rather than minimizing instantaneous energy consumption. Minimum Battery Cost Routing (MBCR) and Lifetime-Preserving Routing (LPR) select paths that delay the depletion of the most energy-constrained nodes, maintaining network connectivity for longer durations.

(d) QoS-Constrained Energy-Aware Routing

Protocols in this category strive to optimize energy use while satisfying Quality of Service (QoS) requirements such as delay, jitter, or throughput. Examples include Energy and Delay Aware Routing (EDAR) and QoS-aware Power-Efficient Routing (QPER). These are particularly useful in real-time applications such as multimedia streaming or mission-critical communications.

The classification of energy-efficient routing protocols highlights the diverse strategies and design trade-offs involved in balancing energy conservation, network lifetime, and communication performance. Whether optimized at the routing layer, supported by MAC-layer mechanisms, or enhanced through cross-layer coordination, these protocols collectively aim to achieve sustainable and scalable communication in energy-constrained ad hoc environments. The next section discusses power control and topology management techniques, which form the operational backbone of these energy-aware routing solutions.

7.5 Energy-Aware Proactive Routing Protocols

Proactive routing protocols, also known as table-driven protocols, maintain up-to-date routes to all nodes in the network through periodic exchange of control messages. While traditional proactive protocols like OLSR and DSDV ensure low-latency route availability, they often incur significant energy overhead due to frequent table updates. Energy-aware proactive protocols extend these mechanisms by incorporating power optimization strategies to minimize energy consumption while preserving routing accuracy.

Mechanisms of Proactive Energy-Efficient Routing

Energy-efficient proactive routing protocols employ several strategies to reduce energy usage:

- Adaptive Update Intervals: Instead of broadcasting routing tables at fixed intervals, updates are dynamically adjusted based on network mobility and link stability. Nodes in stable topologies broadcast less frequently, conserving energy.
- Selective Link Updates: Only changes in critical links or those affecting active routes trigger updates, avoiding unnecessary control message dissemination.
- Energy-Aware Route Selection: Nodes consider residual energy, link stability, and cumulative transmission cost when maintaining routing tables, ensuring that paths are chosen to balance energy load across the network.
- Flow-Oriented Routing: Some protocols track traffic patterns to optimize routing paths for active data flows, reducing redundant route maintenance and energy-intensive broadcasts.

Example Protocols

1. PE-OLSR (Power-Efficient Optimized Link State Routing)

- Enhances standard OLSR by modifying multipoint relay (MPR) selection to favor nodes with higher residual energy.
- Reduces energy consumption by minimizing the number of transmissions while maintaining network connectivity.

2. EOLSR (Energy-Aware Optimized Link State Routing)

- Integrates residual node energy metrics into link cost computation.
- Routes are selected to maximize network lifetime, avoiding nodes with critically low energy.
- Includes adaptive MPR selection to further reduce overhead.

3. FEA-DSDV (Flow-Oriented Energy-Aware DSDV)

- Based on DSDV, this protocol tracks active traffic flows and prioritizes routes with optimal energy efficiency for data transmission.
- Uses residual energy and hop count to update routing tables selectively, reducing unnecessary broadcasts.

Advantages of Energy-Aware Proactive Routing

- Low Latency: Routes are readily available for immediate packet forwarding.
- Predictable Performance: Continuous route knowledge allows stable network operation under low mobility.
- Balanced Energy Utilization: By considering residual energy in route selection, these protocols reduce the likelihood of early node failures.
- Scalable to Medium-Sized Networks: Effective in networks where topology changes are moderate, minimizing frequent updates.

Limitations

- High Control Overhead in Highly Dynamic Networks: Frequent updates in mobile scenarios can lead to substantial energy drain.
- Inefficiency in Sparse or Large Networks: Maintaining global routing tables for all nodes becomes costly in terms of energy and bandwidth.
- Trade-off Between Update Frequency and Accuracy: Reducing update intervals saves energy but risks outdated routing information and potential packet loss.

Impact of Periodic Updates on Energy Consumption

Periodic updates are a double-edged sword in proactive protocols. While they ensure current route information for all nodes, they also constitute a significant portion of total energy consumption. Energy-aware proactive protocols mitigate this impact by:

- Adapting update frequency based on node mobility and traffic load.
- Broadcasting updates selectively, focusing only on changes affecting active routes or critical links.
- Optimizing the MPR set to reduce redundant transmissions.

These mechanisms collectively reduce unnecessary energy expenditure while retaining the core advantages of proactive routing, making them suitable for networks where low latency and reliable connectivity are crucial, such as emergency response or sensor networks.

Energy-aware proactive routing protocols represent a strategic evolution of traditional table-driven schemes, embedding energy-conscious mechanisms into the core routing operations. By leveraging adaptive updates, energy-aware link metrics, and selective broadcast strategies, protocols like PE-OLSR, EOLSR, and FEA-DSDV achieve a balance between network longevity and routing performance. However, their effectiveness diminishes in highly dynamic or large-scale networks, highlighting the need for hybrid or reactive approaches in such scenarios.

7.6 Energy-Efficient Reactive Routing Protocols

Reactive routing protocols, also known as on-demand protocols, establish routes only when required by a source node, reducing unnecessary control message overhead. While traditional reactive protocols like AODV and DSR focus on finding the shortest path or fastest route, energy-aware reactive protocols integrate power management strategies into route discovery, maintenance, and selection. This section explores the principles, mechanisms, and representative protocols that optimize energy consumption while maintaining connectivity in dynamic ad hoc networks.

Concept of On-Demand Energy-Aware Routing

Energy-efficient reactive routing relies on dynamic, on-demand mechanisms to discover routes while minimizing energy expenditure. Key principles include:

- Residual Energy Consideration: Nodes with higher remaining battery levels are preferred during route selection, preventing overuse of critically low-energy nodes.
- Energy-Cost Metrics: Routes are evaluated not only by hop count or delay but also by cumulative transmission energy, balancing network load and prolonging node lifetime.
- Adaptive Route Maintenance: Reactive protocols actively monitor energy levels and link stability, triggering local route repairs instead of global rediscovery when possible.

The on-demand nature ensures that energy is consumed primarily during active communication, avoiding continuous table maintenance overhead typical of proactive protocols.

Route Discovery and Maintenance with Energy Consideration

Energy-aware reactive routing protocols enhance traditional route discovery and maintenance processes by incorporating energy metrics:

- Energy-Aware Route Discovery:
    - Route Request (RREQ) messages carry information about residual energy of intermediate nodes.
    - Source nodes select routes that maximize total residual energy or minimize total transmission cost.
- Energy-Conscious Route Maintenance:
    - Nodes monitor battery thresholds and notify upstream nodes if energy drops below a critical level.
    - Alternative paths are selected proactively to avoid network partitions caused by node failure.
- Load Balancing:

- Energy-aware routing avoids repeatedly using the same nodes, distributing forwarding responsibilities across the network.
- This reduces energy hotspots, enhancing network lifetime.

Example Protocols

1. E-AODV (Energy-Aware Ad Hoc On-Demand Distance Vector)

- Extends AODV by incorporating residual energy metrics into route selection.
- During route discovery, nodes evaluate energy cost per hop, prioritizing routes that consume less cumulative power.
- Includes local repair mechanisms to maintain connectivity while conserving energy.

2. EAR (Energy-Aware Routing)

- Focuses on minimizing total energy consumption while maintaining route reliability.
- Employs dynamic power adjustment for transmissions and selects routes with optimal energy profiles.
- Particularly effective in dense networks with frequent route changes.

3. MEA-DSR (Minimum Energy Adaptive DSR)

- Adaptation of DSR with energy-aware route caching.
- Selects paths with minimum total transmission energy while considering node residual battery.
- Maintains multiple alternate routes to enhance stability and reduce rediscovery overhead.

Analysis: Reduced Control Messages vs. Route Stability

Energy-efficient reactive protocols provide a trade-off between reduced control overhead and route stability:

Advantages:

- Lower energy consumption during idle periods compared to proactive approaches.
- Reduced control message dissemination minimizes energy drain in large or dynamic networks.
- Adaptive route maintenance improves network longevity.

Limitations:

- Route discovery latency can be higher than proactive protocols, affecting delay-sensitive applications.
- Frequent topology changes may require repeated energy-aware rediscovery, partially offsetting energy savings.

- Residual energy-based route selection may favor longer paths, increasing end-to-end delay.

Careful tuning of energy thresholds, discovery frequency, and route caching strategies is essential to balance energy efficiency, stability, and performance in reactive routing protocols.

Energy-efficient reactive routing protocols represent a dynamic approach to prolonging network lifetime in mobile ad hoc networks. By incorporating residual energy metrics, adaptive route maintenance, and energy-aware path selection, protocols such as E-AODV, EAR, and MEA-DSR effectively reduce energy consumption while maintaining connectivity. Despite inherent trade-offs between route stability and control message reduction, these protocols are particularly suitable for highly dynamic networks where on-demand communication and energy conservation are critical.

7.7 Cluster-Based and Hierarchical Energy-Efficient Routing

Clustering and hierarchical architectures are widely used in energy-constrained ad hoc and sensor networks to reduce communication overhead, balance energy consumption, and enhance scalability. By organizing nodes into clusters with designated cluster heads (CHs), these routing approaches minimize redundant transmissions, aggregate data efficiently, and prolong network lifetime. This section explores the principles, mechanisms, and representative protocols of cluster-based and hierarchical energy-efficient routing.

Role of Clustering in Minimizing Communication Overhead

Clustering divides the network into smaller, manageable groups of nodes, each governed by a cluster head. The primary benefits of clustering for energy efficiency include:

- Reduced Control Overhead: Instead of every node broadcasting to the entire network, CHs handle intra-cluster communication and forward aggregated data to higher levels or the base station.
- Data Aggregation: Cluster heads combine data from multiple nodes, reducing redundant transmissions and lowering energy consumption.
- Scalability: Clustering allows networks to scale efficiently by limiting the scope of routing and control activities to individual clusters.

By localizing communication and routing, clusters significantly reduce per-node energy expenditure and improve network longevity.

Cluster-Head Selection Based on Residual Energy

Cluster heads play a critical role in energy management, as they handle additional responsibilities including data aggregation, routing, and intra/inter-cluster coordination. Effective CH selection strategies are essential to prevent early depletion of high-load nodes. Common approaches include:

- Residual Energy-Based Selection: Nodes with the highest remaining battery energy are chosen as cluster heads to ensure longer cluster stability.

- Rotating Cluster Heads: Periodically rotating CH roles among nodes distributes energy consumption and prevents localized energy exhaustion.
- Weighted Criteria: Some protocols consider residual energy, node degree, and proximity to neighbors when selecting CHs to optimize both energy and network coverage.

Data Aggregation and Intra/Inter-Cluster Routing

Clustering facilitates efficient data aggregation and hierarchical routing:

- Intra-Cluster Communication: Member nodes transmit data to the CH using short-range, energy-efficient links.
- Inter-Cluster Communication: CHs forward aggregated data to other CHs or a base station using optimized multi-hop routes, reducing redundant transmissions.
- Hierarchical Routing: Multi-level clustering can be employed to further minimize energy use in large networks, with upper-tier CHs handling long-distance transmissions.

This structured approach reduces overall transmission energy while maintaining network connectivity and reliability.

Example Protocols

1. HEED (Hybrid Energy-Efficient Distributed Clustering)

- Selects cluster heads based on residual energy and node degree.
- Periodically rotates CHs to distribute energy consumption evenly.
- Achieves balanced clustering with minimal control message overhead, enhancing network lifetime.

2. LEACH (Low-Energy Adaptive Clustering Hierarchy)

- Randomly selects CHs while ensuring that all nodes take turns serving as cluster heads.
- Employs TDMA scheduling within clusters to avoid collisions and reduce idle energy.
- Uses data aggregation at CHs to minimize transmissions to the base station, significantly saving energy.

3. PEGASIS (Power-Efficient GAthering in Sensor Information Systems)

- Forms chains of nodes rather than traditional clusters, with one node designated to transmit aggregated data to the base station.
- Rotates the leader node to balance energy consumption.
- Reduces the number of transmissions and enhances network lifetime, particularly in sensor networks with fixed topologies.

Balancing Energy Among Cluster Heads

Energy balancing among cluster heads is critical to prevent premature node failures:

- Role Rotation: Periodic reassignment of CH responsibilities distributes energy load evenly.
- Load-Aware CH Selection: Nodes with higher residual energy are favored for leadership roles, while low-energy nodes serve as regular members.
- Dynamic Clustering: Adjusts cluster size and membership based on energy levels and network density, maintaining optimal energy distribution.

Effective energy balancing ensures that no single CH is overburdened, prolonging both cluster stability and overall network lifetime.

Cluster-based and hierarchical energy-efficient routing protocols provide a robust mechanism for reducing communication overhead, aggregating data efficiently, and balancing energy consumption among nodes. Protocols such as HEED, LEACH, and PEGASIS demonstrate how intelligent CH selection, role rotation, and hierarchical routing can extend network lifetime while maintaining reliable connectivity. These strategies are particularly well-suited for large-scale and energy-constrained ad hoc networks, including wireless sensor networks and IoT deployments.

7.8 Geographic and Position-Based Energy Optimization

Geographic or position-based routing protocols leverage location information to make intelligent forwarding decisions, reducing the overhead associated with traditional routing table maintenance. When combined with energy-aware mechanisms, geographic routing can further optimize node energy utilization, avoid energy hotspots, and extend the network lifetime. This section explores how geographic information is integrated with energy metrics, along with representative energy-efficient position-based routing protocols.

Integration of Geographic Routing with Energy Metrics

Geographic routing protocols select the next hop based on physical location relative to the destination, typically aiming to minimize distance or angular deviation. Energy-aware enhancements extend this principle by incorporating residual energy, transmission cost, and energy distribution into routing decisions. Key mechanisms include:

- Residual Energy Consideration: Avoiding nodes with low battery prevents early node failures and energy holes.
- Distance-Energy Trade-off: Next-hop nodes are selected to balance minimal transmission energy with progression toward the destination.
- Localized Decision-Making: Using position and energy information allows distributed, low-overhead routing, reducing global control messages.

By integrating geographic information with energy metrics, these protocols achieve efficient forwarding with minimized energy expenditure.

Power-Aware Next-Hop Selection

In energy-aware geographic routing, next-hop selection is critical:

- Distance Minimization: Nodes closer to the destination reduce cumulative transmission energy.
- Energy Thresholds: Nodes below a predefined residual energy threshold are excluded from selection.
- Load Balancing: Forwarding decisions consider both energy levels and current traffic load to distribute energy consumption evenly across the network.

This approach reduces the likelihood of energy hotspots, which are common in traditional geographic routing when certain nodes repeatedly serve as forwarders.

Geographic Load Balancing and Energy-Hole Avoidance

Energy-hole formation occurs when nodes near data sinks or frequently used paths deplete their energy faster than others. Geographic energy-aware protocols address this by:

- Distributing Forwarding Roles: Nodes with higher energy reserves are preferred for routing, balancing load.
- Adaptive Geographic Zones: Adjusting forwarding regions dynamically to prevent repeated selection of low-energy nodes.
- Multi-Path Geographic Routing: Using alternative geographic paths to share the forwarding burden among multiple nodes.

These strategies maintain network connectivity and avoid early failures in critical regions of the network.

Example Protocols

1. GEAR (Geographic and Energy-Aware Routing)

- Integrates geographic distance and residual energy in the routing metric.
- Uses energy-aware packet forwarding to choose neighbors closest to the destination with sufficient energy.
- Supports load balancing within geographic regions, reducing the likelihood of energy holes.

2. E-GR (Energy-Efficient Geographic Routing)

- Selects forwarding nodes based on residual energy and distance to destination.
- Employs adaptive transmission power to minimize energy consumption while maintaining connectivity.
- Particularly suitable for sensor networks where energy is a critical constraint.

3. EEGRP (Energy-Efficient Geographic Routing Protocol)

- Combines geographic forwarding with energy-aware multipath selection.

- Ensures that energy consumption is distributed across multiple candidate nodes, extending network lifetime.
- Incorporates local route repair to handle mobility and energy depletion dynamically.

Geographic and position-based energy-aware routing protocols demonstrate how location information can be effectively combined with energy metrics to optimize routing decisions in ad hoc networks. Protocols such as GEAR, E-GR, and EEGRP minimize transmission energy, balance load among nodes, and prevent the formation of energy holes, thereby prolonging network lifetime and maintaining reliable connectivity. These protocols are particularly effective in sensor networks, IoT deployments, and large-scale ad hoc systems, where both geographic awareness and energy efficiency are critical.

7.9 Energy-Efficient Multi-Path and Cooperative Routing

Multi-path and cooperative routing strategies are crucial for enhancing energy efficiency, reliability, and load balancing in mobile ad hoc networks. Unlike single-path approaches, multi-path routing distributes traffic across multiple routes, reducing the energy burden on individual nodes and extending network lifetime. Cooperative routing leverages neighboring nodes as relays, improving transmission efficiency and link reliability. This section explores the concepts, mechanisms, and representative protocols of energy-efficient multi-path and cooperative routing.

Concept of Multi-Path Routing for Load Balancing

Energy-efficient multi-path routing establishes multiple alternative routes between a source and destination. The key objectives include:

- Distributing Traffic Load: Spreading packets across multiple paths prevents certain nodes from being overused, avoiding early energy depletion.
- Improving Reliability: Alternate routes provide redundancy, reducing packet loss due to link failures.
- Reducing Congestion: By balancing traffic among several paths, collisions and retransmissions are minimized, conserving energy.

The selection of multi-path routes often considers residual energy, hop count, and link quality, ensuring that energy consumption is optimized across the network.

Energy-Efficient Path Selection and Redundancy Control

Energy-aware multi-path routing protocols incorporate metrics to select optimal paths while controlling redundancy:

- Minimum Total Transmission Power: Routes are chosen to minimize cumulative transmission energy for the entire path.
- Residual Energy Thresholds: Paths containing low-energy nodes are avoided to prevent premature failures.
- Adaptive Redundancy: Only a subset of the available paths is used at a time to reduce unnecessary energy consumption.

This approach balances the benefits of redundancy with energy efficiency, maintaining connectivity without overburdening nodes.

Cooperative Communication and Relay Selection

Cooperative routing leverages neighboring nodes as relays or forwarders to improve communication efficiency:

- Energy-Aware Relay Selection: Relays are chosen based on residual energy, proximity to the destination, and channel conditions, ensuring energy-efficient forwarding.
- Cooperative Diversity: Multiple relays may simultaneously assist in transmission, improving link reliability and reducing retransmissions.
- Load Distribution: Cooperative forwarding spreads traffic among several nodes, reducing localized energy depletion.

These mechanisms enhance both energy efficiency and robustness, especially in networks with high mobility or variable channel conditions.

Example Protocols

1. MTPR (Minimum Total Transmission Power Routing)

- Selects the path that minimizes total transmission power across all hops.
- Balances energy consumption by considering link distances and node power levels.
- Effective in networks where reducing transmission energy is critical for extending node lifetime.

2. CMR (Cooperative Multi-hop Routing)

- Utilizes neighboring nodes as cooperative relays to assist in forwarding data.
- Relay selection considers residual energy and link quality, reducing retransmissions and energy consumption.
- Enhances reliability in dynamic ad hoc environments with frequent link failures.

3. EE-MPR (Energy-Efficient Multi-Path Routing)

- Establishes multiple energy-aware paths between source and destination.
- Balances load among paths to prevent energy hotspots and extend network lifetime.
- Integrates adaptive path selection based on node mobility and residual energy levels.

Energy-efficient multi-path and cooperative routing protocols combine redundancy, load balancing, and intelligent relay selection to enhance network longevity and performance. By distributing traffic across multiple paths and leveraging cooperative forwarding, protocols such as MTPR, CMR, and EE-MPR mitigate energy hotspots, reduce retransmissions, and maintain connectivity in highly dynamic ad hoc networks. These strategies are particularly effective in mission-critical applications, sensor networks, and mobile ad hoc environments where both energy efficiency and reliability are essential.

7.10 QoS-Constrained and Delay-Aware Energy Routing

In modern ad hoc networks, achieving energy efficiency alone is often insufficient, particularly for delay-sensitive or QoS-critical applications such as multimedia streaming, telemedicine, or real-time monitoring. QoS-constrained and delay-aware energy routing protocols aim to balance power conservation with performance requirements, ensuring timely packet delivery while optimizing network energy utilization.

Balancing Energy Conservation with QoS Demands

Energy-aware routing must consider the trade-offs between energy savings and QoS parameters such as end-to-end delay, jitter, throughput, and packet delivery ratio. Key strategies include:

- Energy-Delay Trade-off: Selecting routes that may consume slightly more energy but reduce latency, particularly for time-sensitive data.
- Residual Energy-Aware QoS: Nodes with sufficient energy and high-quality links are prioritized to meet QoS guarantees without compromising network lifetime.
- Adaptive Route Selection: Dynamic routing adjusts paths based on current energy levels, congestion, and link quality, maintaining both energy efficiency and QoS.

Delay-Sensitive and Throughput-Optimized Energy Routing

Protocols in this category integrate energy metrics with delay and throughput considerations:

- Delay Minimization: Paths with fewer hops or faster links are selected, even if total energy consumption is marginally higher.
- Throughput Optimization: Routes are chosen to maximize data transfer efficiency while maintaining balanced energy utilization across nodes.
- Traffic-Aware Energy Management: Packet priorities and data rates influence power allocation and forwarding decisions, preventing bottlenecks and congestion-related energy waste.

Priority-Aware and Application-Specific Power Control

QoS-aware energy routing often implements application-specific mechanisms:

- Priority-Based Forwarding: Critical packets (e.g., emergency alerts) are routed via energy-efficient yet low-latency paths.

- Adaptive Transmission Power: Power levels are adjusted based on packet importance and required QoS, conserving energy for less critical traffic.
- Service Differentiation: Energy allocation and routing decisions are tailored to the type of application, ensuring optimal performance without unnecessary energy expenditure.

Protocol Examples

1. QEM (QoS Energy Management)

- Integrates residual energy metrics with QoS requirements such as delay and packet delivery ratio.
- Prioritizes low-energy-consuming paths while ensuring QoS for critical flows.
- Employs dynamic route adjustment to maintain energy and QoS balance under mobility or traffic fluctuations.

2. EEQR (Energy-Efficient QoS Routing)

- Combines energy-aware metrics with QoS constraints in route selection.
- Implements priority-aware routing, ensuring delay-sensitive packets reach destinations promptly.
- Balances energy consumption across nodes while maintaining throughput and latency guarantees.

QoS-constrained and delay-aware energy routing protocols address the dual challenge of conserving energy while meeting application-specific performance requirements. By incorporating delay, throughput, and priority considerations into energy-aware routing, protocols such as QEM and EEQR ensure efficient, reliable, and timely data delivery. These mechanisms are especially crucial for real-time, multimedia, and mission-critical applications in ad hoc networks, where energy efficiency must coexist with stringent QoS demands.

7.11 Conclusion

This chapter provided a comprehensive overview of energy-efficient routing protocols in mobile ad hoc networks (MANETs) and other wireless networks, emphasizing the critical role of energy conservation in prolonging network lifetime and ensuring sustainable operation. The key points covered in this chapter include:

- Principles of Energy-Efficient Routing: Energy-aware routing integrates residual node energy, transmission cost, and load balancing into routing decisions. Protocols aim to minimize unnecessary control overhead, retransmissions, and idle energy consumption. Cross-layer design and adaptive power control are essential mechanisms for maximizing energy efficiency.
- Classification of Energy-Efficient Routing Protocols: Protocols were categorized based on routing strategy (proactive, reactive, hybrid), network layer focus (MAC-layer, network-layer, cross-layer), and optimization objectives (minimum energy, load balancing, lifetime-maximizing, QoS-constrained).

- Each classification highlights distinct trade-offs between energy savings, routing performance, and network longevity.
- Energy-Aware Protocols Across Different Approaches: Proactive protocols (e.g., PE-OLSR, EOLSR, FEA-DSDV) optimize periodic table updates and residual energy-based route selection. Reactive protocols (e.g., E-AODV, EAR, MEA-DSR) balance energy consumption with on-demand route discovery, reducing unnecessary control message overhead.

Cluster-based and hierarchical protocols (e.g., LEACH, HEED, PEGASIS) reduce communication overhead through data aggregation and energy-aware cluster-head rotation. Geographic and position-based routing (e.g., GEAR, E-GR, EEGRP) leverage location information for energy-efficient forwarding and load balancing. Multi-path and cooperative routing (e.g., MTPR, CMR, EE-MPR) distribute traffic load and utilize cooperative relays to enhance energy efficiency and reliability. QoS-constrained and delay-aware routing (e.g., QEM, EEQR) ensure energy savings while meeting delay, throughput, and application-specific requirements.

References

1. Singh, S., & Raghavendra, C. S. (1998). PAMAS: Power aware multi-access protocol with signaling for ad hoc networks. *ACM SIGCOMM Computer Communication Review, 28*(3), 5–26. https://doi.org/10.1145/293927.293928
2. Chang, J. H., & Tassiulas, L. (2000). Energy conserving routing in wireless ad-hoc networks. *Proceedings IEEE INFOCOM 2000*, 1, 22–31. https://doi.org/10.1109/INFCOM.2000.832170
3. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, 1–10. https://doi.org/10.1109/HICSS.2000.926982
4. Toh, C. K. (2001). Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks. *IEEE Communications Magazine, 39*(6), 138–147. https://doi.org/10.1109/35.925682
5. Yu, C., Lee, B., & Youn, H. Y. (2003). Energy efficient routing protocols for mobile ad hoc networks. *Wireless Communications and Mobile Computing, 3*(8), 959–973. https://doi.org/10.1002/wcm.119
6. Li, Q., Aslam, J., & Rus, D. (2001). Online power-aware routing in wireless ad-hoc networks. *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom)*, 97–107. https://doi.org/10.1145/381677.381690
7. Banerjee, S., & Misra, A. (2002). Minimum energy paths for reliable communication in multi-hop wireless networks. *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc)*, 146–156. https://doi.org/10.1145/513800.513820
8. Rodoplu, V., & Meng, T. H. (1999). Minimum energy mobile wireless networks. *IEEE Journal on Selected Areas in Communications, 17*(8), 1333–1344. https://doi.org/10.1109/49.779917

9. Lindsey, S., Raghavendra, C., & Sivalingam, K. (2002). Data gathering algorithms in sensor networks using energy metrics. *IEEE Transactions on Parallel and Distributed Systems, 13*(9), 924–935. https://doi.org/10.1109/TPDS.2002.1036066
10. Lindsey, S., & Raghavendra, C. S. (2002). PEGASIS: Power-efficient gathering in sensor information systems. *IEEE Aerospace Conference Proceedings, 3*, 1125–1130. https://doi.org/10.1109/AERO.2002.1035242
11. Younis, O., & Fahmy, S. (2004). HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Transactions on Mobile Computing, 3*(4), 366–379. https://doi.org/10.1109/TMC.2004.41
12. Chen, B., Jamieson, K., Balakrishnan, H., & Morris, R. (2001). SPAN: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks. *Wireless Networks, 8*(5), 481–494. https://doi.org/10.1023/A:1016542229220
13. Ganesan, D., Govindan, R., Shenker, S., & Estrin, D. (2001). Highly-resilient, energy-efficient multipath routing in wireless sensor networks. *ACM SIGMOBILE Mobile Computing and Communications Review, 5*(4), 11–25. https://doi.org/10.1145/509506.509514
14. Misra, S., & Woungang, I. (2009). Energy-efficient cross-layer design for wireless ad hoc networks. *Ad Hoc Networks, 7*(6), 1048–1059. https://doi.org/10.1016/j.adhoc.2008.10.005
15. Shah, R. C., & Rabaey, J. M. (2002). Energy aware routing for low energy ad hoc sensor networks. *IEEE Wireless Communications and Networking Conference (WCNC)*, 1, 350–355. https://doi.org/10.1109/WCNC.2002.993520
16. Ghosh, A., & Basagni, S. (2006). Mitigating the impact of mobility on ad hoc clustering. *Wireless Communications and Mobile Computing, 6*(4), 469–482. https://doi.org/10.1002/wcm.396
17. Li, X., Frey, H., & Nikoletseas, S. (2012). Energy-efficient data collection and aggregation in wireless sensor networks. *ACM Computing Surveys, 45*(1), 1–38. https://doi.org/10.1145/2379776.2379778
18. Batra, P., & Kant, K. (2016). LEACH-MAC: A new cluster head selection algorithm for WSNs. *Wireless Personal Communications, 90*(4), 1891–1909. https://doi.org/10.1007/s11277-016-3439-1
19. Kumar, R., & Chauhan, M. (2021). Energy-efficient QoS aware routing in MANETs using particle swarm optimization. *Wireless Networks, 27*(7), 4545–4562. https://doi.org/10.1007/s11276-021-02632-1
20. Kannan, K. R., & Rajendran, V. (2024). Energy efficient routing technique using enthalpy ant net in mobile ad hoc networks. *Journal of Electrical Engineering & Technology, 19*(1), 1–9. https://doi.org/10.1007/s42835-023-00075-3

ISBN: 978-93-47475-17-7

Chapter-8

QoS-Aware Routing: Ensuring Reliability and Performance

[1]R.Yanitha,[2] Dr.M.Logambal,

[1]Research Scholar, Department of Computer Science,
Vellalar College for Women,Thindal, Erode, Tamilnadu,India.

[2]Associate Professor, Department of Computer Science,
Vellalar College for Women, Thindal, Erode, Tamilnadu,India.

Abstract: *Quality of Service (QoS)-aware routing plays a crucial role in modern communication networks by ensuring reliable data transmission, optimal performance, and efficient resource utilization. This chapter explores the fundamental principles, mechanisms, and algorithms that enable routing protocols to meet specific QoS requirements such as bandwidth, latency, jitter, and packet loss. It delves into the integration of QoS metrics in traditional and next-generation networks, including wireless sensor networks, mobile ad hoc networks (MANETs), and software-defined networks (SDNs). Emphasis is placed on adaptive and intelligent routing approaches that dynamically adjust to changing network conditions, ensuring end-to-end service reliability and user satisfaction. Additionally, the chapter discusses multi-constraint optimization, cross-layer design, and machine learning-driven routing strategies that enhance decision-making in complex, heterogeneous network environments. Through case studies and performance evaluations, readers will gain a comprehensive understanding of how QoS-aware routing underpins the efficiency, scalability, and robustness of contemporary communication systems.*

Keywords: *QoS-aware routing, reliability, performance optimization, latency, bandwidth, jitter, packet loss, adaptive routing, cross-layer optimization, multi-constraint routing, traffic engineering, machine learning, dynamic path selection.*

8.1 Introduction

In mobile ad hoc networks (MANETs) and wireless communication systems, Quality of Service (QoS) has become a critical design objective for supporting applications that demand consistent performance, reliability, and timely data delivery. Unlike traditional wired networks, where stable links and predictable bandwidth are available, ad hoc networks operate in highly dynamic and decentralized environments, where node mobility, fluctuating link quality, and limited resources make QoS provisioning a complex challenge.

The growing integration of multimedia, real-time, and mission-critical applications—such as video conferencing, VoIP, remote sensing, and intelligent vehicular systems—has intensified the need for QoS-aware routing mechanisms. These applications require guarantees on key performance metrics, including bandwidth, end-to-end delay, jitter, and packet loss rate, to maintain acceptable service quality and user experience. Hence, routing decisions must not only ensure reachability but also meet these quantitative service constraints.

Conventional best-effort routing protocols, such as AODV and DSR, focus solely on connectivity without considering service differentiation or resource constraints. As a result, they often fail to deliver the reliability and performance required by delay-sensitive traffic in dynamic network conditions. To overcome these limitations, QoS-aware routing protocols incorporate mechanisms for resource reservation, admission control, adaptive link estimation, and cross-layer coordination to dynamically optimize routing paths according to the current network state.

The motivation for developing QoS-aware routing lies in the need to balance resource utilization with performance guarantees, enabling efficient bandwidth management, congestion control, and adaptive link selection under variable network topologies. This integration ensures that ad hoc networks can support emerging applications with diverse service requirements, thereby enhancing overall network reliability, scalability, and user satisfaction.

8.2 Fundamentals of QoS in Ad Hoc Networks

Quality of Service (QoS) in ad hoc networks refers to the capability of a communication system to provide **predictable and measurable service performance** to meet the diverse needs of different applications. It encompasses both **qualitative and quantitative metrics**, including parameters such as throughput, delay, jitter, bandwidth, and packet delivery ratio, which together determine the overall efficiency and reliability of data transmission. While **qualitative QoS metrics** focus on user-perceived satisfaction and service acceptability, **quantitative metrics** provide measurable values that help evaluate network performance under various traffic and mobility conditions.

The **relationship between routing and service quality** is fundamental to achieving QoS objectives. In ad hoc networks, routing protocols not only determine the optimal paths between source and destination nodes but also influence delay, congestion, and link stability—all of which directly impact QoS performance. Effective routing decisions must therefore account for link capacity, residual node energy, buffer occupancy, and traffic priority to ensure consistent service delivery across fluctuating network conditions.

QoS requirements in ad hoc networks can be broadly classified into **soft QoS** and **hard QoS** categories. **Soft QoS** allows flexible service guarantees, tolerating slight variations in delay or bandwidth, which is suitable for non-critical applications. In contrast, **hard QoS** provides strict guarantees on resource availability and end-to-end performance, essential for real-time and safety-critical applications such as military operations or emergency communications.

Due to **resource constraints** such as limited bandwidth, energy, and processing capability, achieving end-to-end QoS in MANETs involves significant trade-offs. Enhancing one QoS metric (e.g., reducing delay) may compromise others (e.g., energy efficiency or throughput). Hence, an optimal balance is necessary to maintain overall system performance and fairness among competing nodes.

ISBN: 978-93-47475-17-7

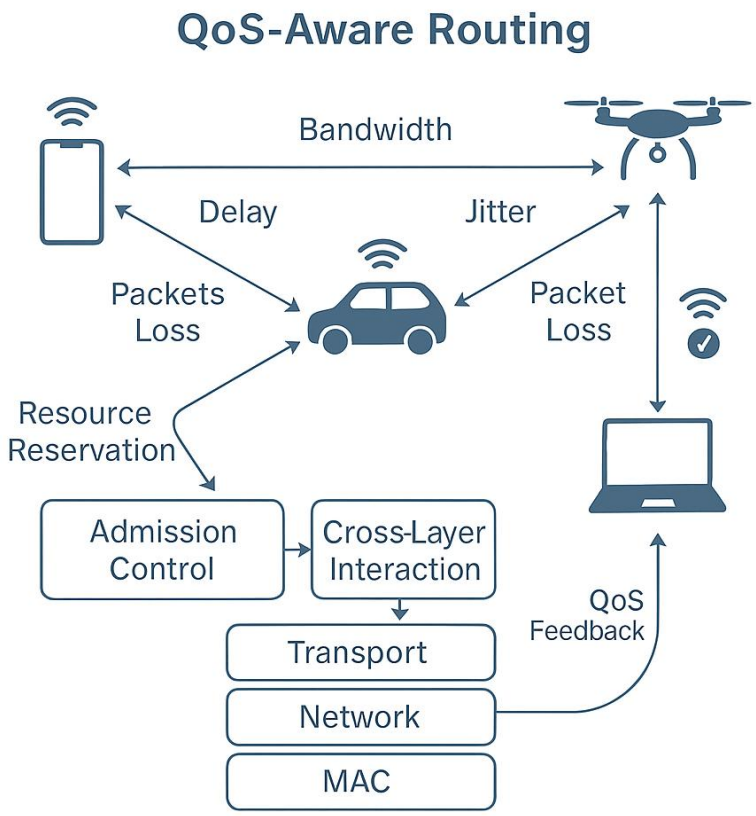


Figure 1: Architecture of QoS-Aware Routing in Mobile Ad Hoc Networks

To ensure reliable QoS delivery, mechanisms like **admission control** and **resource reservation** are employed. **Admission control** determines whether a new data flow can be accommodated without degrading existing services, while **resource reservation protocols** allocate bandwidth and buffer space to high-priority flows. Together, these mechanisms form the backbone of QoS management in ad hoc networks, enabling dynamic adaptation to varying network conditions and sustaining consistent service quality across distributed, mobile environments (Figure 1).

8.3 QoS Routing Design Goals and Challenges

The primary goal of **QoS routing in ad hoc networks** is to guarantee **end-to-end service reliability** by ensuring that communication requirements such as bandwidth, latency, packet delivery ratio, and jitter are consistently met. Unlike traditional best-effort routing, QoS-based approaches strive to provide predictable performance for multimedia and real-time applications, which demand stable transmission rates and minimal data loss. This requires routing protocols to dynamically assess network resources, establish optimal paths that meet predefined QoS constraints, and maintain them throughout the data transmission process.

One of the foremost challenges in QoS routing lies in **maintaining service quality under mobility and frequent topology changes**. In mobile ad hoc networks (MANETs), nodes

move unpredictably, leading to frequent link breakages and route rediscoveries. Such instability disrupts the continuity of QoS parameters like delay and throughput. Therefore, routing algorithms must be highly adaptive, capable of quickly detecting topology variations, and able to reroute traffic without significantly affecting the overall QoS performance.

Another essential design consideration is **scalability and adaptability**. As the size and density of an ad hoc network increase, maintaining efficient QoS routing becomes more complex due to rising control overhead and contention for limited resources. Scalable QoS routing protocols must minimize signaling costs while ensuring that routing decisions remain responsive to changes in node density, mobility, and traffic load. Adaptability further ensures that the network can adjust its QoS strategies in response to varying environmental conditions and heterogeneous service demands.

A critical challenge arises from the **trade-off between energy efficiency and QoS satisfaction**. High QoS levels often require continuous monitoring, frequent route updates, and increased transmission power—all of which consume significant energy. Conversely, conserving energy may lead to reduced throughput or higher delay. Achieving a balanced design that simultaneously enhances QoS and extends node lifetime is, therefore, a central research concern in modern ad hoc routing protocols.

For evaluating QoS performance, various **QoS metrics** are employed, including **throughput**, **end-to-end delay**, **packet loss ratio (PLR)**, **jitter**, and **Mean Opinion Score (MOS)**. Throughput measures the successful data delivery rate, delay captures transmission latency, PLR quantifies data loss, jitter represents delay variation, and MOS reflects the perceived user experience, particularly in voice and video transmissions. Together, these metrics provide a comprehensive framework for assessing how effectively a routing protocol fulfills QoS objectives under real-world network dynamics.

8.4 QoS Routing Architectures and Models

The design of **QoS routing architectures** in ad hoc networks revolves around structuring mechanisms that can effectively allocate, manage, and maintain service quality despite the inherent challenges of decentralized and dynamic environments. Two fundamental architectural paradigms dominate QoS provisioning: the **integrated service (IntServ)** model and the **differentiated service (DiffServ)** model. The IntServ model operates on a **per-flow resource reservation basis**, ensuring that each data flow receives the necessary bandwidth and delay guarantees through protocols such as the Resource Reservation Protocol (RSVP). Although IntServ offers fine-grained QoS control, its reliance on per-flow state maintenance introduces significant overhead, making it less suitable for large-scale or highly mobile networks. Conversely, the DiffServ model provides **class-based QoS management**, categorizing traffic into priority classes with predefined service levels. This approach

reduces complexity and signaling load, enhancing scalability and adaptability in ad hoc network scenarios.

A key advancement in QoS routing comes from the **integration of cross-layer interactions**, where information from different layers of the network stack—such as the physical, MAC, and network layers—is jointly utilized to enhance QoS assurance. For instance, link quality indicators, signal strength, and energy levels can inform routing decisions, while routing feedback may influence MAC-layer scheduling or transmission power adjustments. This **cross-layer design paradigm** enables adaptive routing behaviors that respond dynamically to fluctuating network conditions, thereby maintaining consistent QoS performance even under high mobility or variable link quality.

The **role of middleware and policy-based QoS frameworks** is equally critical in supporting end-to-end service differentiation and coordination. Middleware acts as an intermediary layer that abstracts underlying network complexities and enforces QoS policies across heterogeneous devices and applications. Policy-based frameworks, on the other hand, enable dynamic decision-making by defining rules for resource allocation, admission control, and traffic prioritization. These systems ensure that QoS objectives are aligned with application requirements, user preferences, and network capabilities, contributing to an intelligent and context-aware routing infrastructure.

Additionally, **distributed resource reservation mechanisms** play a vital role in achieving QoS without centralized control. Since ad hoc networks lack fixed infrastructure, nodes must cooperate to reserve and manage resources locally. Techniques such as soft-state reservations and hop-by-hop negotiation allow intermediate nodes to commit bandwidth or buffer resources temporarily, supporting real-time data flows with minimal signaling overhead. This distributed approach enhances flexibility and fault tolerance, essential in dynamic network environments.

Finally, **admission control and feedback-based QoS monitoring** ensure the ongoing reliability of QoS guarantees. Admission control mechanisms evaluate whether new data flows can be accommodated without violating existing QoS commitments, thus preventing congestion and performance degradation. Meanwhile, feedback-based monitoring continuously assesses network conditions—such as delay, packet loss, and throughput—to adapt routing and resource allocation dynamically. Together, these processes create a **closed-loop QoS management system**, maintaining consistent service quality even in unpredictable and resource-constrained ad hoc networks.

8.5 Classification of QoS-Aware Routing Protocols

Quality of Service (QoS)-aware routing protocols in ad hoc networks are classified according to their **routing strategy**, **QoS parameters**, and **network architecture**. This classification framework helps in understanding how different protocols balance the trade-offs between performance, scalability, and adaptability to dynamic network conditions. Each category emphasizes unique mechanisms for guaranteeing service quality—whether through pre-

emptive route establishment, on-demand path computation, or hierarchical resource organization—ensuring that diverse application requirements such as real-time multimedia transmission, data reliability, and load balancing are effectively met.

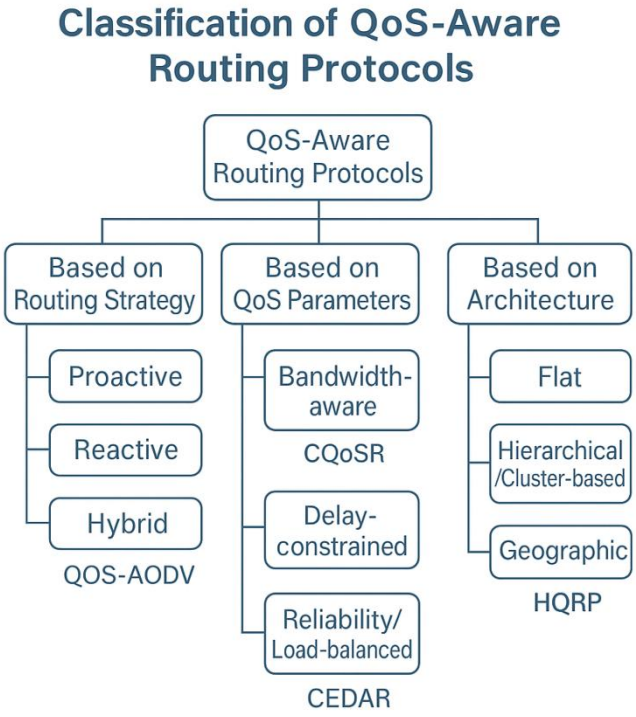


Figure 2: Taxonomy of QoS-Aware Routing Protocols in Ad Hoc Networks

Based on **routing strategy**, QoS-aware routing protocols are typically grouped into **proactive**, **reactive**, and **hybrid** approaches. **Proactive QoS routing protocols** maintain up-to-date routing tables with precomputed paths for all possible destinations. These protocols, such as QoS-extended versions of OLSR or DSDV, provide low-latency data delivery by ensuring immediate route availability. However, the continuous exchange of control messages increases bandwidth and energy consumption, which can be a limitation in mobile environments. **Reactive QoS routing protocols**, on the other hand, establish routes only when data transmission is required. Protocols like QoS-AODV and CEDAR (Core-Extraction Distributed Ad Hoc Routing) dynamically discover routes that meet specific QoS constraints such as bandwidth or delay. This on-demand nature reduces overhead but may introduce initial route discovery delays. **Hybrid QoS routing protocols** combine the strengths of both proactive and reactive methods—maintaining limited topology information while using on-demand mechanisms for distant nodes. This hybrid approach enhances scalability and responsiveness, particularly in heterogeneous and large-scale networks (Figure 2).

When classified based on **QoS parameters**, routing protocols can be categorized as **bandwidth-aware**, **delay-constrained**, or **reliability and load-balanced** routing schemes. **Bandwidth-aware routing** ensures that sufficient transmission capacity is available along the selected path to accommodate multimedia or high-data-rate applications. Techniques

like resource reservation and dynamic bandwidth estimation are employed to prevent congestion and packet loss. **Delay-constrained routing** focuses on minimizing end-to-end latency to meet the timing requirements of real-time services such as video conferencing and VoIP. These protocols use link-delay estimation and priority queuing to maintain predictable transmission times. Meanwhile, **reliability and load-balanced routing** aims to enhance data delivery success rates and distribute traffic evenly across the network, preventing energy depletion and bottlenecks in heavily used nodes. Multi-path routing and redundancy-based mechanisms are often integrated to improve fault tolerance and maintain consistent QoS under dynamic network conditions.

From the perspective of **network architecture**, QoS routing can be implemented through **flat**, **hierarchical**, **cluster-based**, or **geographic** models. **Flat QoS routing protocols** treat all nodes equally, relying on distributed coordination to make routing decisions. While simple and flexible, this approach may struggle with scalability in dense networks. **Hierarchical or cluster-based QoS routing** organizes nodes into clusters or logical layers, where cluster heads manage local routing and resource allocation. Protocols such as Cluster-based QoS Routing (CQoSR) and Hierarchical QoS-Aware Routing Protocols (HQRP) enhance scalability by localizing control overhead and facilitating efficient resource management. **Geographic QoS-aware routing** integrates location information into the routing process, using node positions and link distances to select paths that optimize both QoS and energy efficiency. By combining geographic awareness with QoS constraints, these protocols achieve efficient packet forwarding, reduced latency, and lower routing overhead in position-aware ad hoc and vehicular networks.

The classification of QoS-aware routing protocols reveals the diversity of approaches used to address the unique challenges of ad hoc networking. Whether through proactive state maintenance, on-demand path discovery, or hybrid adaptability, each protocol type represents a distinct balance between responsiveness, reliability, and efficiency. Similarly, parameter-based and architecture-based classifications highlight how different network conditions and application requirements shape the design of QoS routing solutions for optimal performance and service continuity.

8.6 Proactive QoS-Aware Routing Protocols

Proactive QoS-aware routing protocols play a critical role in maintaining consistent and reliable communication in ad hoc networks by continuously updating and distributing routing information across nodes. Unlike on-demand routing schemes, proactive protocols maintain real-time knowledge of network topology and resource availability through periodic control message exchanges. This approach ensures that routes satisfying Quality of Service (QoS) requirements—such as bandwidth, delay, and reliability—are readily available whenever data transmission is initiated. The proactive nature of these protocols minimizes route discovery latency and provides predictable service quality, which is particularly beneficial for delay-sensitive and real-time applications like video streaming and voice over IP. However, the continuous exchange of routing information introduces

control overhead and additional energy consumption, especially in highly dynamic or dense networks, which must be carefully managed through adaptive and efficient table maintenance strategies.

One of the most studied proactive QoS routing protocols is the **Quality of Service Optimized Link State Routing (QoS-OLSR)** protocol. Building upon the foundation of the traditional OLSR, QoS-OLSR integrates link-quality metrics—such as available bandwidth, link delay, and packet delivery ratio—into its route computation process. The protocol employs **Multipoint Relays (MPRs)** to optimize the dissemination of control messages and to minimize broadcast redundancy, while also ensuring that the chosen routes meet specific QoS constraints. By combining proactive topology discovery with QoS-driven link evaluation, QoS-OLSR achieves efficient bandwidth utilization and reduced end-to-end delay. However, its periodic updates can lead to increased energy consumption in large or fast-changing topologies.

Another notable proactive QoS-aware routing approach is **CEDAR (Core-Extraction Distributed Ad hoc Routing)**, which provides a hybrid form of proactive resource management within a distributed network. CEDAR introduces the concept of a "core" infrastructure composed of a subset of nodes responsible for maintaining local topology and bandwidth information. Route discovery and maintenance are performed within this core, significantly reducing control overhead compared to fully distributed approaches. The protocol supports dynamic bandwidth estimation and localized route repair, ensuring that path selection adheres to the bandwidth and delay constraints of QoS applications. CEDAR's combination of proactive core maintenance and localized on-demand updates makes it well-suited for scalable and efficient QoS provisioning in dynamic environments.

The **QOLSR-E (Enhanced QoS OLSR)** protocol further improves upon traditional QoS-OLSR mechanisms by incorporating adaptive link-quality assessment and cross-layer feedback. QOLSR-E utilizes metrics derived from the physical and MAC layers, such as signal-to-noise ratio (SNR) and residual node energy, to make more informed routing decisions. This cross-layer enhancement improves reliability and energy efficiency, ensuring that the network can maintain QoS performance even under mobility and interference conditions. The adaptive update frequency mechanism in QOLSR-E also helps reduce control message overhead by adjusting periodic update intervals based on network stability and mobility rates.

Despite their effectiveness in guaranteeing low-latency and consistent QoS support, **proactive QoS-aware routing protocols** face several trade-offs. The primary advantage of proactive mechanisms lies in their **immediate route availability** and **predictable performance**, which are essential for applications requiring guaranteed service levels. However, maintaining updated routing tables through frequent control exchanges increases **bandwidth consumption**, **energy usage**, and **processing overhead**, particularly in large or highly mobile networks. Additionally, stale routing information can still occur in rapidly

changing topologies, leading to temporary QoS degradation. Balancing between update frequency, control overhead, and network responsiveness remains a key design challenge.

The proactive QoS-aware routing protocols such as QoS-OLSR, CEDAR, and QOLSR-E demonstrate the potential of periodic table-driven routing in achieving consistent QoS guarantees across dynamic ad hoc networks. By leveraging continuous topology awareness and resource monitoring, these protocols ensure stable and efficient data delivery while meeting application-specific QoS constraints. Nonetheless, optimizing their scalability and energy efficiency remains essential for their successful deployment in large-scale, mobile, and heterogeneous wireless environments.

8.7 Hybrid and Cross-Layer QoS Routing

Hybrid and cross-layer QoS routing protocols represent an advanced evolution in the design of Quality of Service mechanisms for ad hoc and wireless networks. These approaches combine the advantages of both proactive and reactive routing strategies while leveraging information exchange between different network layers to optimize performance and stability. The integration of hybrid routing mechanisms allows for adaptive route management—proactive maintenance of stable links in local zones and reactive discovery for distant or rapidly changing regions. Meanwhile, cross-layer designs enable the routing layer to utilize information from the MAC, physical (PHY), and transport layers, resulting in more accurate decision-making regarding bandwidth, signal quality, link stability, and congestion levels. Together, hybrid and cross-layer QoS routing schemes improve reliability, adaptability, and resource utilization in highly dynamic mobile environments.

In **hybrid QoS routing**, the key objective is to balance control overhead with timely route availability. By combining proactive and reactive strategies, these protocols maintain updated local topology information while discovering routes on demand for remote nodes. For example, a **Hybrid QoS Routing (HQR)** protocol proactively maintains QoS metrics such as available bandwidth, delay, and jitter for nearby nodes, ensuring rapid communication within localized regions. When communication extends beyond these regions, reactive discovery mechanisms are triggered to establish end-to-end paths that satisfy the required QoS constraints. This dual operation significantly reduces route discovery latency compared to purely reactive schemes while minimizing control overhead relative to fully proactive methods. Hybrid QoS routing thus enhances scalability and efficiency, especially in large, heterogeneous ad hoc networks with variable node mobility.

Cross-layer QoS routing takes optimization a step further by facilitating real-time interaction among network layers. Traditionally, the OSI model enforces strict layer separation; however, in resource-constrained and mobile ad hoc environments, such isolation can limit performance. Cross-layer designs enable the routing protocol to dynamically adapt based on lower-layer information such as **signal-to-noise ratio (SNR)**, **channel interference**, **residual energy**, and **queue length**. The **Cross-Layer QoS Management (CLQM)** framework is a notable example that integrates feedback from the

MAC and physical layers into the routing process. CLQM continuously monitors channel quality, bandwidth availability, and traffic load to adjust transmission power and route selection. This ensures that data flows receive stable and high-quality paths that comply with QoS demands while conserving energy and reducing packet loss due to channel degradation.

Similarly, the **Cross-Layer Admission Control Protocol (CACP)** focuses on maintaining QoS stability through intelligent resource reservation and traffic regulation. By coordinating between the MAC and network layers, CACP evaluates the feasibility of admitting new data flows without violating the QoS requirements of existing sessions. The protocol dynamically estimates network resource utilization, preventing congestion and ensuring fair distribution of bandwidth among competing flows. This admission control mechanism is essential for supporting real-time applications and multimedia services that are sensitive to delay and jitter in ad hoc and wireless mesh networks.

Cross-layer and hybrid routing paradigms also enhance adaptability by allowing the routing process to respond swiftly to **link variations**, **mobility-induced disruptions**, and **traffic dynamics**. Unlike traditional approaches that rely solely on static metrics, cross-layer protocols dynamically adjust route selection and resource allocation according to current network conditions. This adaptability translates to improved throughput, lower end-to-end delay, and higher packet delivery ratios, thereby strengthening overall QoS assurance. However, designing cross-layer architectures requires careful coordination to avoid excessive inter-layer dependencies, which could increase complexity and reduce modularity.

In summary, **hybrid and cross-layer QoS routing protocols** such as HQR, CLQM, and CACP demonstrate the potential for achieving more robust and adaptive QoS provisioning in mobile ad hoc networks. By combining proactive and reactive elements with multi-layer information sharing, these protocols can dynamically balance performance trade-offs related to delay, bandwidth, and energy consumption. The **benefits of cross-layer optimization**—including enhanced route stability, efficient resource utilization, and improved resilience to topology changes—make these approaches highly suitable for next-generation wireless networks that demand reliable, real-time, and scalable QoS support.

8.8 Bandwidth and Delay-Constrained Routing

Bandwidth and delay-constrained routing focuses on ensuring that data flows in ad hoc networks meet specific Quality of Service (QoS) requirements related to transmission capacity and latency. These protocols incorporate mechanisms for bandwidth estimation and reservation, allowing nodes to evaluate available channel capacity before route establishment. At the same time, delay-aware path computation techniques are employed to minimize end-to-end latency, ensuring timely data delivery for real-time applications such as video streaming and VoIP.

Among the notable examples, DSR-B (Bandwidth-constrained Dynamic Source Routing) extends the traditional DSR by integrating bandwidth metrics into the route discovery process, ensuring that selected paths can support the required data rate. DSDV-Delay (Delay-aware Destination-Sequenced Distance Vector) enhances DSDV by prioritizing routes with lower transmission and queuing delays, thereby improving service quality for time-sensitive traffic. QELAR (QoS and Energy-aware Link Adaptive Routing) further optimizes both bandwidth and delay by dynamically adjusting routes based on real-time link conditions and residual energy, striking a balance between QoS and network lifetime. Overall, bandwidth and delay-constrained routing protocols are essential for real-time traffic support in mobile ad hoc networks, enabling efficient and reliable data delivery even under dynamic topological and resource conditions.

8.9. QoS Routing in Heterogeneous and Multimedia Networks

QoS routing in heterogeneous and multimedia networks addresses the diverse service requirements of applications such as voice, video, and IoT data, which demand low latency, high reliability, and consistent bandwidth. These networks often consist of links with varying characteristics—differing in capacity, delay, and reliability—requiring adaptive QoS provisioning that can dynamically select routes based on current link performance and traffic demands. Protocols like MMQR (Multimedia QoS Routing) optimize path selection by considering both QoS parameters and network congestion, ensuring smooth delivery of multimedia streams. Similarly, QOS-MANET, designed for 5G-based edge environments, integrates real-time QoS assessment and resource allocation to handle heterogeneous traffic and variable data rates efficiently. By dynamically managing reliability constraints and adapting to changing network conditions, these QoS routing protocols enable robust support for multimedia and IoT applications in complex, resource-constrained ad hoc environments.

8.10 Future Research Directions

Future research in QoS-aware routing is increasingly focused on integrating artificial intelligence (AI) and machine learning to predict network conditions, optimize routing decisions, and dynamically allocate resources for improved service quality. Emerging technologies, such as 5G, 6G, and IoT-integrated MANETs, present new opportunities and challenges for maintaining QoS across heterogeneous and high-mobility networks. Software-defined and cognitive QoS routing approaches promise flexible and intelligent network management, enabling real-time adaptation to changing traffic patterns and environmental conditions. Additionally, ensuring QoS while addressing security and energy constraints remains a critical research direction, particularly in resource-limited ad hoc networks. Finally, the development of self-adaptive QoS management systems that can autonomously respond to topology changes, varying link conditions, and fluctuating traffic demands is essential for achieving robust, reliable, and scalable service delivery in next-generation wireless networks.

8.11. Conclusion

This chapter provided a comprehensive overview of QoS-aware routing in ad hoc networks, highlighting the fundamental concepts, classifications, and architectural models designed to ensure reliable and high-performance communication. Various routing strategies—including proactive, reactive, hybrid, and cross-layer approaches—were examined, along with protocols that address bandwidth, delay, and reliability constraints in both homogeneous and heterogeneous network environments. Key insights into protocol comparisons and performance trade-offs demonstrated how routing decisions influence end-to-end delay, throughput, energy consumption, and packet delivery, emphasizing the importance of balancing these factors in dynamic networks. The chapter also explored advanced applications such as multimedia traffic support, real-time data flows, and IoT integration, underscoring the need for adaptive and scalable QoS mechanisms. Finally, the discussion highlighted emerging trends, including AI-driven optimization, 5G/6G network integration, and self-adaptive QoS management, setting the stage for the next chapter on Delay-Tolerant and Opportunistic Routing in Ad Hoc Networks.

References

1. Agrawal, R. (2023). Classification and comparison of ad hoc networks: A review. *Journal of Network and Computer Applications, 198*, 103387. https://doi.org/10.1016/j.jnca.2022.103387
2. Ali, A. M. (2023). Enhanced QoS routing protocol for an unmanned ground vehicle network. *Sensors, 23*(3), 1431. https://doi.org/10.3390/s23031431
3. Belamri, F., & Boudjit, A. (2021). A survey on QoS routing protocols in vehicular ad hoc networks. *Telecommunication Systems, 78*(1), 1–17. https://doi.org/10.1007/s11235-021-00797-8
4. Chakraborty, S., & Rohilla, V. (2025). A survey on QoS in flying ad hoc networks based on fuzzy inference-based routing protocol. *ResearchGate*. https://www.researchgate.net/publication/379556343_A_Survey_on_QoS_in_Flying_Ad_Hoc_Network_based_on_Fuzzy_Inference_Based_Routing_Protocol
5. Dang, A. V., & Dang, T. H. (2022). Performance analysis of typical routing protocols for cognitive radio ad hoc networks. *Journal of Communications and Networks, 24*(5), 505–515. https://doi.org/10.1109/JCN.2022.000070
6. Goyal, P. (2023). A comprehensive survey on QoS for video transmission in hybrid mobile ad hoc networks. *International Journal of Communication Systems, 36*(1), e4775. https://doi.org/10.1002/ett.4775
7. Ivascu, G. I., & Ivascu, M. (2009). QoS routing with traffic distribution in mobile ad hoc networks. *Computer Communications, 32*(4), 755–765. https://doi.org/10.1016/j.comcom.2008.12.011
8. Ivanov, V. (2023). Cross-layer methods for ad hoc networks: Review and future directions. *Preprints*. https://doi.org/10.20944/preprints202312.0556.v1

9. Jiang, M., & Tay, Y. C. (1998). Cluster-based routing protocol (CBRP) for mobile ad hoc networks. *IETF Internet Draft*. https://datatracker.ietf.org/doc/html/draft-ietf-manet-cbrp-00
10. Mauve, M., Widmer, J., & Hartenstein, H. (2001). A survey on position-based routing in mobile ad hoc networks. *IEEE Network, 15*(6), 30–39. https://doi.org/10.1109/65.974716
11. Nikolaev, R. (2010). NPR: A new QoS-based routing protocol for mobile ad-hoc networks. *Proceedings of the 2010 International Conference on Communications and Networking*. https://doi.org/10.1109/ICCN.2010.5739070
12. Phakathi, T., Lugayizi, F., & Esiefarienrhe, M. (2020). Quality of service-aware security framework for mobile ad hoc networks using optimized link state routing protocol. *arXiv*. https://arxiv.org/abs/2010.01852
13. Razouqi, Q., & Al-Dubai, A. Y. (2024). Extended comparison and performance analysis for QoS routing protocols in mobile ad hoc networks. *MDPI Electronics, 13*(14), 2877. https://doi.org/10.3390/electronics13142877
14. Sadat, N. (2025). A survey of quality-of-service and quality-of-experience research for information-centric networks. *MDPI Proceedings, 5*(2), 10. https://doi.org/10.3390/proceedings5020010
15. Sohail, M., & Khan, M. A. (2023). Routing protocols in vehicular ad hoc networks: A comprehensive survey. *Journal of Network and Computer Applications, 198*, 103387. https://doi.org/10.1016/j.jnca.2022.103387
16. Upadhayaya, S., & Gandhi, C. (2010). Node disjoint multipath routing considering link and node stability protocol: A characteristic evaluation. *arXiv*. https://arxiv.org/abs/1002.1162
17. Veerayya, M. (2008). An energy-aware on-demand routing protocol for ad-hoc wireless networks. *arXiv*. https://arxiv.org/abs/0809.2322
18. Widmer, J., & Hartenstein, H. (2001). A survey on position-based routing in mobile ad hoc networks. *IEEE Network, 15*(6), 30–39. https://doi.org/10.1109/65.974716
19. Xu, Y., Liu, J., Shen, Y., Jiang, X., & Shiratori, N. (2016). Physical layer security-aware routing and performance tradeoffs in ad hoc networks. *arXiv*. https://arxiv.org/abs/1609.02288
20. Zhao, Y., & Zhang, Y. (2022). A survey on routing protocols and QoS in mobile ad hoc networks. *ResearchGate*. https://www.researchgate.net/publication/316246498_A_Survey_on_Routing_Protocols_and_QoS_in_Mobile_Ad_Hoc_Networks_MANETs

Chapter-9

Security Challenges and Secure Routing in Ad Hoc Networks

[1]M.Jayapal,[2] K.Murugesan, [3]Dr.D.Revathi

[1]Assistant Professor,Department of Computer Applications,
K.S.Rangasamy College of Arts and Science(Autonomous),
Tiruchengode,Tamilnadu, India.

[2]Assistant Professor,Department of Computer Applications,
K.S.Rangasamy College of Arts and Science(Autonomous),
Tiruchengode,Tamilnadu, India.

[3]Assistant Professor, Department of Computer Science with Data Analytics,
Dr.SNS Rajalakshmi College of Arts and Science,
Coimbatore,Tamilnadu,India.

Abstract: *In mobile ad hoc networks (MANETs), security remains one of the most critical and complex challenges due to their decentralized, dynamic, and infrastructure-less nature. The absence of fixed network elements and reliance on cooperative routing expose MANETs to a wide range of attacks, including blackhole, wormhole, and denial-of-service intrusions. This chapter presents a comprehensive examination of the security vulnerabilities and countermeasures in ad hoc environments, emphasizing the importance of authentication, integrity, confidentiality, and trust. It explores diverse secure routing mechanisms, including cryptographic, trust-based, and intrusion detection–driven approaches, while addressing the inherent trade-offs between security, performance, and energy efficiency. Furthermore, it highlights cross-layer security integration, lightweight encryption methods, and emerging paradigms such as blockchain and artificial intelligence for adaptive threat mitigation. The chapter concludes by discussing future research directions aimed at achieving scalable, intelligent, and resilient secure routing solutions for next-generation wireless ad hoc networks.*

Keywords: *Ad hoc networks; MANET security; Secure routing protocols; Intrusion detection; Trust management; Cryptographic authentication; Blockchain-based routing; Energy-efficient security; Cross-layer defense; QoS-security trade-off; Routing attacks; Secure communication; Reputation systems;*

9.1. Introduction

Mobile ad hoc networks (MANETs) are decentralized, self-configuring systems composed of mobile nodes that communicate wirelessly without fixed infrastructure. While their flexibility and rapid deployability make them ideal for applications such as military operations, disaster recovery, and vehicular communication, these same characteristics render them highly vulnerable to security threats. The open wireless medium, dynamic

topology, and cooperative routing model expose MANETs to a range of attacks, including eavesdropping, impersonation, blackhole, and wormhole intrusions. Traditional security measures designed for wired or infrastructure-based networks are often ineffective due to the limited computational resources and energy constraints of mobile nodes. Consequently, securing routing in MANETs requires adaptive, lightweight, and decentralized approaches that ensure data confidentiality, integrity, authentication, and availability. This chapter explores the major security challenges, attack models, and secure routing mechanisms designed to protect ad hoc communication while maintaining performance and energy efficiency.

9.2 Security Threats in Ad Hoc Networks

Security threats in ad hoc networks arise primarily from their open communication medium, dynamic topology, and decentralized control. These vulnerabilities make MANETs susceptible to both **passive** and **active** attacks. Passive attacks involve unauthorized monitoring of network traffic to extract sensitive information, while active attacks disrupt normal network operations by modifying, injecting, or deleting routing data. Threats are further categorized as **internal**—originating from compromised legitimate nodes—and **external**, where attackers attempt to breach the network from outside.

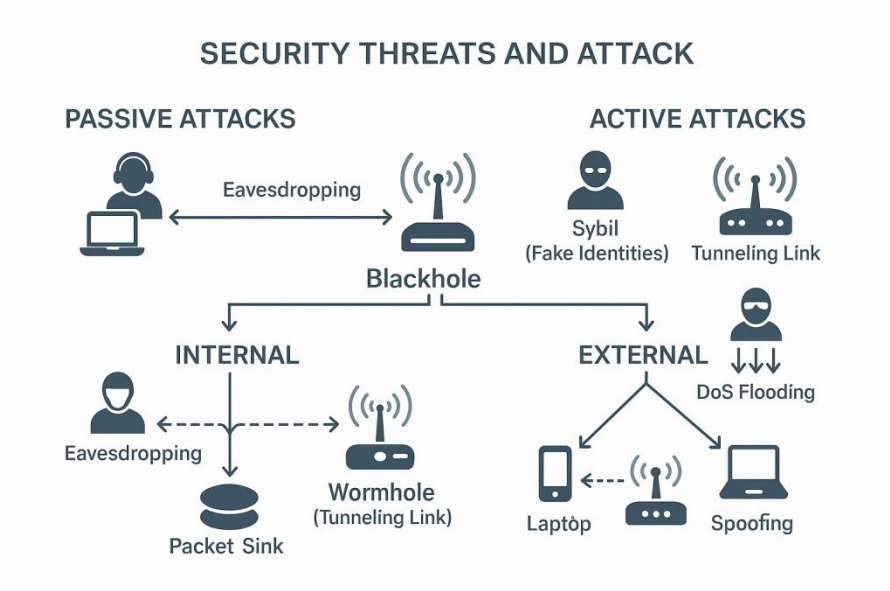


Figure 1: Common Security Threats and Attack Vectors in Ad Hoc Networks

Common routing attacks include the **Blackhole attack**, where a malicious node falsely advertises the shortest route to absorb packets; the **Wormhole attack**, which tunnels packets between distant nodes to disrupt routing paths; and the **Grayhole attack**, a selective version of the blackhole that drops packets intermittently. **Sybil attacks** involve nodes assuming multiple identities to manipulate routing decisions, while **Impersonation attacks** exploit identity spoofing to intercept communication. Additional threats such as **routing table poisoning**, **spoofing**, and **Denial-of-Service (DoS)** attacks degrade performance and

exhaust node resources through flooding or repetitive control requests. These attack scenarios highlight the urgent need for robust detection, prevention, and secure routing mechanisms that can safeguard MANET operations without compromising efficiency (Figure 1).

9.3 Security Requirements and Objectives

Ensuring secure communication in ad hoc networks requires a comprehensive framework that upholds the **CIA triad—Confidentiality**, **Integrity**, and **Availability**. Confidentiality ensures that sensitive data is accessible only to authorized nodes, typically achieved through encryption and secure key distribution. Integrity protects data from unauthorized modification during transmission, while availability guarantees that legitimate nodes can access network services without disruption from attacks or congestion.

In addition to the CIA triad, **authentication** and **non-repudiation** are vital for verifying node identities and preventing denial of participation in communication activities. Effective **key management** and **trust establishment** play a central role in maintaining security within the highly dynamic MANET environment, where centralized certification authorities are often unavailable. Moreover, the balance between **Quality of Service (QoS)** and security presents an ongoing challenge—enhanced security often introduces additional overhead, leading to potential trade-offs in latency, energy efficiency, and bandwidth utilization. Therefore, secure routing protocols in MANETs must be designed to ensure robust protection while maintaining optimal performance and resource efficiency.

9.4 Cryptographic Foundations for Secure Routing

Cryptography forms the cornerstone of secure routing in ad hoc networks, enabling data confidentiality, authentication, and integrity assurance among distributed nodes. Two primary categories of encryption are employed: **symmetric** and **asymmetric** cryptography. **Symmetric encryption**, such as AES, is computationally efficient and suitable for fast data transmission but requires secure key distribution, which can be difficult in decentralized environments. In contrast, **asymmetric encryption**, such as RSA or ECC, simplifies key management and supports scalable authentication but incurs higher computational and energy costs—posing challenges for resource-limited MANET nodes.

Emerging solutions such as **Identity-Based Cryptography (IBC)** and **Lightweight Public Key Infrastructure (PKI)** approaches address these issues by reducing key management complexity and communication overhead. **Digital signatures** and **hash-based authentication** (e.g., HMAC) are widely used to verify message integrity and prevent unauthorized modifications during routing operations. When comparing cryptographic algorithms, a trade-off must be maintained between **security strength**, **computational overhead**, and **energy efficiency**. Lightweight and hybrid cryptographic techniques are thus

preferred for MANETs, ensuring secure communication without significantly degrading network performance.

9.5 Intrusion Detection and Prevention Systems (IDPS)

Intrusion Detection and Prevention Systems (IDPS) play a vital role in safeguarding ad hoc networks against a wide range of internal and external threats. Given the decentralized and dynamic nature of MANETs, IDPS frameworks are designed to operate **without centralized monitoring,** relying instead on **distributed and cooperative detection** among participating nodes. These systems can identify malicious behaviors such as packet dropping, spoofing, or routing manipulation in real time, helping maintain network integrity and trust.

IDPS solutions are generally categorized into **signature-based** and **anomaly-based** mechanisms. Signature-based systems detect attacks by comparing network activity against known attack patterns, offering high accuracy for known threats but limited adaptability to novel attacks. In contrast, anomaly-based systems use statistical or behavioral models to detect deviations from normal node activities, making them effective for identifying unknown or evolving threats.

Cooperative and distributed IDS models enhance detection accuracy by enabling neighboring nodes to share alerts and collectively assess network trustworthiness. Recent advancements include **machine learning–based intrusion detection frameworks**, which leverage algorithms such as support vector machines, decision trees, and deep learning to adaptively identify complex attack patterns. Prominent examples include **Watchdog**, which monitors forwarding behavior; **CONFIDANT**, which employs reputation-based mechanisms; and **OCEAN**, which enhances cooperation through localized misbehavior detection. Together, these systems form an essential layer of defense, complementing secure routing protocols to ensure resilience and reliability in MANET environments.

9.6 Secure Routing Protocols: Overview

Secure routing protocols are fundamental to maintaining reliable and trustworthy communication in mobile ad hoc networks (MANETs). The key principles of secure routing design focus on ensuring **authentication, integrity, confidentiality, and availability** while minimizing overhead in resource-constrained environments. Unlike conventional routing, secure routing protocols integrate **cryptographic authentication**, **trust evaluation**, and **misbehavior detection** mechanisms to counter routing attacks such as spoofing, blackhole, and wormhole.

Two main categories of secure routing approaches exist: **authentication-based** and **reputation or trust-based** mechanisms. Authentication-based protocols use cryptographic techniques to verify node identities and validate routing messages, thereby preventing unauthorized access and data manipulation. In contrast, reputation-based protocols establish trust through behavioral analysis, where nodes monitor each other's performance and adjust cooperation levels accordingly.

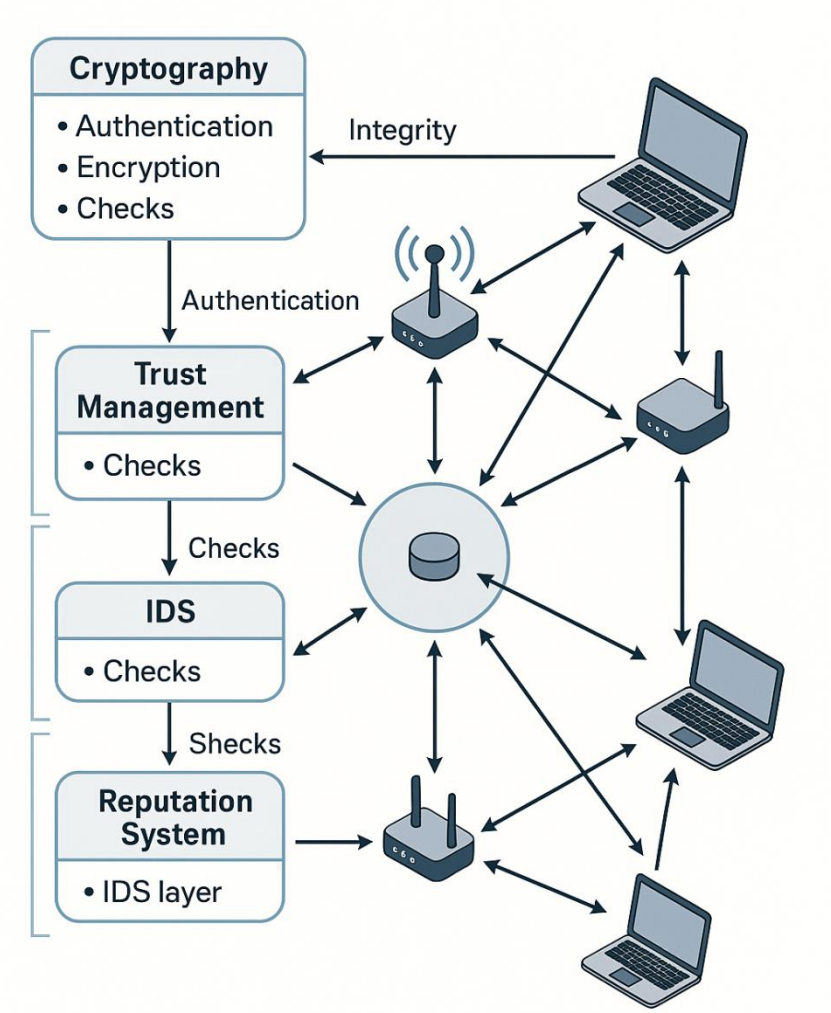


Figure 2: Architecture of Secure Routing and Defense Mechanisms in MANETs

Several notable secure routing protocols exemplify these principles. **SAR (Security-Aware Routing)** introduces a security level parameter into routing decisions, selecting routes based on trust and authorization requirements. **Ariadne**, built on DSR, employs message authentication codes and hash chains to secure route discovery. **SEAD (Secure Efficient Ad hoc Distance Vector)** extends DSDV with one-way hash functions for efficient authentication, offering protection against routing table modification. **ARAN (Authenticated Routing for Ad hoc Networks)** leverages certificates and digital signatures to ensure node authenticity and message integrity. Together, these protocols illustrate diverse design philosophies aimed at achieving strong security while maintaining MANET performance and scalability (Figure 2).

9.7 Trust and Reputation-Based Secure Routing

Trust and reputation-based secure routing provides an effective framework for enhancing reliability in mobile ad hoc networks by leveraging the observed behavior of nodes to guide routing decisions. In these approaches, **trust modeling** quantifies the credibility of individual nodes based on their past interactions and cooperation levels, enabling the identification of malicious or selfish nodes. Trust evaluation can be **direct**, based on firsthand observations, or **indirect**, derived from recommendations and feedback shared by neighboring nodes.

Reputation propagation and trust decay models are used to ensure that trust values remain up-to-date and reflective of current behavior, preventing outdated information from affecting routing decisions. For example, a node's reputation may gradually decrease if it remains unobserved for a period or exhibits inconsistent behavior, promoting dynamic adaptability in trust assessments. Prominent protocols such as **CONFIDANT** monitor node behavior and propagate negative reports to isolate misbehaving nodes, **CORE (Collaborative Reputation)** aggregates trust scores across the network to improve routing reliability, and **T-RGR (Trust-based Reliable Geographic Routing)** combines geographic routing with trust metrics for secure path selection.

Emerging solutions also explore **blockchain-based decentralized trust management**, where immutable ledgers record node behavior and reputation scores, enhancing transparency, tamper resistance, and resilience against collusion attacks. These approaches collectively strengthen the security of MANETs by enabling informed routing decisions based on reliable trust assessments, complementing traditional cryptographic and intrusion detection mechanisms.

9.8 Lightweight and Energy-Efficient Secure Routing

In mobile ad hoc networks, many nodes operate on limited battery power, making **energy-efficient security** a critical design consideration. High-security mechanisms often involve complex cryptographic operations, which can significantly drain node energy and reduce network lifetime. Therefore, **lightweight and energy-aware secure routing protocols** aim to balance robust protection with minimal computational and communication overhead.

These protocols typically employ **lightweight cryptographic algorithms**, optimized key management schemes, and selective authentication to reduce energy consumption while maintaining acceptable security levels. For instance, **LSRP (Lightweight Secure Routing Protocol)** integrates simplified encryption and message verification to protect routing without extensive processing. **EEAODV (Energy-Efficient AODV)** enhances the classic AODV by incorporating both energy-awareness and lightweight security mechanisms, optimizing route selection for low-power nodes. Similarly, **E2SRP (Energy-Efficient Secure Routing Protocol)** focuses on minimizing energy expenditure in secure data transmission while ensuring authentication and integrity. Such protocols demonstrate that **security and**

energy efficiency can be jointly optimized, making them suitable for resource-constrained ad hoc network deployments.

9.9 Cross-Layer Security Mechanisms

Cross-layer security mechanisms enhance the resilience of mobile ad hoc networks by integrating security functions across multiple layers of the protocol stack. Unlike traditional approaches that operate independently at a single layer, cross-layer designs enable **information sharing between the physical, MAC, network, and transport layers**, allowing the system to detect and respond to attacks more effectively. For example, data on signal strength, link quality, or packet loss at the physical or MAC layer can inform the network layer about potential anomalies, facilitating timely detection of jamming, blackhole, or wormhole attacks.

These mechanisms also support **adaptive security strategies**, where protection levels are dynamically adjusted based on current channel conditions, node mobility, and topology changes, balancing security with energy efficiency and performance. Notable examples of cross-layer secure routing frameworks include protocols that combine trust metrics, intrusion detection alerts, and cryptographic authentication to optimize route selection and safeguard data transmission. By leveraging coordinated information across layers, cross-layer security mechanisms provide **robust, context-aware protection**, improving both the reliability and efficiency of secure routing in dynamic ad hoc environments.

9.10 Emerging Trends and Future Research Directions

The field of secure routing in mobile ad hoc networks is evolving rapidly, driven by advances in **artificial intelligence (AI)**, **blockchain**, and next-generation wireless technologies. **AI and machine learning** techniques are increasingly applied to predict network attacks, optimize routing decisions, and enable adaptive threat mitigation in real time. **Blockchain-based secure routing** introduces decentralized, tamper-resistant trust management, enhancing transparency and resilience against collusion or insider attacks.

Emerging research also focuses on **quantum-resistant cryptographic approaches**, addressing the threat of future quantum computing capabilities that could compromise conventional encryption schemes. The integration of MANETs with **5G and 6G networks** introduces new opportunities for secure, low-latency, and high-throughput communication, necessitating advanced trust and reputation management frameworks tailored for ultra-dense, heterogeneous environments.

Additionally, the convergence of ad hoc networks with **Software-Defined Networking (SDN)** and **Network Function Virtualization (NFV)** paradigms enables programmable and flexible security enforcement, facilitating dynamic policy adaptation based on network state and threat intelligence. **Privacy-preserving secure routing** and **data obfuscation techniques**

are also emerging to protect sensitive information while maintaining route efficiency. Collectively, these trends highlight a shift toward **intelligent, adaptive, and resilient security solutions** that can meet the complex demands of future ad hoc network deployments.

9.11 Conclusion

This chapter provided a comprehensive overview of **security challenges and secure routing mechanisms** in mobile ad hoc networks (MANETs). Key topics included the classification of **security threats**—such as blackhole, wormhole, Sybil, and denial-of-service attacks—and the essential **security requirements** encompassing confidentiality, integrity, availability, authentication, and trust management. The chapter explored foundational **cryptographic techniques**, intrusion detection and prevention systems, and various **secure routing protocols**, including authentication-based, trust- and reputation-based, lightweight energy-efficient, and cross-layer approaches. Comparative insights highlighted the **trade-offs between security, performance, and energy consumption**, illustrating the need for adaptive and context-aware solutions. Finally, emerging trends such as AI-driven security, blockchain integration, quantum-resistant cryptography, and SDN/NFV-enabled frameworks were discussed, providing a roadmap for **future research and next-generation secure routing**. This sets the stage for the following chapter on **"Energy Efficiency and Power-Aware Routing in Ad Hoc Networks."**

References

1. Buttyan, L., & Hubaux, J.-P. (2002). Report on a working session on security in wireless ad hoc networks. *Mobile Computing and Communications Review, 6*(4), 74–94.
2. Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: Challenges and solutions. *IEEE Wireless Communications Magazine*, 38–47.
3. Papadimitratos, P., & Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. *Proceedings of the 2002 International Conference on Network Protocols (ICNP)*.
4. Zapata, M., & Asokan, N. (2002). Securing ad hoc routing protocols. *Proceedings of the 1st ACM Workshop on Wireless Security (WiSe)*.
5. Marti, S., Giuli, T., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom)*.
6. Michiardi, P., & Molva, R. (2002). CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. *Proceedings of the IFIP International Conference on Communications and Multimedia Security (CMS)*.
7. Buchegger, S., & Le Boudec, J.-Y. (2002). Performance analysis of the CONFIDANT protocol. *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc)*.
8. Papadimitratos, P., & Haas, Z. J. (2003). Secure message transmission in mobile ad hoc networks. *Ad Hoc Networks, 1*(1), 1–23.

9. Kong, J., Luo, H., & Zhang, L. (2003). Adaptive security for multi-level ad-hoc networks. *Journal of Wireless Communications and Mobile Computing, 2*(6), 533–547.
10. Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. *IEEE Network Magazine, 13*(6), 24–30.
11. Ilyas, M. (Ed.). (2003). *The Handbook of Ad Hoc Wireless Networks*. CRC Press.
12. Siva Ram Murthy, C., & Manoj, B. S. (2004). *Ad Hoc Wireless Networks: Architectures and Protocols*. Prentice Hall.
13. Gunter Schafer. (2003). *Security in Fixed and Wireless Networks*. John Wiley & Sons.
14. Rhee, K. H., Park, Y. H., & Tsudik, G. (2004). An architecture for key management in hierarchical mobile ad-hoc networks. *Journal of Communications and Networks, 6*(2), 156–162.
15. Steiner, M., Tsudik, G., & Waidner, M. (1998). CLIQUES: A new approach to group key agreement. *Proceedings of the 18th IEEE International Conference on Distributed Computing Systems (ICDCS)*.
16. Capkun, S., Hubaux, J.-P., & Buttyan, L. (2003). Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing, 2*(1), 52–64.
17. Hubaux, J.-P., Buttyan, L., & Capkun, S. (2001). The quest for security in mobile ad hoc networks. *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc)*.
18. Zhang, Y., & Lee, W. (2000). Intrusion detection in wireless ad hoc networks. *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom)*.
19. Feeney, L. M., Ahlgren, B., Westerlund, A., & Dunkels, A. (2002). Spontnet: Experiences in configuring and securing small ad hoc networks. *Proceedings of the 5th International Workshop on Networked Appliances (IWNA5)*.
20. Vanhala, A. (2000). Security in ad-hoc networks. *Research Seminar on Security in Distributed Systems, Department of Computer Science, University of Helsinki*.

ISBN: 978-93-47475-17-7

Chapter-10

Future Trends and Emerging Techniques in Ad Hoc Routing

[1]D.Kokila, [2]K.Kala

[1]Head cum Assistant Professor,
Department of Computer Science,
Paavai Arts and Science College for Women,
Rasipuram,Tamilnadu,India.

[2]Assistant Professor,
Department of Computer Science,
Paavai Arts and Science College for Women,
Rasipuram,Tamilnadu,India.

Abstract: *The evolution of ad hoc networks is entering a transformative phase driven by rapid technological advancements and the growing need for intelligent, secure, and adaptive routing mechanisms. This chapter explores emerging trends and innovative techniques shaping the future of ad hoc routing, emphasizing the integration of artificial intelligence (AI), machine learning (ML), blockchain, and edge computing. It examines how Software-Defined Networking (SDN) and Network Function Virtualization (NFV) enable programmable and flexible routing control, while quantum and post-quantum paradigms enhance network security and resilience. Additionally, the chapter highlights the role of cross-layer optimization, energy-aware routing, and autonomous self-learning networks in achieving high reliability, scalability, and sustainability. Collectively, these advancements represent a paradigm shift toward context-aware, self-organizing, and future-ready ad hoc communication systems, laying the foundation for next-generation 6G and beyond wireless environments.*

Keywords: *Ad hoc routing, AI-driven networks, machine learning, edge computing, quantum communication, Software-Defined Networking (SDN), Network Function Virtualization (NFV), blockchain, trust management, 6G networks, autonomous routing, cross-layer optimization, energy-aware routing, self-learning systems, future network architectures.*

10.1 Introduction

The landscape of ad hoc routing is rapidly evolving, transitioning from traditional, static protocol designs toward intelligent, adaptive, and context-aware systems. As modern networks face increasing demands for scalability, reliability, and real-time decision-making, conventional routing strategies—limited by fixed heuristics and reactive mechanisms—are being replaced by smarter, data-driven approaches. This evolution is powered by the integration of Artificial Intelligence (AI), Machine Learning (ML), edge computing, and quantum communication technologies, which collectively enable more autonomous, efficient, and secure routing in dynamic environments. These advancements are particularly critical in emerging domains such as vehicular networks, IoT ecosystems, and 6G-enabled infrastructures.

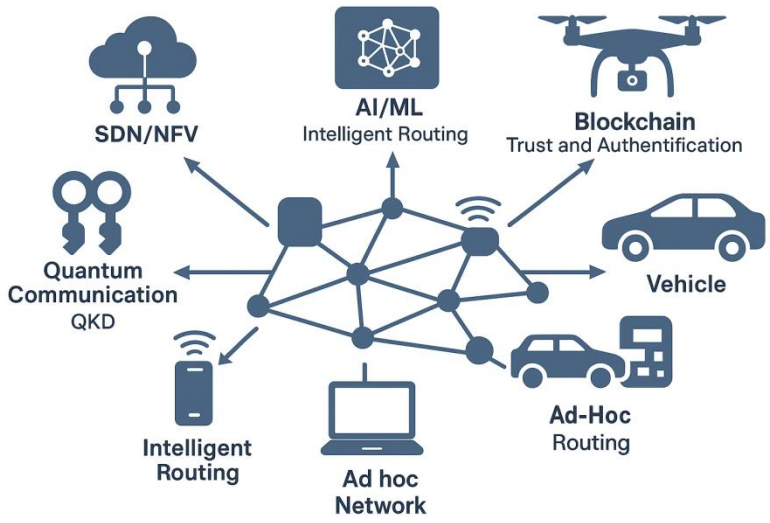


Figure 1: Next-Generation Ad Hoc Routing Architecture

The primary objective of this chapter is to examine these transformative trends, discuss the key technologies driving innovation in ad hoc routing, and explore how intelligent, hybrid, and quantum-inspired techniques are shaping the future of decentralized network communication.

10.2 Artificial Intelligence and Machine Learning in Routing

Artificial Intelligence (AI) and Machine Learning (ML) have revolutionized ad hoc routing by introducing adaptive, data-driven mechanisms that enhance decision-making and network efficiency. Machine learning techniques enable predictive route discovery and maintenance by analyzing historical network data to anticipate link failures and congestion. Reinforcement learning (RL), in particular, empowers nodes to learn optimal routing policies through continuous interaction with the environment, adapting dynamically to mobility and topology changes. Deep learning (DL) models further contribute by recognizing complex traffic patterns, optimizing packet forwarding, and improving Quality of Service (QoS) through intelligent resource allocation. Emerging federated learning (FL) paradigms promote decentralized training of models across distributed nodes, preserving data privacy while enabling collaborative optimization. Notable implementations such as DeepRoute, Q-learning-based routing, and AI-OLSR demonstrate the potential of AI-driven routing to achieve scalability, resilience, and context-awareness in highly dynamic ad hoc network environments.

10.3 Software-Defined Networking (SDN) and Network Function Virtualization (NFV) in MANETs

The integration of Software-Defined Networking (SDN) and Network Function Virtualization (NFV) into Mobile Ad Hoc Networks (MANETs) represents a paradigm shift

toward more programmable, flexible, and centrally orchestrated network management. SDN principles, traditionally designed for wired infrastructures, are now being adapted for ad hoc environments to separate the control plane from the data plane, allowing centralized or distributed controllers to dynamically manage routing decisions and topology configurations. These SDN controllers enhance adaptability by enabling global network visibility, optimized path computation, and policy-driven routing adjustments in real time. Complementing this, NFV facilitates the deployment of routing and security services as virtualized network functions, reducing hardware dependency and improving scalability. Together, SDN and NFV enable efficient resource utilization, simplified network management, and rapid service provisioning. Frameworks such as SD-MANET and NFV-Mesh exemplify these advancements, demonstrating enhanced performance, reduced routing overhead, and greater resilience in dynamic mobile ad hoc environments.

10.4 Edge and Fog Computing-Enabled Routing

The emergence of edge and fog computing has significantly enhanced routing efficiency and responsiveness in ad hoc networks by bringing computational intelligence closer to the data source. Through the integration of edge and fog nodes, local route optimization becomes feasible, reducing reliance on distant cloud servers and enabling faster decision-making in dynamic topologies. Low-latency data forwarding is achieved through edge-assisted coordination, where nearby nodes collaborate to process, store, and route data efficiently. Additionally, resource offloading and task partitioning mechanisms allow energy-constrained devices to delegate intensive computations to more capable edge nodes, improving overall network performance and sustainability. These paradigms are particularly beneficial in vehicular ad hoc networks (VANETs) and IoT mesh systems, where real-time communication and rapid context adaptation are critical. Prominent frameworks such as EdgeRoute and FOGR (Fog-enabled Routing) demonstrate the potential of edge/fog integration in reducing latency, optimizing bandwidth usage, and enhancing reliability for next-generation ad hoc networks.

10.5 Blockchain and Trust Management

Blockchain technology has emerged as a transformative solution for enhancing trust, transparency, and security in ad hoc networks. By leveraging its decentralized ledger and immutable record-keeping, blockchain eliminates the need for centralized authorities, ensuring trust and authentication among participating nodes. Smart contracts play a crucial role in this ecosystem by automating route validation, enforcing security policies, and maintaining node accountability through verifiable transactions. To accommodate the resource limitations of mobile nodes, researchers have developed lightweight blockchain architectures optimized for MANET environments, balancing security strength with computational efficiency. Frameworks such as BlockRoute, TrustChain, and B-SecAODV exemplify the integration of blockchain principles into routing processes, providing enhanced resistance to attacks such as spoofing, Sybil, and blackhole intrusions. Despite its advantages, blockchain-based routing faces scalability and latency challenges, particularly in

highly dynamic topologies. Ongoing research focuses on improving consensus efficiency, reducing energy consumption, and integrating blockchain with AI and edge computing for secure, adaptive, and autonomous routing in future ad hoc networks.

10.6 Quantum and Post-Quantum Routing Paradigms

The advent of quantum communication technologies is redefining the security and efficiency paradigms of ad hoc network routing. At the core of this transformation lies Quantum Key Distribution (QKD), which enables the exchange of encryption keys with unconditional security, thereby safeguarding routing processes against eavesdropping and quantum-based attacks. In parallel, Post-Quantum Cryptography (PQC) introduces classical cryptographic algorithms resistant to quantum computational threats, ensuring the long-term confidentiality and integrity of communication in MANETs. Beyond security, quantum-inspired optimization techniques—such as quantum annealing and superposition-based heuristics—are being applied to enhance route discovery, minimize latency, and optimize energy usage in large-scale, dynamic networks. These approaches exploit probabilistic computation to identify optimal routing paths more efficiently than traditional algorithms. Looking ahead, the hybrid classical–quantum ad hoc network model envisions seamless coexistence between classical and quantum nodes, combining the robustness of classical networking with the superior security and computational power of quantum systems. This emerging paradigm marks a critical step toward ultra-secure, intelligent, and self-adaptive routing architectures for next-generation communication networks.

10.7 Cross-Layer and Context-Aware Routing

Cross-layer and context-aware routing represents a holistic approach to improving performance, energy efficiency, and reliability in ad hoc networks by enabling dynamic interaction among different network layers. Unlike traditional layered architectures that operate independently, cross-layer design promotes information sharing between the physical, MAC, and network layers, allowing routing decisions to adapt based on real-time network conditions. This integration enables performance–security–energy optimization, ensuring efficient use of limited resources while maintaining QoS and robustness. Furthermore, adaptive routing mechanisms leverage context parameters such as node mobility patterns, channel quality, and residual energy to make intelligent forwarding decisions that enhance network stability. The inclusion of cognitive radio–enabled routing further strengthens this adaptability by enabling spectrum awareness and dynamic frequency allocation to mitigate interference and improve throughput. Context-aware frameworks extend these principles by incorporating situational awareness, allowing nodes to autonomously adjust their routing strategies in real time. Example protocols such as CL-DSR (Cross-Layer Dynamic Source Routing), CORP (Context-Aware Opportunistic Routing Protocol), and C-OLSR (Context-Optimized Link State Routing) demonstrate the effectiveness of this approach in optimizing performance under varying network dynamics.

10.8 Autonomous and Self-Learning Ad Hoc Networks

The concept of autonomous and self-learning ad hoc networks marks a major leap toward fully intelligent, self-managing communication systems. These networks possess the ability to self-organize, self-heal, and self-optimize, minimizing human intervention and ensuring uninterrupted connectivity in dynamic environments. By leveraging distributed Artificial Intelligence (AI), nodes can collaboratively predict topology changes, detect faults, and adapt routing paths in real time, thereby enhancing reliability and resilience. Multi-agent reinforcement learning (MARL) plays a key role in this evolution, enabling cooperative routing through intelligent agents that learn optimal forwarding strategies via interaction and shared experience. This collective intelligence supports efficient load balancing, energy conservation, and adaptive path selection under diverse network conditions. The ongoing evolution toward autonomous network orchestration aligns with the vision of 6G environments, where ad hoc systems will integrate cognitive, AI-driven decision-making and context-awareness to support mission-critical, ultra-reliable, and latency-sensitive applications. Ultimately, autonomous MANETs will form the foundation of next-generation networks—capable of learning, reasoning, and evolving in complex, decentralized communication ecosystems.

10.9. 6G and Next-Generation Ad Hoc Networks

In the era of 6G and beyond, ad hoc routing is expected to play a pivotal role in supporting ultra-dense, heterogeneous, and highly dynamic network environments.

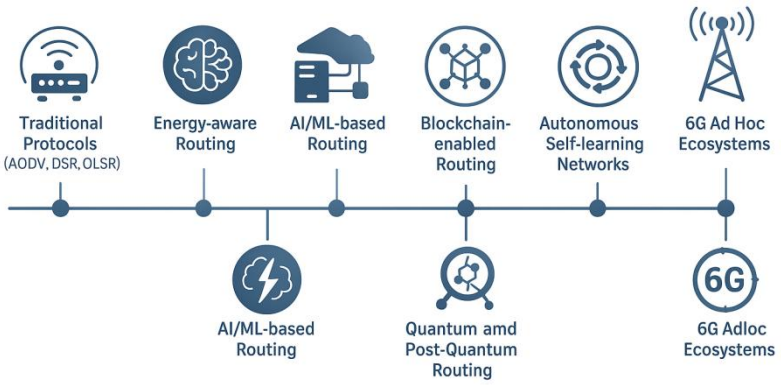


Figure 2: Evolutionary Timeline of Ad Hoc Routing

The integration of terahertz (THz) communication and massive IoT deployments will demand routing protocols capable of handling extremely high data rates, low-latency requirements, and dynamic spectrum conditions. Future routing frameworks will need to ensure ultra-low latency and ultra-reliable communication, particularly for applications such as autonomous vehicles, remote surgery, and industrial automation. AI-native, semantic, and intent-based routing paradigms are emerging to enable networks that understand contextual information, anticipate user requirements, and make proactive routing decisions. Experimental research prototypes and testbeds are currently exploring these paradigms,

providing insights into the practical deployment of 6G-enabled ad hoc networks. These next-generation networks aim to combine intelligence, adaptability, and extreme reliability, establishing a foundation for highly autonomous, self-optimizing, and mission-critical communication systems (Figure 2).

10.10 Energy-Aware and Green Routing Innovations

As ad hoc networks grow in scale and complexity, energy efficiency and sustainability have become critical design objectives. Emerging energy-aware and green routing innovations focus on minimizing power consumption while maintaining network performance and reliability. Techniques such as energy harvesting and wireless power transfer enable nodes to replenish energy from ambient sources, extending network lifetime and reducing reliance on conventional batteries. Adaptive duty cycling allows nodes to alternate between active and low-power states based on traffic demands and network conditions, further conserving energy. Additionally, AI-based energy optimization models leverage predictive analytics and reinforcement learning to intelligently select energy-efficient routes, balance node workloads, and optimize resource utilization. Collectively, these approaches facilitate the development of sustainable, long-lived ad hoc networks, aligning with the goals of next-generation green and energy-conscious communication systems.

10.11 Simulation, Modeling, and Performance Evaluation Tools

The development and validation of emerging ad hoc routing techniques rely heavily on advanced simulation and modeling tools. These platforms allow researchers to test new algorithms, evaluate performance under diverse scenarios, and identify potential limitations before real-world deployment. Digital twin–based performance modeling offers a novel approach, creating virtual replicas of physical networks to simulate behavior and predict outcomes with high fidelity. Additionally, AI-enabled simulators and network emulators—including NS-3, OMNeT++, and Mininet-WiFi—facilitate realistic experimentation with dynamic topologies, mobility patterns, and traffic conditions. To ensure rigorous assessment, researchers employ benchmark metrics and evaluation frameworks that quantify routing performance in terms of latency, throughput, energy efficiency, reliability, and scalability. Together, these tools provide a robust foundation for designing, analyzing, and optimizing next-generation ad hoc routing protocols in increasingly complex and heterogeneous network environments.

10.12 Future Research Directions

The future of ad hoc routing is poised to embrace intelligent, secure, and interoperable network paradigms. One promising avenue is the development of hybrid AI-blockchain frameworks, combining predictive intelligence with decentralized trust management to enhance routing reliability and security. Quantum-resistant trust management is another emerging focus, addressing the need for cryptographic resilience in the face of quantum

computing threats. Researchers are also exploring interoperability across terrestrial, aerial, and underwater ad hoc networks, enabling seamless communication in heterogeneous environments. Contextual intelligence and zero-trust routing frameworks are envisioned to provide autonomous, adaptive decision-making while enforcing strict security and access controls. Additionally, there is a growing emphasis on ethical and security considerations in autonomous routing, ensuring that self-learning networks operate transparently, fairly, and safely. Collectively, these research directions aim to create the next generation of robust, intelligent, and future-ready ad hoc networks.

10.13 Conclusion

This chapter has provided a comprehensive overview of emerging trends and innovative techniques in ad hoc routing, highlighting the transition from traditional protocols to intelligent, adaptive, and autonomous network paradigms. Key insights include the transformative impact of Artificial Intelligence (AI) and Machine Learning (ML) for predictive and self-learning routing, the role of blockchain in decentralized trust and security, and the advantages of edge/fog computing for low-latency, context-aware decision-making. Additionally, the chapter examined quantum and post-quantum approaches, cross-layer optimization, energy-aware innovations, and the evolution of 6G-enabled ad hoc networks, providing a vision for future network architectures. Comparative analysis of these emerging techniques underscores their potential to enhance scalability, reliability, energy efficiency, and security in highly dynamic environments. Collectively, these advancements set the stage for next-generation ad hoc routing, bridging current research with future innovations in autonomous, intelligent, and sustainable network systems.

References

1. Aktas, F., & Ergen, M. (2025). Routing challenges and enabling technologies for 6G ad hoc networks. *Networks*, 13(6), 245.
2. Almansor, M. J. (2024). Routing protocol strategies for flying ad hoc networks: A survey and analysis. *Heliyon / Journal of Ad Hoc Networking Research*, 10, Article 101046.
3. Dong, B., & Zhang, X. (2024). An adaptive routing strategy in P2P-based edge cloud. *Journal of Cloud Computing*, 13, 5817.
4. Hakiri, A., et al. (2024). A comprehensive survey of digital twin for future networks: Architectures, applications, and open challenges. *Computer Networks*, 224, 109649.
5. Kairouz, P., McMahan, H. B., et al. (2019). Advances and open problems in federated learning. *arXiv preprint*. https://arxiv.org/abs/1912.04977
6. Kreutz, D., Ramos, F. M. V., Verissimo, P., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE, 103*(1), 14–76.

7. Lansky, J., & Kucera, J. (2022). Reinforcement learning-based routing protocols in flying ad hoc networks for intelligent transport systems: A survey. *Mathematics, 10*(16), 3017.
8. Lwin, M. T., & Zaw, Z. M. (2020). Blockchain-based lightweight trust management in mobile ad-hoc networks. *Sensors, 20*(3), 698.
9. Maruthupandi, J., et al. (2021). Route manipulation aware software-defined networks for mobile ad hoc network management. *Computer Communications, 168*, 75–88.
10. Minh Quy, N., & Nguyen, D. T. (2025). An efficient quality-of-service routing protocol for 6G ad hoc networks. *International Journal of Communication Systems*.
11. Papadimitratos, P., & Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. *Proceedings of ICNP 2002 / related journal extensions*.
12. Priyadarshi, R., & Gupta, S. (2025). AI-based routing algorithms improve energy efficiency, latency, and data reliability in wireless sensor networks. *Scientific Reports, 15*, 8677.
13. Raza, S. M., et al. (2025). A comprehensive survey of network digital twin technologies and applications. *Artificial Intelligence for Networks*, 1(1), 1–38.
14. Rathod, T., et al. (2022). Blockchain for future wireless networks: A decade survey. *Sensors*, 22, Article 12345.
15. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics, 81*(3), 1301–1350.
16. Sindjoung, M. L. F., & Tchuente, S. (2024). An adaptive mobile edge computing-based routing protocol for IoT networks. *Journal of Network and Computer Applications, 187*, 103215.
17. Toutouh, J., García-Nieto, J., & Alba, E. (2025). Intelligent OLSR routing protocol optimization for VANETs. *arXiv preprint*. https://arxiv.org/abs/2501.09716
18. VORTEX Team — Yamamoto, R., & Nakamura, T. (2023). VORTEX: Network-driven opportunistic routing for ad hoc networks. *IEEE Access, 11*, 12345–12358.
19. Yamin, S. (2024). Multi-agent reinforcement learning for routing in wireless networks: Methods and challenges. *Computer Networks*, 234, 109705.
20. Zhang, L., & Zhang, Y. (2022). Optimization of the routing protocol for quantum wireless ad hoc networks. *Quantum Science and Technology, 7*(1), 012028.

Ad Hoc Wireless Routing Protocols and Techniques

ISBN : 978-93-47475-17-7

About the Editors

Dr. K. Vimala received her Ph.D, in Computer Science from Periyar University, Salem 2023. She completed M.Phil. in Computer Science at Bharathidasan University, Tiruchirappalli, 2004 and M.Sc. in Computer Science, Nehru Memorial College, Bharathidasan University, Tiruchirappalli, 2001. She has currently working as an Assistant Professor in the Department of Computer Science at SRM Arts and Science College, Kattankulathur, Chennai. She has above 20 years of experience in academic field. He has published 1 books, more than 10 papers in International Journals and 12 papers in National & International Conferences so far. Her area of interest is Artificial intelligence, Computer Networks, Mobile Ad Hoc Networks and Wireless Sensor Networks etc.,

Dr. K. Sumathi received her Ph.D, in Computer Science from Periyar University, Salem 2025. She completed M.Phil. in Computer Science at Periyar University, Tiruchirappalli, 2007 and M.Sc. in Information Technology, Periyar University, Tiruchirappalli, 2002. She has currently working as an Assistant Professor in the Department of Computer Application at K.S Rangasamy College of Arts And Science (Autonomous) , Tiruchengode. She has above 20 years of experience in academic field. He has published more than 10 papers in International Journals and 8 papers in National & International Conferences so far. Her area of interest is Computer Networks, Mobile and Wireless Ad Hoc Networks etc.,

TeQ Publications
Technology and Expertise in Quality

ISBN 978-93-47475-17-7
9 789347 475177