University of Zawia

Faculty of Sciences

Department of Computer Science

Postgraduate Program

Research Proposal for a Master's Degree in Computer Science

Enhancement Routing Protocol of Mobile Ad-hoc Networks for Controlling Packet Flooding when Network Dynamics Change

تحسين بروتوكول التوجيه لشبكة Ad-hoc المتنقلة لاجل التحكم فى فيضان الحزم عندما تكون فى حالة التغير الديناميكى

Submitted By: AISHA ALFITORY ALMGTOF

Supervisor: Dr EL BAHLUL FGEE

Academic Year

A thesis submitted to the Faculty of Sciences, University of Zawia, in fulfillment of the requirements for the degree of Master of Science in the Department of Computer Science

07/09/2025

الإقرار

أقرّ أنا ....، بأن ما اشـتملت عليه الرسـالة إنما هو نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حتمًا وورد، وأن هذه الرسالة ككل أو أي جزءٍ منها لم يقدّم من قبل لنيل أي درجة علمية، أو بحث علمي لدى أي مؤسـسـة تعليمية أو بحثية أخرى، وللجامعة حق توظيف الرسالة أو الأطروحة والاستفادة منها مصـدرًا مرجعيًا للمعلومات، لأغراض الاطلاع أو الإعارة أو النشر بما لا يتعارض وحقوق الملكية الفكرية المقررة بالتشريعات النافذة.

التوقيع..............................

التاريخ: ..../......./20م

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

﴿ وَمَا تَوْفِيقِي إِلاَّ بِاللَّهِ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ ﴾

صدق الله العظيم

سورة هود /الاية "88"

إهـــــــداء

إلى من كانا بعد الله سرّ وجودي، وسند عمري...

إلى والديّ العزيزين، منبعي الأول في الحنان، وجناحيّ في الحياة، جزاكما الله عني خير الجزاء، وحفظكما لي نورًا وعونًا.

وإلى شـــريك حياتي، زوجي الحبيب، الداعم الأول لمســـيرتي، الذي ســـاندني بصـــبره وتشـــجيعه... كل الامتنان والحب.

وإلى صـــغـاري الأحبّـة، الـذين منحتهم من وقتي وعقلي وقلبي، فـأعطوني بـدورهم دافعًا للاســـتمرار... أهديكم ثمرة هذا الجهد، عسى أن يكون لكم فخرًا في مستقبل الأيام.

Abstract

This study investigates enhancing self-organizing wireless mobile network (MANET) performance using the Optimized Link State Routing Protocol (OLSR) with Multi-Point Relay (MPR) transmission. MANET routing protocols manage node mobility using metrics to assess link quality. OLSR employs MPRs to identify routes, relaying Hello and Topology Control (TC) messages for link-state information distribution. Since Hello and TC intervals significantly impact link state, even brief link failures can degrade performance. This work improves OLSR performance by adaptively adjusting Hello and TC intervals for faster route recovery, minimizing overhead, and ensuring route freshness. OPNET Modeler simulations compare the enhanced OLSR with traditional OLSR, GRP, and AODV protocols. The evaluation occurs in various MANET scenarios using a Voice over Internet Protocol (VoIP) application, focusing on WLAN delay, throughput, and data dropped.

الملخص:

تبحث هذه الدراســة في تحســين أداء شــبكة الهاتف المحمول اللاســلكية (MANET) باســتخدام بروتوكول توجيه حالة الرابط المُحسَّـن (OLSR) مع إرســال التتابع متعدد النقاط (MPR). تدير بروتوكولات توجيه MANET حركة العقد باســتخدام مقاييس لتقييم جودة الرابط. يســتخدم OLSR ميكانيكية MPR لتحديد المســارات، ونقل رســائل TC(Hello & Topology Control) لتوزيع معلومات حالة الرابط. نظرًا لأن فترات Hello و TC تؤثر بشكل كبير على حالة الرابط، فإن حتى أعطال الرابط المستديمة يمكن أن تؤدي إلى تدهور الأداء داخل الشبكة. يحسن هذا العمل أداء OLSR من خلال ضـبط فترات (Hello & TC intervals) بشـكل تكيفي لاسـتعادة المسـار بشـكل أسـرع وتقليل الحمل الزائد. في هذه الفرضـية يتم مقارنة بين OLSR المُحسَّـن وبروتوكولات OLSR التقليدية و GRP و AODV. يحدث التقييم في ســيناريوهات MANET المختلفة باســتخدام تطبيق Voice over Internet Protocol (VoIP)، مع التركيز على تأخير WLAN والإنتاجية وفقدان البيانات. تم تحليل كافة النتائج باســـتخدام الرســـوم البيانية والإحصائيات عن طريق برنامج المحاكاة OPNET Modeler

Table of Contents

List of Tables

List of Figures

List of Abbreviations

WANETs	Wireless ad hoc networks
SPANs	smartphone ad hoc networks
VANETs	vehicular ad hoc networks
IMANET's	Internet-based Mobile Ad hoc Network
FANETs	Flying Ad hoc Network
MANET	Mobile Ad-Hoc Network
AODV	Ad Hoc On-Demand Distance Vector Protocol
OLSR	Optimized Link State Routing
E-OLSR	Enhanced Optimized Link State Routing
GRP	Geographic Routing Protocol
RERR	Route Error
RREP	Route Reply
RREQ	Route Request
RREP-ACK	Route Reply Acknowledgment
PDR	Packet Delivery Ratio
GPS	Global Positioning System
MPR	Multipoint Relay
VoIP	Voice over IP
AP	Access Point
BTS	Base Station Transceiver
BSSs	Basic Service Sets
SANET	static ad hoc networks
QoS	Quality of Service
RF	Radio frequency
IR	Infra Red
PAN	Personal Area Networks
BAN	Body Area Network
PAN	Personal Area Network
WLAN	Wireless Local Area Network
Wi Max	Worldwide Interoperability for Microwave Access
INVANET	Intelligent Vehicle Ad-hoc Networks
V2R	vehicles and roadside infrastructure

INVANET	Intelligent Vehicle Ad-hoc Networks
V2V	Vehicle-to-Vehicle
V2R	vehicles and roadside infrastructure
DQ	Destination Query
NIG	Network Information Gathering
TTL	Time To Live
RWP	Random Way Point
IEEE	Institute of Electrical and Electronics Engineers
Wi-Fi	Wireless Fidelity
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
FTP	File Transfer Protocol
IP	Internet Protocol

Chapter One :
Introduction

1.1 Overview

Wireless ad hoc networks (WANETs) and mobile ad hoc networks (MANETs) consist of groups of mobile devices that connect without a fixed infrastructure [1]. These networks can be used in various applications, including smartphone ad hoc networks (SPANs), vehicular ad hoc networks (VANETs), Internet-based Mobile Ad hoc Networks (IMANETs), Military or Tactical MANETs, Flying Ad hoc Networks (FANETs), and Hub-Spoke MANETs [2][3]. MANET, or WANET, is classified as an ad hoc network because it operates without fixed routes or infrastructure. In this type of network, each device, or node, plays an active role in routing information by sharing data. In mobile ad hoc networks (MANETs), collections of mobile devices communicating without infrastructure, information routing adapts dynamically based on the network's state and routing algorithms. Characterizing a MANET requires key parameters like node count, link density, and mobility rate[4]. MANETs forego centralized control, relying on self-organization and management instead of fixed infrastructure. Each node acts as both host and router due to limited wireless range[5].

Enhancing OLSR for efficient network communication requires several key improvements. Optimizing Multi-Point Relay (MPR) selection reduces redundant routing table entries, improving both size and convergence speed[6]. MPR relays Hello and Topology Control (TC) messages, essential for link-state discovery and distribution. Hello and TC message intervals are crucial for network stability[7]. Even brief link failures can cause significant performance issues. Implementing adaptive Hello intervals—faster in unstable networks for quicker detection, slower in stable networks to reduce overhead—improves performance effectively[8].

1.2 CLASSIFICATION OF MANETs ROUTING PROTOCOLS

MANET routing protocols are classified based on network structure, communication model, routing strategy, and state information, with routing strategy and network structure being the most common factors. Routing protocols are classified into two categories based on their strategies: 1. Table-driven and 2. Source-initiated (on-demand). Additionally, they can be categorized according to network structure as Flat topology-based (Uniform) routing, hierarchical routing, or geographic (position-assisted) routing[9].

Flat topology-based routing protocols are classified into reactive (source-initiated/on-demand), proactive (table-driven), and hybrid categories. Flat routing covers both routing protocols based on the routing strategy[10]. The classification of MANET routing protocols is shown in Figure 1.1.

This thesis examines topology- and position-based routing protocols in MANETs [11].

This section outlines the core features of three protocols: the reactive, topology-based AODV (Ad Hoc On-Demand Distance Vector Protocol); the proactive, topology-based OLSR (Optimized Link State Routing); and the position-based GRP (Geographic Routing Protocol)[12].The classification of MANET routing protocols is shown in Figure 1. 1.

Extensive studies using OPNET 14.5 have validated these protocols. Ad-hoc routing protocols offer improved scalability in wireless networks compared to infrastructure-based networks because of their decentralized design[13].

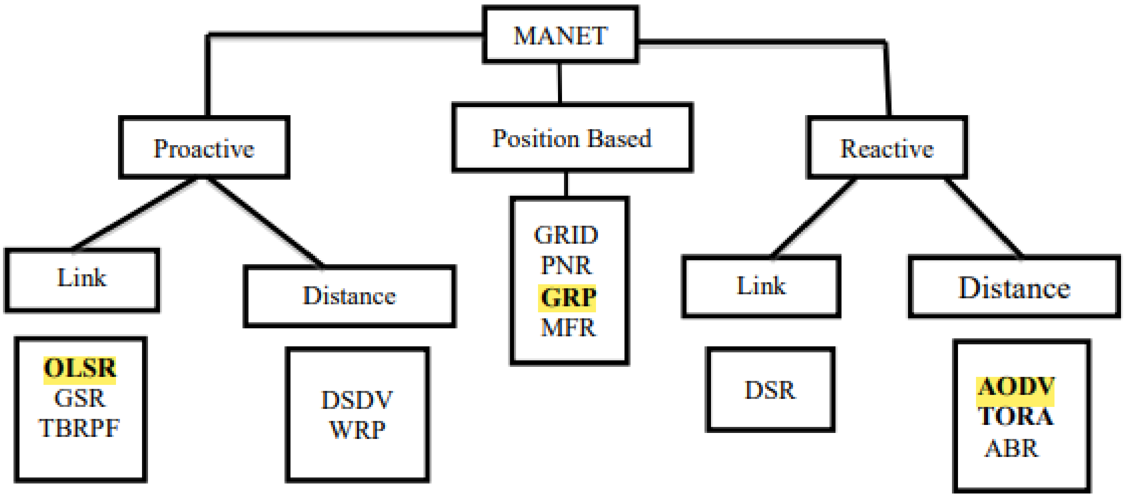

Figure 1. 1: Classification of MANET Routing Protocols[12].

1.2.1 Ad-hoc On-Demand Distance Vector (AODV)

AODV is a reactive routing protocol that maintains a routing table to store route information, helping to determine paths between a source and a destination. It includes four types of control messages: Route Error (RERR), Route Reply (RREP), Route Request (RREQ), and Route Reply Acknowledgment (RREP-ACK). AODV employs route discovery for data communication and broadcasts route error messages (RERR) to enhance packet delivery ratio (PDR). Its strengths include low network overhead and reliability in wireless mesh networks. The fundamental operations of AODV are detailed below [14].

1.2.2 Geographic Routing Protocol (GRP)

The Geographic Routing Protocol (GRP) is a position-based, proactive routing protocol developed by OPNET that selects routes based on the shortest geographical distance. Each mobile node utilizes GPS for accurate location tracking, which enables efficient data dissemination by partitioning the network into quadrants. When entering a new area, nodes update their location for flooding. They use a 'HELLO' packet to exchange information about neighbours and locations. The protocol also features route locking, allowing a node to backtrack and send a packet to the previous node if it cannot forward it, aiding navigation around blocked paths[15][16].

GRP partitions a network into quadrants to minimize route flooding. Each quadrant is defined as a square with user-specified dimensions measured in meters. The global area is segmented into these quadrants according to latitude and longitude coordinates, which span from -90 to +90 for latitude and from -180 to +180 for longitude. By knowing the position of a node, you can easily identify the quadrant it is in. The world is split into these quadrants, with latitude and longitude ranges from (-90, 180) to (+90, +180), each shaped like a quarter circle. Each quarter circle consists of squares. The user specifies the size of each quarter circle in meters. When flooding occurs, each node receives the locations of all reachable nodes. Flooding is triggered when a node moves beyond a set distance or enters a new quadrant. Both GPS coordinates and fixed reference points are used [15][16].

GRP improves performance through backtracking, using the Global Positioning System for accurate node locations. However, during shorter periods, GRP may work less efficiently, resulting in a higher packet drop rate due to more blocked routes[16].

1.2.3 Optimized Link State Routing (OLSR)

The Optimized Link State Routing (OLSR) protocol employs a proactive, table-driven routing approach that incorporates an optimized link-state algorithm. It significantly reduces the number of broadcast messages when transmitting data by implementing a system called Multipoint Relay (MPR). OLSR effectively reduces the high maintenance load of table-driven routing protocols, making it ideal for large, dense networks. It works well in distributed environments and is especially suited for dense, mobile networks[17]. Compared to traditional protocols, OLSR offers greater stability, reduces unnecessary flooding, and decreases control message retransmissions. Its main function is to select MPRs, which are essential for efficient message dissemination. MPRs forward broadcast messages, optimizing network-wide communication. OLSR nodes use Hello and TC messages for network control and maintain routing tables for all available paths. However, this method can increase network overhead and may lead to delays in larger networks[18]. The protocol relies on two primary control messages: Hello and TC messages. Hello messages are sent every 2 seconds, but require multiple transmissions to ensure consistency, which can cause them to miss rapid quality changes. Sharing these measurements across the network is necessary for informed routing decisions, yet this process often introduces significant delays. For example, OLSR's TC messages, sent every 5 seconds, are often delayed before being included in route calculations. As a result, routing protocols typically respond to link failures rather than preventing them. [19][20][21].

Link-state changes are detected by the periodic transmission and reception of hello packets, which indicate current link status. The frequency of these packets determines the sensitivity of link-state detection, with shorter intervals providing higher responsiveness. In the Optimized Link State Routing (OLSR) protocol, hello packets assess the link states between neighbouring nodes and facilitate the identification of two-hop neighbours. Each node broadcasts hello packets containing information about its neighbouring nodes, enabling all nodes to maintain both a neighbours table and a two-hop neighbours table based on the received packets[22].

1.3 Problem Statement

OLSR uses HELLO messages and TC messages to discover neighbors and maintain routes. Sending these messages too often creates unnecessary overhead, while sending them too slowly can lead to outdated routes and packet loss:

- Too many HELLO and TC messages = Wasted bandwidth (bad for network efficiency).
- Too few HELLO and TC messages = Broken routes when nodes move/disconnect (bad for reliability).

1.4 Proposed Solution

This thesis proposes a solution for adjusting HELLO and TC message intervals using neighbor feedback to minimize overhead while maintaining fresh routes. The solution is presented through key steps:

- Adjusts the intervals of HELLO and TC timing to be optimal according to network stability.
- This reduces wasted traffic while keeping connections strong, making it better.

1.5 Thesis Objective and Goal

This thesis aims to improve OLSR performance and compare it with three traditional routing protocols: OLSR, AODV, and GRP. The performance evaluation focuses on WLAN delay, throughput, and data drop metrics. The thesis objectives are explained in the following steps:

- The enhancement for OLSR routing can be made more efficient by optimizing the frequency of HELLO and TC messages, thus reducing unnecessary traffic while maintaining strong connections.
- Reduce data overhead, improve efficiency, and achieve a higher data transmission success rate.

Determining the optimal timing for retransmitting HELLO and TC messages in light, dense networks and node mobility, based on the interval between received HELLO packets from neighboring nodes.

1.6 Methodology

Achieving an optimal adjustment of HELLO and TC message timing in the OLSR by leveraging neighbor feedback involves tuning the message intervals to balance overhead reduction and route freshness. Here are the key steps for optimal adjustment:

1 **Neighbor Feedback Mechanism**:

- Nodes periodically collect feedback from neighbors regarding:
  - Link stability (signal strength, packet loss).
  - Route freshness (how recently topology updates were received).
  - Network congestion (delay, queueing effects).
- Feedback can be piggybacked in HELLO/TC messages.

2 **Adaptive HELLO Message Interval Adjustment:**

    - Increase HELLO interval if neighbors report stable links (light networks, low mobility) to reduce overhead.
    - Decrease HELLO interval if neighbors report frequent topology changes (dense networks, high mobility) to improve route freshness.

3. **Adaptive TC Message Interval Adjustment:**
    - **Increase the TC interval** if the network topology is stable (neighbors report minimal changes).
    - **Decrease the TC interval** if topology changes frequently (to ensure up-to-date routes).
    - Adjust based on **TC message validity time** (if a neighbor's TC expires too soon, decrease interval).

This methodology will focus on topology-based (proactive, reactive) and position-based (geographical) routing protocols with the aim of evaluating the performance of Enhanced OLSR (E-OLSR) with traditional OLSR, AODV, and GRP. These routing protocols are selected due to their excellent performance, as noted in research on Mobile Ad Hoc Networks (MANETs). To demonstrate the performance of enhanced OLSR, experimental simulations will be used to explain the effectiveness of the enhanced protocol. Different scenarios are implemented, involving the transmission of voice over IP (VoIP) through the network. The evaluation focuses on several key metrics, including delay, throughput, and data drop. In this study, OPNET Modular has been used for modelling and simulation. Various scenarios are implemented with different quantities of mobile nodes (30, 40, 50, and 60) with speeds up to 10 m/s and a workspace of 2000m x 2000m.

1.6.1 Validation & Convergence

Simulations/tests: The performance of enhanced OLSR will be compared against traditional OLSR, which uses default intervals for HELLO and TC messages. Simulation parameters are detailed in Chapter 4.

1.7 Literature Review

Researchers have analyzed MANET routing protocols using diverse simulators and traffic data.

- Diaa Eldein Mustafa Ahmed, Hala A. Ebrahim, Othman Omran Khalifa, "Performance Evaluation of AODV, OLSR, and GRP for Transmitting Video Conferencing over MANETs". This paper analyzes the performance of AODV, OLSR, and GRP for video conferencing over MANETs using OPNET 14.5. It aims to identify which protocol best supports video conferencing by assessing QoS metrics such as end-to-end delay, jitter, packet delivery ratio, throughput, and WLAN load under different network conditions. OLSR and GRP perform better than AODV in end-to-end delay and jitter, indicating that proactive protocols are preferable for delay-sensitive applications. OLSR also excels in throughput within dense networks, while AODV is better for network load due to its reactive nature. The study concludes that OLSR and GRP are suitable for video conferencing, but tuning their routing parameters could further reduce packet loss and congestion.

- Siyu Dong, Hong Zhang, "An MPR Set Selection Algorithm Based on Set Operation". In this paper, the analysis of the OLSR routing protocol's MultiPoint Relay (MPR) set indicates that it performs effectively in typical environments but faces challenges in more complex situations due to a limited reduction in nodes. This paper introduces a new algorithm for selecting MPRs that utilizes cycle and set operations, which enhances transmission success rates, although it may slightly increase delay. Future research will focus on optimizing this algorithm to improve its performance across various environments. This paper focuses on improving Multipoint Relay (MPR) set selection in the OLSR protocol using set and cycle operations. This algorithm aims to reduce unnecessary nodes in the MPR set, reducing network load and improving transmission success rate. Its drawbacks include increased latency from computational and implementation complexity, due to set and union operations requiring additional memory and computation compared to traditional methods. It also lacks details regarding message timing adjustment and neighbor feedback.
- Esmot Ara Tuli, Mohtasin Golam, Dong-Seong Kim, and Jae-Min Lee, "Performance Enhancement of Optimized Link State Routing Protocol by Parameter Configuration for UANET". This paper examines the performance of various topology-based routing protocols through simulations in different UANET environments. It specifically enhances the OLSR protocol to create E-OLSR, which surpasses the standard defined in RFC 3626. In terms of performance metrics such as throughput, delay, and data dropped, E-OLSR outperforms four other protocols (AODV, OLSR, DSR, and GRP). Additionally, a qualitative analysis of these routing protocols is provided, focusing on key factors like mobility, traffic density, routing overhead, and data rate. This research will guide network engineers in selecting the best routing protocol for diverse UANET implementation scenarios.

Hello interval parameters define the frequency of hello messages, used for neighbor discovery and maintenance. TC-interval parameters define the frequency of TC messages, used for topology discovery. These periodic intervals impact network overhead and route convergence.

Drones require more frequent updates due to rapid movement, so optimized OLSR might use shorter, fixed intervals. The goal here was to handle high mobility and dynamic topologies typical in drone networks. To improve mobile ad-hoc network (MANET) performance, adjustments can be made to time intervals. The goal is to find the best balance between minimizing overhead and maintaining route freshness, ensuring fast response times.

A need to compare the two environments exists. In this MANET study, OLSR hello and TC intervals are minimized to one and two seconds, respectively, which increases the number of packets.

On the other hand, for drones, the optimized OLSR might have lower hello intervals. However, the parameter-tuning approach in drones might involve higher frequencies to cope with mobility, leading to more hello packets than in MANETs, where intervals are adjusted dynamically. "In the UANET study by (Tuli et al. 2023), waiting times (including neighbor, topology, duplicate message, message ID, and HNA message holding times) were reduced to enable faster detection of lost nodes. Additionally, the willingness parameter was increased to 6 (high) from the default value of 3 to improve data transfer efficiency. However, the study did not specify the hello and TC interval values.

- Trilok Kumar Saini, Subhash C. Sharma, "Flexible multipoint relay selection for suitable route in mobile ad hoc networks". The paper proposed work that improves the MPR selection mechanism in OLSR, leading to better algorithm performance. This enhancement was achieved by incorporating specific fields into the packet structures and creating logic to make decisions based on available information. Simulation results demonstrate improved performance and applicability for mobile ad hoc networks. However, we also identified limitations that may impact the project's scope, such as dependence on the physical layer, insufficient information about selected nodes, and the possibility of manipulating trust parameters. We consider these findings to be useful for future developments.

The main difference between in this thesis and this paper is that in this paper, MPR selection is improved by exploiting information contained in HELLO messages (e.g., neighbors, traffic, battery), and then disseminating the results via TC messages, while in this thesis, the HELLO/TC message cycle is adaptively adjusted.

- Madhavi S. Avhankar, Dr. Janardan A. Pawar, Snehankita Majalekar, Suwarna S. Kedari. "Mobile Ad Hoc Network Routing Protocols – Using OPNET Simulator". This paper examines three commonly used routing protocols in Mobile Ad Hoc Networks (MANETs) and compares their performance through simulations in a 5 km x 5 km fixed-size network with 25 to 100 mobile nodes, using OPNET Modeler 14.5. The findings indicate that as the number of mobile nodes rises, OLSR outperforms AODV and GRP in both throughput and delay. As a result, the paper concludes that OLSR offers better performance than AODV and GRP in fixed-size MANETs with different numbers of mobile nodes. This research could be useful for those studying these protocols in MANETs.
- Halim Berradi, Ahmed Habbani, Nada Mouchfiq, and Mohammed Souidi, "Improvement of OLSR Protocol Using the Hello Message Scheme Based on Neighbors' Mobility". This paper examines how mobility affects routing protocols in Ad Hoc Networks and suggests an enhancement to the OLSR protocol that takes into account the geographical locations of neighboring nodes. Our objective is to extend the lifespan of routing paths for both data traffic and control messages by reducing the impact of node mobility. We estimate the remaining life of nodes based on their distance and send HELLO messages when nodes move out of Wi-Fi range to refresh topology information. Simulations show that our enhancement leads to fewer lost packets and reduced overall delays compared to the traditional OLSR version.

1.8 Thesis organization

This thesis is presented in seven main chapters:

- **Chapter 1** introduces MANET, presents related work, research questions, and the problem statement for this study.
- **Chapter 2** offers an overview of wireless networks, discussing their advantages and disadvantages, classifications, and the concept of ad hoc networks. It also examines the background, characteristics, configurations, and applications of mobile ad-hoc networks.
- **Chapter 3** describes different types of routing and classifies MANET protocols into three categories: reactive, proactive, and geographic routing.
- **Chapter 4** describes the research methodology, offering a step-by-step guide for conducting effective simulations in case studies.

- **Chapter 5** presents performance metrics---data dropped, delay, and throughput---of the AODV, GRP, and OLSR routing protocols. It offers a direct comparison of results between these protocols and concludes with a summary of their performance.
- **Chapter 6** evaluates the proposed enhancement scheme's performance. Simulations compared the enhanced OLSR's overall performance with the conventional OLSR.
- **Chapter 7** presents the conclusion and possible future work related to the research study.

Chapter Two:
Mobile Ad-hoc Network (MANETs)

2. 1 Introduction

A Mobile Ad hoc Network (MANET) is a type of Wireless Ad hoc Network (WANET) that supports numerous applications across various fields[28]. This chapter provides a detailed description of wireless networks, including their advantages, disadvantages, and further explanations

This study evaluates the effectiveness of different routing protocols in Mobile Ad Hoc Networks (MANETs). It concentrates on three types: topology-based (proactive OLSR and reactive AODV) and position-based (GRP [11]). The topology-based protocols are further classified as proactive, reactive, or hybrid[11]. The evaluation will focus on key metrics such as delay, throughput, and data loss that occur in MANETs, aiming to assess the performance of an enhanced OLSR compared to traditional OLSR, GRP, and AODV. The best-performing protocol among these will be selected.

2.2 Introduction to MANET

Mobile Ad Hoc Networks (MANETs) are decentralized, autonomous wireless systems composed of mobile nodes such as personal computers, mobile phones, personal digital assistants (PDAs), MP3 players, and digital cameras. These nodes communicate via wireless links, including radio waves and infrared. Characterized by their dynamic nature, MANETs facilitate peer-to-peer communication without reliance on a fixed infrastructure or predefined topology. While offering flexibility and adaptability, MANETs often present security challenges. These infrastructure-less networks are self-configurable, self-organizing, and self-managing, enabling nodes to move freely and arbitrarily within the network.[10][29][30].

These wireless nodes serve various roles: they can act as senders, receivers, or routers. As senders, they transmit messages to other nodes in the network; as receivers, they accept incoming messages. When functioning as routers, they forward packets to their destinations or the next router, and they can also buffer packets for later transmission. These nodes can be found in vehicles, ships, airplanes, or carried by individuals using small electronic devices[30][31].

Mobile ad hoc networks (MANETs) exhibit dynamism and adaptability, rendering them valuable across diverse applications. Their rapid deployment capabilities and requirement for only minimal configuration in exigent circumstances, including natural disasters, augment their utility. [31].
Ad-hoc applications, valuable in military and civilian operations like rescue and firefighting,

face capability constraints due to mobility, node density, topology changes, radio propagation, power consumption, network lifetime, computational power, and localization challenges[32].

Nodes in a network experience limitations in battery life, storage capacity, CPU power, and bandwidth. To enhance the speed of data transmission, it is necessary to reduce power consumption. In Mobile Ad Hoc Networks (MANETs), routing protocols define the rules for identifying the best path to send packets between nodes. These protocols utilize algorithms to discover routes and serve two main purposes: selecting the path from the source node to the destination node and ensuring that messages arrive at their intended destinations. The second purpose involves using the appropriate method to transmit data packets effectively[11], as illustrated in Figure 2.1.

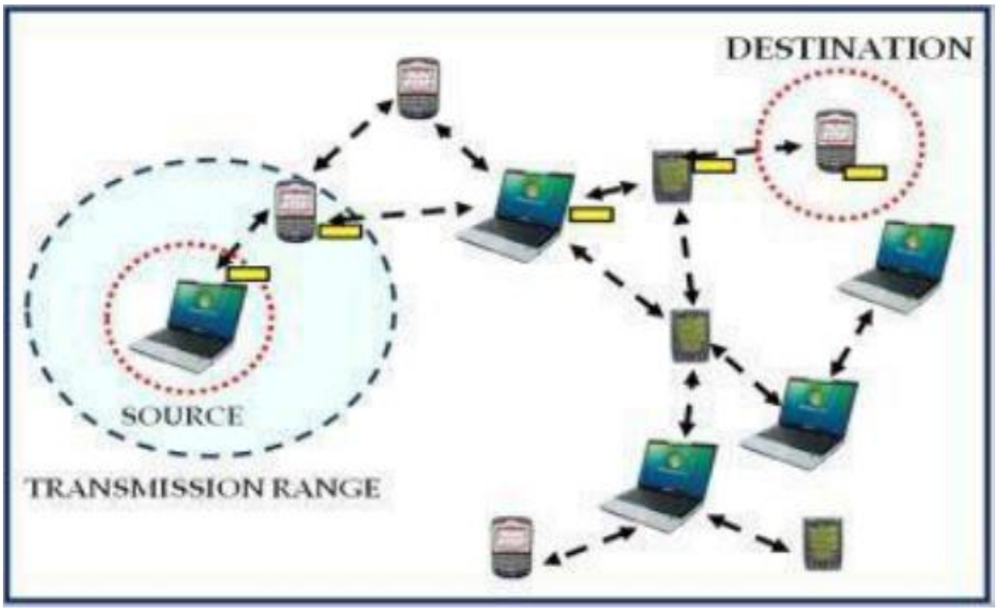

Figure 2.1: Data Transmission in MANET[3].

2.3 Wireless Network

Researchers are working to improve network performance in wireless communication and mobile devices. Their goal is to ensure that people can access information quickly, anytime, and anywhere.

A wireless network refers to the transmission and reception of data between two or more devices using wireless links, such as radio frequencies or infrared radiation, without physical connections like wires or cables, as long as the devices are within transmission range[31][10].

The following section discusses the advantages and disadvantages of wireless networks.

2.3.1 Advantages and Disadvantages of Wireless Networks

The following table show the advantages and disadvantages of wireless networks

Table 2.1: Advantages and Disadvantages of the Wireless Networks

Advantages	Disadvantages
.Mobility: Available everywhere on laptops and field devices.	Signal Interference: It can also be affected by obstacles like weather.
Economic: No wiring needed, so installation is easy and cheap.	Security risks: Signals vulnerable to compromise.
Easy to connect: Easy to install where cabling is difficult.	Health Risks: Prolonged RF exposure may harm health.
Quick Setup: Faster connections without cables.	Bandwidth Reduced: More connections lead to slower performance.
Durable: Resistant to weather and wear.	Additional Costs: Installation may incur extra equipment expenses.
Resilient: Less impacted by disasters like floods or fires.	Challenging Setup: Non-tech users might face setup difficulties.
Easy File Sharing: Wireless sharing saves time.	Reduced Speeds: Expect slower file transfers than wired connections.
Multiple Devices: Connect many users at once.	Range Limitations: Signal strength weakens with distance.
Social Media Access: Simple sharing on social platforms.	Dependence on Radio Waves: Connectivity relies on radio waves, affecting performance.
Increased Productivity: Collaborate anytime, anywhere.	
Cable-Free: Simplified connections without cables.	
Basic Needs Met: Covers essential internet needs, even if slower.	

Wireless networks are mainly divided into two categories: infrastructure wireless networks and infrastructure-less wireless networks (Ad-hoc)[31][10].

2.4 Classifications of Wireless Networks

Wireless networks can be classified in several ways, depending on factors such as the coverage area, network architecture, or the method used to access the radio channel[36]. One common classification divides wireless networks into two main categories based on their system architecture[37]: the first is infrastructure-based wireless networks with an Access Point (Cellular Networks), and the second is infrastructure-less wireless networks without an Access Point (ad-hoc wireless networks).

Ad-hoc networks serve several purposes, including military reconnaissance, attacks, civilian rescue operations, and firefighting. Initially, researchers categorized them into three types: MANET, VANET, and FANET. However, they did not account for underwater ad-hoc networks (UWVANET), which are significant for both military and civilian applications. The revised classification now recognizes four types: MANET, VANET, FANET, and UWVANET, as shown in Figure 2.2[38].

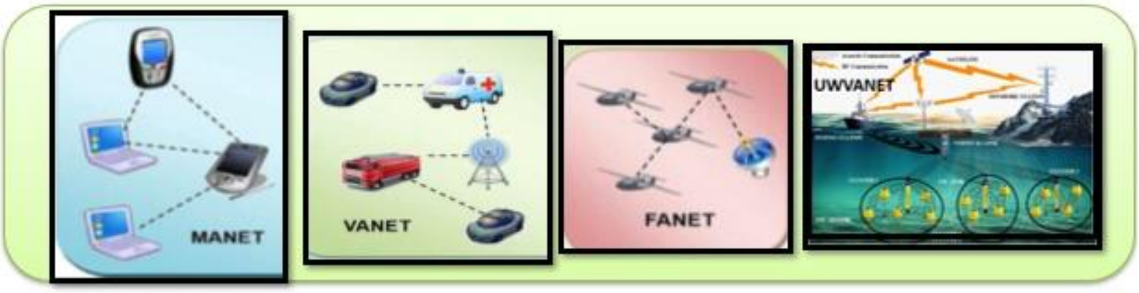

Figure 2.2: New Classification of Ad-hoc Network[38].

Figure 2.3 shows various wireless network types, including their basic categories and common examples. This chapter will mainly discuss Mobile Ad Hoc Networks (MANETs), which are the central topic of this thesis.

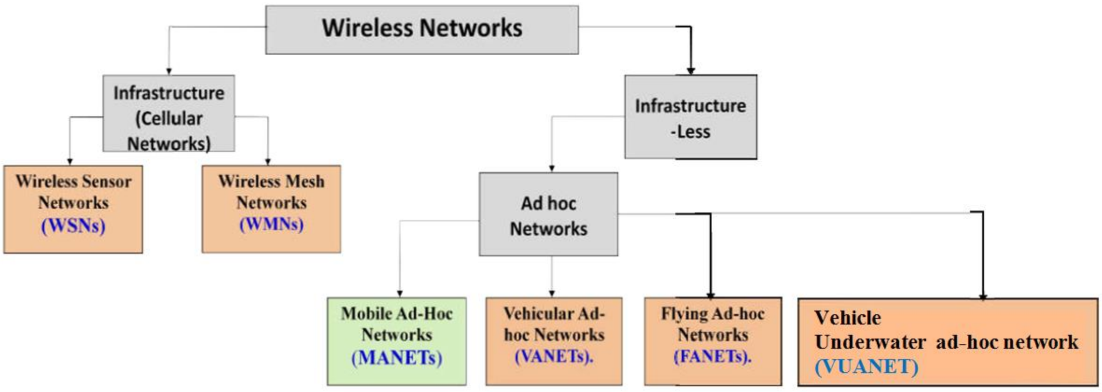

Figure 2.3: Classification of Wireless Networks

2.4.1 infrastructure-based wireless networks (Cellular Networks)

In this network type, a node can only join via a communication infrastructure, such as an Access Point (AP), Base Station Transceiver (BTS), wireless bridge, or wireless access router, as shown in Figure 2.4 [36].

All base stations and access points connect to the main network using wired links—such as fiber optic, twisted pair, or coaxial cables—or through wireless connections. A wireless node can connect to any access point within its radio range. An Access Point (AP) serves as the central coordinator for all devices within the network, facilitating connections and managing communication between Basic Service Sets (BSSs) to establish necessary communication routes. When a device wishes to send data to another device, it notifies the AP, which must be within the range of the sending station. If any node falls outside this range, communication will fail[39].

The main disadvantages of this AP-based wireless service include high overhead from maintaining and creating routing tables for all nodes, as the AP must keep its Basic Service Set (BSS) ready for network communication[40].

Infrastructure-based wireless networks are commonly implemented in various settings, including airports, offices, homes, and hospitals. In these locations, clients establish Internet connectivity via access points, facilitating reliable and efficient communication [2].

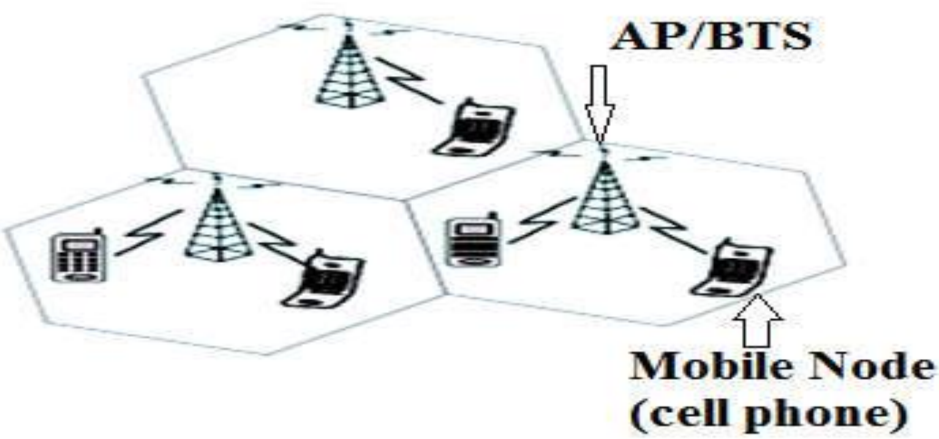

Figure 2.4: Infrastructure Network (Cellular Network)[10].

2.4.2 Infrastructure-Less Networks (Without Access Point or Ad-hoc Networks)

Ad-hoc Networks operate without any fixed infrastructure (infrastructure-less) and any central control[40].

The term "ad hoc" is derived from Latin and is defined as "for this," "for this purpose," or "for this (only)" [41][36].

An ad-hoc network consists of independent wireless devices that communicate via a wireless medium, such as radio waves or infrared, without depending on infrastructure like routers or access points. In this configuration, devices connect directly and serve as routers, forwarding data to other devices. Devices can freely join or leave the network, known as "peer-to-peer" mode[38][32] (shown in Figure 2.5).

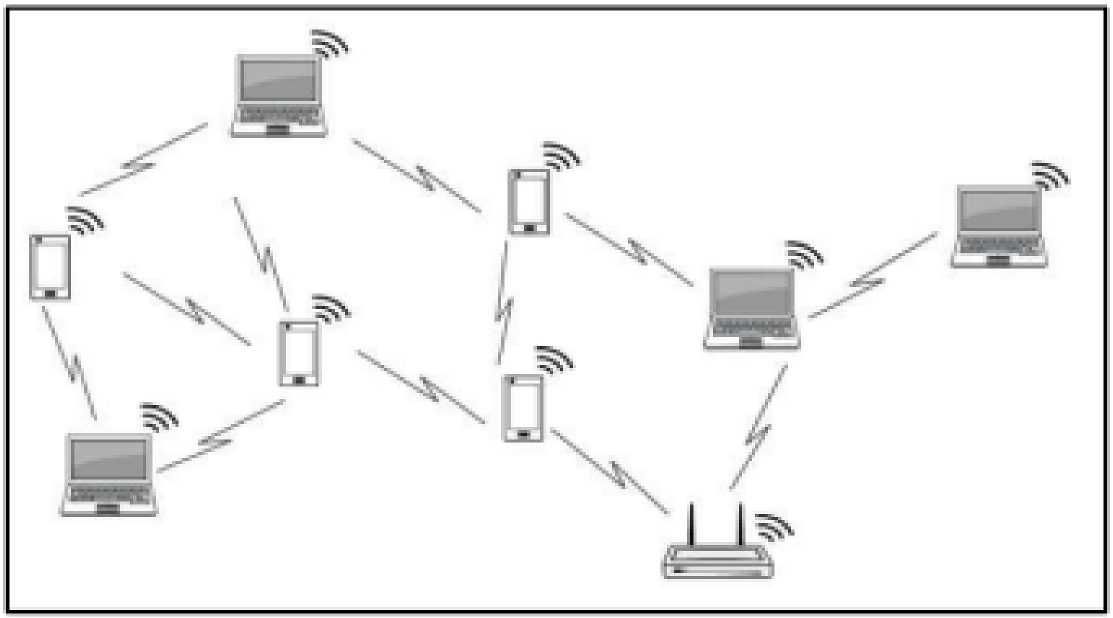

Figure 2.5: Infrastructure-less Network (Ad-Hoc Networks)[36].

2.5 The primary characteristics of an ad hoc network are as follows:

1 **Mobility:** This characteristic pertains to the movement of individual nodes or groups along either random or predetermined paths. Such mobility significantly influences routing and the performance of the network, as it necessitates continuous updates regarding the locations of the nodes when they shift positions.

2 **Multi-hopping:** This feature enables data to traverse through multiple nodes prior to arriving at its intended destination. It necessitates careful consideration of potential obstacles, spectrum reuse, and strategies for energy preservation to ensure optimal network operation.

3 **Self-organizing:** Ad hoc networks possess the inherent ability to autonomously establish their configuration settings and organizational structure, thus facilitating efficient deployment and adaptability in dynamic environments.

4 **Energy Conservation:** Given that mobile devices typically operate on limited battery supplies, it is critical to prioritize energy-efficient protocols in order to extend the operational lifespan of these devices.

5 **Scalability:** An increase in the number of nodes within an ad hoc network can complicate the management of routing and configuration, potentially adversely affecting the overall performance and reliability of the network[42].

2.6 Classifications of an ad hoc network

This ad hoc network is simple to set up and offers flexibility since devices are not required to remain connected. Ad hoc networks can be classified into two primary categories: Static Ad Hoc Networks (SANET) and Mobile Ad Hoc Networks (MANET).

2.6.1 Static Ad hoc Networks (SANET)

The wireless network consists of stationary nodes that either have low mobility or cannot move, enabling hosts to communicate through established connections[43].

2.6.2 Mobile Ad hoc Networks (MANET)

MANETs are wireless networks that operate without infrastructure or centralized control, functioning as autonomous systems that usually have a routable networking environment on top of a link-layer ad hoc network. They consist of a collection of mobile devices, such as smartwatches, laptops, cell phones, MP3 players, digital cameras, Personal Digital Assistants (PDAs), or any device with wireless capability, whether mobile or stationary, that can be a node in a MANET. For instance, an airplane or a ship equipped with a wireless radio can serve as a node in the network, just like a stationary personal computer, which has both a transmitter and a receiver with smart antennas. These nodes are interconnected through wireless links, enabling a self-configurable network topology where each node can move freely, resulting in dynamic connections [36][3][44][45].

Nodes communicate directly with each other in a peer-to-peer manner due to the lack of fixed infrastructure[36].

In a Mobile Ad hoc Network (MANET), there is no need for pre-existing infrastructure or central administration; each node is self-managed and self-configured. All nodes in the network function as either routers (servers) or as clients for other devices. When a node acts as a router, it serves as both a transmitter and a receiver for communication. If the destination is within the source's transmission range, the nodes can communicate directly without the need for a third party. This is known as "single-hop communication." If the destination is not directly reachable, communication relies on the nearest neighbor, which is called "multi-hop communication"[43][44][45].

When a node acts as the source, it requires other devices, also acting as nodes, to send the data. Each node can also be the destination. Overall, nodes operate in a developed, distributed manner, forming a mobile mesh network[44][45].

The network's topology changes constantly as mobile nodes join and leave. This frequent joining and leaving of mobile nodes in the network consumes a significant amount of energy[46].

The major challenges in ad hoc networks are routing and the characteristics of wireless communication, particularly due to increased interference and the possibility of asymmetric connections during data transmission. In these networks, effective communication relies on choosing a suitable routing algorithm, as the network continuously expands, contracts, and changes, complicating node communication. Therefore, having a robust and efficient routing protocol is crucial[36][47][48].

Ad hoc routing protocols are designed to handle the changing conditions of Mobile Ad Hoc Networks (MANETs). The success of these protocols depends on how much battery power the nodes use and how well they manage network traffic. It's important how fast the protocol can adjust when a connection is disrupted[47]. Some examples of ad hoc routing protocols are AODV, OLSR, and GRP. A more in-depth discussion of OLSR, AODV, and GRP can be found in Chapter 3 of this thesis.

Mobile Ad hoc Networks (MANETs) are specialized wireless networks that function autonomously without the need for dedicated infrastructure or centralized control. These networks are characterized by their ability to provide a routable networking environment supported by a link-layer ad hoc network. MANETs encompass a diverse range of mobile devices, including smartwatches, laptops, smartphones, MP3 players, digital cameras, and Personal Digital Assistants (PDAs), as well as any device equipped with wireless capabilities, irrespective of whether it is mobile or stationary. Notably, an aircraft or a maritime vessel outfitted with a wireless radio can serve as a node within the network, similar to a stationary personal computer that possesses both transmission and reception capabilities, such as smart antennas. The nodes within the network are interconnected via wireless links, facilitating a self-configuring network topology characterized by the mobility of each node, which leads to dynamic connections among the devices[36][3][44][45].

In a MANET, nodes engage in direct communication in a peer-to-peer fashion due to the absence of fixed infrastructure[36].

Each node is self-managed and self-configured, eliminating the need for pre-existing infrastructure or centralized administration. All nodes within the network may function as either routers (servers) or clients for other devices. When a node operates as a router, it plays the dual role of both transmitter and receiver for communications. If the destination node lies within the transmission range of the source node, direct communication occurs without the intervention of a third party, commonly referred to as "single-hop communication." Conversely, if the destination is beyond direct reach, communication must occur through the nearest neighbor node, known as "multi-hop communication"[43][44][45].

When a node acts as a source, it relies on other nodes to facilitate data transmission; each node is also capable of serving as a destination. As such, the nodes operate within a sophisticated, distributed framework, establishing a mobile mesh network. The topology of the network is in perpetual flux as mobile nodes enter and exit, which can lead to substantial energy consumption[44][45][46].

Significant challenges inherent to ad hoc networks include routing complexities and the unique characteristics of wireless communications, particularly heightened interference and the potential for asymmetric connections during data transmission. Effective communication within these networks is contingent upon the selection of appropriate routing algorithms, as the network's dynamic nature compels continual expansion and contraction, thereby complicating inter-node communication. Consequently, the development of robust and efficient routing protocols is imperativee[36][47][48].

Ad hoc routing protocols are specifically designed to accommodate the evolving conditions inherent in MANETs. The success of these protocols is influenced by factors such as battery power management and network traffic regulation, as well as their responsiveness to disruptions in connectivity[47]. Examples of prominent ad hoc routing protocols include AODV, OLSR, and GRP. A more comprehensive examination of OLSR, AODV, and GRP is presented in Chapter 3 of this thesis.

2.7 Advantages and Disadvantages of MANET

The following table show the advantages and disadvantages of MANET.

Table 2.2: Advantages and Disadvantages of the MANET

Advantages	Disadvantages
MANET connects with future 4G for tasks and communication anywhere[31][49][50].	Dynamic network structure obscures malicious node detection[49][50].
Installation is easy and requires little user input[50][31]..	High latency delays inactive node data[50].
Ad hoc networks access the Internet for multiple devices[31]..	Limited node resources (processing, bandwidth, storage) impair performance[49][51].
Ideal when fixed infrastructure is too costly or unreliable[31].	. Ad-hoc networks are more vulnerable to attacks[50][51].
The capacity, range, and energy aspects support the integration of these technologies with existing cellular infrastructures, enhancing coverage and connectivity[31]..	Wireless interference increases errors[51].
Each node acts as both a router and a host, independent of central network management, increasing system resilience[50][3]..	. Energy efficiency algorithms extend operation[51].
Reliability has improved through various methods[50].	Mobile nodes complicate dynamic routing; multicast needs multi-hop[52].
Base station planning and installation require less detail[31]..	Fluctuating communication quality hinders QoS management in dynamic environments[52].

2.8 CHARACTERISTICS OF MANET

There are several characteristics of MANETs, some of which are explained below:

1. **Dynamic Topologies:** In Mobile Ad hoc Networks (MANET), nodes move freely and at different speeds, causing quick and unpredictable changes in the network. The links between nodes can be two-way (symmetric) or one-way (asymmetric). This results in a high number of users and a lot of movement among them [3][10].
2. **Limited Bandwidth:** The bandwidth for wireless networks is significantly lower than wired networks due to factors such as multiple access, noise, congestion, signal interference, frequent changes in the links, and multipath fading[53].
3. **Infrastructure-less Nature (Peer-to-Peer Nature):** Since the nodes can move freely, the communication between nodes is peer-to-peer. There is no predefined base station or organization, and all devices have an equal role in the network. This means that each node

can act as a host and a router, demonstrating autonomous behavior, and the connectivity between nodes is intermittent. Therefore, the protocols designed for these nodes need to be robust enough to handle distributed topologies[10][53].

4. **Multi-Hop Routing:** MANETs enable multi-hop routing when the source and destination nodes are too far apart to communicate directly. Since the transmission radius is limited, messages pass through several nodes, with each node acting as a router to forward the packets[10][51].
5. **Constrained Resources (Light-weight Terminals):** In most cases, the nodes used in MANET devices are small handheld devices with limited CPU capability, low-power storage (battery-operated), and small memory size[10][51].
6. **Limited Device Security:** MANET devices are small, portable, and can operate anywhere, which raises the chances of them being lost, damaged, or stolen[10].
7. **Limited Physical Security:** Due to their wireless nature, MANETs are vulnerable to attacks like eavesdropping, jamming, spoofing, and Denial of Service (DoS) attacks. Although their decentralized design eliminates single points of failure, they are less secure than traditional networks. With nodes managing all tasks, security becomes complex, necessitating attention to eavesdropping and DoS threats. The lack of a centralized firewall further restricts routing and host security[10][49].
8. **Short-range Connectivity:** MANET employs radio frequency (RF) or infrared (IR) technology for short-range communication. It utilizes multi-hop routing to connect distant nodes and can be quickly deployed for temporary network connectivity without a fixed infrastructure[10].
9. **Distributed Nature of Operation:** MANET operates in a distributed manner mainly for two reasons: the diversity of the participating nodes and the lack of a central authority. This situation requires that network management tasks be shared among the different nodes[54].
10. **Easy and Rapid Deployment:** MANET provides advantages over wireless networks, including rapid deployment and reduced dependence on fixed infrastructure, allowing for quick network formation without base stations or system administrators[27].
11. **Heterogeneity in Node and Link Capabilities:** Network nodes may have multiple radio interfaces with varying capabilities across frequency bands, creating asymmetric links. Furthermore, differences in software and hardware can lead to varied processing abilities, complicating the design of adaptable protocols and algorithms[10].

12. **Fluctuating Link Capacity:** High bit-error rates in MANETs can be significant. Multiple sessions sharing a path experience noise, fading, and interference, and typically have less bandwidth than wired networks, due to the variety of wireless links involved in communication[10].

2.9 Manet's Applications

MANET's features—self-configuration, low deployment costs, flexibility, and infrastructure independence—are increasingly important as their applications grow in the commercial, military, and private sectors. They are particularly suited for environments with limited or no communication infrastructure, or where existing systems are too expensive or inadequate, such as for communications among autonomous vehicles, aircraft, and ground troops in battlefield scenarios where fixed infrastructure is lacking. MANETs are used in various applications, including [10][52][55]:

2.9.1 Military Applications:

In military establishments, information sharing is very confidential and must be encrypted. Ad hoc networks allow the use of standard networking technology to securely maintain encrypted communication between soldiers, vehicles, and military headquarters. The fundamental principles of ad hoc networks originate from this field[56][57].

2.9.2 Network For Emergency Services:

MANET is extremely useful for establishing communication during emergencies such as fires, floods, or earthquakes. In these circumstances, existing infrastructure may be damaged or non-operational. MANETs are particularly valuable because they do not require any fixed infrastructure to facilitate communication between affected individuals and rescue teams[57][58].

2.9.3 Education System:

The education system can greatly benefit from MANET, making learning more advanced, updated, and engaging. MANETs facilitate various educational environments, such as virtual conference rooms, online admissions, virtual classrooms, and e-learning, ensuring that students unable to attend school or university for any reason still have access to education. Additionally, online meetings, lectures, and e-student support services can be organized to share information and assist students with any questions they may have[57][59].

2.9.4 Civilian and Household Networking:

MANETs, including Personal Area Networks (PAN) and Bluetooth, facilitate information sharing in homes and offices, enabling easy setup of e-conferences and virtual meeting rooms. They support data exchange between portable devices like smartphones, cameras, printers, TVs, tablets, and laptops, and can also aid civil projects in remote areas[57][40].

2.9.5 Commercial and Business Applications:

MANETs enable e-payments anytime and anywhere, facilitating time-saving e-trading at trade fairs[57].

2.9.6 Sensor Network:

Every day, electronic devices have smart sensors and actuators that make our tasks easier. MANET enhances this system by enabling the monitoring of environmental factors such as temperature, chemical detection, and wildfire alerts. The technology tracks animal movements and aids in healthcare by utilizing wearable sensors in Body Sensor Networks to diagnose health problems. Additionally, these sensors can detect biochemical changes, chemical leaks, and instances of theft in shopping malls. RFID applications are useful for inventory tracking and toll collection; however, the battery life of sensors often limits their longevity [57][58][60].

2.10 Manet Architecture

The architecture of MANET is illustrated in the diagram (Figure 2.6). It is divided into four main layers: Middleware & Application, Networking, Enabling Technologies, and Cross-Layer.

2.10.1. Middleware & Application:

Wireless technologies like WiFi, Bluetooth, IEEE 802.11, WiMAX, and Hyper LAN have boosted the use of ad hoc technology and applications in fields like emergency services, disaster recovery, and environmental monitoring. MANET's flexibility makes it valuable for practical situations such as home networking, sensor networks, and more. New mobile ad hoc frameworks eliminate the need for middleware by requiring each application to handle its services[61][62].

2.10.2. Networking:

The networking protocols need to be redesigned for a self-configuring, dynamic, and unstable peer-to-peer communication environment. The aim is to develop reliable end-to-end services from a sender to a receiver using one-hop transmission services. A location service is required to dynamically map the address of the receiver device to its current location in the network[61].

2.10.3. Enabling Technologies:

Include antennas, medium access control, power control, and others, categorized by coverage area[62].

- **Body Area Network (BAN):** Connects wearable computing devices within a range of 1 to 2 meters[61].
- **PAN (Personal Area Network):** This network connects mobile services around an individual within a range of up to 10 meters[62].
- **WLAN (Wireless Local Area Network):** Has a communication range of 100 to 500 meters, enabling connection within a single building or across multiple buildings[61].

2.10.4. Cross Layers:

The MANET architecture has several layers that manage the system. It focuses on using energy efficiently and providing better service quality.

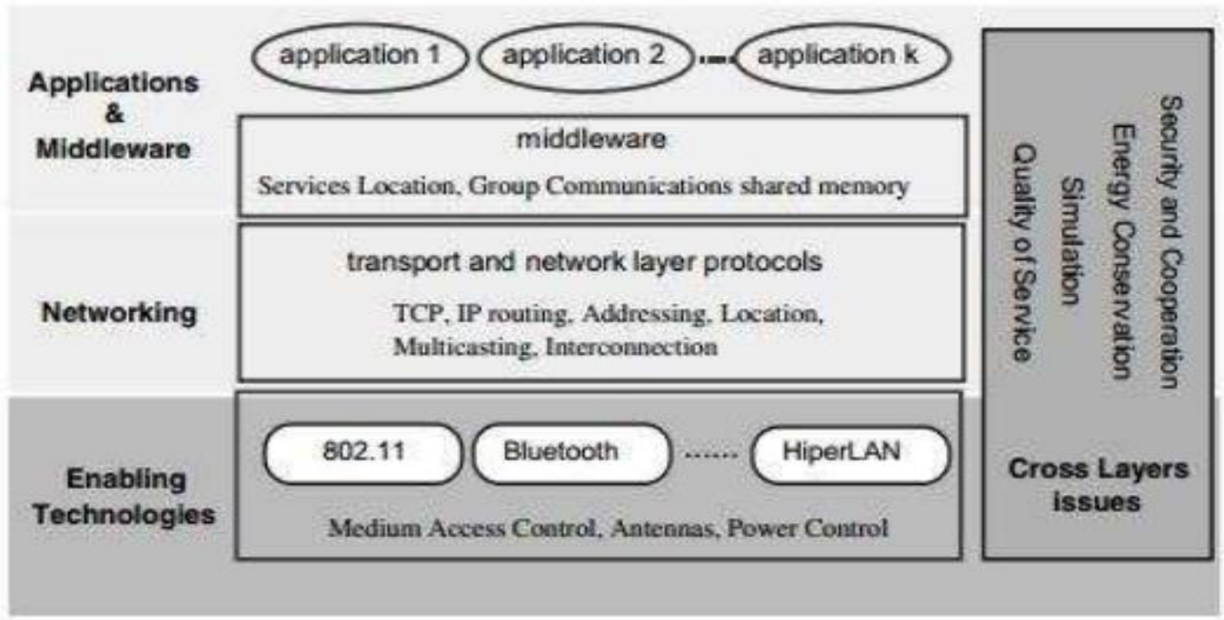

Figure 2.6: Architecture of MANET[61]

2.11 Types of MANET

2.11.1. Vehicular Ad Hoc Network (VANET)

It is a type of mobile network that allows communication between nearby vehicles (and roadside equipment). Its main purpose is to improve safety and comfort for travelers by equipping each vehicle with a special electronic device that creates a network for passengers. This network functions independently of traditional infrastructure or client-server systems. Each vehicle with VANET technology acts as a node, capable of receiving and sending messages wirelessly. Key features include collision warnings, road sign alerts, and real-time traffic updates, providing drivers with important information for their journeys. Additionally, passengers can enjoy multimedia content and internet access within the vehicle's wireless range. VANET also supports automatic payments for parking and tolls, among other usages[34][63].

2.11.2. Intelligent Vehicle Ad-hoc Networks (INVANET)

Uses artificial intelligence to improve communication between vehicles (V2V) and between vehicles and roadside infrastructure (V2R). Its primary goal is to address roadside emergencies, like vehicle accidents. When a vehicle equipped with an INVANET device is in an accident, it automatically sends out an alarm[34]

2.11.3. Internet-Based Mobile Ad hoc Networks (iMANET)

Combines traditional wired networks, like the Internet, with Mobile Ad Hoc Networks (MANET) to provide users with ongoing access to Internet services and information. The increasing demand for internet connectivity has driven the creation of iMANET, which employs Internet protocols such as TCP/UDP and IP. It uses a network-layer routing protocol to automatically connect mobile nodes and establish routes [34][61].

2.11.4. Flying Ad Hoc Network (FANET)

It is composed of unmanned aerial vehicles (drones), providing mobility and connectivity to remote areas[29].

2.11.5. Smartphone Ad hoc Network (SPANC)

It enables the formation of a peer-to-peer network independent of cellular carriers, wireless access points, or traditional infrastructure, allowing peers to join or leave without disrupting the network[29].

Chapter Three:
Routing Protocols in MANET

3.1 Introduction

Routing is the process of transferring information from a source to a destination within an internetwork, typically passing through one or more intermediary nodes. [12]

The routing process consists of two primary activities. The first is identifying optimal routing paths by selecting the shortest route that minimizes both the number of intermediate nodes and transmission time. The second activity involves transmitting data in packets by establishing connections and communication among mobile ad hoc network (MANET) nodes. This process depends on specific communication rules between nodes, known as protocols.

Protocols are defined as rules that facilitate communication between devices, including mobile nodes, computers, and other electronic devices. In mobile ad hoc networks, routing protocols enable mobile nodes to establish connections and exchange data packets. Routing in these networks primarily relies on routing tables to manage data paths[5].

Routing protocols employ metrics such as hop count to determine the most efficient path for packet delivery. Routing algorithms generate and update routing tables that contain comprehensive route information for data packets[12].

The type of routing information maintained depends on the specific algorithm implemented. Routing tables record the direction of data packets, and route selection may vary for different packets. Typical routing table entries include the destination IP address and the next hop toward the target node [12].

During the routing process, data packets are transmitted using different methods. The first method is unicast, where the source sends data packets directly to one specific destination. The second method is multicast, in which the source sends data packets to a select group of multiple nodes within the network. The third method is broadcast, where the source sends messages to all nodes, both nearby and far away, in the network. An example of broadcasting is flooding, which is commonly used[5].

3.2 Routing protocols processes

Routing operations in Mobile Ad Hoc Networks (MANETs) occur in three stages, as illustrated in Figure 3.1.

Routing protocols work in three steps: first, they discover routes; second, they forward data; and third, they maintain the routes.

1. The routing process begins with the route exploration stage, when a node needs to establish a connection with another node and begins searching for a route.

2. Communication begins when a path to the target is found, and here, the forwarding data stage begins. If a link is interrupted during data transmission due to node movement or power failure, an alternative path must be provided to ensure continuous communication.

3. The route maintenance phase deals with Communication outages. At this stage, when the node detects a path interruption, it tries to search for an alternative path in the local cache. If an alternative route cannot be found in memory, the node starts the route exploration phase again to find a new route to the same destination

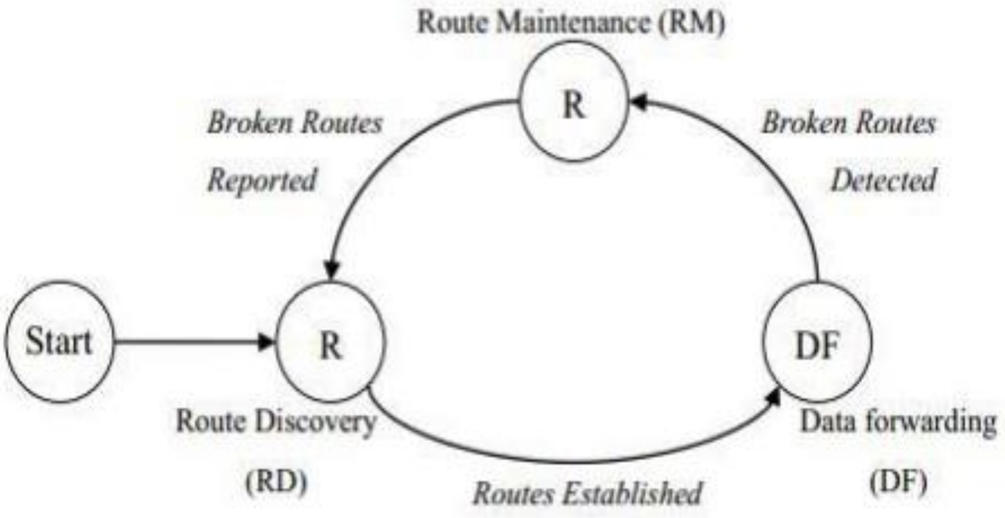

Figure 3.1: Stages of the routing process in networks[64].

3.3 Objectives Routing Protocols.

All routing protocols should aim to enable communication between routers in various locations, ensure correct and efficient routing decisions, share information with nearby routers, construct error-free routing tables, and discover existing routes [65].

3.4 Routing algorithms classification

Routing is mainly classified into two main types, as follows

3.4.1 Static routing

Administrators manually configure this routing type to direct data packets to specific destinations permanently[43]. Once these routes are established, no administrator can change them[31]. A network administrator typically creates a static routing table [34], eliminating the need for the router to generate its routing tables[43]. This routing table operates independently of the network's current status, so it doesn't depend on whether the destination is active[34].

Static routing is typically used for small networks. Network administrators have better control and understanding because they set up the paths themselves. This allows them to choose the most reliable routes for specific types of traffic. Static routing is easy to set up and requires less processing power and memory, which is a significant advantage. However, a major drawback is that when the network topology changes, manually reconfiguring the routes can become very challenging[65].

3.4.2 Dynamic Routing

Dynamic routes are chosen by routing protocols. This process is automated by the router, which directs traffic based on the routing table[65][31].

Dynamic routing has several advantages, including flexibility and the ability to reduce traffic overload. It allows for different paths to be used when forwarding data packets from the source to their destinations[43]. When a router is added or removed from the network, it communicates its status by flooding the network with information packets. This ensures that all routers become aware of the changes. This process is similar to how network segments operate in dynamic routing[34].

Although dynamic routing protocols provide numerous advantages, they also present some challenges. In dynamic routing, routing tables are created based on routing protocols and their path calculation algorithms. A notable disadvantage is that dynamic routing protocols typically demand greater processing power and memory resources. Additionally, each dynamic routing protocol employs different methods and techniques to determine the best path[65].

Dynamic routes are divided into two main types: interior gateway routing protocols(IGP), which help select routes within a single autonomous system, and exterior gateway routing protocols(EGP), which handle routing between different autonomous systems[65]. Routing protocols can be classified as shown in Figure 3.2.

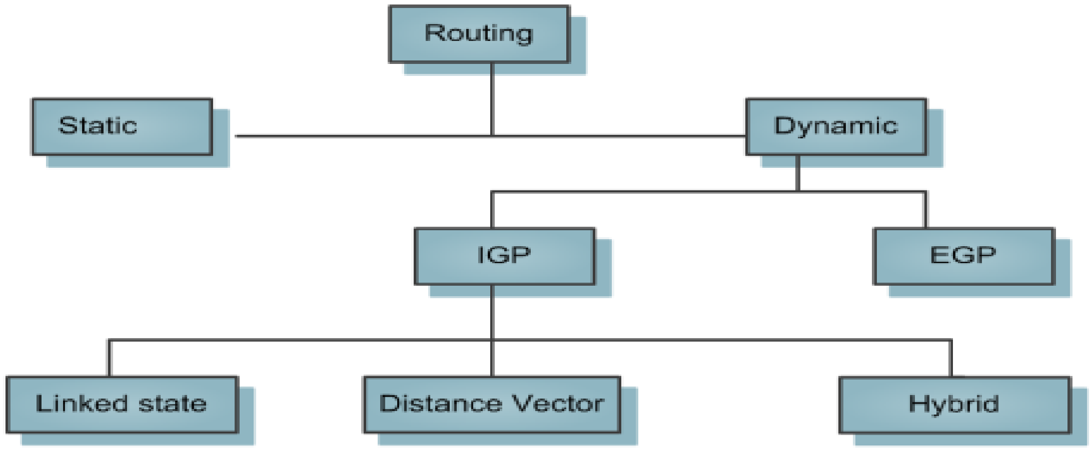

Figure 3.2: Classification of Routing Protocols[65]

3. 5 Classification of Traditional Dynamic Routing Protocols

Dynamic routing protocols are classified based on the information exchanged among routers and how they utilize this data to create their routing tables[34]. Protocols such as distance vector, link state, and source routing are commonly used in networks . Most of the available protocols can be classified into one of these categories.

3.5.1 Distance Vector Protocols

Distance Vector protocols, as the name suggests, focus on two primary parameters to determine the best route: Distance and Vector. "Direction" indicates the address of the next hop and the exit interface. In contrast, "Distance" refers to metrics such as the number of hops. A major example of Distance Vector Routing Protocols is the Routing Information Protocol (RIP). Both RIP Version 1 and RIP Version 2 utilize the Bellman-Ford algorithm to calculate the paths[65][66].

The Routing Information Protocol (RIP) uses "hop-count" as its metric, meaning lower numbers are preferred for routing decisions. RIP is mainly designed for smaller networks and has a maximum hop limit of 15 [65].

In a distance vector routing algorithm, each node maintains a routing table that contains the destination IP address, the distance to that destination, and the next node along the path. The router periodically broadcasts this information to its neighboring nodes and updates its routing table based on the information it receives. This process ensures that the routing tables are always current, allowing the router to select the shortest route to the destination. Both table-driven and on-demand protocols can use distance vector routing[50]. Unlike source routing, routers that use the distance vector protocol do not know the complete path to a destination[66].

A problem with the distance vector routing protocol is that it does not have complete knowledge of the full network's structure[65]. One example of a distance vector routing protocol is AODV, which is one of the protocols used in this message.

3.5.1.1 Advantages and Disadvantages of Distance Vector routing protocols.

The following table shows the advantages and disadvantages of the distance vector routing protocol.

Table 3.1: Advantages and Disadvantages of the Distance Vector routing protocols

Advantages	Disadvantages
Simple algorithms, which work well in smaller networks.	Probability of occurrence of routing loops.
Easy to implement.	Periodic updates can slow down the conjunction.
Use less memory and processing power compared to Link-State Routing (LSR).	Limit on the number of hops in DVR protocols.
	The Bellman-Ford algorithm has fewer metrics than Link-State protocols [65].

3.5.2 Link-State Protocols

Link-state routing is based on the idea that each node creates a graph representing the entire network's connectivity, illustrating how the nodes are connected. Each node independently determines the best path to every possible destination, generating its routing table. This method differs from distance-vector routing protocols, in which nodes share their routing tables with their neighboring nodes[66].

The link-state routing algorithm, often called the Shortest Path First (SPF) algorithm, is based on Dijkstra's technique and can be utilized by both table-driven and on-demand routing protocols[55].

In a link-state protocol, nodes share connectivity information through continuous HELLO messages, communicating details about their neighbors instead of full routing tables. This method reduces broadcast overhead and ensures reliable communication[55][66].

Each node must first identify its connected ports. Then, periodically and in response to any link changes, nodes exchange HELLO messages and send link-state advertisements (LSAs) to identify themselves and their connected nodes, including a sequence number[66].

To create a connectivity map, nodes exchange Link-State Advertisement (LSA) information that details neighboring devices. Any changes in links are communicated through a process called flooding. Each node maintains a consistent database, known as a topology table, which tracks the link costs throughout the network. This data is used to construct a routing table that includes link costs, paths, and neighboring nodes. Dijkstra's algorithm is applied to determine the optimal path and cost for each link. Although link-state protocols are more resilient, they are also more complex compared to distance vector (DV) protocols [65][66].

Two link-state routing protocols are the OSPF routing protocol, an example of a wired network, and the OLSR (Optimized Link State Routing) routing protocol, an example of a Mobile Ad hoc Network[55].

3.5.2.1 Advantages and Disadvantages of Link-State Routing Protocol

The following table shows the advantages and disadvantages of the Link-State routing protocol.

Table 3.2: Advantages and Disadvantages of the Link-State Routing Protocol

Advantages	Disadvantages
Each router shares the same database.	Requires a lot of memory.
Supports a hierarchical structure.	Difficult to set up and understand.
Maintains multiple paths for destinations in the topology table.	Uses advanced algorithms.
Ensures efficient, rapid connection without loops.	Needs more processing power.
Utilizes more precise metrics [65].	Often fails to adjust to link changes quickly [65].

Other Dynamic routing can be classified as:-

3.5.3 Source routing

Source routing is a technique. Each data packet contains information about the entire path to be followed in the network, and puts this routing information in the packet's header. Based on this information, the sending node determines the best route to the destination. The intermediate nodes only pass the packet along without needing to store any routing details. Many routing algorithms use the broadcasting mechanism to distribute control information, i.e., send it from the source node to all network nodes. The source node sends its routing table information to all neighboring nodes, which in turn send this information to their neighboring nodes, thus reaching all network nodes. This technique simplifies troubleshooting, enhances trace-route functions, and allows the sender to explore all possible routes to a host. Additionally, it gives the sender control over network performance by enabling the selection of specific routes to avoid congestion in other areas. However, a disadvantage is that the packet size increases, as each packet must carry the complete path information [66][67][68].

3.6 Routing in Mobile Ad-hoc Networks

Routing protocols define the rules for transferring packets between nodes in a Mobile Ad Hoc Network (MANET). They outline the primary parameters that guide this communication[15]. Ad-hoc nodes in wireless networks serve two main functions: they act as routers to direct data packets to various nodes in the network, and also serve as hosts themselves. This dual role presents several challenges in ad-hoc wireless networks, which lack a fixed infrastructure. These challenges include dynamic changes in network topology, limited bandwidth, restricted battery power at each node, frequent link failures, interference, and limited resources. As a result of these challenges, traditional routing protocols are typically unsuitable for Mobile Ad-hoc networks for several key reasons.

- Distance vector and link-state routing protocols are designed for use within static network environments, rather than in dynamic or changing situations.
- Traditional routing protocols use control packets that are sent at regular intervals. This approach can be costly in mobile wireless networks because it uses bandwidth, drains battery power, and puts a strain on the processors of wireless nodes.

Routing discovery and maintenance are crucial challenges in these networks. In this section, we will focus on the most significant issues affecting the development of routing protocols for MANET [34][11].

3.6.1 Problems with routing in Mobile Ad-hoc Networks

1**. Asymmetric links:** Traditional wired networks typically have symmetric links, which provide a stable and fixed connection. On the other hand, ad-hoc networks consist of mobile nodes that often change their positions. For example, in a Mobile Ad-hoc Network (MANET), if node B sends a signal to node A, it doesn't give any information about the quality of the return connection from node A to node B[69].

2**. Routing Overhead:** In wireless ad-hoc networks, nodes often change locations. This causes outdated routes in the routing table, resulting in unnecessary routing work[34].

3. Dynamic Topology: A major challenge of ad-hoc routing is that the network structure is often unstable. Mobile nodes can move, and the characteristics of the communication medium may change. As a result, routing tables in ad-hoc networks need to adapt to these changes in topology, requiring flexible routing algorithms. In contrast, in a fixed network, routing tables are updated every 30 seconds. However, this update frequency may be too low for the rapidly changing conditions in ad-hoc networks [68].

4. Interference: Interference is a significant issue in mobile ad-hoc networks. This occurs because the connections between nodes can be unstable and change continually due to transmission conditions. One transmission may interfere with another, and a node can overhear signals from other nodes, which could result in errors in overall communication [34][68].

3.7 Characteristics of an Ideal Routing Protocol for MANETs

A routing protocol must have the following fundamental characteristics:

1- Every device can self-start and self-organize[47].
2- It must be completely distributed[70].
3- Capable of adjusting to quick changes in network structure by proposing new routes[70][71].
4- Transmission must be dependable to minimize message loss[70].
5- The devices should be quickly converged once the network structure is stable[47][70].
6- Make the best use of bandwidth, computing power, memory, and battery life[70].
7- Presents a specific level of Quality of Service (QoS)[70].
8- It should be a loop-free, multi-hop environment among the devices, have minimal control overhead, be aware of Quality of Service (QoS), be energy-aware, be location-aware, and be security-aware[47][70][71].
9- It can also handle larger networks[47].

At present, there is no routing protocol for mobile wireless networks (MANETs) that incorporates all the desired features. This lack of development is due to the protocols for MANETs still being underdeveloped.

3.8 Main design criteria for routing protocols in MANETs

1. The primary design criteria are:
2. Scalability and reliability.
3. Dynamic topology support.
4. Route maintenance and updates.
5. Distributed processing with lightweight computations.
6. Simplicity and ease of implementation.
7. Fault tolerance[70].

3.9 CLASSIFICATION OF MANETs ROUTING PROTOCOLS

Routing protocols in Mobile Ad Hoc Networks (MANETs) can be classified in various ways. The most common classifications are based on the routing strategy and the network structure[34]. This is illustrated in Figure 3.3.

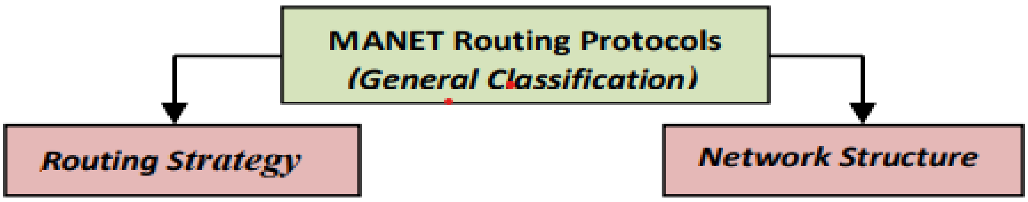

Figure 3.3: 1:MANETs routing protocols (Main Classification)[70].

Routing protocols can be classified based on their routing strategy into two categories: table-driven and source-initiated (which includes demand-driven, source-driven, or on-demand), as illustrated in Figure 3.4.

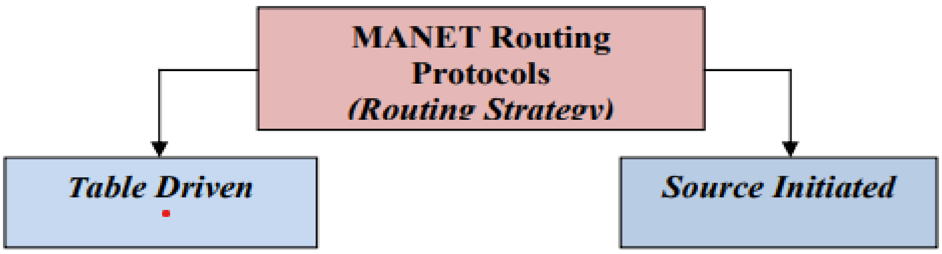

Figure 3.4: MANETs routing classification based on (routing strategy)[70]

Depending on the network structure, there are three types of routing: Uniform (flat) routing, hierarchical routing, and geographic (location-based) routing [34][70]. Flat routing covers both routing protocols based on the routing strategy (both the table-driven and the source-driven routing protocols) [34], as shown in Figure 3.5.

In this section, we will discuss routing protocols based on network structure. This subject is important because it has attracted significant interest from researchers and the industry[70].

In this thesis, I will focus on two main categories of routing protocols for MANET: Topology-based (proactive and reactive) protocols and Position-based (geographical) protocols. This is because the three protocols used for research fall under them, which are AODV (Ad Hoc On-Demand Distance Vector Protocol), which is reactive (On-demand); OLSR (Optimized Link State Routing), which is proactive (Table-driven); both AODV and OLSR are Topology-based protocols, and GRP (Geographic Routing Protocol), which is a Position-based Routing Protocol, to evaluate the performance of Enhanced OLSR (E-OLSR) with traditional OLSR, GRP, and AODV.

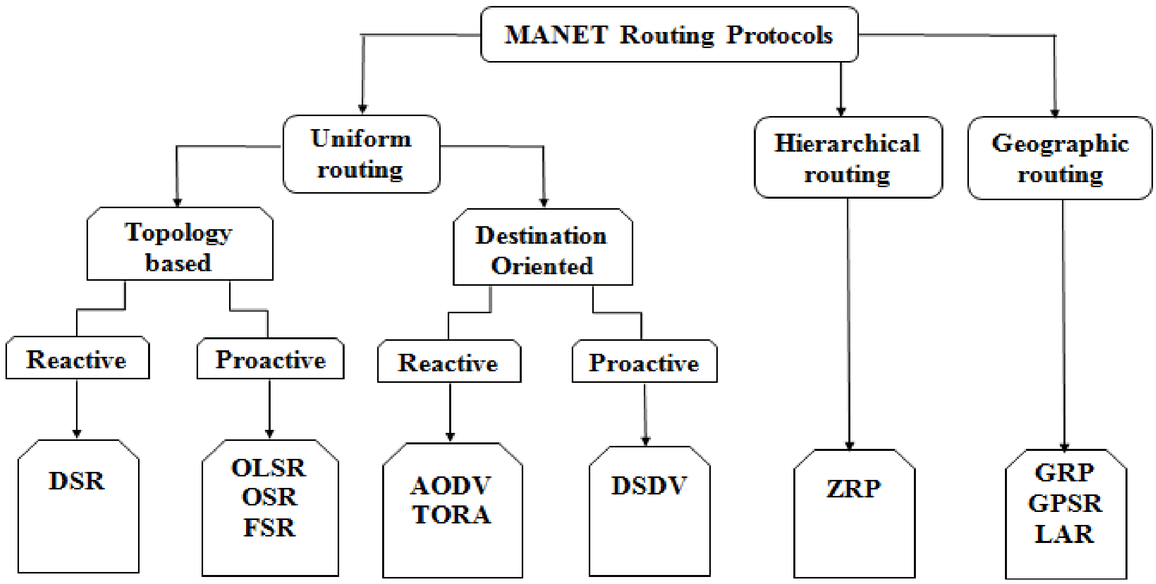

Figure 3.5: MANETs routing classification based on the (Network Structure)[71].

3.9.1 Flat Routing (Uniform) or (Topology Based)

These protocols need topology information from all communicating nodes to establish and maintain the optimal data transmission route. Topology-based routing protocols require comprehensive topology information to determine packet forwarding and routing paths[72].

Topology-based routing protocols typically perform worse than geographical (position-based) routing protocols, which utilize additional information to ascertain node locations. Routing protocols often rely on knowledge of node topology when making decisions. They can be categorized into three types: proactive (table-driven), reactive (on-demand), and hybrid routing protocols[11][70].

3.9.1.1 1Proactive or (Table Driven)

The network is constantly checked to find all possible routes between nodes. This enables the discovery of new routes while ensuring that the current routes remain valid[70]. Proactive routing primarily relies on link-state (LS) protocols[73]. These protocols use routing tables to maintain and regularly update routing information in response to changes in the network structure. Control messages are continuously exchanged throughout this process[42][69]. This protocol is designed to be proactive, meaning that each mobile node maintains an up-to-date routing table for all other nodes in the network. This approach reduces delays in determining routes. To maintain accurate tables, nodes must frequently share routing information, even if they are not actively using those routes[72]. And they are periodically updated whenever there is a change in the network structure [42]. Control messages are sent at regular intervals, even when no data is transmitted. This redundancy makes proactive routing protocols inefficient as they unnecessarily consume bandwidth[31].

The proactive routing algorithm consists of three steps: neighbor/link sensing, multipoint relaying, and link-state messaging and route calculation[47].

The main advantage of these routing protocols is that nodes receive route information instantly, enabling them to initiate a session immediately[47].

The main disadvantages are that the nodes store excessive data for managing routes and that it takes considerable time to reorganize when a link fails[46]. Furthermore, routing protocols use different numbers of tables. Proactive protocols aren't ideal for large networks because they require each node to keep track of every other node in its routing table. This increases routing table overhead and consumes more bandwidth[34].

We will discuss OLSR and GRP in our thesis report as examples of proactive routing protocols.

3.9.1.1.1 Optimized Link State Routing (OLSR) protocol

The OLSR protocol is an enhanced link-state algorithm commonly used in Mobile Ad Hoc Networks (MANETs), Vehicular Ad hoc Networks (VANETs), and Underwater Ad hoc Networks (UANETs). Clausen and Jacquet (2003) optimized link-state routing for large, dense networks by using selected nodes known as multipoint relays (MPRs)[24].

The Optimized Link State Protocol (OLSR) is a proactive routing protocol, meaning routes are always readily available when required[74]. It is also called a table-driven protocol because it consistently maintains and updates its routing table[31].

Each node (or device) in the network keeps a routing table that shows how to reach every other node[10]. This table provides quick access to routing information whenever it's needed. The OLSR protocol uses a step-by-step (hop-by-hop) routing method, where each node uses its information to send packets. This method works well for networks with random and uneven traffic[55][76].

OLSR works well in large and crowded mobile networks because it uses MPRs to optimize performance: the bigger and denser the network, the better the optimization compared to the standard link-state algorithm[76]. OLSR is an improved version of the standard link-state protocol[72].

OLSR is an optimized link-state protocol that employs Multipoint Relays (MPRs) to minimize retransmissions within a region, thereby reducing overhead and saving battery life. Figure 3.6 compares MPR flooding with traditional full flooding. In full flooding, all nodes retransmit control messages, causing duplicates. MPR flooding limits retransmission to MPR nodes, reducing overhead. Each node selects neighbor MPRs for efficient packet retransmission. MPR nodes keep a selector set of nodes that select them[42].

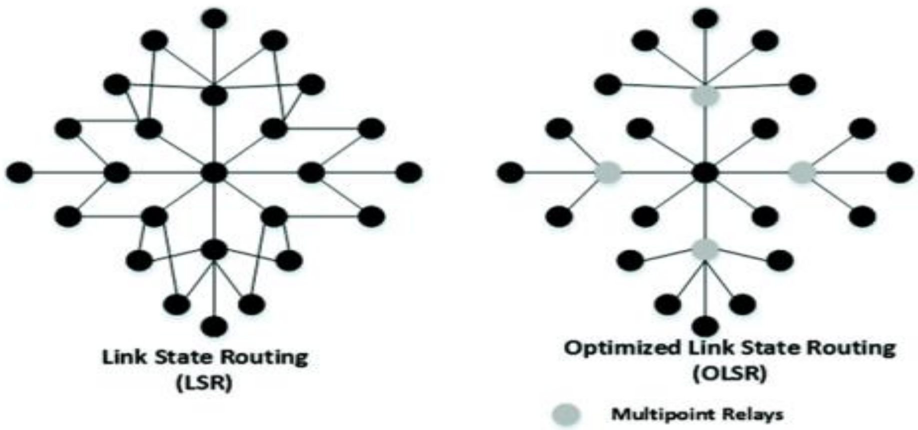

Figure 3.6: Route construction using MPR in the OLSR protocol[76].

The selected set of MPRs ensures coverage of all nodes within two hops. This configuration ensures that all nodes within this radius (neighbors of neighbors) have symmetric links with the MPR nodes, actually connecting them to every node within two hops. Information about the MPR is updated whenever changes are detected in nodes one or two hops away. This set should also be the smallest group needed to send out the fewest packets. MPR (Multipoint Relay) refers to a neighboring node that a node chooses to forward packets to.

When there are changes in the network topology, every node must select a group of its neighboring nodes to retransmit its packets. This group is known as the MPRs of that node. Nodes that are not included in the MPR set will only read and process the packets but will not retransmit them[72][[76]. Because only the node chosen as the Multi-Point Relay (MPR) sends out control messages. This MPR node creates link state information only with itself and the nodes it selects as MPRs. In the OLSR protocol, choosing the MPR set is very important. This choice directly affects how well the network performs[10]. To select the MPRs, each node periodically sends out hello messages that include a list of its one-hop neighbors[72]. OLSR uses three types of control messages: HELLO, Topology Control (TC), and Multiple Interface Declaration (MID) messages[76].

1. **HELLO messages** are used to determine the status of connections, detect neighboring nodes, and allow neighbors to select a Multipoint Relay (MPR) set during this process. This MPR set indicates which neighboring nodes have chosen a specific node as their MPR. As a result, this node can identify its own MPR set. HELLO messages are only sent to devices that are one hop away[71][75]. These messages are sent at predetermined intervals in OLSR to determine link status, as shown in Figure 2.3. If node A and node B are neighbors, node A sends a HELLO message to node B. If node B receives this message, it indicates that the link may be asymmetric. If node B then replies with the same HELLO message to node A, this is considered an asymmetric (unidirectional) link. On the other hand, if node A and node B can communicate both ways, it is classified as a symmetric (bi-directional) link, as shown in Figure 3.7. The HELLO messages provide information about all neighboring nodes, enabling each mobile node to keep a table that tracks all its multi-hop neighbors[31].

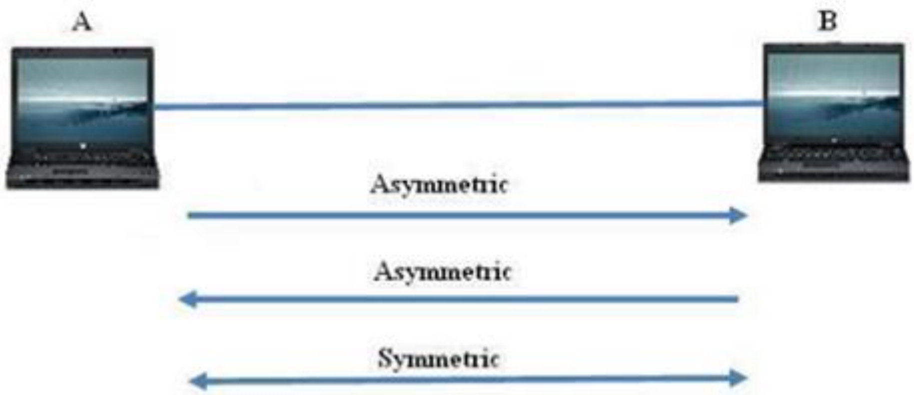

Figure 3.7: HELLO messages in SANET using OLSR[31]

2. **Topology Control (TC) messages** are used by nodes in a network to communicate their MPR (MultiPoint Relay) selector sets and to update their topology tables. This is essential for creating the intra-forwarding database required for packet routing. Only MPR nodes transmit TC packets, while other nodes receive and process these packets without forwarding them. When a node receives a TC message, it updates its topology table to include the most recent connections. This information is then utilized to construct the routing table for packet transmission, following a backtracking process in descending order. Each node collects important control information and stores it for the protocol's operation, as illustrated in Fig. 3.8. The protocol keeps track of next-hop information to efficiently send packets to their destinations using MPR nodes[42][74][76].

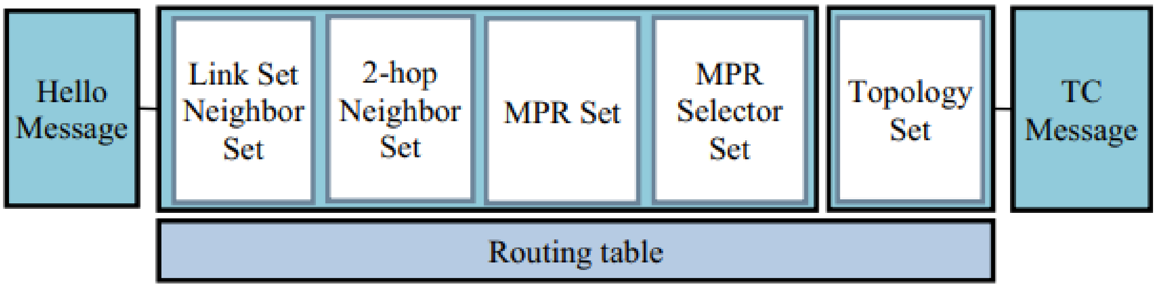

Figure 3.8: Messages and information hold[24].

3. **MULTIPLE INTERFACE DECLARATION (MID) MESSAGES** are produced by an OLSR node with multiple OLSR interfaces to inform other OLSR nodes about its active interfaces in the OLSR routing domain. These messages include a list of interface addresses linked to the main address. Due to potential size limitations, this list may be partial, but all MID messages detailing a node's interface set must be fully parsed within a specified refreshing period (MID_INTERVAL). The information shared through these MID messages assists each node in constructing its routing table and is broadcast across the network exclusively by MPRs .

A network node with multiple interfaces should not generate MID messages if only one interface is active in the mobile ad hoc network (MANET) and running the Optimized Link State Routing (OLSR) protocol[45][21][78].

OLSR mechanism

Figure 3.9 shows how the OLSR protocol works. It includes three main parts: the link-state awareness module, the routing discovery module, and the routing calculation module [22][21].

1. In the link-state awareness module, each node sends a HELLO message to its neighbors regularly. This helps check the status of the links and identify one-hop and two-hop neighbors. The information from the HELLO messages is stored in a neighbor table. Each node sets a holding time for every neighbor; if this time expires, the neighbor is removed. To calculate the MPR set, the HELLO packets in OLSR must detect link states among neighbor nodes and compute the two-hop neighbors. Additionally, each MPR is assigned a sequence number to identify the most recent MPR recorded in its MPR table [45].

2. The routing discovery module determines the MPR set based on the neighbor and two-hop neighbor tables. The MPR mechanism significantly reduces routing overhead while maintaining a clear view of the network topology [22]. MPR acts as an intermediary node or an interface, enabling communication between all nodes and a selected node. Each node chooses its MPR set from its one-hop neighbors and shares this selection in HELLO messages broadcast to all nodes. Nodes only broadcast and forward TC messages through MPR nodes. Using MPR selectors and TC messages, nodes update their topology tables to include the MPRs of other nodes [45]. Each node has a routing table that contains all known destinations, which it tracks using its MPR (Multi-Point Relay) nodes. When a HELLO message is received, the following occurs:

- First, the neighbor list is updated, considering whether the connection is symmetric or asymmetric.
- Second, hop sets are created to record pairs of nodes, indicating which two-hop neighbors can be reached via a specific one-hop neighbor.
- Finally, the MPR set is updated to reflect the nodes selected as MPRs [45][21].

MPR nodes send packets to the nodes that selected them and inform all the selecting nodes and the entire network through Topology Control (TC) packets. Regular nodes that are not MPRs can receive and process control packets, but they cannot forward them or affect the network structure of other nodes [45][42].

3. The routing calculation module creates a routing table using the 1-hop and 2-hop neighbor tables and the topology table generated by the previous modules. The OLSR routing protocol updates the routing table whenever there are changes to the neighbor or topology table [22][42]. Each entry in the topology table has a holding time. When this time expires, the entry becomes invalid and is removed. The topology table contains the following information:

1. **Destination Addresses:** These are MPR selectors from the TC message that show which nodes need to forward messages.
2. **Destination's MPR:** These are the last-hop nodes to the destination that sent the TC messages and provide routes to the MPR selectors.
3. **MPR Selector Sequence Number:** This number represents the latest set of MPR selectors and is incremented only when the set changes.
4. **Holding Time:** This is the length of time an entry remains valid in the topology table [42].OLSR selects the optimal path using a minimum-hop method [22].

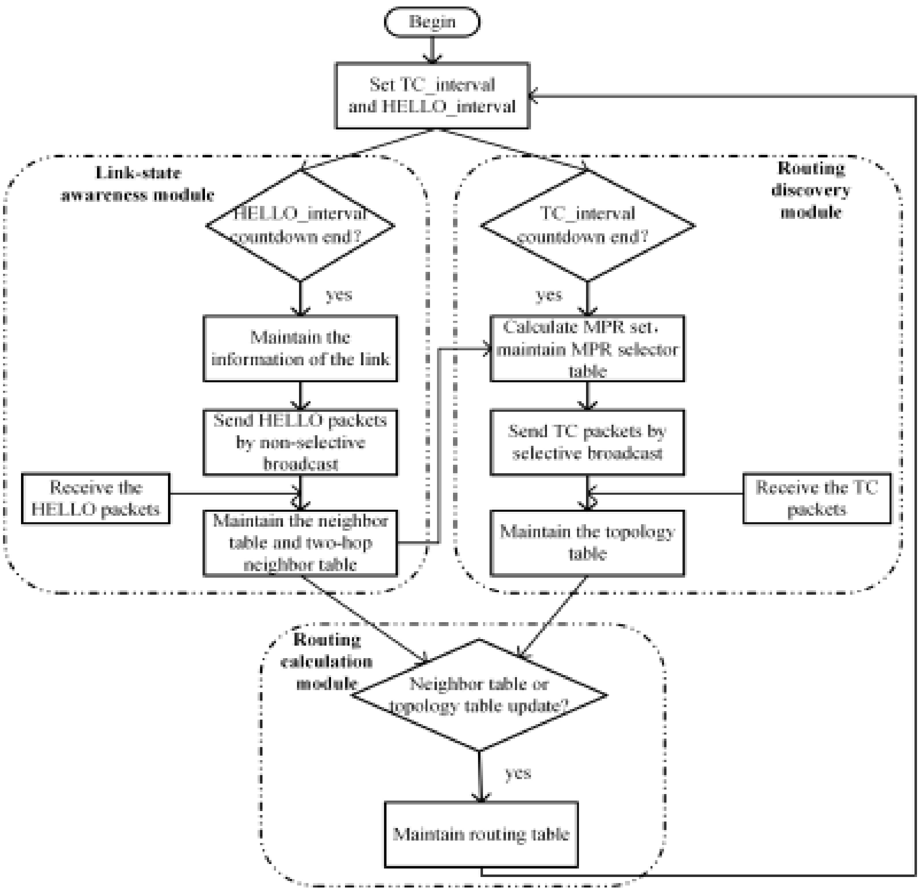

Figure 3.9: Schematic diagram of OLSR routing protocol[22].

Advantages and Disadvantages of the OLSR Routing Protocol

The following table shows the advantages and disadvantages of the OLSR routing protocol.

Table 3.3: Advantages and Disadvantages of the OLSR Routing Protocol

Advantages	Disadvantages
OLSR minimizes delay, suiting latency-sensitive apps.	OLSR routing tables list all routes, which can be large.
OLSR is user-friendly, has fewer issues, and needs no central routing.	More mobile users increase control messages.
OLSR suits fast-changing ad hoc networks.	OLSR link repair is slow
OLSR control messages: unreliable, periodic, unordered.	OLSR needs more processing power for route calculation.
OLSR is simple, interacts with the routing table, and needs no IP header changes [72][79].	OLSR's delay is more variable.
	Not ideal for fast-changing networks due to state propagation overhead[70][79].

3.9.1.2 Reactive Routing Protocols (On Demand)

Reactive routing protocols are on-demand protocols that establish routes only when needed. [47][34]. They employ a route discovery process that floods the network with route query requests when a packet requires routing, utilizing either source routing or distance vector routing. Source routing embeds routing information directly in packet headers, eliminating the need for routing tables; however, this approach results in high network overhead. On the other hand, distance vector routing relies on next-hop and destination addresses, requiring nodes to maintain active route information until it is no longer needed or until a timeout occurs, which helps prevent outdated routes [80]. Reactive protocols require less memory and storage than proactive ones, as they do not constantly update route tables[70].

The main disadvantages include high latency in route finding and the potential for network congestion. When the source node intends to send data, it begins the route determination process, which involves a search. This increases the waiting time for the source. Additionally, extreme flooding during this process can lead to congestion in the network[66][47].

This thesis analyzes AODV, with simulation details in Chapter 5.

3. 9.1.2 .1Ad Hoc On-Demand Distance Vector Routing (AODV) protocol

Ad Hoc On-Demand Distance Vector Routing (AODV) is a reactive “on-demand” routing protocol, meaning that routes are established only when needed. It uses a distance vector algorithm, which measures distances in hops to all available routers. This approach minimizes the number of broadcasts by creating routes only when requested[79]. Which means each node maintains a routing table of active paths and periodically broadcasts a hello message to track its neighbors. Nodes store only next-hop information, not the complete route[81][45].

The AODV algorithm is an enhanced version that combines elements of both the Destination-Sequenced Distance Vector (DSDV) and Dynamic Source Routing (DSR) algorithms. It combines DSDV's periodic updates, sequence numbers, and hop-by-hop counts with DSR's route request (RREQ) and route maintenance. [70]. The protocol supports unicast, broadcast, and multicast communication[79].

AODV prevents routing loops by assigning a unique ID to each request packet. This solution fixes the distance vector problem of counting to infinity[81].

AODV Features: Each active route has a specific lifetime recorded in the table. When this lifetime expires, the route becomes invalid and is removed from the table[82][79].

AODV can manage different speeds of movement and types of data traffic. It uses two main mechanisms to create and keep connections between nodes: 1. Route Discovery. 2. Route Maintenance[79].

There are four types of control messages used in the AODV routing algorithm for the discovery and maintenance of the route, and it is:

1. Route Request Message (RREQ)
2. Route Reply Message (RREP)
3. Route Error Message (RERR)
4. Hello Messages: To discover the network, all nodes exchange hello messages with their neighbors [82][45].

1. Route Discovery mechanism.

In the route discovery process, as shown in Figure 3.10, routes are established when required. When a source needs to reach a destination, it first checks its routing table for the destination's route information[81]. Each node in the AODV ad hoc network maintains a routing table holding information about recent routes by storing the following data:

1. Destination node IP address.
2. Destination sequence number.

3. Hop Count: Number of hops to destination.
4. Next hop for packet forwarding.
5. The valid time for a route.
6. Active neighbor list[45] .

Every node in the network must have a route table entry that includes the latest sequence number of the node. This entry is refreshed whenever the node receives RREQ or RERR messages[45]. If the routing table has a route, the source will send packets to the destination. If no route exists, the source will queue the message and broadcast a Route Request (RREQ) throughout the network[81].

The RREQ includes specific information, as detailed below.

1. Source IP Address.
2. Destination IP Address.
3. Source Sequence Number: Source Sequence Number: This is the most recent sequence number used in this route.
4. Destination Sequence Number: This is the latest sequence number received from the source for any route to the destination.
5. Request ID.
6. Time to live (TTL).
7. Hop Count: number of hops from the source to the intermediate node trying to find the destination.[45]

A Route Request (RREQ) is identified by both the source address and the request ID. Each time the source node sends a new RREQ, it increases the request ID. When a node receives the RREQ message, it checks if the request has reached its destination.

If it hasn't, the node checks if it has received the same RREQ before by looking at the request ID and source ID. If it has received it earlier, the node will discard the message.

If the node receives a new RREQ, it will re-broadcast it to its neighbors and increment the hop count [45][82].

As the Route Request (RREQ) travels from one node to another, it automatically establishes a reverse path from each of these nodes back to the source. Each node that receives the packet records the address of the node from which it was received. This process is known as Reverse Path Setup[34].

The reverse path is used to send the RREP message back to the source, while a forward path is established during the transmission of the RREP message. This forward path can be considered the reverse of the reverse path(a complete route). Data transmission begins as soon as this forward path is set up[82][45].

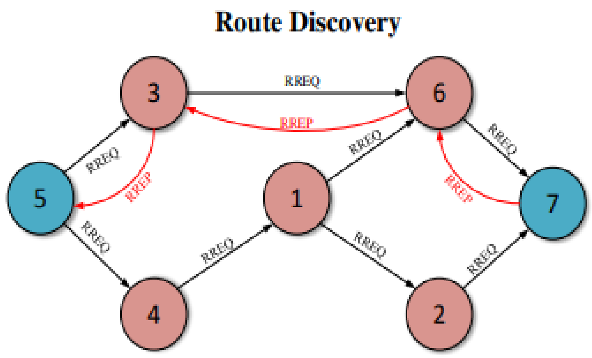

Figure 3.10: Route Discovery Process (RREQ and RREP) for AODV[81]

2-Route Maintenance Mechanism in AODV

One of the most important features of a Mobile Ad Hoc Network (MANET) is node mobility. When one of the nodes in the communication path moves outside the transmission range of its neighboring node while sending data, it can lead to link failures. In this case, when a node loses contact, the node immediately preceding it sends a Route Error (RERR) packet to its preceding node. This process repeats until the RERR packet reaches the source node, as shown in Figure 3.8. When the source node receives the RERR, it compares it with its routing table. The broken route is then deleted, and the source node generates a new RREQ (Route Request) to discover an alternate path .

The following parameters are contained in the route reply message :

1. Source Address.
2. Destination Address.
3. Destination Sequence Number.
4. Hop Count.
5. Life Time.

The source node initiates a search for another path by broadcasting the RREQ packet again, as shown in Figure 3.11. Additionally, hello packets are used to predict possible route loss; each node periodically sends a hello packet to its neighboring nodes to verify their presence. If a response is not received, it indicates that there has been a path interruption[83][81][82].

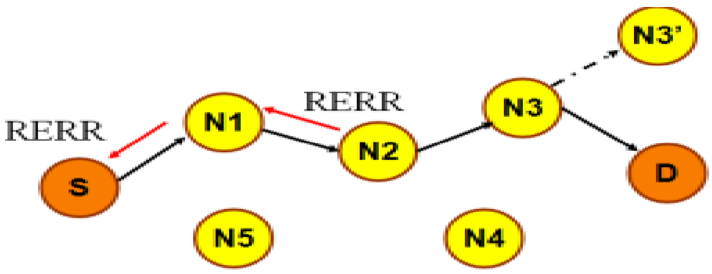

Figure 3.11: AODV Route Maintenance Process[72]

Example for Path discovery in the routing protocol AODV

The source node S wants to send data to the Destination node D, as in the network shown in the figure3.12.

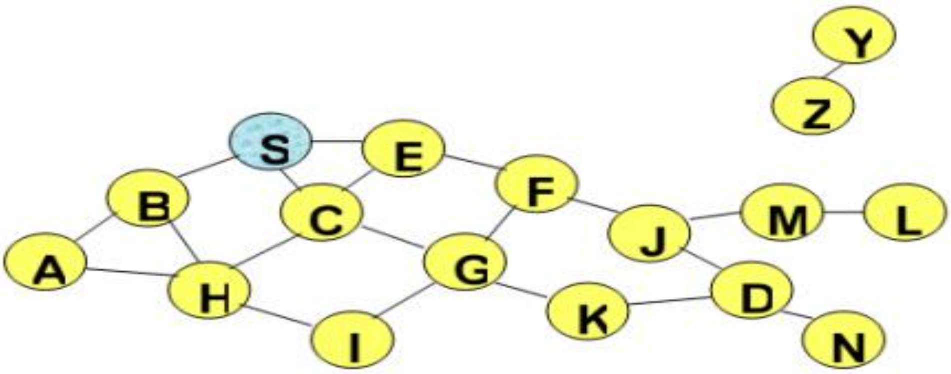

Figure 3.12: MANET network consisting of 17 nodes[83]

In the first stage, Node S discovers the path by sending an RREQ packet to its neighboring nodes, exemplified in our nodes B, C, and E as shown in Figure 3.13.

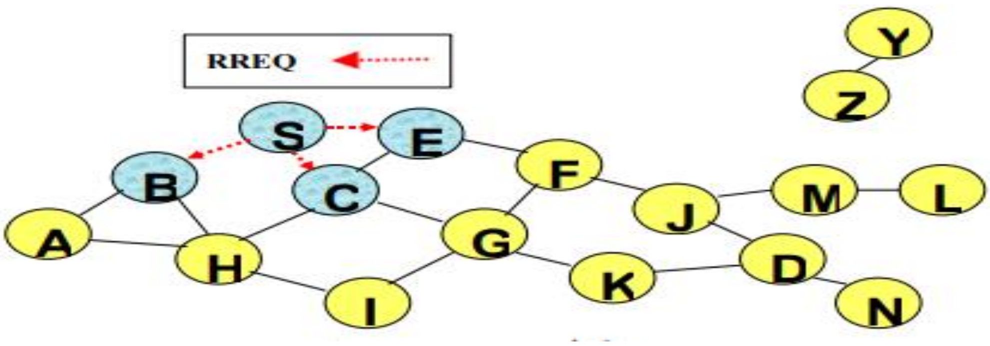

Figure 3.13: The first stage of path discovery in the AOD protocol[83].

In the second stage, Nodes B, C, and E create a reverse path to the source node S. The neighboring nodes of node S, which are B, C, and E, in turn, send the RREQ packet to their neighboring nodes, as shown in Figure 3.14.

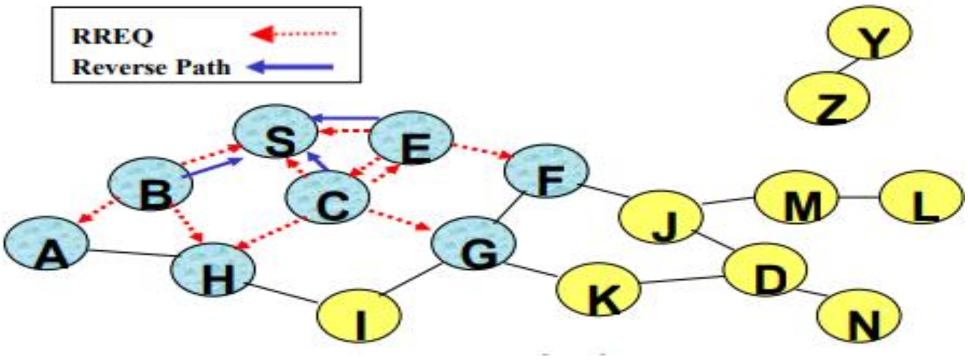

Figure 3.14: The second stage of path discovery in the AOD protocol[83].

In the third stage, Node C receives the RREQ packets from Node G and H but does not forward them because it has already forwarded them, as shown in Figure 3.15.

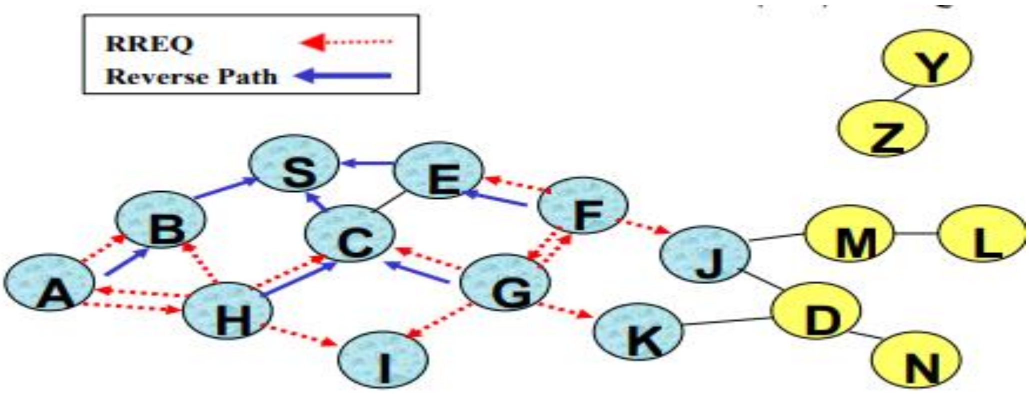

Figure 3.15: The third stage of path discovery in the AOD protocol[83].

In the fourth stage, the nodes receiving the RREQ packets will continue sending them to their neighboring nodes until they reach the Destination node D, as shown in Figure 3.16.

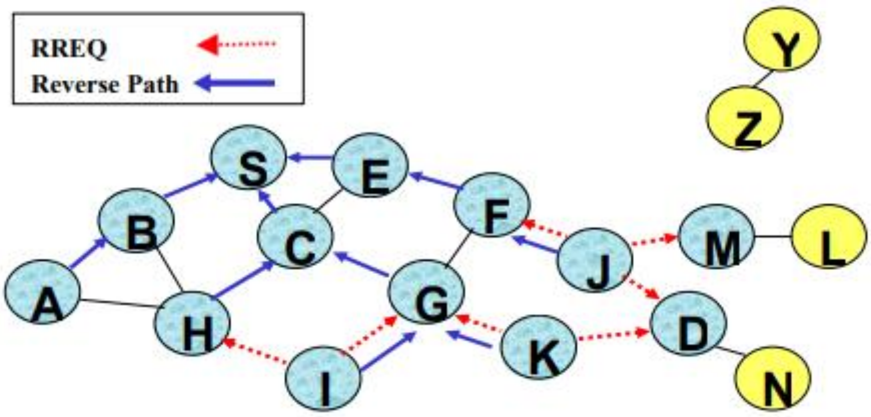

Figure 3.16: The fourth stage of path discovery in the AOD protocol[83].

In the Fifth stage, the Destination node D does not send any RREQ packet because it is the Destination node, as shown in Figure 3.17.

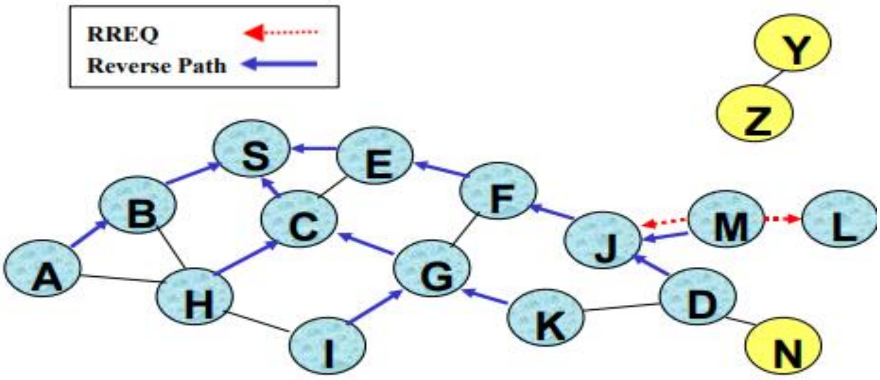

Figure 3.17: The Fifth stage of path discovery in the AOD protocol[83].

In the sixth stage, Nodes that cannot be reached by node S do not receive the RREQ packet, as in the case of node Y and Z, while nodes to which the path passes by the target node D also do not receive the RREQ packet, as in the case of node N, as in Figure 3.18.

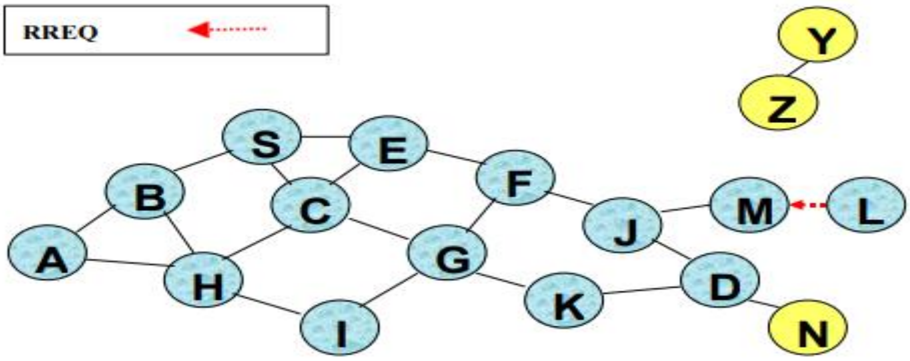

Figure 3.18: The sixth stage of path discovery in the AOD protocol[83].

In the seventh stage, The Reverse path is determined from the destination node D to the source node S as shown in Figure (3.19).

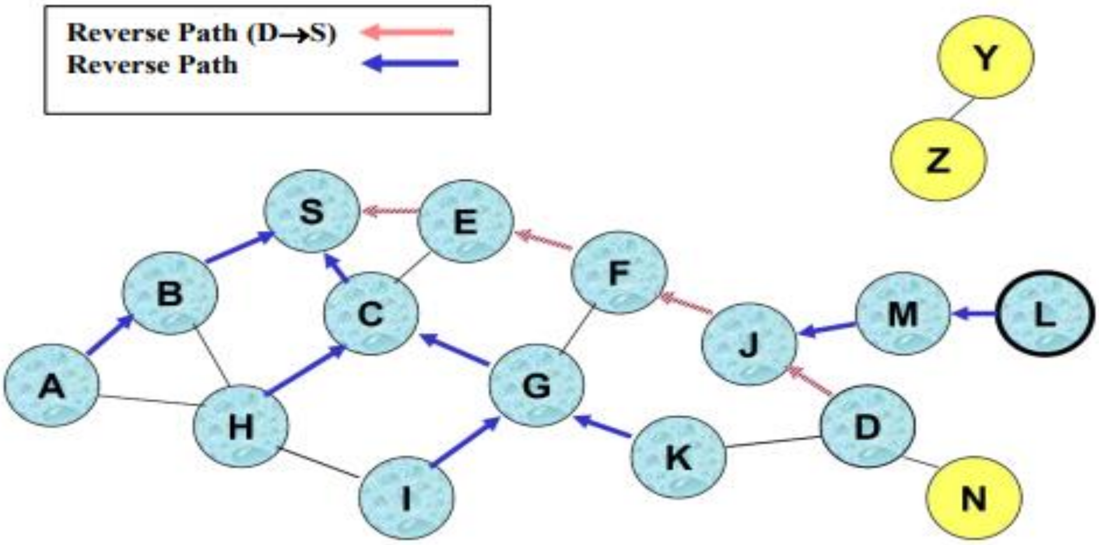

Figure 3.19: The seventh stage of path discovery in the AOD protocol[83].

In the eighth stage, the path between the source node and the destination node is completed when the RREP packet travels through the reverse path and reaches the source node, as shown in Figure 3.20.

These connections represent the path that data will take from source node S to destination node D.

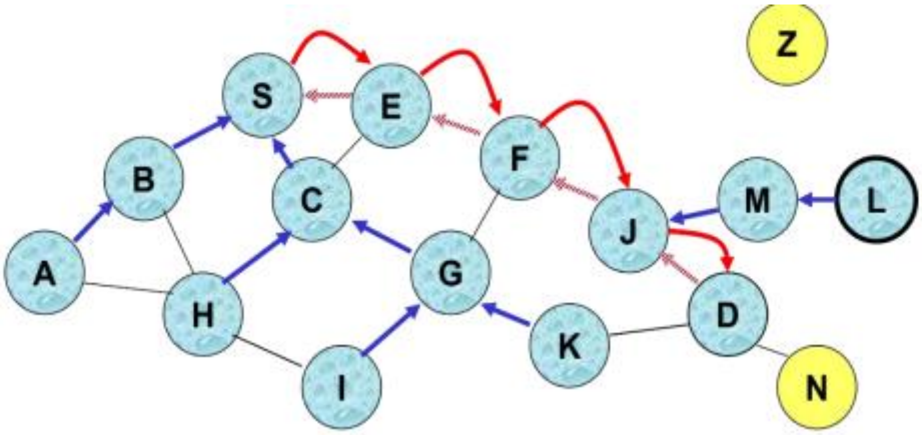

Figure 3.20: The seventh stage of path discovery in the AOD protocol[83].

In the ninth stage, the source node begins sending data to the destination node via the best path (with the fewest number of hops) that was chosen in the path discovery stage, as shown in Figure 3.21.

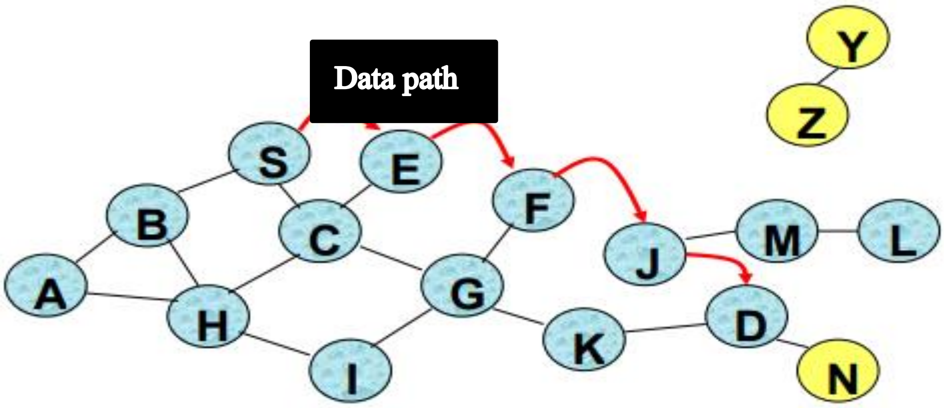

Figure 3.21: The seventh stage of path discovery in the AOD protocol [83].

Advantages and Disadvantages of AODV Routing Protocol

The following table shows the advantages and disadvantages of the **AODV** routing protocol.

Table 3.4: Advantages and Disadvantages of the AODV Routing Protocol

Advantages	Disadvantages
AODV's fast adaptation to network changes makes it suitable for dynamic	AODV takes a long time to create the routing table[79].
AODV handles unicast/multicast for mobile nodes[79].	Routing entries expire despite valid links[28].
AODV quickly finds the newest route.	Route found when flow starts[28].
AODV reduces overhead by not source routing.	Too many route replies and beacons waste bandwidth, reducing network efficiency[70].
AODV: flat routing, no central manager, all devices equal.	Valid routes can expire; setting expiry is hard[79].
AODV avoids loops using destination sequence numbers.	Larger networks reduce performance[79].
Shorter RREPs (higher sequence number or fewer hops) trigger route updates[79][69].	

3.9.2 Geographic routing (position-based routing) Protocols

Geographic routing, also known as geo-routing, refers to recently developed protocols that operate independently of network topology, designed for large, distributed networks[70].

In position-based protocols, nodes determine their locations using the Global Positioning System (GPS). Nodes communicate with nearby nodes by sending out a beacon at regular intervals to determine their positions. Data forwarding decisions rely on the destinations' locations in the packet header and the positions of neighboring source nodes, without the need for route discovery, maintenance, or knowledge of network topologies [72][70].

Geographic routing uses GPS coordinates to find the best routes to a specific destination[71]. Each node needs to know where it is located and the position of its direct neighbor to send the data packet[55].

The advantages include simplified network management through a location-based topology, improved scalability, enhanced route formation, and reduced packet overhead[71][55].

Disadvantages include the requirement for each node to know its neighbors' locations and the issue of inaccurate node positions, leading to increased network load[70][55].

3.9.2.1 Geographic Routing Protocol or Gathering-based Routing Protocol (GRP)

GRP is a custom MANET routing protocol by OPNET that determines routes based on the shortest geographical distance between the source and destination, classifying it as a proactive routing protocol due to its dependence on the Greedy algorithm, which requires each node to keep one or more routing tables that contain updated information about its neighboring nodes. For different quadrants, it maintains the highest level of information about neighboring quadrants[55]. This algorithm assumes that each node knows its GPS location. Although GRP is categorized as proactive, a source node can initiate route discovery if no route to the destination is available[84][85].

GRP, also known as the Gathering-based Routing Protocol, allows the source node to gather routing information for the destination. It begins by sending a Destination Query (DQ) across the network, which is relayed to neighboring nodes until reaching the destination. Once there, the destination node broadcasts a Network Information Gathering (NIG) packet to its neighbors. The source node calculates the optimal route using collected data and begins transmitting data packets immediately[13][86][84].

GRP minimizes flooding by organizing routing within square quadrants or neighborhoods, as shown in Figure 3.22[85]. The size of each neighborhood can be set using a global attribute[86]. A main feature of GRP is its regional and hierarchical packet forwarding strategy, which reduces flooding overhead. Each higher-level neighborhood is systematically divided into four smaller lower-level neighborhoods[87].

When a node moves into a new area, it updates its location. Nodes use a 'HELLO' protocol to communicate with their neighbors and share their positions. If a route becomes blocked, a backtracking method allows packets to return to the last node to find a new route. If the node that receives a backtracking packet has no alternative route, it will return to its previous node to look for one. If no alternate route is found after all possible backtracks, the packet is dropped and discarded[71][55][84].

Consider a system with two top-level neighborhoods, A and B. Within A, we have neighborhoods Aa, Ab, Ac, and Ad; within B, we have Ba, Bb, Bc, and Bd. Additionally, Aa contains Aa1, Aa2, Aa3, and Aa4, while Bb includes Bb1, Bb2, Bb3, and Bb4. When a node moves more than a specified distance or crosses a quadrant boundary, it sends a message with its new position to all recipients[87].

For example, in Fig. 3.22, when a node moves from Aa1 to Aa2 (within the level 2 quadrant), a beacon message is broadcast to quadrant Aa, the upper layer of the node. Similarly, if a node moves from quadrant Aa2 to Ac1 (within the level 1 quadrant), the flooding message is sent only to nodes within quadrant A, rather than the entire network[85][86].

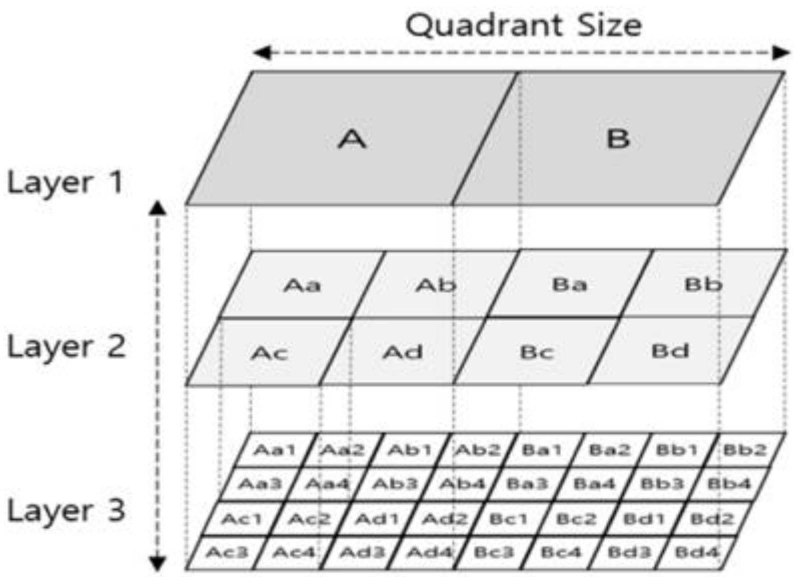

Figure 3.22: regional quadrant strategy in GRP[85]

Each node maintains three tables: destination, neighbor, and backtracking. First, the destination table indicates whether the node has information about a specific destination; nodes update this table upon receiving flooded location information. Second, the neighbor table, updated via hello message exchanges, stores the location information of neighboring nodes. Finally, the backtracking table records the node that forwarded a data packet. This table is used to route packets back to the previous node if no closer neighbor exists or if destination information is lacking[85][87].

GRP utilizes two forwarding strategies: Greedy Forwarding and Face-2 Routing Perimeter.

1. Greedy forwarding involves sending information to the neighbor that is closest to the destination node, as shown in Figure 3.23. The message is gathered using a positioning method, such as GPS[70][83][84].

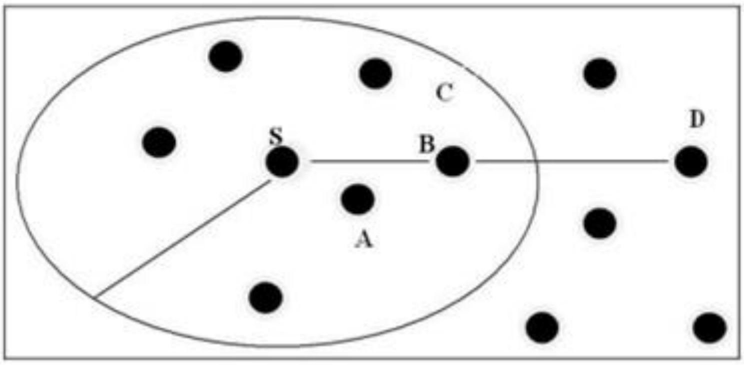

Figure 3. 23: greedy routing strategies[83].

2. Perimeter routing, also known as the Face-2 Algorithm, is a technique where, if a node cannot find a forward path, it forwards the packet to the node that shows the least backward progress. This approach is based on the concept of planar graphs, which are graphs that do not have intersecting edges, as shown in Figure 3.24 [71][83][84].

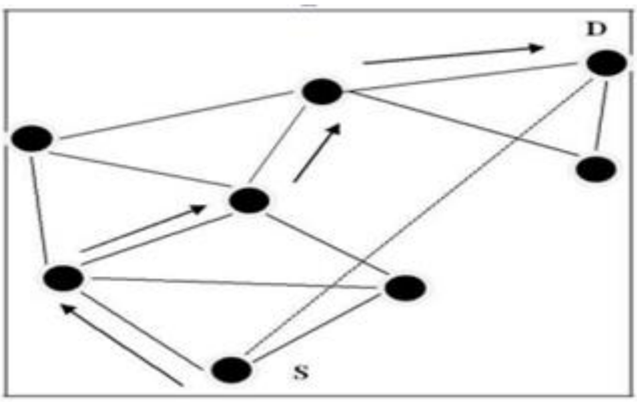

Figure 3. 24: planner graph traversal[83].

Advantages and Disadvantages of GRP Routing Protocol

The table below outlines the advantages and disadvantages of the GRP routing protocol.

Table 3.5: Advantages and Disadvantages of the OLSR Routing Protocol

Advantages	**Disadvantages**
Route discovery and management are not needed.	Requires position-determining services.
GRP allows for scalability.	GPS devices do not work in tunnels[71].
It works well with a high node mobility model[71].	

CHAPTER FOUR:
Simulations, Design, and Implementation

4. Simulation, Design, and Implementation

4.1 Evaluation Platform

This chapter discusses the MANET network modeling, configuration, and implementation. The student version of OPNET Modeler 14.5 was used to create different scenarios. This modular tool features an easy-to-use interface and a comprehensive selection of modules, allowing users to effectively build suitable simulation environments.

4.2 Networks Model Configuration

The network model was designed to remove network elements for creating scenarios, particularly by using the startup wizard for MANET scenarios in this thesis.

4.2.1 Network Components and Attributes

Various network components and attributes have been utilized to establish a MANET network that meets the specific requirements of their scenarios. The network components include:

4. 2. 1. 1 MANET Network Elements and Attributes

- MANET workstation nodes are workstations executing a source-destination application using UDP/IP.
- Application Configuration: This consists of a name and a description table that specifies various parameters, such as frame size and traffic type, for different applications (e.g., voice, video conferencing, etc.).
- Profile_Config node: This component is utilized to create user profiles that accurately generate application-layer traffic across different nodes in a Mobile Ad Hoc Network (MANET).
- Mobility Configuration: A mobility configuration object stores random mobility parameters as profiles for easy reusability.
- Wireless Server: A mobile subscriber station node model with server functionality.
- Rx Group: The "wlan_rxgroup" option will consider transmitters with "wlan_rxgroup" specified as the Rx group.

4.2.2 Model Configuration Parameters

Application Configuration: To create a simulation model in OPNET, you use an object known as the Application Definition attribute. This attribute contains several predefined applications, including Database, E-mail, FTP, HTTP, Video, and Voice. The type of service is used within the Application Definition attribute to define applications (Voice). The voice application, configured using the voice table shown in Figure 4.1, is modeled for a Best-Effort service to support VoIP calls. The voice application employs the G.711 encoder scheme for MANET.

Profile Configuration: After configuring the Application Definition attributes, you need to set the Profile Definition attributes to determine how the application behaves. Figure 4.2 shows the Profile configuration and details the attributes used in the models. This includes the simulation's start time, which is consistently set between 100 and 110 seconds.

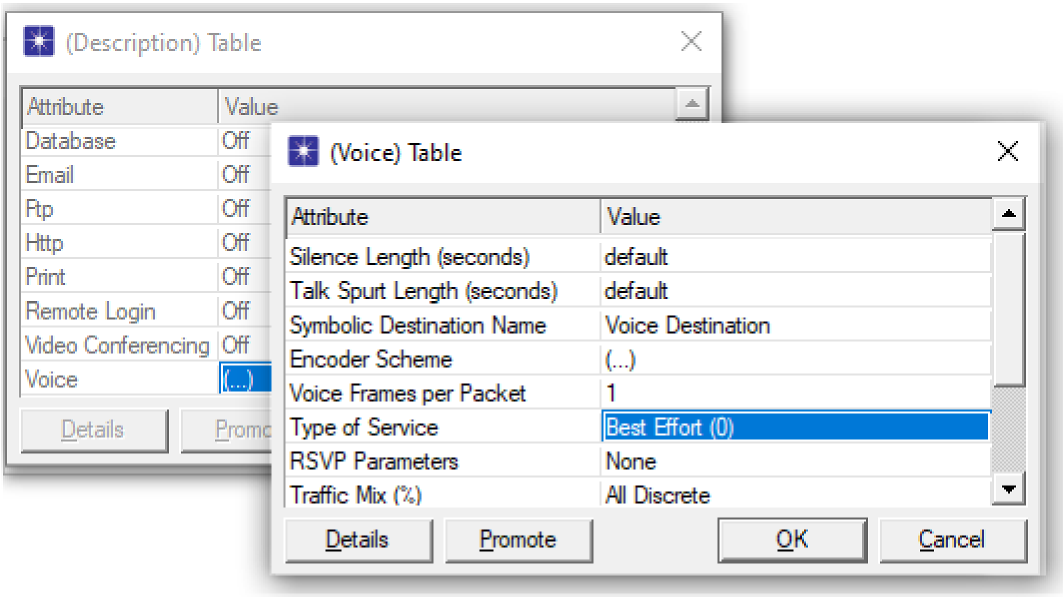

Figure 4.1: Application Definition Configurations

The simulation lasts for 5 minutes, during which the Voice application operates continuously until all applications have finished. Voice calls between the source and destination begin at 5 seconds and 10 seconds. New calls are added every 5 seconds, according to the profile, and this pattern continues until the simulation ends. As a result, the number of Voice calls increases consistently at regular intervals throughout the network model.

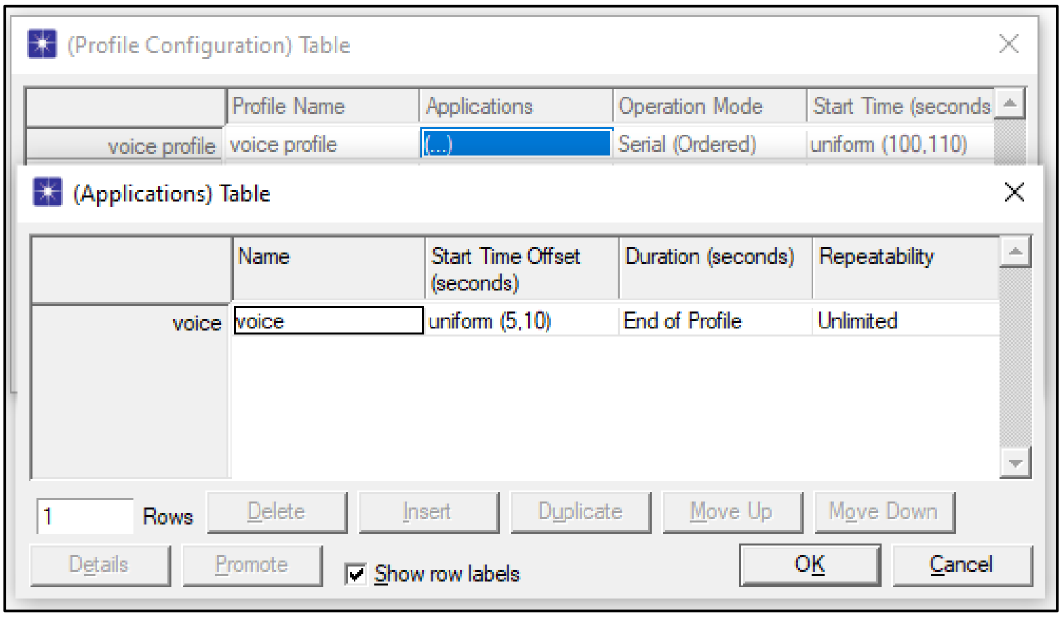

Figure 4.2: Profile Definition Configurations

4.2.3 Network Simulation Parameters

Table 4.1 displays the MANET traffic and voice generation parameters utilized in the simulation models.

Table 4.1: Network Simulation Parameters

Parameter	Value
Start Time (seconds)	100
Packet Inter-arrival Time (sec)	Exponential 1
Packet Size (bits)	Exponential 1024
Destination IP Address	Random
Stop Time (sec)	End of Simulation
Number of Nodes	30, 40, 50, and 60
Simulation Time	300 sec (5 min)
Simulation Area	2000 m X 2000 m
Node Speed	10 m/s
Routing Protocols	AODV, GRP, OLSR, and EOLSR
HELLO Interval (OLSR)	2 Sec
Adaptive HELLO Interval (EOLSR)	1 Sec (Optimal)
TC Interval (OLSR)	5 Sec

Parameter	Value
Adaptive TC Interval (EOLSR)	2 Sec (Optimal)
Node Movement Model	Random waypoint
Data Rate	11mbps
Application Name	Voice
Simulator	OPNET Modeler 14.5

4.2.4 AODV, GRP, and OLSR protocols parameters

Figures 4 (3, 4, and 5) show the required parameters for AODV, GRP, and OLSR routing protocols, respectively.

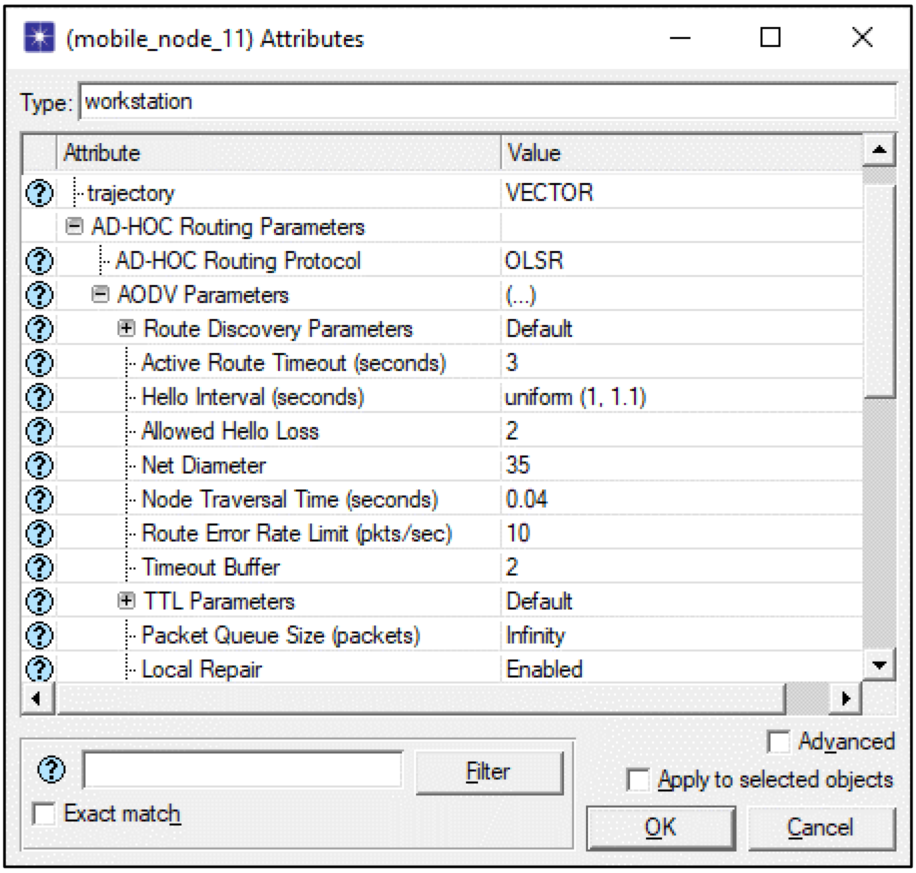

Figure 4.3: AODV protocol parameters

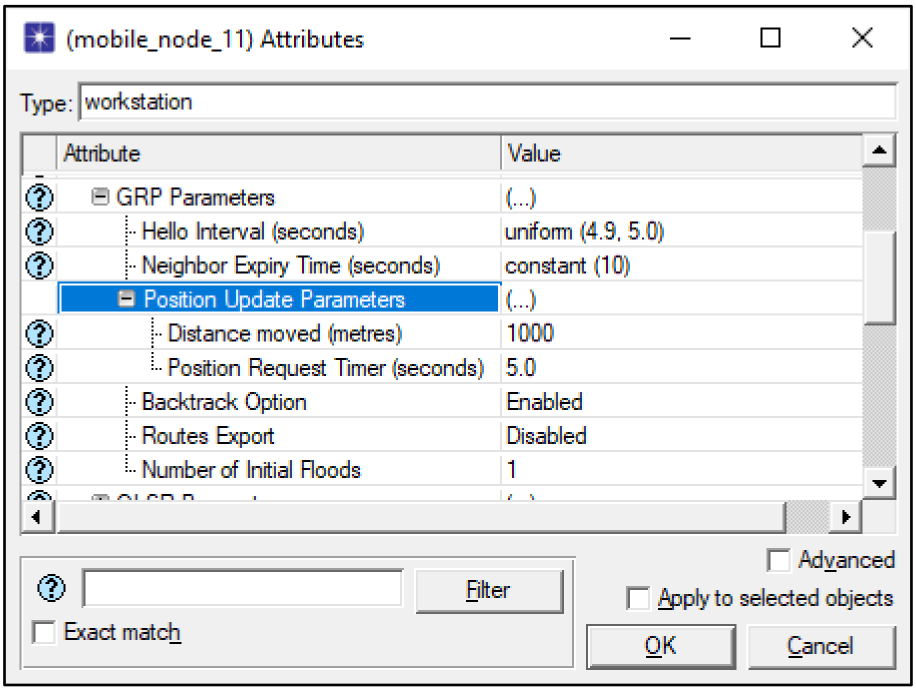

Figure 4. 4: GRP protocols parameters

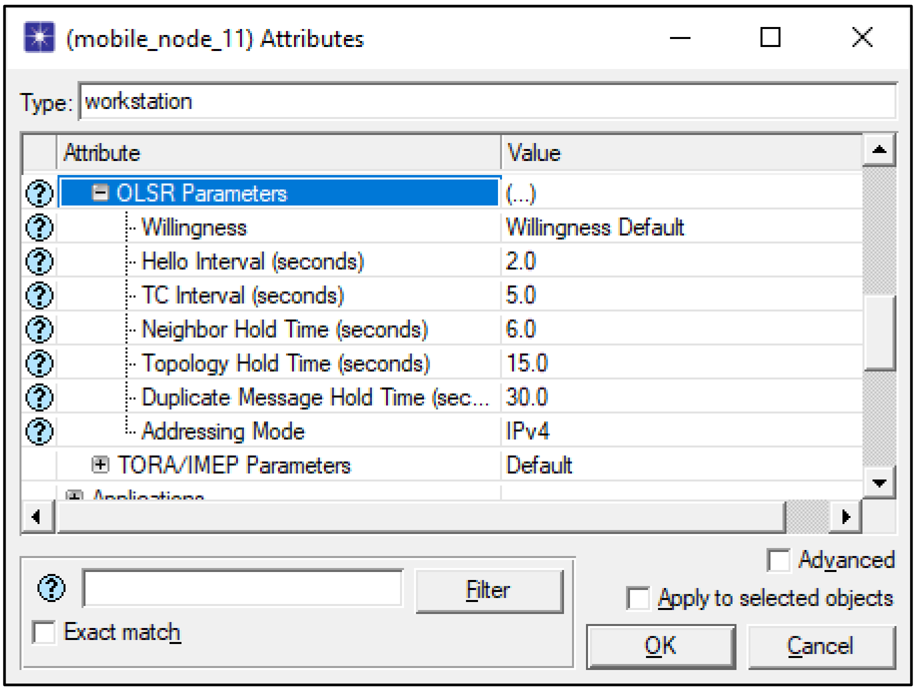

Figure 4.5: OLSR protocol parameters

4.3 Simulation Design

Design multiple simulation models to compare the performance of AODV, GRP, and traditional OLSR routing protocols with enhanced OLSR over MANET. Create various scenarios to simulate routing protocols for voice transmission, taking into account factors like delays, data throughput, and data dropped. A campus network was designed in an area measuring 2000m x 2000m, as detailed in Table 4.1. Wireless LAN mobile nodes with a data rate of 11Mbps were distributed throughout this area. The simulation used a random waypoint mobility model, which explains movement patterns clearly. In this model, mobile nodes move at a constant speed of 10 m/s until they reach their destination.

4.3.1 MANET Simulations Scenarios

- **AODV Scenarios:**
  - Topology consists of 30, 40, 50, 60 nodes, moving with 10ms
- **GRP Scenarios:**
  - Topology consists of 30, 40, 50, 60 nodes, moving with 10ms
- **OLSR (baseline scenarios):**
  - Topology consists of 30, 40, 50, 60 nodes, moving with 10ms
- **EOLSR (enhancement scenarios):**
  - Topology consists of 30, 40, 50, 60 nodes, moving with 10ms
  - **Parameters**: Hello interval: 2s (baseline) → 1s (enhanced)
  - **Parameters:** TC interval: 5s (baseline) → 2s (enhanced)

4.4 MANET Models

Figure 4.3 explains the network topology featuring various routing protocol models and mobile nodes. In MANET simulation scenarios, workstations, referred to as mobile nodes, act as both source and destination nodes. These mobile nodes initiate voice calls in voice scenarios.

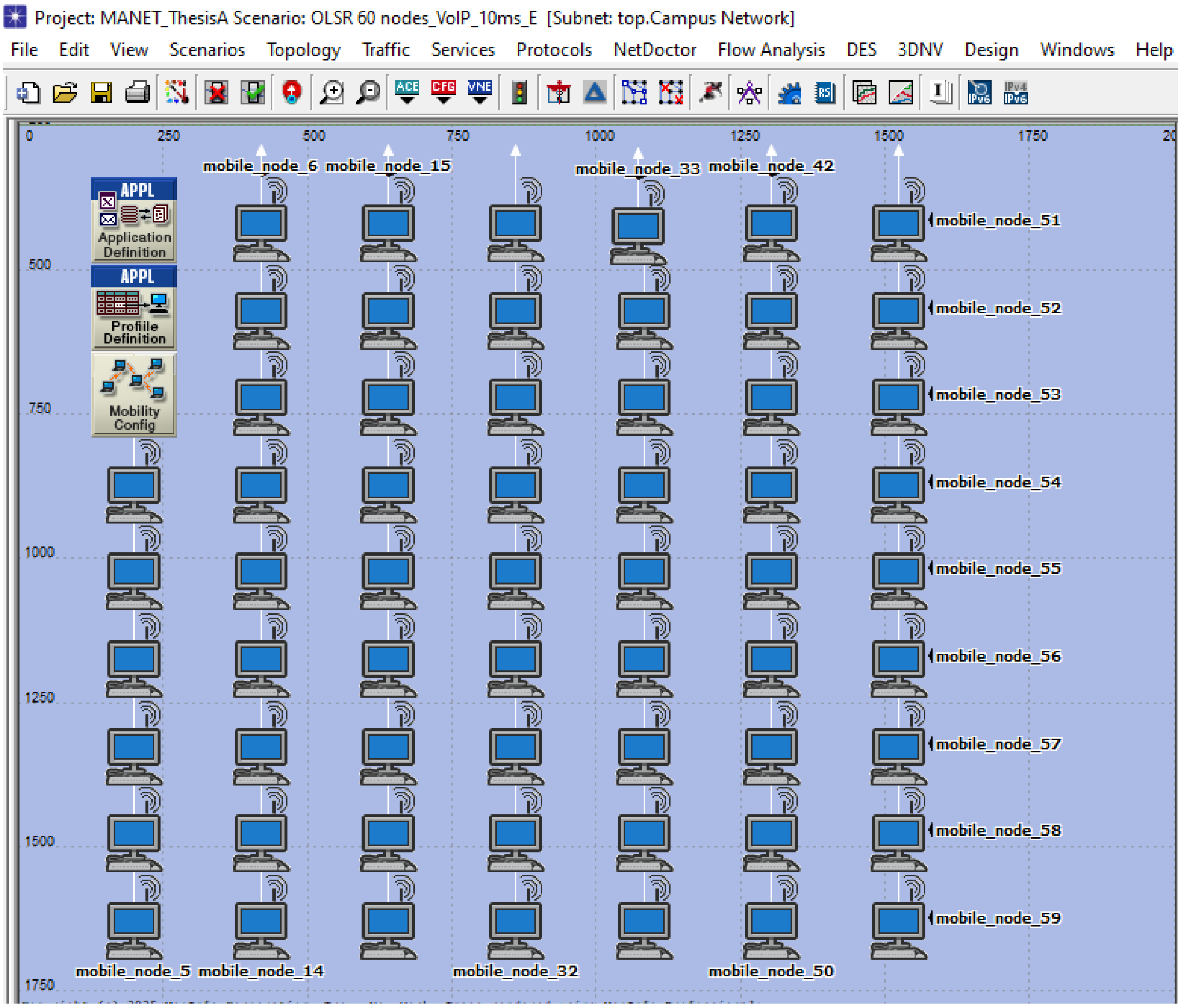

Figure 4.6: Simulating 60 nodes

4.5 Simulation Run-Time

The simulation run time is set to 300 seconds (5 min). The simulation is implemented in OPNET Modeler 14.5 on a TOSHIBA laptop with Windows 10, an HP i5, 2.5 GHz CPU, and 4.00 GB.

CHAPTER FIVE:
Analyzing AODV, OLSR, and GRP before Enhancement Simulation Results

5.1 Performance Metrics of AODV, GRP, and OLSR Routing Protocols

This section evaluates the traditional AODV, GRP, and OLSR routing protocols. We implemented different scenarios to test their performance in Mobile Ad Hoc Networks (MANET) and to identify a dependable routing protocol. We examined parameters like delay, throughput, and data loss, particularly for WLAN with voice applications. The findings are displayed in graphs and tables.

5.1.1 Comparison of WLAN Delay for Different Routing Protocols

To evaluate voice traffic performance in a Mobile Ad-hoc Network (MANET), we focused on the delay metric, which includes all delays from buffering during the route discovery process. Wireless delay is a key factor in evaluating voice quality in MANETs. The results in Table 5.1 and Figure 5.1 indicate that WLAN delays are high for voice traffic when using the AODV protocol. This is mainly because AODV has a slow process for establishing connections, which results in higher network delays due to its reactive characteristics. During route discovery, AODV generates significant routing traffic by broadcasting RREQ packets throughout the network, which further increases both delay and routing overhead. As demonstrated in Table 5.1 and Figure 5.1, the AODV protocol exhibits a significantly high delay across all cases of mobile node density.

Table 5.1: Comparison of WLAN Delay (sec) for Different Routing Protocols vs. Node Density

Routing Protocol	30 nodes	40 nodes	50 nodes	60 nodes
AODV	0.579	5.188	6.141	6.656
GRP	0.259	0.965	1.681	1.786
OLSR	0.230	1.029	1.876	1.965

OLSR has a lower delay than both GRP and AODV when there are 30 nodes present. However, as the number of nodes increases, OLSR's delay becomes higher than that of GRP. When the number of nodes exceeds 30, OLSR experiences increased delays. In comparison, GRP has lower delays than both traditional OLSR and AODV when there are more than 30 mobile nodes. Each mobile node using GRP is equipped with a Global Positioning System (GPS) for accurate location tracking, which helps optimize the flooding process by dividing it into quadrants. According to Figure 5.1 and Table 5.1, the GRP routing protocol performs better than AODV and OLSR in reducing network delay.

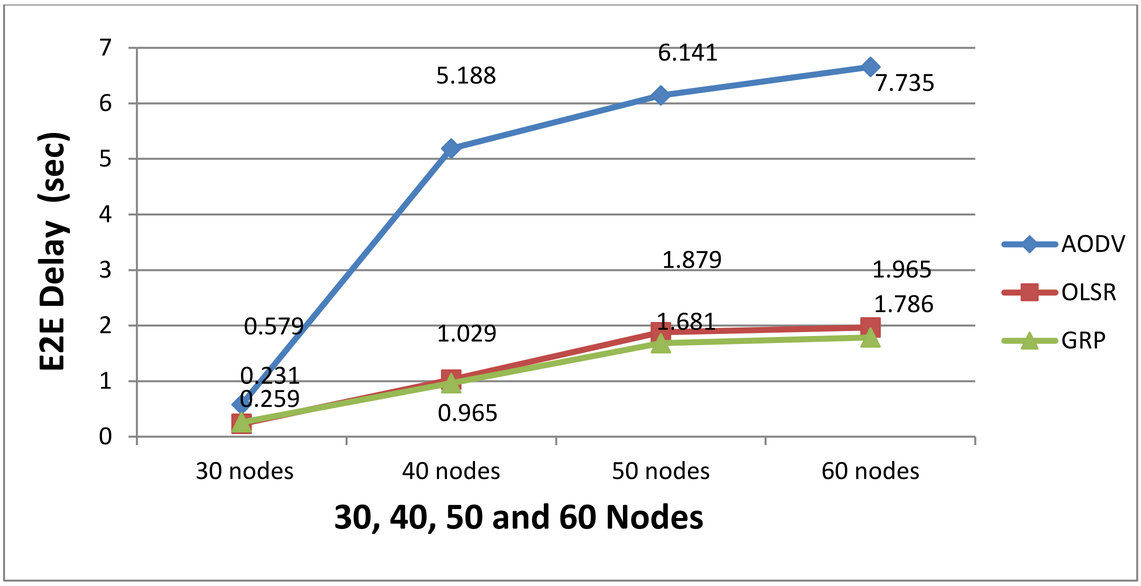

Figure 5.1: Comparison of WLAN Delay (sec) for Different Routing Protocols

5.1.2 Comparison of WLAN Throughput for Different Routing Protocols

Throughput refers to the total amount of data that the receiver node successfully obtains from the sender node, divided by the time it takes to receive the last packet. It is measured in bits per second (bps). Throughput measures network robustness, and simulations show that optimal throughput occurs with fewer mobile nodes. A routing protocol's effectiveness is often evaluated by its throughput.

Table 5.2 displays the throughput measurements for all the routing protocols under study. OLSR and AODV are the two routing protocols that consistently achieve the highest throughput across all levels of mobile node density. As shown in Table 5.2, as the number of nodes increases, the throughput of AODV also increases moderately. In OLSR, the throughput increases moderately but sees a more significant rise when the network size reaches 50 nodes. GRP demonstrates lower throughput performance. Table 5.2 and Figure 5.2 show that GRP offers the lowest throughput among the three protocols, while OLSR achieves the highest. In proactive protocols like OLSR, each node maintains knowledge of routes to destinations, which improves data transmission efficiency. OLSR uses a table-driven, multi-point relay (MPR) broadcast system, contributing to its better throughput compared to other protocols. As the network size increases from 40 to 50 nodes, the throughput rises from approximately 1.4 Mbps to 2.2 Mbps. This proactive approach allows OLSR to effectively deliver data packets between nodes, as all routes are pre-established.

Table 5.2: Comparison of WLAN Throughput (bits/sec) for Different Routing Protocols

Routing Protocol	30 nodes	40 nodes	50 nodes	60 nodes
AODV	1,292,436	1,553,586	1,875,320	2,091,889
GRP	679,099	798,148	1,051,236	1,378,920
OLSR	1,057,438	1,375,875	2,155,041	2,068,120

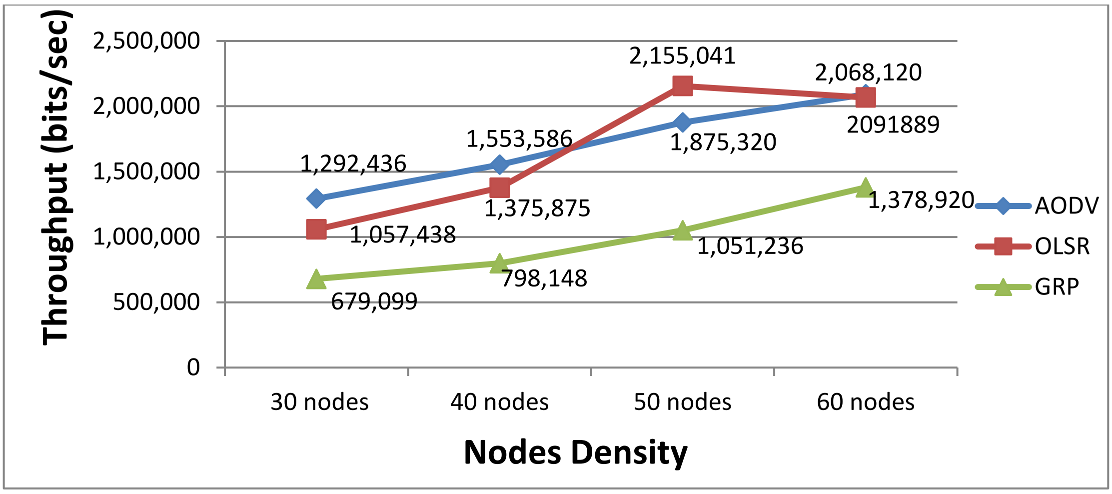

Figure 5. 2: Comparison of WLAN Throughput (bits/sec) for different Routing Protocols

5.1.3 Comparison of WLAN Data Dropped for Different Routing Protocols

The routing protocol sends a packet to its destination when it arrives at the network layer if there is a known, valid route. If no route is available, the packet is held queue until a route is found. Table 5.3 and Figure 5.3 show the total wireless data drop of different network sizes. The OLSR protocol has the lowest data drop, followed by AODV, while GRP experiences the highest data drop. As the number of nodes increases, the data drop in GRP also increases moderately, but the increase reaches a high level when the network size reaches 60 nodes. Table 5.3 and Figure 5.3 show that OLSR performs better than other protocols across all mobile densities. Additionally, it is capable of transmitting real-time data that is sensitive to information loss.

Table 5.3: Comparison of WLAN Data Dropped (bits/sec) for Different Routing Protocols

Routing Protocol	30 nodes	40 nodes	50 nodes	60 nodes
AODV	231	1,110	3,136	8,551
GRP	761	5,039	7,430	23,171
OLSR	56	1,030	2,305	2,738

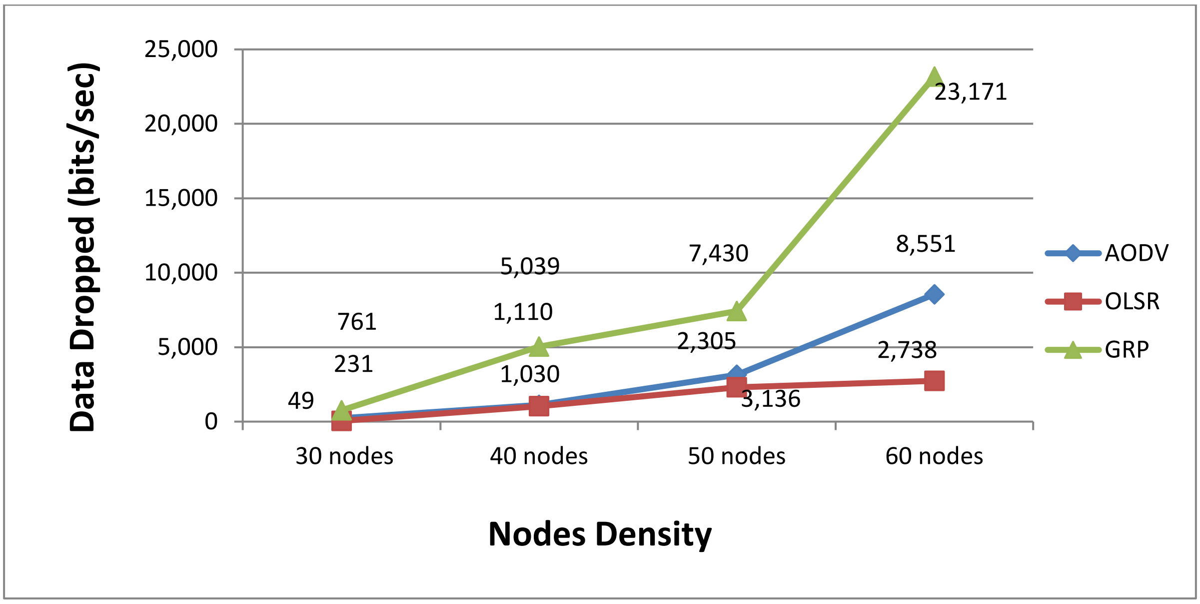

Figure 5.3: Comparison of WLAN Data Dropped (bits/sec) for Different Routing Protocols

5.2 Summary Results of Different Routing Protocols

Based on Table 5.4 and the earlier performance evaluation of the MANET routing protocols AODV, GRP, and OLSR for voice transmission across various network models with differing node density and mobility, the following conclusions are drawn:

1. GRP performed better than OLSR and AODV in terms of delay, especially as the network size increased. This is because geographic routing protocols scale better for MANETs, as they do not require maintaining up-to-date routing tables or a global view of the network topology and its changes.
2. AODV exhibits higher delays because it requires significant processing and time to construct routing tables reactively.

3. OLSR performs better than the other routing protocols in terms of throughput and data drop, especially in larger networks.
4. Initially, OLSR has a lower delay than GRP. However, as the number of nodes increases, OLSR's delay also increases. Therefore, OLSR does not perform optimally in terms of delay as the network scales.

This chapter explained the research methodology for evaluating different MANET routing protocols to determine their effectiveness in transmitting real-time data under various mobile densities. We initially examined the performance of three popular MANET routing protocols: reactive (AODV), proactive (OLSR), and geographic (GRP). Each protocol has its advantages and disadvantages in transmitting real-time data. From this study, we identified some weaknesses in the current MANET routing protocols:

1. No super protocol can ensure all the necessary QoS parameters, such as minimal delay, minimal data dropped, and maximum throughput.
2. The results indicate that no routing protocol can offer efficient routing for all network sizes without modifications, regardless of the number of nodes and mobility.

Table 5.4: Summary Results of Traditional Protocols (AODV, GRP, OLSR)

Metrics	Node Density	Routing Protocol		
		AODV	GRP	OLSR
Delay	30	0.579	0.259	0.230
	40	5.188	0.965	1.029
	50	6.141	1.681	1.876
	60	6.656	1.786	1.965
Throughputs	30	1,292,436	679,099	1,057,438
	40	1,553,586	798,148	1,375,875
	50	1,875,320	1,051,236	2,155,041
	60	2,091,889	1,378,920	2,068,120
Data Dropped	30	231	761	56
	40	1,110	5,039	1,030
	50	3,136	7,430	2,305
	60	8,551	23,171	2,738

When aiming to improve existing MANET routing protocols for efficient real-time transmission, it is important to consider specific features. These include selecting a routing protocol that can reliably handle delay, throughput, and data drops, particularly for real-time traffic like voice, which is highly sensitive to delay. This study found that the OLSR routing protocol, while strong in throughput and packet loss, did not perform optimally in terms of delay as networks scaled. As a result, it was decided to enhance the OLSR routing protocol to better support real-time traffic in MANETs. The details of this enhancement will be discussed in the next chapter.

Chapter Six:
Performance Evaluation of Enhanced OLSR Routing Protocol

6.1 Enhancement OLSR Routing Protocol

Existing MANET routing protocols struggle with reliable, low-delay transmission of real-time traffic. A protocol with significant adaptive capabilities is needed. OLSR offers a potential solution but requires enhancements, such as improvements to the HELLO and TC message mechanisms, to minimize delay. The OLSR protocol dynamically optimizes the hello message frequency based on varying node mobility. The standard OLSR sends hello messages every 2 seconds and TC messages every 5 seconds. The enhanced version reduces these intervals to 1 and 2 seconds, respectively, to highlight their effect.

6.1.1 Performance Metrics of WLAN through OLSR and Enhanced OLSR Routing Protocol

This study reviews a new routing protocol for MANET communication and proposes an enhanced OLSR, termed E-OLSR, for mobile ad hoc networks. The study offers several important contributions: it enhances the configuration settings of the OLSR protocol for Mobile Ad Hoc Networks (MANETs) across different node densities; it evaluates the performance of routing protocols using the OPNET simulator by developing realistic MANET scenarios, demonstrating that the optimized OLSR configurations are more effective than the default settings; and it compares traditional topology-based routing protocols (AODV, GRP, and OLSR) with the optimized E-OLSR, focusing on performance metrics such as throughput, delay, and data drop rate.

This section describes the common parameters used in the simulations. A mobile ad hoc network of 30, 40, 50, and 60 nodes is examined, with nodes randomly placed in a 2000 m × 2000 m area. The nodes' movement follows the random waypoint model, and the network has a fixed capacity of 11 Mbps. The following section presents the experimental results and analysis of the simulations, focusing on key routing protocol metrics: average delay in seconds, throughput in bits per second, and data dropped in bits per second. Lastly, all results related to the performance of E-OLSR are evaluated, plotted, and analyzed.

6.1.1.1 Comparison of WLAN Delay through E-OLSR and OLSR Routing Protocols

In scenarios with low node density (30 nodes), as illustrated in Figure 6.1, E-OLSR and OLSR display similar wireless delays. This is attributed to the network's stability and minimal topology changes. Additionally, the use of shorter HELLO and TC intervals in E-OLSR does not significantly affect the delay. This delay is primarily based on queuing delay, which remains unaffected due to sparse node distribution and an uncongested network. However, as the number of mobile nodes increases beyond 40, delays improve significantly, decreasing progressively at 40, 50, and 60 nodes. E-OLSR performs better than OLSR in terms of delay, particularly when the number of nodes exceeds 40.

Table 6.1: WLAN Delay (sec) of E-OLSR Compared to OLSR Routing Protocol

Routing Protocol	30 nodes	40 nodes	50 nodes	60 nodes
OLSR	0.231	1.029	1.876	1.965
E-OLSR	0.173	0.864	1.571	1.656

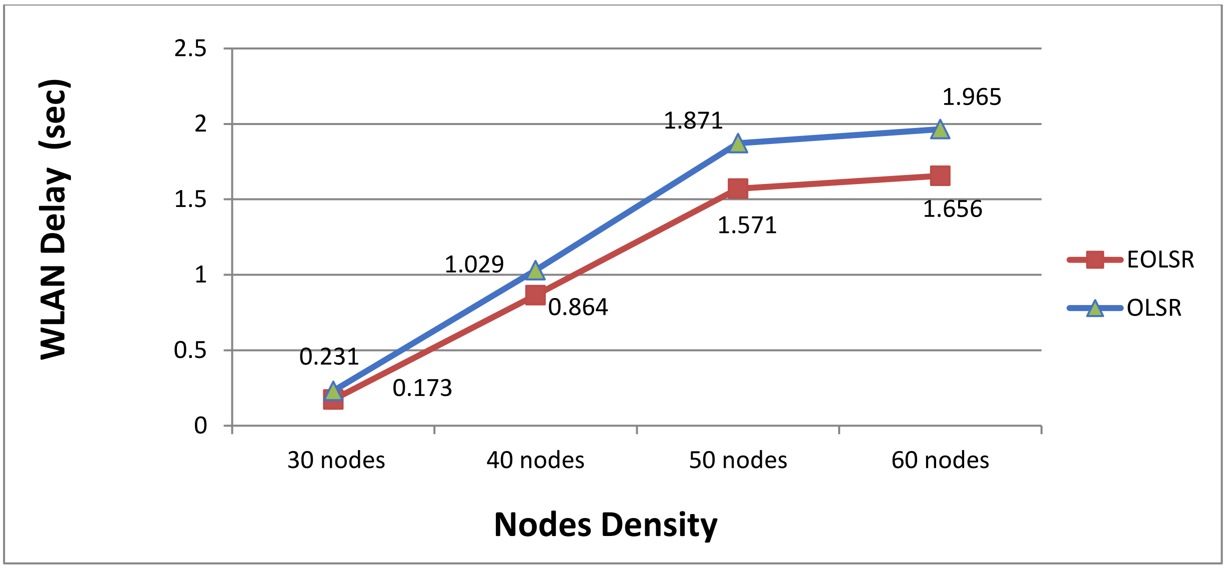

Figure 6.1: WLAN Delay of E-OLSR Compared to OLSR Routing Protocol

6.1.1.2 Comparison of WLAN Throughput through E-OLSR and OLSR Routing Protocol

The primary goal here is to achieve maximum throughput. Figure 6.2 and Table 6.2 display the network's performance in terms of throughput as the number of nodes varies. In comparing throughput, it is clear that E-OLSR performs better than OLSR when traffic loads range from 30 to 50 nodes. This performance difference becomes more pronounced as the number of nodes increases to 60. This research found that as the number of nodes increased, the throughput of E-OLSR improved. However, the throughput of traditional OLSR decreased when more than 50 mobile nodes were used. In traditional OLSR, mobile nodes have difficulty finding paths as the number of nodes increases. This is visible in the figure, as the throughput dropped a little when the density exceeded 50. The enhancements in the E-OLSR protocol significantly improved the data transfer rate in MANET.

Table 6.2: WLAN Throughput (bits/sec) of E-OLSR Compared to OLSR

Routing Protocol	30 nodes	40 nodes	50 nodes	60 nodes
OLSR	1,057,438	1,375,875	2,155,041	2,091,889
EOLSR	1,620,115	2,490,768	3,935,288	7,675,261

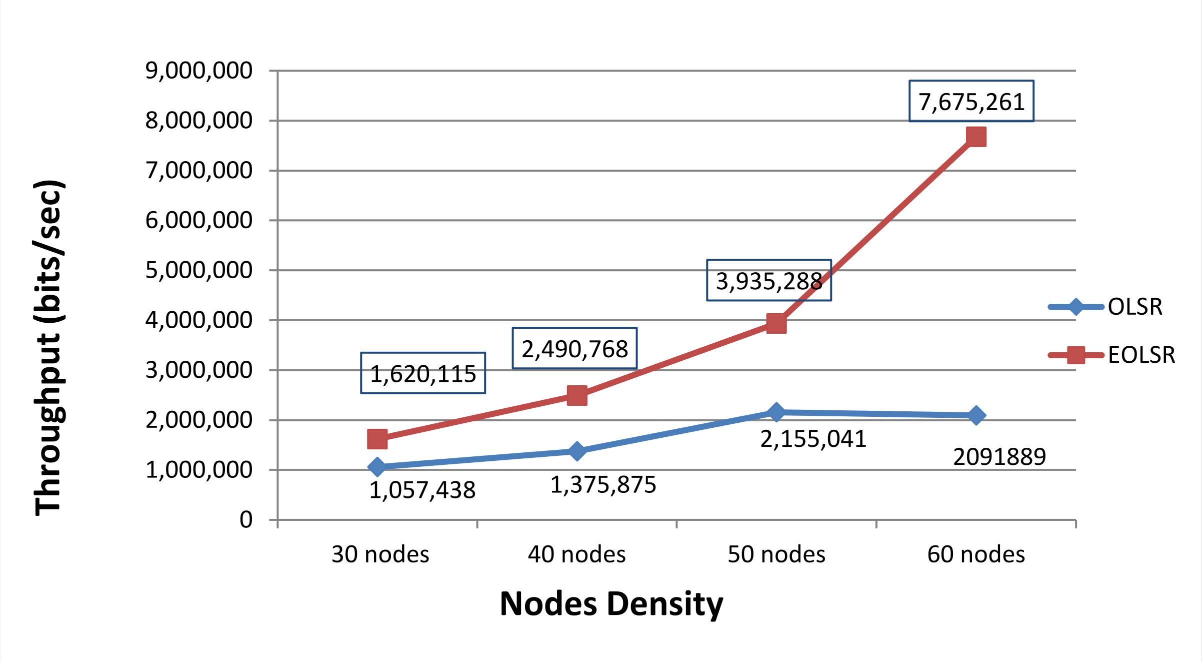

Figure 6.2: WLAN Throughput (bits/sec) of E-OLSR Compared to OLSR Routing Protocol

6.1.1.3 Comparison of WLAN Data Dropped through E-OLSR and OLSR Routing Protocols

This section presents experimental results comparing the performance of OLSR and E-OLSR routing protocols. Table 6.3 and Figure 6.3 show the results for the two routing algorithms, displaying different packet drop rates for various network sizes. When there are 30 nodes in the network, there is no significant difference in data dropped between E-OLSR and OLSR. The results are nearly equal due to low node density and minimal topology changes. The short HELLO and TC message intervals in E-OLSR have little effect on data drop performance. However, as shown in Table 6.3 and Figure 6.3, node density significantly affects data drop performance for both routing protocols when the network size exceeds 40 nodes. As the number of nodes increases, the data dropped also increases for both routing protocols. The observation results indicate that the data drop rate changes with network topology changes. It was found that the rate of data dropped changes at a similar level in both routing protocols, as shown in Table 6.3 and Figure 6.3.

Table 6. 3: WLAN Data Dropped (bits/sec) of E-OLSR Compared to OLSR

Routing Protocol	30 nodes	40 nodes	50 nodes	60 nodes
OLSR	56	1,030	2,305	2,738
E-OLSR	49	797	2,173	2,510

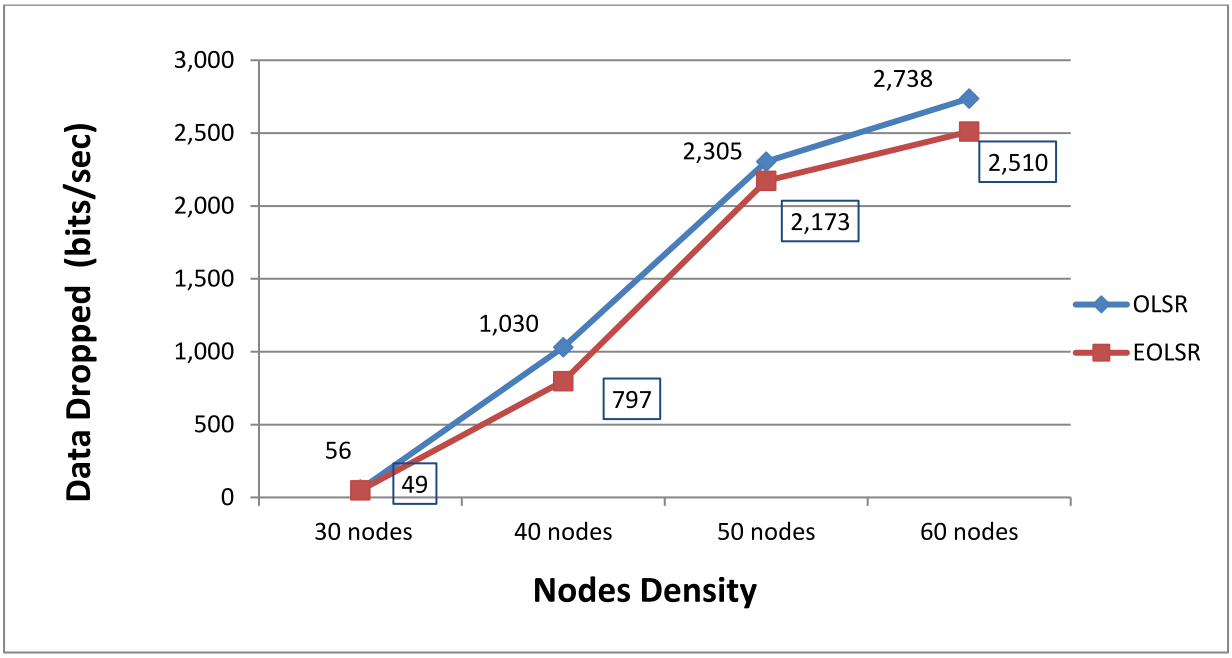

Figure 6. 3: WLAN Data Dropped (bits/sec) of E-OLSR Compared to OLSR Routing Protocol

6.2 Summary and Discussion

After evaluating traditional MANET routing protocols such as AODV, GRP, and OLSR, it is clear that the modified E-OLSR performs better than other routing protocols in terms of WLAN delay, throughput, and data dropped. This conclusion is based on the data presented in chapters 5 and 6. A detailed comparison between E-OLSR and other routing protocols is provided in Table 6.4.

Table 6. 4: Summary of Results of E-OLSR Compared to Different Routing Protocols

Metrics	Node Density	Routing Protocol			
		AODV	GRP	OLSR	E-OLR
Delay	30	0.579	0.259	0.230	0.173
	40	5.188	0.965	1.029	0.864
	50	6.141	1.681	1.876	1.571
	60	6.656	1.786	1.965	1.656
Throughputs	30	1,292,436	679,099	1,057,438	1,620,115
	40	1,553,586	798,148	1,375,875	2,490,768
	50	1,875,320	1,051,236	2,155,041	3,935,288
	60	2,091,889	1,378,920	2,068,120	7,675,261
Data Dropped	30	231	761	56	49
	40	1,110	5,039	1,030	797
	50	3,136	7,430	2,305	2,173
	60	8,551	23,171	2,738	2,510

By calculating the enhancement ratio of E-OLSR compared to OLSR, AODV, and GRP in terms of delay performance, the delay values of E-OLSR can be compared to those of the respective protocols. The enhancement ratio is calculated by dividing the delay of each protocol by the delay of E-OLSR across varying node densities. The results are as follows:

Enhancement Ratios:

1. E-OLSR vs OLSR:

30 Nodes: 0.230/0.173 = 1.33 → E-OLSR is 1.33 times better (or 33% improvement).

40 Nodes: 1.029/0.864 = 1.19 → E-OLSR is 1.19 times better (or 19% improvement).

50 Nodes: 1.876/1.571 = 1.19 → E-OLSR is 1.19 times better (or 19% improvement).

60 Nodes: 1.965/1.656 = 1.19 → E-OLSR is 1.19 times better (or 19% improvement).

2. E-OLSR vs AODV:

- 30 Nodes: 0.579/0.173 = 3.35 → E-OLSR is 3.35 times better (or 235% improvement).
- 40 Nodes: 5.188/0.864 = 6.00→ E-OLSR is 6.00 times better (or 500% improvement).
- 50 Nodes: 6.141/1.571 = 3.91 → E-OLSR is 3.91 times better (or 291% improvement).
- 60 Nodes: 6.656/1.656 = 4.02 → E-OLSR is 4.02 times better (or 302% improvement).

3. E-OLSR vs GRP:

- 30 Nodes: 0.259/0.173 = 1.50→ E-OLSR is 1.50 times better (or 50% improvement).
- 40 Nodes: 0.965/0.864 = 1.12 → E-OLSR is 1.12 times better (or 12% improvement).
- 50 Nodes: 1.681/1.571 = 1.07 → E-OLSR is 1.07 times better (or 7% improvement).
- 60 Nodes: 1.786/1.656 = 1.08→ E-OLSR is 1.08 times better (or 8% improvement).

Summary:

- E-OLSR consistently outperforms OLSR, AODV, and GRP in terms of delay performance across all node densities.
- The highest improvement is observed against AODV, with enhancement ratios ranging from 3.35x to 6.00x.
- The improvement over GRP is more modest but still significant, especially at lower node densities (e.g., 1.50x at 30 nodes).
- Against OLSR, E-OLSR shows a stable improvement of around 1.19x to 1.33x.

These ratios highlight the superior delay performance of E-OLSR compared to the other routing protocols, as explained in Figure 6.4.

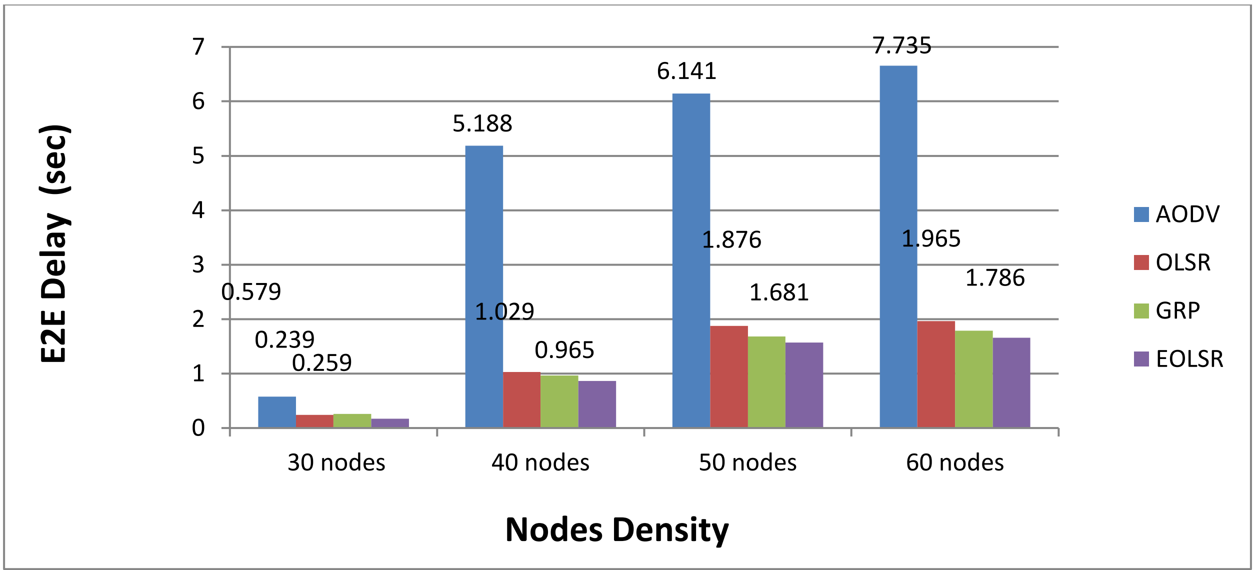

Figure 6.4: WLAN Delay of E-OLSR Compared to Different Routing Protocols

Here are the enhancement ratios of E-OLSR against OLSR, AODV, and GRP in terms of data dropped performance, calculated for each node density:

1. E-OLSR vs OLSR (Improvement in Data Drop Reduction)

- 30 Nodes: 56/49 = 1.14
  → E-OLSR is 1.14x better (14% fewer drops).
- 40 Nodes: 1030/797 = 1.29 → E-OLSR is 1.29x better (29% fewer drops).

- 50 Nodes:2305/2173 = 1.06 → E-OLSR is 1.06x better (6% fewer drops).
- 60 Nodes: 2738/2510 = 1.09 → E-OLSR is 1.09x better (9% fewer drops).

Summary:

E-OLSR consistently outperforms OLSR, with the most significant improvement at 40 nodes (1.29x).

2. E-OLSR vs AODV (Improvement in Data Drop Reduction)

- 30 Nodes: 231/49 = 4.71 → E-OLSR is 4.71x better (371% fewer drops).
- 40 Nodes: 1110/797 = 1.39 → E-OLSR is 1.39x better (39% fewer drops).
- 50 Nodes: 3136/2173 = 1.44
  → E-OLSR is 1.44x better (44% fewer drops).
- 60 Nodes: 8551/2510 = 3.41 → E-OLSR is 3.41x better (241% fewer drops).

Summary:

E-OLSR dramatically outperforms AODV, especially at 30 nodes (4.71x) and 60 nodes (3.41x).

3. E-OLSR vs GRP (Improvement in Data Drop Reduction)

- 30 Nodes: 761/49 = 15.53 → E-OLSR is 15.53x better (1453% fewer drops).
- 40 Nodes: 5039/797 = 6.32 → E-OLSR is 6.32x better (532% fewer drops).
- 50 Nodes: 7430/2173 = 3.42 → E-OLSR is 3.42x better (242% fewer drops).
- 60 Nodes: 23171/2510 = 9.23 → E-OLSR is 9.23x better (823% fewer drops).

Summary:

E-OLSR shows massive improvements over GRP, with the most striking results at 30 nodes (15.53x) and 60 nodes (9.23x).

Key Takeaways:

1- E-OLSR vs OLSR:

- Moderate improvement (1.06x–1.29x), best at 40 nodes (1.29x).

2- E-OLSR vs AODV:

- Significant improvement (1.39x–4.71x), best at 30 nodes (4.71x).

3- E-OLSR vs GRP:

- Extreme improvement (3.42x–15.53x), best at 30 nodes (15.53x).

E-OLSR is most effective against GRP, reducing data drops by orders of magnitude in high-density scenarios. It also performs better than AODV and OLSR, although it is only a little better than OLSR. See Figure 6.5.

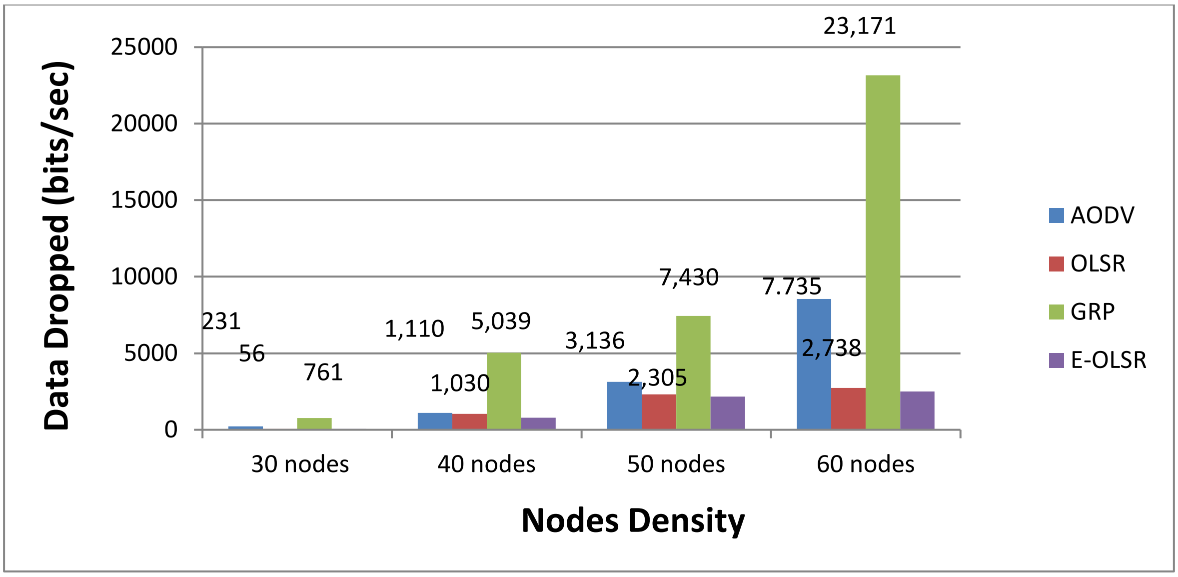

Figure 6. 5: WLAN Data Drop of E-OLSR Compared to Different Routing Protocols

Here are the enhancement ratios of E-OLSR against OLSR, AODV, and GRP in terms of throughput performance, calculated for each node density:

1. E-OLSR vs OLSR (Throughput Improvement)

- 30 Nodes: 1,620,115/1,057,438 = 1.53
  → E-OLSR is 1.53x better (53% higher throughput).
- 40 Nodes: 2,490,768/1,375,875 = 1.81
  → E-OLSR is 1.81x better (81% higher throughput).
- 50 Nodes: 3,935,288/2,155,041 = 1.83 → E-OLSR is 1.83x better (83% higher throughput).
- 60 Nodes: 7,675,261/2,068,120 = 3.71 → E-OLSR is 3.71x better (271% higher throughput).

Summary:

E-OLSR significantly outperforms OLSR, with the most dramatic improvement at 60 nodes (3.71x).

2. E-OLSR vs AODV (Throughput Improvement)

- 30 Nodes: 1,620,115/1,292,436 = 1.25
  → E-OLSR is 1.25x better (25% higher throughput).
- 40 Nodes: 2,490,768/1,553,586 = 1.60
  → E-OLSR is 1.60x better (60% higher throughput).
- 50 Nodes: 3,935,288/1,875,320 = 2.10 → E-OLSR is 2.10x better (110% higher throughput).

- 60 Nodes: 7,675,261/2,091,889 = 3.67 → E-OLSR is 3.67x better (267% higher throughput).

  Summary:

E-OLSR shows substantial gains over AODV, especially at 50 nodes (2.10x) and 60 nodes (3.67x).

3. E-OLSR vs GRP (Throughput Improvement)

- 30 Nodes: 1,620,115/679,099 = 2.39 → E-OLSR is 2.39x better (139% higher throughput).
- 40 Nodes: 2,490,768798,148=3.12798,1482,490,768=3.12

  → E-OLSR is 3.12x better (212% higher throughput).
- 50 Nodes:3,935,288/1,051,236 = 3.74 → E-OLSR is 3.74x better (274% higher throughput).
- 60 Nodes:7,675,261/1,378,920 = 5.57 → E-OLSR is 5.57x better (457% higher throughput).

Summary:

E-OLSR delivers exceptional throughput gains over GRP, peaking at 60 nodes (5.57x).

Key Takeaways:

1. E-OLSR vs OLSR:

   1.53x–3.71x improvement, with the largest gain at 60 nodes (3.71x).
2. E-OLSR vs AODV:

   1.25x–3.67x improvement, most pronounced at 60 nodes (3.67x).
3. E-OLSR vs GRP:

   2.39x–5.57x improvement, dominating at 60 nodes (5.57x).

Trend Analysis:

- E-OLSR performs better in terms of throughput as the number of nodes increases. It shows the most improvement in networks with a high density of nodes (for example, 60 nodes).
- E-OLSR's throughput is 5.57 times greater than GRP's throughput when using 60 nodes, representing the most significant difference between the two.

E-OLSR is most effective against GRP, increasing throughput by orders of magnitude in high-density scenarios. It also consistently outperforms AODV and OLSR, though the gains over OLSR are more modest. See Figure 6.6.

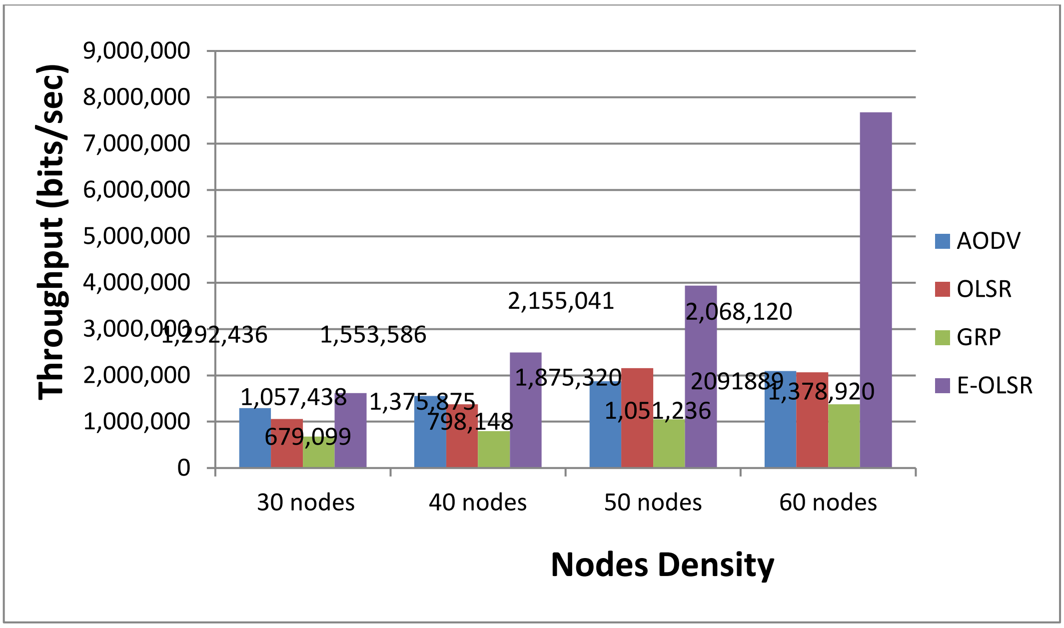

Figure 6. 6: WLAN throughput of E-OLSR compared to different Routing protocols

CHAPTER SEVEN:
Conclusion and Future Work

7.1 Conclusion

Firstly, this thesis studied different routing protocols operating in various environmental scenarios, each with unique attributes. The selection of appropriate protocols significantly enhances the reliability of a network. In mobile ad hoc networks, routing protocols should be cascaded as indicated by this research. Mobile ad hoc networks utilize two categories of routing protocols: reactive and proactive. Each category serves specific purposes, so choosing between them is important for optimal network performance. In this thesis, I have implemented several simulation scenarios for three routing protocols: AODV, GRP, and OLSR. Voice traffic was transmitted through MANET to explain the effect of voice traffic when utilizing these routing protocols. The performance of the three protocols was evaluated based on delay, throughput, and data loss. The aim was to evaluate the performance of these three routing protocols in a MANET based on specified parameters. The main issue was choosing a dependable protocol to solve the latency problem. Based on the concluded results and performance evaluations, no existing MANET routing protocols can transmit real-time data across different mobile densities. No routing protocol can simultaneously support all metrics or provide efficient routing for all network sizes without modifications, regardless of the number of nodes or mobility. Each protocol has its advantages and disadvantages for transmitting real-time data. However, OLSR is more efficient for real-time applications. It nearly meets the requirements for these applications due to its strong performance in two key areas: throughput and data loss. One disadvantage of OLSR is that it can cause delays in the WLAN when transmitting voice over a MANET. Therefore, there is a need to improve the OLSR protocol to better support real-time traffic.

Secondly, it is necessary to enhance the OLSR routing protocol to meet the requirements of transmitting real-time traffic and providing the best performance for the most important voice transmission requirements, which include minimizing delay and data dropped. The main issue in OLSR is when sending HELLO and TC messages. HELLO message traffic refers to the time interval between two consecutive HELLO messages in a one-hop neighborhood, which helps gather neighborhood information. To achieve optimal performance in scenarios with slow speeds and low scalability, it is important to send HELLO messages less frequently to reduce overhead. But in scenarios with dense and sparse network topologies, it is necessary to send HELLO messages more frequently by reducing the intervals to identify neighboring nodes better.

While TC message traffic refers to the time interval between two consecutive TC messages by an MPR selector set, which helps gather topology information. To achieve optimal performance in scenarios with slow speeds and a scalable network, it is important to send TC messages less frequently because they report minimal changes. But in the case of a dense network and high mobility (topology changes frequently), it is necessary to send TC messages more frequently by reducing the intervals to ensure up-to-date routes because nodes leave and enter the network very frequently, resulting in improved delay, data dropped, and throughput for the E-OLSR routing protocol in MANET.

The results indicate that the enhanced configuration of the OLSR routing protocol (E-OLSR) effectively supports large networks of up to 60 nodes for voice communication.

7.2 Future Work

To enhance the work presented in this thesis, it would be best to consider a wide range of ideas:

1-Quality of service (QoS) metrics(These metrics include several key dimensions, such as latency, jitter, packet loss, bandwidth, and availability.),

2-Different traffic generators (e.g., HTTP, FTP, video conferencing,.)

3-Mobility models (e.g., Gauss-Markov model: This model simulates the behavior of mobile nodes that tend to move within a specific path, yet can deviate from that path, which more accurately represents human mobility),

4-Wi-Fi (wireless fidelity: When evaluating Wi-Fi rates, it's important to consider several key factors. First, the speed of the internet connection is paramount. Measured in megabits per second (Mbps), higher speeds typically translate to smoother browsing, quicker downloads, and more robust streaming capabilities.)rates,

5- Test higher node speeds, different transmission power, and various simulation scenarios.

6- Applying the concept of adaptability to different routing protocols.

This includes examining different transmission region parameters and distances.

References

[1] Aadri, A., & Idrissi, N. (2018). An advanced comparative study of MANETs routing protocols under varied number of nodes and mobility rate. *Journal of Communications, 13*(6).

[2] Abdo, A. H. (2018). *Studying the impact of HELLO messages on routing algorithms in UAANET* [Master's thesis, Higher Institute for Applied Sciences and Technology].

[3] Abdullah, A. M., Ozen, E., & Bayramoglu, H. (2019). Investigating the impact of mobility models on MANET routing protocols. *International Journal of Advanced Computer Science and Applications, 10*(2), 25–35.

[4] Abid, A. M. (2016, December). *Performance evaluation of OLSR routing protocol for VoIP applications under IPv6 environment* [Master's thesis, Sudan University of Science and Technology].

[5] Ahmed, D. E. M. (2020, October). *Enhanced scheme for video transmission over mobile ad hoc networks based on optimized link state routing protocol* [Master's thesis, Sudan University of Science & Technology].

[6] Ahmed, D. E. M., & Khalifa, O. O. (2017, July). Performance evaluation of enhanced MANETs routing protocols under video traffics, for different mobility and scalability models using OPNET. *American Journal of Engineering Research (AJER).*

[7] Ahmed, D. E. M., & Khalifa, O. O. (2017). A comprehensive classification of MANETs routing protocols. *International Journal of Computer Applications Technology and Research, 6*(3), 141–158.

[8] Ahmed, D. E. M., Ebrahim, H. A., & Khalifa, O. O. (2020). Performance evaluation of AODV, OLSR, and GRP for transmitting video conferencing over MANETs. *International Journal of Computer Science and Information Security, 18*(4).

[9] Al-Dhief, F. T., Sabri, N., Salim, M. S., Fouad, S., & Aljunid, S. A. (2018). MANET routing protocols evaluation: AODV, DSR and DSDV perspective. *MATEC Web of Conferences, 150*.

[10] Al-Shareeda, M. A., & Manickam, S. (2022, July 27). Man-in-the-middle attacks in mobile ad hoc networks (MANETs): Analysis and evaluation. *Symmetry.*

[11] Alkahtani, S. M., & Alturki, F. (2021). Performance evaluation of different mobile ad-hoc network routing protocols in difficult situations. *International Journal of Advanced Computer Science and Applications, 12*(1), 158–167.

[12] Ali, A. K. S., & Kulkarni, U. V. (2015). Characteristics, applications and challenges in mobile ad-hoc networks (MANET): Overview. *International Journal of Electronics & Communication (IIJEC), 3*(12).

[13] Avhankar, M. S., Pawar, J. A., Majalekar, S., & Kedari, S. S. (2022). Mobile ad hoc network routing protocols – Using OPNET simulator. International Journal of *Scientific and Research Publications, 12*(2).

[14] Avhankar, M. S., Pawar, J. A., Majalekar, S., & Kedari, S. S. (2022). Mobile ad hoc network routing protocols using OPNET simulator. International Journal on Recent *and Innovation Trends in Computing and Communication, 10*(1), 1–7.

[15] Badri, A., Mouiz, A., Baghdad, A., & Sahel, A. (2019). Performance evaluation of OLSR and AODV routing protocols with different parameters in mobile ad-hoc networks using NS2 simulator. In *Proceedings of the 5th International Conference on Computer and Technology Applications* (pp. 134–139). ACM.

[16] Barak, D. D. (2017). Mobile ad-hoc networks and its application in current scenario. *International Journal of Latest Trends in Engineering and Technology, 9*(4), 232–236.

[17] Berradi, H., Habbani, A., Mouchfiq, N., & Souidi, M. (2020). Improvement of OLSR protocol using the HELLO message scheme based on neighbors' mobility. *Journal of Communications, 15*(7), 512–520.

[18] Bouallegue, R., Naimi, S., Busson, A., & Vèque, V. (2018). Metric anticipation to manage mobility in mobile mesh and ad-hoc wireless networks. *Annals of Telecommunications, 73*(11–12), 787–802.

[19] Boukerche, A. (2009). *Algorithms and protocols for wireless and mobile ad hoc networks*. Wiley.

[20] Clausen, T. (Ed.), & Jacquet, P. (Ed.). (2003, October). *Optimized link state routing protocol (OLSR)* (RFC 3626). IETF

[21] Datey, S. G., & Ansari, T. (2015). Mobile ad-hoc networks: Its advantages and challenges. International Journal of Electrical and Electronics Research, 3(2), 491–496.

[22] Dhar, S. (2005). MANET: Applications, issues, and challenges for the future. International Journal of Business Data Communications and Networking.

[23] Dhwaj Barak, D. (2017). Mobile ad-hoc networks and its application in current scenario. International Journal of Latest Trends in Engineering and Technology, 9(4), 232–236.

[24] Dong, S., & Zhang, H. (2021). An MPR set selection algorithm based on set operation. In 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC).

[25] Dua, M., Ranga, V., Mehra, K., Kardam, P., & Bahsakhetre, S. M. (n.d.). Performance evaluation of AODV, DSR, DSDV mobile ad-hoc protocols on different scenarios: An analytical review. Department of Computer Engineering, National Institute of Technology, Kurukshetra.

[26] Dharwisho, H. Y. (2019). Performance evaluation and comparison of GRP and OLSR routing protocols for video streaming over mobile ad hoc networks using OPNET 14.5. Journal of Engineering Sciences and Information Technology, 3(3), 16–44.

[27] Eldein Mustafa Ahmed, D., & Khalifa, O. O. (2017). A comprehensive classification of MANETs routing protocols. International Journal of Computer Applications Technology and Research, 6(3), 141–158.*

[28] Eng. Abdullah Sardar. (2018). Developing routing protocol in MANET based on the power of network devices [Master's thesis, University of Aleppo].

[29] Frikha, M. (2013). Ad hoc networks. Wiley.

[30] Ganesh Datey, S., & Ansari, T. (2015). Mobile ad-hoc networks: Its advantages and challenges. International Journal of Electrical and Electronics Research, 3(2), 491–496.

[31] Geetha, M., Umarani, R., & Kiruthika, R. (2010). A comparative study of gateway discovery protocol in MANET. International Journal of Computer Applications, 11(2), 16–22.

[32] Gorantala, K. (2006, June 15). Routing protocols in mobile ad-hoc networks [Technical report]. Umeå University, Department of Computing Science.

[33] Guo, X., Cao, Y., Wang, J., & Jiang, Y. (2021). A new solution based on optimal link-state routing for named data MANET. China Communications, 18, 213–229.

[34] Hamed Taha Mohammed, H. E. (2017, November). Performance evaluation of AODV, OLSR and GRP routing protocols in vehicular highway environment [Master's thesis, Alneelain University].

[35] Hasan, M. Z., Hasan, M. Z., & Hussain, M. Z. (2020). Mobile ad-hoc networking (MANET). Journal of Computer Science.

[36] Hinds, A., Ngulube, M., Zhu, S. Y., & Al-Aqrabi, H. (2013). A review of routing protocols for mobile ad-hoc networks (MANET). International Journal of Information and Education Technology, 1–5.

[37] Huhtonen, A. (2004, April 26–27). Comparing AODV and OLSR routing protocols. Helsinki University of Technology, Telecommunication Software and Multimedia Laboratory.

[38] Islam, M., & Jin, S. (2019). An overview of research on wireless communication networks. Advances in Wireless Communications and Networks, 5(1), 19–28.

[39] Jaiswal, T., & Kidwai, N. R. (2022). MANETs: Challenges and future research scope. International Journal of Engineering and Advanced Technology, 12(2).

[40] Kaur, H., Singh, H., & Sharma, A. (2016). Geographic routing protocol: A review. International Journal of Grid and Distributed Computing, 9(2), 245–254.

[41] Kaur, J., & Gurm, R. K. (2014). A review of current routing protocols for MANETs. International Journal of Scientific Research in Computer Science Applications and Management Studies, 3(1).

[42] Kaur, P. (2016). An overview on MANET—Advantages, characteristics and security attacks. In 4th International Conference on Advancements in Engineering & Technology (ICAET 2016).

[43] Kazakov, G. (2023). Estimation of the achievable performance of mobile ad hoc networks with optimal link state routing. Inventions, 8, 108.

[44] Kelsie, N., & Rennie, E. (2022, April 26). Ad hoc network. Internet Policy Review, 11(2).

[45] Khamkar, R. R., & Poskar, S. S. (2021). How important mobile ad hoc network (MANET) is? International Research Journal of Engineering and Technology (IRJET), 8(2).

[46] Khan, M. A., Khan, I. U., Safi, A., & Quershi, I. M. (2018). Dynamic routing in flying ad-hoc networks using topology-based routing protocols. Drones, 2(3), 27.

[47] Khan, R. A., & Tariq, M. A. (2019). A survey on wired and wireless network. Lahore Garrison University Research Journal of Computer Science and Information Technology.

[48] Khatri, P., & Rajvanshi, P. R. (2020). A relative study about mobile ad-hoc network (MANET): Applications, standards, protocols, architecture, and recent trends.

[49] Khudayer, B. H., Alzabin, L. R., Anbar, M., Tawafak, R. M., Wan, T.-C., AlSideiri, A., Malik, S. I., & Al-Amiedy, T. A. (2023). A comparative performance evaluation of routing protocols for mobile ad-hoc networks. International Journal of Advanced Computer Science and Applications, 14(4).

[50] Kim, B.-S., Ullah, S., Kim, K. H., Roh, B., Ham, J.-H., & Kim, K.-I. (2020). An enhanced geographical routing protocol based on multi-criteria decision making method in mobile ad-hoc networks. Ad Hoc Networks, 103, 102157.

[51] Kumar, R., & Dave, M. (2021). An improved MPR selection strategy for OLSR protocol to minimize control overhead in MANETs. IEEE Access, 9, 156823–156835.

[52] LEGO, K., Singh, P. K., & Sutradhar, D. (2010). Comparative study of ad hoc routing protocol AODV, DSR and DSDV in mobile ad-hoc network. Indian Journal of Computer Science and Engineering, 1(4), 364–371.

[53] Li, Y., Wang, J., & Zhang, Y. (2022). Reinforcement learning-based MPR selection for OLSR in UAV networks. Computer Networks, 214, 109131.

[54] Mannam, R. R., & Zabin, M. (2012, June 13). Comparative performance analysis of MANET routing protocols in internet-based mobile ad-hoc networks. Linnaeus University, School of Computer Science, Physics and Mathematics.

[55] Mannam, R. R., & Zabin, M. (2012, June 13). Comparative performance analysis of MANET routing protocols in internet-based mobile ad-hoc networks. Linnaeus University, School of Computer Science, Physics and Mathematics.

[56] Mehta, A., & Saini, R. (2015). A review paper on security in mobile ad hoc network. International Journal of Advanced Research in Science and Engineering, 4(8).

[57] Mittal, P., Singh, P., & Rani, S. (2013). Performance analysis of AODV, OLSR, GRP and DSR routing protocols with database load in MANET. International Journal of Research in Engineering and Technology, 2(9).

[58] Mohammed Abid, A. (2016, December). Performance evaluation of OLSR routing protocol for VoIP applications under IPv6 environment [Master's thesis, Sudan University of Science and Technology].

[59] Mounir, F. (2013). Ad hoc networks. Wiley.

[60] Muni, R., & Malhotra, R. (2020). Mobile ad hoc network. International Journal of Scientific Research & Engineering Trends, 6(3).

[61] Nabben, K., & Rennie, E. (2022). Ad hoc network. Internet Policy Review, 11(2).

[62] Naimi, S., Busson, A., Vèque, V., & Bouallegue, R. (2018). Metric anticipation to manage mobility in mobile mesh and ad-hoc wireless networks. Annals of Telecommunications, 73(11–12), 787–802.

[63] Noureddine, S., & Sougath, C. (2023). Election of MPR nodes and detection of malicious nodes based on a Byzantine fault in the OLSR protocol: Case of a scale-free network. Electronics, 12.

[64] Nwabueze, C. (2010). Mobile ad hoc network (MANET) architecture and implementation analysis. Natural and Applied Sciences Journal, 11(1).

[65] Ragab, A. R. (2020). A new classification for ad-hoc network. International Journal of Interactive Mobile Technologies (iJIM), 14(14).

[66] Ranga, V., Dua, M., Mehra, K., Kardam, P., & Bahsakhetre, S. M. (n.d.). Performance evaluation of AODV, DSR, DSDV mobile ad-hoc protocols on different scenarios: An analytical review. Department of Computer Engineering, National Institute of Technology, Kurukshetra.

[67] Refaat Ragab, A. (2020). A new classification for ad-hoc network. International Journal of Interactive Mobile Technologies (iJIM), 14(14).

[68] Saini, T. K., & Sharma, S. C. (2020). Flexible multipoint relay selection for suitable route in mobile ad hoc networks.

[69] Saini, T. K., & Sharma, S. C. (2020). Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept. Ad Hoc Networks, 102–148.

[70] Saleem, T., & Ullah, K. (2010, November). Performance issues of routing protocols in mobile ad-hoc networks [Master's thesis, Blekinge Institute of Technology].

[71] Sarao, P. (2018). Comparison of AODV, DSR, and DSDV routing protocols in a wireless network. Journal of Communications, 13(4), 175–181.

[72] Schiller, J. (2000). Mobile communications. Addison-Wesley.

[73] Shanshan, S. (2005, July 15). Dynamic feedback mechanisms in trust-based DSR [Master's thesis, Danmarks Tekniske Universitet].

[74] Singh, K., & Kumar, A. (2016). Mobile ad-hoc network: Applications and challenges. International Journal of Engineering and Technology, 8(2), 183–185.

[75] Sobti, R. (2015). A study on challenges and issues on MANET. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 4(9).

[76] Soni, N. (2020). Multicast routing protocols in mobile ad hoc networks. International Journal of Recent Technology and Engineering, 9(1).

[77] Taha Mohammed, H. E. H. (2017, November). Performance evaluation of AODV, OLSR and GRP routing protocols in vehicular highway environment [Master's thesis, Alneelain University].

[78] Tuli, E. A., Golam, M., Kim, D.-S., & Lee, J.-M. (2022). Performance enhancement of optimized link state routing protocol by parameter configuration for UANE. Drones, 6.

[79] Vankar, M. S., Pawar, J. A., Majalekar, S., & Kedari, S. S. (2022). Mobile ad hoc network routing protocols – Using OPNET simulator. International Journal of Scientific and Research Publications, 12(2).

[80] Virendra, D., Umre, J., & Chopra, A. (n.d.). Different network threats and issues based on wireless ad hoc networks: A survey details.

[81] Yaoy, J.-M., Wang, Y.-X., Li, Q., Mao, H.-K., Abd El-Latif, A. A., & Chen, N. (2022). An efficient routing protocol for quantum key distribution networks. arXiv preprint.

[82] Yahya Darwisho, H. (2019). Performance evaluation and comparison of GRP and OLSR routing protocols for video streaming over mobile ad hoc networks using OPNET 14.5. Journal of Engineering Sciences and Information Technology, 3(3), 16–44.

[83] Yang, C., Cao, Y., Wang, J., & Jiang, Y. (2021). A new solution based on optimal link-state routing for named data MANET. China Communications, 18, 213–229.

[84] Zulkifl Hasan, M., Hasan, M. Z., & Hussain, M. Z. (2020). Mobile ad-hoc networking (MANET). Journal of Computer Science.

[85] Hekmat, A. A. (2018). Studying the impact of HELLO messages on routing algorithms in UAANET [Master's thesis, Higher Institute for Applied Sciences and Technology].

[86] Hussey, R., Huff, E., Shinwari, Z., & Hnatyshin, V. (2018). A comparative study of proactive and reactive geographical routing protocols for MANET. Department of Computer Science, Rowan University.

[87] Kaur, J., & Gurm, R. K. (2014). A review of current routing protocols for MANETs. International Journal of Scientific Research in Computer Science Applications and Management Studies, 3(1).

[88] Kaur, H., Singh, H., & Sharma, A. (2016). Geographic routing protocol: A review. International Journal of Grid and Distributed Computing, 9(2), 245–254.

[89] Darwisho, H. Y. (2019). Performance evaluation and comparison of GRP and OLSR routing protocols for video streaming over mobile ad hoc networks using OPNET 14.5. Journal of Engineering Sciences and Information Technology, 3(3), 16–44.

.