الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj - Bouira -
Tasdawit Akli Muḥend Ulḥağ - Tubirett -
Faculté des Sciences et des Sciences Appliquées

وزارة التعليم العالي والبحث العلمي
جامعة أكلي محند أولحاج
-البويرة-
كلية العلوم والعلوم التطبيقية

Référence : ...../MM/ 2023

المرجع:...../م م/ 2023

Master thesis

Presented to

Department : Electrical Engineering
Domain : Sciences and Technologies
Branch : Telecommunications
Specialty : Telecommunication Systems

Presented by:

MEKHAZNI Ouassim

And

SEHTALI Mohamed

Theme

Comparative analysis of different routing protocols in MANET

Presented on: **03/07/2023**

In front of the jury composed of:

President: Dr. Mourad NOURINE	M.C.A
Examinator: Dr. Bilal SAOUD	M.C.A
Directed by: Dr. Med. Lamine BOUCENNA	M.C.A

Dedication

I am profoundly grateful for the unwavering support and guidance I have received from the remarkable individuals who have been instrumental in my journey.

I dedicate this work to myself, as it is a testament to my resilience, dedication, and unwavering commitment to personal growth and academic excellence.

To my parents

To my siblings

To my friends

And to all who gave me the motivation I needed.

Ouassim

Dedication

I am deeply grateful to the Almighty ALLAH for His unwavering strength, guidance, and perseverance that have carried me through my academic journey, without which none of my achievements would have been possible.

My heartfelt appreciation goes to my parents for their unconditional love, support, and belief in my abilities, which have been the bedrock of my educational pursuits.

I extend my sincere gratitude to my dedicated academic advisor, Dr BOUCENNA Mohamed Lamine, for his invaluable guidance and insightful feedback that have shaped the direction of our research

Mohamed

Acknowledgement

I would like to begin by expressing my deepest gratitude to the Almighty Allah for His blessings, guidance, and strength throughout this journey of completing our thesis.

I extend my heartfelt appreciation to our parents, their constant encouragement and belief in our abilities have propelled us forward.

I would like to express my sincere gratitude to our esteemed thesis supervisor, Dr. Boucenna Mohamed Lamine, for his invaluable guidance, mentorship, and continuous support.

I am grateful to the members of the jury who accepted to evaluate our project.

I would also like to acknowledge the academic staff and researchers who have contributed to the field of study, as their work has provided us with a solid foundation and inspiration for our research.

Lastly, I would like to thank all our friends and colleagues who have provided assistance, encouragement, and a collaborative environment throughout our thesis journey.

To everyone mentioned and to those who have supported us in various ways, we extend our heartfelt appreciation. Your contributions have been invaluable, and we are truly grateful for your involvement in our thesis.

Abstract

Wireless networks have revolutionized communication by enabling connectivity without the need for physical cables. They provide flexible and convenient access to information and services, supporting various devices and applications. Among wireless networks, ad hoc networks stand out as self-configuring networks formed by wireless devices without the need for a pre-existing infrastructure, and for the communication to be established we use routing protocols and algorithms.

In our comparative study, we analyzed some of these routing protocols precisely, Ad hoc On-Demand Distance Vector (AODV), Destination-Sequenced Distance Vector (DSDV), and Optimized Link-State Routing (OLSR) where we evaluated these protocols based on different metrics through different scenarios.

Key Words: Routing protocols, AODV, DSDV, OLSR, Ad hoc Networks**.**

Table of Contents

List of Figures

List of tables

List of Acronyms

PRNET Packet Radio Network

DARPA Defense Advanced Research Project Agency

MANET Mobile Ad hoc Network

WSN Wireless Sensor Networks

WMN Wireless Mesh Network

VANET Vehicular Ad hoc Network

APs Access Points

AODV Ad hoc On Demand-Distance Vector

OLSR Optimized Link-State Routing

DSDV Destination-Sequenced Distance Vector

ZRP Zone Routing Protocol

O-AODV Optimized Ad hoc On Demand-Distance Vector

NS-3 Network simulator 3

RREQ Route Request

RREP Route Reply

RERR Route Error

PDR Packet Delivery Ratio

General Introduction

In the era of ubiquitous wireless communication, the prevalence of mobile devices and the need for seamless connectivity have driven significant research efforts towards Mobile Ad Hoc Networks (MANET). They serve as a critical foundation for establishing communication in dynamic and self-configuring wireless environments, without relying on a fixed infrastructure. With their inherent versatility, MANET find applications in diverse domains such as military operations, disaster management, vehicular networks, and more.

An ad hoc wireless network is characterized by its composition of mobile nodes that utilize wireless transmission for communication, without depending on a centralized infrastructure like base stations or access points. The mobile devices themselves act as routers, enabling connectivity within the network. The ability to rapidly deploy these networks anywhere and at any time, without the complexities of infrastructure setup, makes them invaluable in various scenarios. Military operations can establish communication among soldiers during tactical missions, even in enemy territories, without relying on fixed communication infrastructure. Emergency systems can facilitate communication among rescue personnel in disaster-stricken areas, enabling effective coordination. Furthermore, ad hoc networks find utility in applications such as cooperative industrial robotics and traffic management.

The efficacy of communication in MANET critically hinges upon the selection of efficient routing techniques and protocols. Unlike traditional networks, MANET face unique challenges due to the absence of a centralized infrastructure and the dynamic nature of network topologies. Consequently, numerous routing techniques and protocols have emerged to address these challenges and optimize network performance.

This thesis aims to undertake a comprehensive comparative analysis of various MANET routing techniques. Through this analysis, the thesis seeks to delve into the workings, strengths, and limitations of different routing protocols, enabling a deeper understanding of their performance characteristics. Key metrics such as Packet Delivery Ratio (PDR), Throughput, Delay, and the impact of network density and mobility will be evaluated to provide valuable insights into the effectiveness of these techniques.

The thesis is titled "Comparative Analysis of Different Routing protocols in MANET" and is divided into three chapters, each addressing distinct aspects of ad hoc networks. Our first chapter provides an overview of MANET, highlighting their unique characteristics, advantages, and real-world applications. This chapter establishes the foundation for comprehending the challenges associated with these networks.

The second chapter delves into the intricacies of routing in MANET, exploring various routing techniques and protocols. It discusses fundamental concepts, classifies routing protocols, and examines their underlying mechanisms. Additionally, this chapter analyzes the strengths and weaknesses of prominent routing protocols, shedding light on their suitability for different network scenarios.

The final chapter focuses on the simulation and evaluation of MANET routing techniques. A simulation environment will be established to study the performance of selected routing protocols under diverse network conditions. This chapter aims to provide quantitative insights into the comparative analysis of routing techniques. Furthermore, an innovative solution will be proposed to address congestion and network saturation, contributing novel ideas for controlling these issues in MANETs.

By undertaking this comparative analysis, the research seeks to enhance our understanding of MANET routing techniques, their performance characteristics, and their suitability for different network scenarios. The findings of this research will help network designers and researchers in selecting and designing efficient routing solutions, ultimately facilitating the development of robust and reliable wireless communication networks.

Chapter 1:
Introduction to Ad Hoc Networks

1. Introduction:

Today, instant access to information and data is a necessity, driven by advancements in wireless communication technologies and the popularity of portable devices like smartphones and laptops. This has led to an increased demand for networks that support mobility, giving rise to the concept of ad hoc networks. Ad hoc networks aim to expand mobility by allowing mobile nodes to form a decentralized and self-organizing infrastructure. Unlike traditional networks, which rely on fixed infrastructure, ad hoc networks enable dynamic connections between nodes, creating networks on the go. These networks have found applications in various domains, offering flexibility and adaptability for communication and information sharing in resource-constrained environments.

In this chapter, we will explore the wireless networks field, with a specific focus on ad hoc networks. We will introduce the concept of wireless networks and delve into the different types and classifications of ad hoc networks. Furthermore, we will examine some of the main applications where ad hoc networks play a crucial role in establishing communication and facilitating information sharing.

2. Wireless networks:

Wireless networks are communication networks in which devices are able to exchange and share data without the need for cables or wired connection. The communication in wireless networks happens through the use of radio signals and that's how information is transmitted between devices.

Wireless networks offer many advantages including mobility, through these networks, devices can be connected while moving. The inconvenience of physical cables is eliminated which adds flexibility and easy access to information anywhere any time.

Wireless networks have changed the way we communicate, with the mobility and flexibility they provide and enable a wide range of applications and use to enhance our connectivity.

2.1. Categories of Wireless networks:

Wireless networks are divided into two different classes.

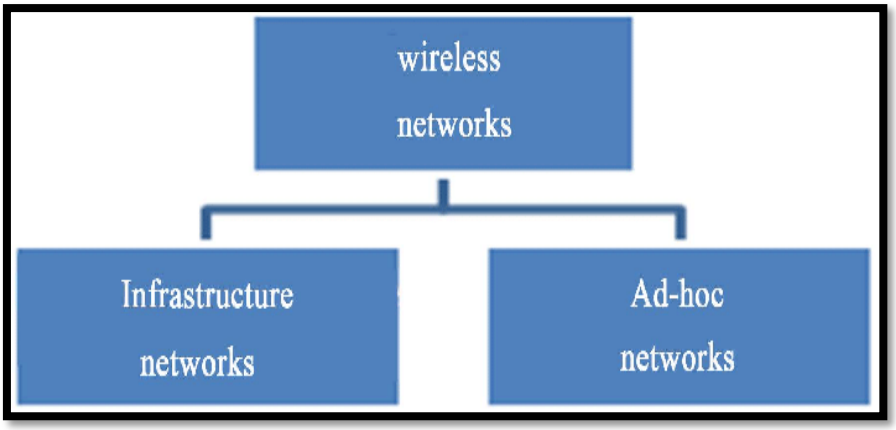

Figure 1.1: Categories of Wireless Networks.

- **With infrastructure:** In infrastructure mode, the communication relies on a fixed third party that is the central infrastructure which consists of wireless access points (APs), and a wired network as shown below.

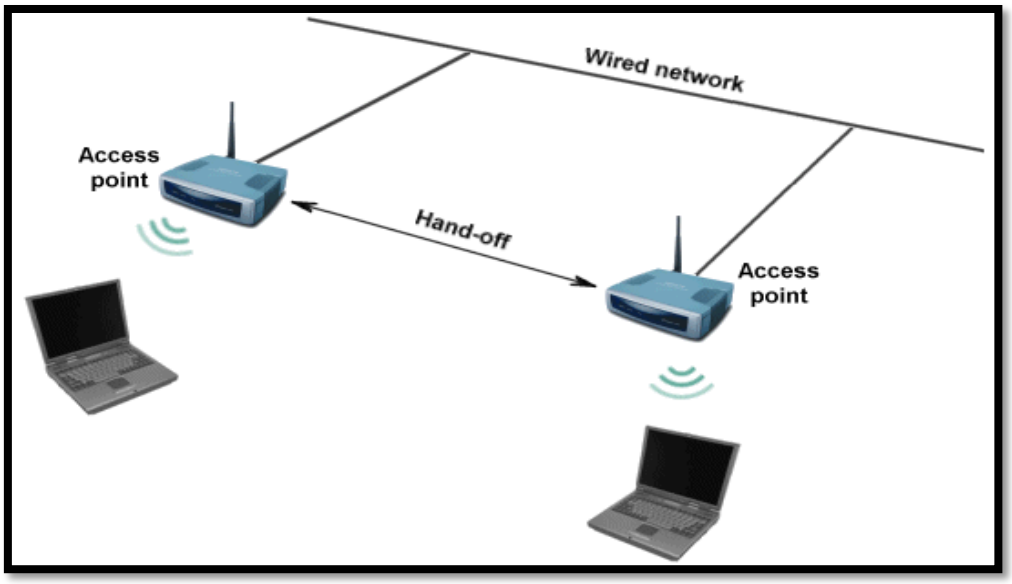

Figure 1.2: Network with Infrastructure

Wireless nodes communicate with each other and with the central infrastructure through wireless access points, each access point act as a central coordinator between all the nodes [1]. Any node can join the network through the AP. The access points manage connections between Basic Set Services and help in establishing routes when needed.

Infrastructure networks can be used in various environments such as homes, offices, and public spaces, they offer convenience and ease of use, however, since all communication goes through

the central infrastructure, the access point manage routing information for all the connected devices, as the network grows bigger, the overhead of maintaining routing problems can become large [2].

- **With no infrastructure:** In contrast to infrastructure networks, infrastructure less networks or Ad hoc Networks operate without relying on any centralized administration. Also known as mobile ad hoc networks (MANET), the communication in these networks is achieved through the cooperation of the hosts within the network [1].

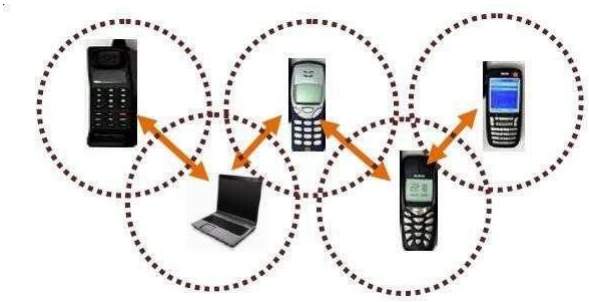

Figure 1.3: Mobile Ad hoc Network

2.2. History of Ad hoc Networks:

Ad hoc networking is a concept that has been in development for many years, it can be traced back to 1972, it was the first generation of ad hoc networks when they were called Packet Radio Network (PRNET) [3], the Defense Advanced Research Project Agency (DARPA) dedicated research using packet-switched radio communication to provide best communication between computers and urbanized PRNET [4].

They were first introduced to improve communication in the military because of their dynamic nature. They first didn't get much attention, however, in early 90's with the development in wireless technologies and arrival of Wi-Fi, Bluetooth, and ZigBee…, ad hoc networks became a very known field of research, so, researchers started to develop algorithms, and protocols for the sake of making ad hoc networks better and performing. Today, ad hoc networks remain an important area of research to develop new protocols, and algorithms, and applications.

2.3. Classification of Ad hoc Networks:

Ad hoc networks encompass three main types: mobile ad hoc networks (MANET), wireless sensor networks (WSN), and wireless mesh networks (WMN). While these networks present shared characteristics and similarities, they differ in other factors such as mobility and energy consumption, responding to different use cases.

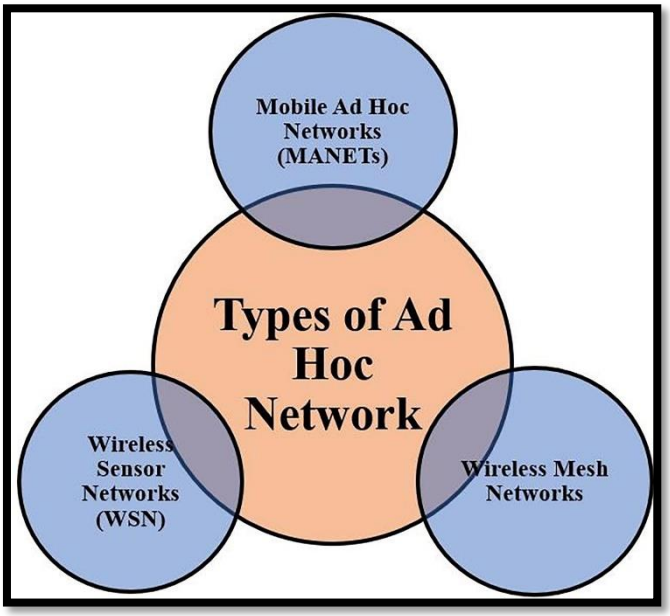

Figure 1.4: Ad hoc Networks types.

- **Mobile Ad hoc Networks (MANET):**

MANET, stands for Mobile Ad hoc Network**,** which is a type of ad hoc network distinguished by the mobility of its nodes. MANET consist of a collection of mobile nodes interconnected wirelessly forming a self-configuring network with no fixed infrastructure [5], each node in this network is allowed to move in a random and unpredictable way resulting in a highly dynamic topology that changes frequently. In such networks, communication occurs through multi-hop paths where packets are forwarded by intermediate nodes. Each and every node in MANET is able to act as both a host and a router which make the transmission of data easier [6].

Mobile ad hoc networks were originally designed as versatile networks, with regards to their real-world implementation and industrial acceptance.[7], The applications of MANET are known and made to be specialized networks made for a known purpose or to solve a specific problem.

This network has given use to many applications in the commercial, military, and private sectors, for example in the military, there are devices that are connected, and ad hoc would allow them to maintain a network to circulate the information between the soldiers or headquarters. This type of network could also be used in rescue operations after natural or man-made disasters, where the network must be established fast enough to allow the rescuers to communicate and coordinate their rescue operations in order to help the people [8].

Other applications or types of MANET exist, such as:

- Vehicular ad hoc network (VANET): they share the same principle as MANET, although the mobility in this network is much higher since it enables the communication between mobile vehicles or the devices contained within to create services that are particularly relevant to such an environment.
- Flying ad hoc networks (FANET): a network composed of aerial vehicles (UAVs), such as drones, that could be used in search operations… etc.

There are also other types of MANET such as IMANET, INVANET…etc. however, with this many applications and more, there are still some design and security issues and challenges to overcome and that's what makes MANET one of the biggest research areas in networking.

- **Wireless Sensor Networks (WSN):**

Wireless Sensor Networks (WSN) are another type of infrastructure-less wireless networks that consist of distributed autonomous networks [9], the primary objective of WSN is monitoring physical or environmental events, such as pressure, temperature, sound and so on.

In WSN numerous sensor nodes are deployed in the area, they have the capacity to collect data which will be transmitted to one base station called the sink node. The sink node acts as a central processing unit to manage, process, and analyze the collected data [10].

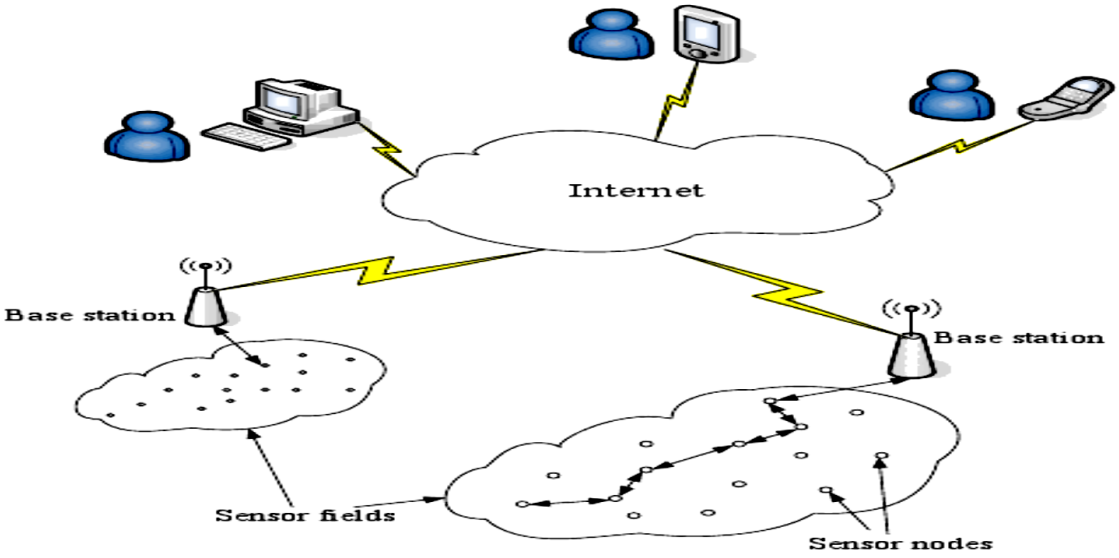

Figure 1.5: Accessing WSN.

The nodes are limited in some aspects like storage capacity, processing speed, and communication bandwidth due to their tiny size, they can be randomly dispersed in a geographical zone called a capture zone. Sensor nodes are typically battery-equipped and energy efficient in order to prolong the lifespan of the nodes, each node is composed with a transducer, transceiver, and a microcomputer, the transducer is responsible for generating electrical signals based on sensed effects, the transceiver receives commands from a central computer and then forwards the data to that computer, and the microcomputer stores the output received from the sensor.

Sensor nodes can operate in either continuous or event-driven modes, allowing wireless sensor devices to be equipped with actuators, so the sensor can act upon certain conditions. These networks are usually specifically referred to as wireless sensor and actuator networks [11].

Wireless sensor networks cover a large variety of applications in different areas, such as environmental monitoring, health monitoring, military applications, and applications in security.

- Environmental monitoring: WSN have the ability to collect data about many environmental parameters in real-time, they can be used to monitor the air quality by measuring carbon monoxide for example, or other pollutants, they can also monitor the weather conditions using parameters such as temperature, humidity, and wind speed, this can help detect potential harmful events such as storms and hurricanes, in general, WSN are very important and have big potential in environmental monitoring that can help detect potential changes and promote sustainability [12].
- Military applications: WSN are very good at providing real-time awareness and detecting potential changes and threats, therefore they are very used in the military, they can be used in battlefield surveillance, and target tracking by collecting data using parameters such as motion, temperature, and pressure and then send it to the command center for decision making [12].
- Security applications: one application of WSN in security, is perimeter security; it can be applied by placing sensors around buildings, borders, or any sensitive areas to detect intruders and unauthorized access, sensors can detect motion, sounds, and other environmental parameters and sends alerts, another potential usage of WSN, public safety where the sensors can monitor traffic state and crowd behavior, and other parameters that could impact public safety [12].

Wireless Sensor Networks offer immense potential across various domains through providing real-time monitoring and sensing capabilities. Their ability in responding to threats and collecting valuable data facilitates proactive measures, and enables informed decision-making.

- **Wireless Mesh Networks (WMN):**

The Wireless Mesh Network (WMN) [13], is a type of network consisting of interconnected radio nodes or small radio transmitters forming a mesh topology where each node is capable of forwarding data to other nodes in the network, creating multiple paths between any two points. The coverage area is sometimes referred to as a mesh cloud [14]. Each node in this network acts as a client and as a router, making the network self-configuring and self-organizing. New nodes are able to join the network automatically, while existing nodes can adjust their routing paths based on the changes occurring in the network.

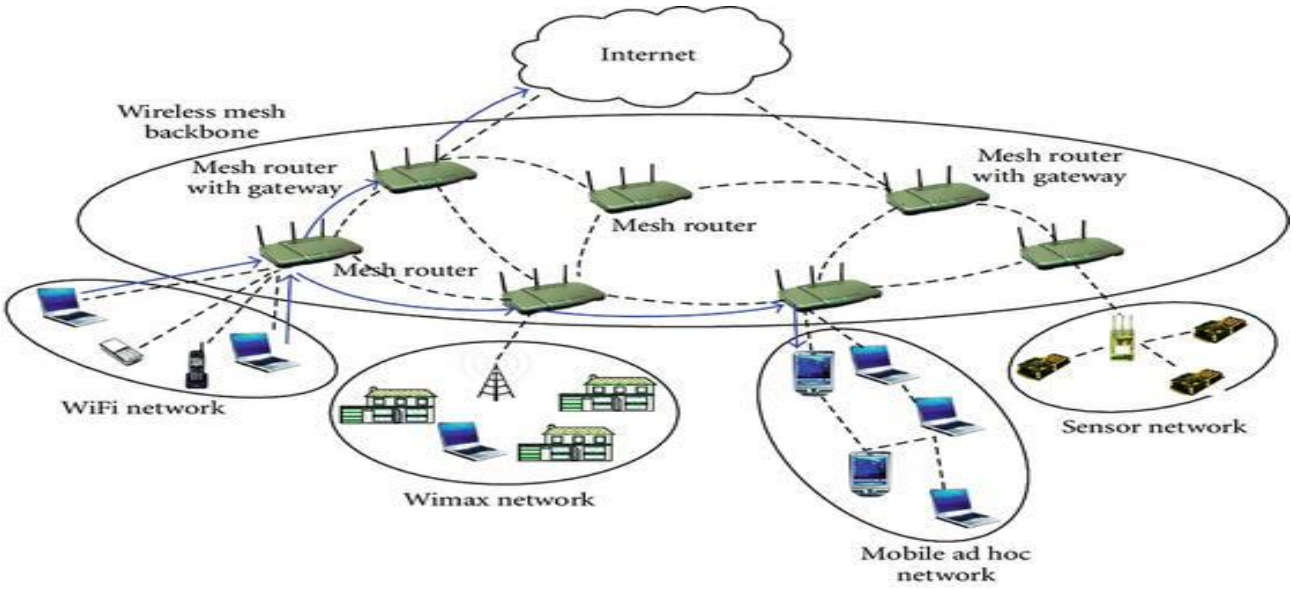

Figure 1.6: Outline of an infrastructure WMN [15]

WMNs are commonly deployed in areas where a wired infrastructure is unavailable or economically impractical. They offer several advantages and different ways of usage, some of the WMNs applications include:

- Public Wi-Fi: WMN are employed to provide Wi-Fi access in public areas like parks, airports, stadiums, and other areas that can be utilized to deploy a mesh network that provides free Wi-Fi to residents and visitors.
- Home automation: utilizing WMN allows devices like security cameras, speakers, and air conditioners to communicate with each other and with a central command, this allows homeowners to control their devices from a distance.

3. Differences between ad hoc network types:

Ad hoc networks share many similarities whether in their characteristics or their applications, but they do differ in some aspects like design and functionality:

- Mobile ad hoc networks, as the name suggests are characterized by their mobility, the nodes in these networks are self-organizing and have a dynamic topology, whereas the topology in WSN is static, and node's locations are pre-defined to monitor specific parameters, WMN are characterized by their mesh topology, with interconnected radio nodes forming a network, where each one of these nodes acting as a router.
- We find a very big difference between nodes capabilities in these networks, in MANET, nodes have much higher processing power, larger memory, and advanced communication interfaces, contrary to nodes in WSN where the main focus is sensing and transmitting data from their

environment, so the nodes are low-power and have limited processing capabilities, nodes in WMNs in the other hand, are close to those in MANETs and have more power than WSNs nodes, enough to handle data routing between nodes and be able to maintain a reliable communication in a dynamic topology.

- In MANET, communication can be established between any nodes of the network, although in WSNs, the communication is always initiated by sink nodes, and communication between sensors is quite rare.

These differences in design, functionality, and communication patterns reflect the specific requirements and objectives of the different ad hoc types, MANET focus on mobility and dynamic communication, WSNs focus on collecting data and sensing, and the WMN leverage the mesh topology for enhanced connectivity.

4. Characteristics of mobile Ad hoc networks:

Mobile ad hoc networks have specific characteristics that distinguish them from other types of ad hoc networks. The key characteristics of MANET include:

- **Distributed operation:** Mobile ad hoc networks are decentralized and do not rely on any infrastructure, the network's control is distributed between the nodes, they cooperate and communicate with each other, and each node work as an intermediary node is needed.
- **Resources limitation:** these networks are usually limited in some aspects, like bandwidth [16], and power, which begs for algorithms and network protocols to be efficient and conserve resources.
- **Limited bandwidth:** one of the main characteristics of wireless networks is that they use radio waves, which makes the bandwidth moderate for hosts [16]
- **Mobility and dynamic topology:** the nodes in the network move freely, and randomly, they can leave the network and others can join, and for that, the network topology can change in a fast and random manner, change in the topology, changes the route between the nodes which causes packet loss.
- **Shared medium:** the wireless communication medium [16] is considered accessible to any entity with appropriate equipment and sufficient resources, as a result, it's impossible to restrict access to the channel.

5. Advantages of mobile ad hoc networks:

Despite their seemingly simple nature in comparison to other network types, Ad hoc networks have emerged as a thriving and one of the most vibrant and active fields as of today [16]. They offer numerous advantages over traditional wireless networks. Some of these advantages include:

- **Flexibility:** Mobile Ad hoc networks are highly flexible and adaptable; they can be deployed on the fly in situations where immediate network connectivity is needed.
- **Decentralization:** Ad hoc networks operate in a decentralized manner, without relying on any administration or infrastructure where each node in the network act as a host and a router.
- **Scalability:** The network size can grow to include more devices when needed, which can be ideal and beneficial in situations where network size can vary significantly.
- **Mobility support:** Mobile Ad hoc networks are highly dynamic by nature, and are designed to accommodate mobile nodes, the network can efficiently support the nodes movement allowing seamless communication as nodes are moving.
- **Cost effectiveness:** MANET are cost-effective in comparison to traditional wireless networks, since they do not require any infrastructure or administration, the costs associated with the deployment of the network and the maintenance are significantly reduced.
- **Increased coverage:** MANET can provide a wider network coverage through the multi-hop communication, where intermediary nodes act as relays allowing data to be transmitted across many nodes and reaching other nodes that may be far.

In summary, they offer many advantages that have contributed to the growing popularity and widespread adoption of mobile ad hoc networks in different fields.

6. Challenges in mobile ad hoc networks:

Despite the advantages and potential of mobile ad hoc networks, they also face many challenges and obstacles that researchers focus on to develop these networks. Some of the key challenges faced by MANET include:

- ***Limited bandwidth*** **[16]:** one of the difficulties of MANET is that the wireless link continues to be weaker in capacity compared to infrastructure networks, in MANET, the communication is made through a shared communication medium, which basically means that network nodes share the bandwidth available, also, nodes in this network, usually have limited transmission range, which means packets would be sent through intermediary nodes to reach their destination, this could result in packet overhead and therefore reduces the available bandwidth.
- ***Routing overhead*****:** due to the mobility of the nodes, frequent links get broken, and some outdated routes are produced in the routing table which leads to unnecessary routing overhead. [17, 1]
- ***The hidden terminal problem*** [16]: this issue is a common occurrence in mobile ad hoc networks, when two nodes cannot detect each other's presence because of the presence of other nodes in the network, for example when nodes A and B, are within range of a common

node C, but they are not in each other's transmission range. This can cause a collision when both A and B send data at the same time which eventually results in data loss and reduce network performance.

- ***Packet losses:*** the presence of interferences, frequent paths break that can be caused by the mobility of the nodes, and collisions, are known factors that result in bad network performance and packet loss.
- ***Battery problems:*** devices in MANET are usually small and lightweight, and to maintain that, they have limitations in power source.
- ***Quality of service*** [1, 18]: QoS, is an important area in MANET, it is the ability to offer a certain level of service quality, it is also a very challenging aspect due to the dynamic nature of the network's topology, and limitations, however, there are several techniques that could improve QoS in MANET, such as traffic engineering, and QoS aware protocols.
- ***Security problems*****:** mobile ad hoc networks have many security concerns, this network is vulnerable to some threats such as eavesdropping or data interception, spoofing, and denial of service (DOS) attacks which is justified by its limitations like the weak processing power and battery life that makes it hard to secure the network.

7. Conclusion:

In this chapter, we provided an introduction to wireless networks and focused on the concept of ad hoc networks. We discussed about the history of ad hoc networks as well as their evolution with time, highlighting their characteristics and advantages over traditional wireless networks, and their various applications they offer.

Additionally, we acknowledged the challenges faced by MANET, such as routing, security, and quality of service. Looking ahead, the next chapter, we will jump deeper into the domain of routing in MANETs, being a critical aspect in ensuring efficient communication. We will explore the different routing protocols that exist in mobile ad hoc networks.

Chapter 2:
Routing protocols in Ad hoc Networks

1 Introduction:

Routing in Mobile Ad hoc Networks (MANET) is a significant and huge research field focused on enabling the transmission of data among nodes in a network with no infrastructure. MANET present many challenges due to the dynamic and constant changes in the network topology caused by the movement of nodes and the constant breaking and making of links, which makes it necessary to develop efficient and adaptive routing protocols that can adjust to the network's nature and maintain connectivity among the nodes.

The general purpose of routing is to find the optimal path to send data from a source node to a destination node while ensuring a reliable delivery, and minimal network overhead, and selecting the best route based on different parameters such as shortest path, least congested path, and available bandwidth.

In this chapter we will delve deeper into the field of routing protocols in Mobile Ad hoc Networks (MANET). We will explore the different types of routing protocols in MANET, their mechanisms and way of functioning, strengths and limitations. Additionally, we will analyze the advantages and disadvantages of each routing protocol type, and how they compare to each other.

2. Definition:

In order for communication to be established between the nodes within their transmission zones, or out of it through intermediary nodes (multi-hop). The activity to make that possible is 'Routing', so what is routing? And what are routing protocols?

Routing is a method or a process of selecting paths through which, information is transmitted from the source node to a specific destination node. Routing protocols are a set of rules and algorithms used by nodes in the network, consist of ensuring a strategy that always guarantees the establishment of optimal and efficient routes between any pair of nodes within the same network.

Routing protocols are selected based on the requirements of the application and the network's characteristics. Efficient routing protocols are a must for ensuring reliability and efficiency in the connectivity of the network.

3. Routing protocols classification:

Routing protocols in ad hoc networks play a crucial role in establishing efficient communication among mobile devices without the need for a fixed infrastructure or centralized control. Ad hoc networks are characterized by their dynamic and self-organizing nature, where nodes cooperatively form a temporary network on the fly. Given the unique challenges of ad hoc networks, routing protocols designed for such environments are classified into various categories based on their characteristics and methodologies [19].

As of today, routing protocols have been developed, and MANET routing protocols can be divided into three categories: Proactive, Reactive, and hybrid routing protocols [20] as shown in figure 2.1.

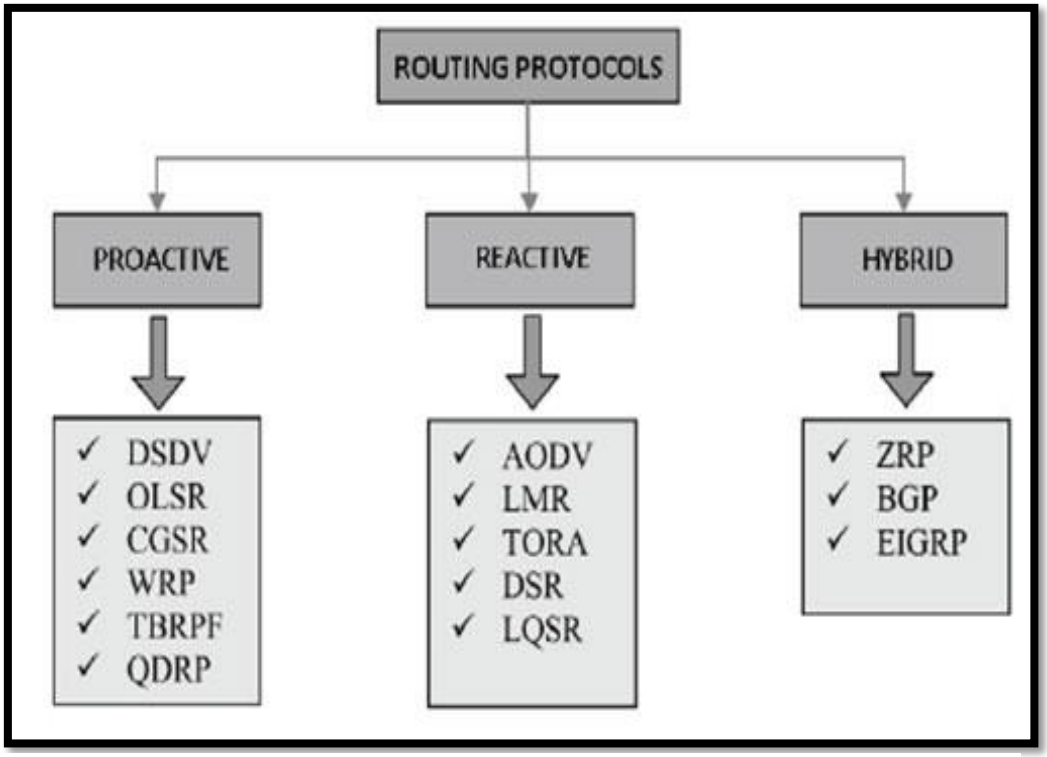

Figure. 2.1: Types of Routing Protocols.

3.1. Proactive routing protocols:

Proactive and also known as table-driven routing protocols [21], they are characterized by the fact that each node must maintain one or several routing tables by constantly exchanging routing information between nodes. Each node maintains a routing table that carry information about paths to all other destination nodes. Whenever there's a change in the network's topology, the information is updated [20]. These types of protocols are known for using link-state routing algorithms that typically flood the link data about their neighbors.

One downside of proactive routing protocols is the increased control overhead [22]. Since these protocols maintain and update routing information even when there is no active transmission, such as OLSR (Optimized Link-State Routing) [23], and DSDV (Destination-Sequenced Demand Vector) [24].

Table-driven routing protocols have the advantage to provide instant access to routing information or in other words, the routing table is always up to date, and also, they have the ability to provide reliable and consistent routing.

3.1.1. Destination-Sequenced Distance-Vector (DSDV):

DSDV falls into the category of proactive routing protocol based on the Bellman-Ford algorithm [24] to calculate routes, in other words, the number of hops it takes for the packets to get to the destination node. This algorithm contributed mainly in solving the routing loop problem.

DSDV uses sequence numbers, each node in the network keeps a routing table that has a sequence number and the distance to reach all other destinations stored. The sequence numbers are even in general if there's a link, else an odd number is used. The destination generates the number and the sender has to send the next update with this number, old entries are easier to be identified and thus avoid rooting loops. [25]

data packets are transmitted with the use of these routing tables and since the network's topology is unpredictable and changes happen quite often, there is a need to maintain consistency and reliability in the routing table, and in order for that to happen nodes exchange routing updates periodically, routing information will be advertised and update packets will be broadcasted for routing table updates.

Update packets are sent to directly connected nodes with their hop count being equal to one [24], the routing table of the neighbors is updated by an increase in the hop count by one, and then these packets will be retransmitted to their neighbor nodes and this will be received by all nodes in the network, if incase, multiple updates are received , the packet with the highest sequence number is used, and if they have the same sequence number, the packet who travelled the least hops will be chosen. If a route is about to change, the transmission of the update packet for the concerned node will be on hold until optimal route is found.

In the DSDV routing protocol, two main types of updates are employed. The first one is a more frequent update known as a "full dump." The full dump update involves advertising the entire routing table information to neighboring nodes [26,27]. The second update is called an "incremental update," [27] which is used more often when the network is stable. Incremental updates are used to disseminate newly changed routing information. Full dump updates are transmitted periodically and

are less utilized in networks with low mobility. On the other hand, incremental updates are transmitted in between full dump updates to communicate the changed routing information. While full dump updates may require multiple Network Protocol Data Units (NPDUs), incremental updates in the other hand consist of small packets that can be sent within a single NPDU [28].

3.1.1.1. Route maintenance in DSDV routing protocol:

Considering the constantly changing topology of ad hoc networks, it is common for routes to fail or links to break when nodes change their positions. In the DSDV routing protocol, when a route failure is detected, the hop count for the broken link is set to infinity [26]. This triggers the node to immediately send update packets to its neighboring nodes, informing them about the new change in the network. Consequently, the neighboring nodes update their routing tables accordingly, eliminating the broken link from their routing paths.

If the node responsible for the broken link rejoins the network, it broadcasts an update packet with a higher sequence number and a specific hop count. This update is then advertised throughout the entire network, informing all nodes that the previously broken link is now usable again. By receiving this update, nodes update their routing tables and restore the route through the revived link.

3.1.1.2. DSDV advantages:

- DSDV utilizes sequence numbers for routing updates which allows nodes to distinguish between newer and older entries, this helps reducing rooting loops and enhances stability in the network [29].
- DSDV is based on the traditional distance-vector routing algorithm, making it compatible with existing routing protocols and infrastructure.

3.1.1.3. DSDV disadvantages:

- DSDV routing protocol updates its routing tables regularly, which requires a large amount of bandwidth to constantly exchange updates between nodes. [26]
- New sequence numbers are necessary whenever there is a change in the network topology, which make DSDV less suitable for highly dynamic networks [26]

3.1.2. Optimized Link-State Routing (OLSR):

Optimized Link-State Routing (OLSR) [23], is a proactive routing protocol that provides immediate availability of routes when needed. OLSR is the optimized version of the link-state protocol [23], meaning that changes in topology trigger the flooding of topological information to all available hosts in the network. To reduce possible network overhead, OSLR employs the concept of

Multipoint Relays (MPRs). MPRs are used to reduce flooding of broadcasts by decreasing the broadcast in other regions of the network.

The figure above (fig. 2.2), (a) shows simple flooding, where the central node C sends packets, and every node that receives it will broadcast it again with the double arrow between two nodes means that they broadcast to each other, in (b), we can see that flooding through multipoint relays (black nodes), has reduced the number of packets as one-hop neighbors that are not MPRs will not broadcast.

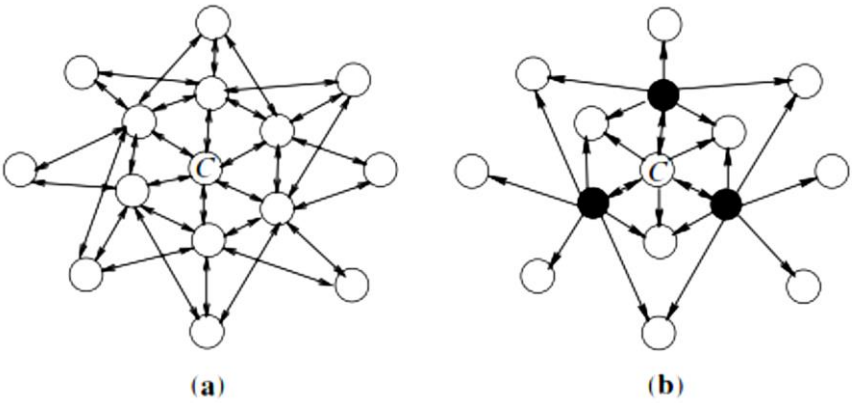

Figure 2.2: Demonstration of simple flooding and flooding through multipoint relays. [30]

In addition to that, OLSR aims to provide the shortest path between nodes, reducing the time interval for control message transmission enhances the protocol in terms of reactivity to changes in the topology.

OLSR uses two types of control messages: Hello, and Topology Control (TC) [23]; Hello messages serve the purpose of obtaining information about the link status and the neighboring nodes, these messages are only sent to neighboring hosts that are within one hop. Using the hello message. OLSR constructs the Multipoint relay (MPR) selector set which describes the chosen hosts to act as MPR, starting from this information, the host can calculate its own set of MPRs. However, TC messages are diffused in all parts of the network, and can only be forwarded by MPRs. TC messages serve the purpose of broadcasting information about the host's advertised neighbors, which includes the MPR selector lists. [31]

In addition to that, OLSR also uses Multiple Interface Declaration (MID) messages [23], which inform the other hosts that the advertising host could have more than one OLSR interface address. These messages are ought to be broadcasted throughout the network by the MPR. Adding to that, Host and Network Association (HNA) messages give the possibility of routing to external addresses by giving external routing information. The HNA message provides network and netmask addresses, enabling the OLSR host to treat the advertising host as a gateway to the announcing set of addresses. The HNA message serves as a more general version of the TC message, the only difference

is that the TC message can notify about the cancellation of the route whereas HNA message information will only be deleted after the expiration time [23].

3.1.2.1. Routing in OLSR:

- Multipoint Relays (MPRs):

MPRs are basically selected nodes from one hop-away neighbor in the OLSR routing protocol, it is used mainly to decrease the number of unnecessary transmissions and thus reduce the information exchange overhead or the overall network traffic. In order for the protocol to be efficient, the MPR set of hosts must be kept small. In OLSR data can only be forwarded by MPRs [32]. Each host in the network selects a set of MPRs, and in order to calculate the optimal set of MPRs, each one of these hosts should acquire information about one-hop and two-hops neighbors. This process is done through the exchange of Hello messages. Which are sent periodically to the neighboring nodes, also, each host can calculate its Multipoint Relay selector set, which the set of chosen nodes.

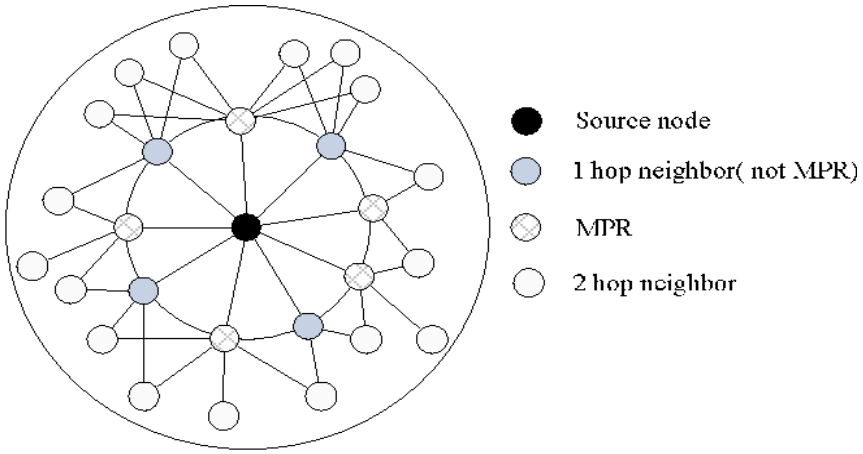

Figure 2.3 : Multipoint relays in OLSR

The MPR selector set is sent in TC messages, they are diffused periodically, so in case of any changes in topology, the network is informed. The TC messages contain a list of all nodes that have selected the sending node as their MPR, and the MPR selector set of these nodes. Only the MPRs are allowed to send TC messages, therefore, the number of broadcast messages needed to diffuse information about topology is reduced.

This whole process makes OLSR able to achieve a balance between the overhead and the need to keep up-to-date topology information.

3.1.2.2. Topology information:

To gather topological information, the selected Hosts to act as MPR have to send TC messages periodically throughout the network. The purpose of this mechanism is for the host to advertise its own links in the network, at least the host's MPR selector set links must be sent.

3.1.2.3. Neighbor detection in OLSR:

Each node periodically diffuses its HELLO messages for neighbor sensing [33], these messages are broadcasted only one hop away and gives each node knowledge about its neighbors.

The hello messages contain information about the quality of links to the node's neighbor and also the node's identity.

3.1.2.4. Multipoint Relay selection:

MPR selection is based on a distributed algorithm. The algorithm consists of nodes exchanging Hello messages which gives information to the host about one and two-hop symmetric neighbors. The neighbors that have the willingness to act as MPR which have a status that differs from WILL_NEVER in the Hello message, have the potential to be chosen as MPR.

3.1.2.5. Routing table calculation:

The routing table in the Optimized Link State Routing protocol is maintained by each host and contains information about available links. The information in the routing table entries includes; Destination address, next address, number of hops to destination, and local interface address [23] this information as we said previously, is obtained through the TC messages and Hello messages (topological set, and local link information base). Whenever changes happen in these sets, the routing table is recalculated. Since it's a proactive protocol, routes should be kept for all the available hosts in the network.

In case of any changes such as the appearance or disappearance of new neighbor links, or the creation or removal of two-hop neighbors, the routing table is changed.

In summary, the routing table calculation in OLSR begins with each node broadcasting a Hello message to inform other neighbors about its presence and gather information about the link state, after receiving the Hello message, each node maintains information regarding 1-hop neighbors, then, each node inform other nodes of its 1-hop neighbors and the quality of their links, this process is done through broadcasting Topology Control (TC) messages, the TC messages are sent periodically, and from the received TC messages, nodes can determine the shortest path to all other nodes in the network, using that, the next hop address for each destination can be calculated and update the routing table accordingly.

3.1.2.6. Advantages and drawbacks of OLSR routing protocol:

- The proactive nature of the OLSR routing protocol means that it maintains routing information of all nodes in the network, and has the ability to distribute this information across all the nodes which gives the nodes possession of complete routing information.

- OLSR uses Multipoint relays which reduce the number of broadcast messages which makes routing more efficient making it suitable for dense networks. however, as a disadvantage, this protocol needs each host to send periodic topology information updates which potentially increases the usage of bandwidth.
- As a drawback, OLSR is a more complex routing protocol which can potentially be difficult to implement and troubleshoot.

3.2. Reactive routing protocols:

Unlike Proactive routing protocols, Reactive routing protocols discover routes only when they are needed or requested. Reactive routing protocols, which are also known as on-demand routing protocols [34], never maintain routing information for every node in the network. The fact that these protocols only discover routes when it's necessary, makes them more scalable than proactive protocols, therefore, more suitable for larger networks.

When a node wants to send a packet to any destination, it starts a route discovery to find a path to the destination. The first procedure is called route discovery; route discovery is initiated by the source node in which the source node broadcast a route request message to its neighbor and this request is to be forwarded again and so on until the message reaches a node that has a valid route to the destination node. Every node that receives the route request messages stores the address of the node that sent it in order to send back a route reply message.[35]

When the route request reaches a node with a valid route, it sends back a route reply message to the source node, route reply message contains route information from the destination node to the source node and that's what allows the source node to send packets to destination using the discovered route.

Another mechanism in reactive routing protocols is called "route caching", it is typically used to prevent routing loops, and the concept is when a node receives a route reply it cashes the information regarding the route in its routing table so the route can be used again if needed.

Reactive routing protocols tend to be vulnerable to route failures, in case of breaking of routes or the need to find new routes, the process of route maintenance comes in handy. This process is responsible for monitoring the route and notifying the sender of any case of errors regarding the route. There are many known examples of widely used reactive routing protocols such as AODV, DSR, and many more protocols.

3.2.1. Dynamic Source Routing (DSR):

Initially designed for MANET, Dynamic Source Routing protocol (DSR) [36], is an on-demand routing protocol, mainly, this protocol was put to work to reduce the wasted bandwidth by

reducing the number of control packets broadcasted for example, or stopping the continuous updates of the routing table. Since it's a reactive routing protocol, in DSR, routes are discovered on request, it relies on two main mechanisms; route discovery, and route maintenance.

3.1.1.1. Route discovery in DSR:

When the source node sends a new packet to the destination node, it includes a source route in the packet header specifying the sequence of hops that should be followed to destination. If the sender node has previously discovered a suitable route, it will be retrieved from its route cache, however, if there's no route in the cache, the route discovery will be initiated to find a path from the source node to the destination node.

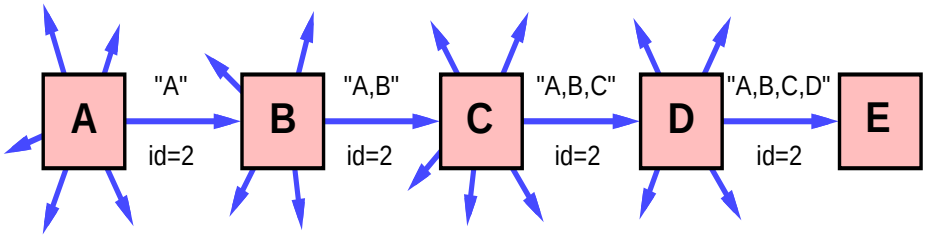

Figure 2.4: Route discovery in DSR: Node A is the source; node E is the destination. [37]

Figure 2.4, shows an example of a route discovery in DSR in which the source node A transmitting a route request message as a single local broadcast message in order to discover a route to the destination node E, this message is received by most nodes in transmission range of A.

Route discovery is started by sending a ROUTE REQUEST message as a single local broadcast packet. This message includes the initiator's and target's identification, along with a unique request ID generated by the initiator. The message is then disseminated to all nodes within the transmission range of the initiator node.

If a node, acting as the target, receives a ROUTE REQUEST message, it responds by sending a ROUTE REPLY message back to the originator. Upon receiving the ROUTE REPLY message, the originator stores it in its Route Cache for future use. However, if the receiver of the ROUTE REQUEST message has already encountered another message with the same request ID, the ROUTE REQUEST is discarded. Otherwise, the node appends its own address to the record, stores it in the ROUTE REQUEST message, and continues transmitting it as a local broadcast packet until it reaches the destination.

When receiving the ROUTE REQUEST message, the destination node would want to reply, thus, it will send a ROUTE REPLY message. The destination node will first check if there's any cached route back to the initiator in its own Route Cache and will use it if found. However, if no cached route is found, the node sending the route reply will perform its own route discovery or

instead, the ROUTE REPLY message is sent back along the reverse path followed by ROUTE REQUEST message, each node in the reverse path appends its own address to the route record and then it forwards the message, when the ROUTE REPLY message reaches the initiator; the source route is complete and will be used to forward data packets.

When a sending node starts a route discovery, it saves the packet that set off the discovery in a buffer called the "send buffer", this buffer contains copies of packets that couldn't have been transmitted by this node because of the source route to destination not being available at the time.

While the packet remains in the Send Buffer, the node should occasionally start new route discovery for the destination address of the packet, but it should be limited in case of the destination would be simply out of reach, and in a similar network state and due the limited wireless transmission range and the mobility of the nodes the network might become partitioned, and for a node in such network, if a new route discovery was started for each packet a large of unnecessary and unproductive routes will be broadcasted. To reduce the overhead from similar route discoveries, a node should use an exponential back-off algorithm. [36,37,38]

In addition to what has been said previously, the DSR routing protocol incorporates additional route discovery features, such as caching overheard routing information, and route request Hop Limits.

3.2.1.2. Caching overheard routing information:

In DSR, nodes can learn about new routes by overhearing routing information from other nodes. A node overhearing any packet should extract usable route information from it and store it in its own Route Cache. [37,38]

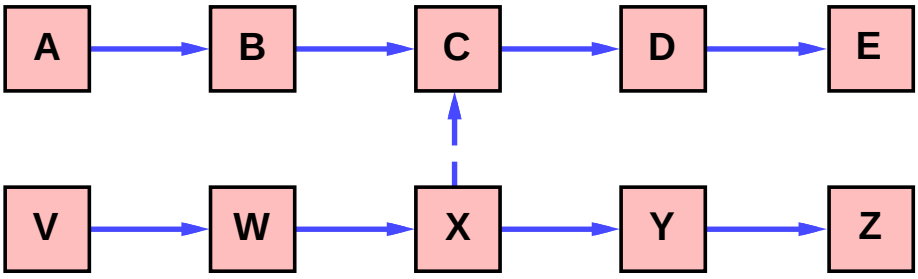

Figure.2.5: Caching overheard routing info**:** Node C overhearing packets from X while C is transmitting to E. [37]

3.1.1.3. Route request hop limits:

In DSR, the route request hop limit is a mechanism with the purpose of preventing flooding of route requests, each ROUTE REQUEST message contains a "hop limit" that could be used to limit the number of allowed nodes to send a copy of that route request or in other words, it specifies the maximum number of hops a route request can travel before it is discarded by a node.

3.2.1.4. Route maintenance in DSR:

When using a source node in packet transmission, each transmitting node ensures that the packet is received by the subsequent node along the route. The packet is retransmitted multiple times until a confirmation receipt is received from the following node.

If the transmission to a node along the path fails, or the link breaks and no confirmation receipt is received, the sender should receive a notification about the failure, this is done through the Route Error message (RERR).and this message will be sent to the originator. For example, let's say node A wants to transmit a packet to node E, so, node A will be responsible of confirmation of receipt at B, and B will be responsible for confirmation at C, and so on. If, for example, C is unable to deliver the packet to the next hop D, C will send a Route Error message stating the fact that the link from C to D is currently broken. Once the originator receives the RERR message, it will remove the failed link from its route cache and then it will either check the Route Cache for another route to the destination or perform another route discovery.[37]

In addition to that, DSR contains many more features for maintaining the routes, and these features include:

- **Packet salvaging:**

Packet salvaging is a useful feature is DSR that helps in routes failures [39]. When a node detects a link failure to the next hop in packet transmission and if the node has possession of another route to the packet's destination in its route cache, this node salvage the packet instead of discarding it, the node in this case searches its own Route Cache for a route from its address to the destination of the packet, and if it finds a route, the node then replaces the original source route by the replacement route and then forwards it to the next hop while indicating that the packet has been salvaged to prevent multiple salvaging of the same packet to stay away from a routing loop.

- **Automatic route shortening:**

Automatic route shortening is designed for performance optimization in the DSR routing protocol [39], if one or more intermediate nodes are no longer necessary, source route could be shortened. If a node overhears a packet carrying a source route, it will check the not yet consumed portion of that route, if the node is not the intended next hop and is named in the remaining portion of the route, it can conclude that the intermediate nodes before itself are not necessary.

Despite the many features that the DSR routing protocol has, DSR's route maintenance mechanism does not locally repair link breakage or link failures, which can cause higher delays in

comparison with table-driven protocols. However, the reactive approach in DSR doesn't need to flood the network with table update messages.

3.2.1.5. Advantages and drawbacks of DSR:

DSR has several advantages, as well as drawbacks. One of the key advantages of Dynamic Source Routing is that it does not require periodic updates or maintenance of routing tables, which concludes in reducing the overhead of routing information exchange, also DSR offers efficient route caching, which can be utilized for subsequent transmissions to the same destination, route caching results in lower latency and an improved network performance.

However, DSR does have some drawbacks. One significant drawback is the increased size of packet headers due to the inclusion of the complete route information. This can lead to higher overhead and reduced network throughput, especially in scenarios with limited bandwidth. [40,41]

Furthermore, DSR is vulnerable to node mobility and network scalability. Frequent node movements can lead to route disruptions and the need for frequent route discoveries. Additionally, as the network size grows, the overhead associated with route discovery and maintenance increases, potentially impacting the overall scalability of the protocol.[41]

3.2.2. Ad hoc On-Demand Distance Vector (AODV):

AODV (Ad hoc On-Demand Distance Vector) [42] is a reactive routing protocol specifically developed for Mobile Ad hoc Networks (MANET). AODV has the ability to rapidly establish routes without requiring continuous route maintenance for nodes that are not actively communicating. Routes in AODV are created and maintained on-demand, minimizing the overhead associated with route management.

The primary objective of AODV is to cater to the requirements of highly mobile networks characterized by frequent changes in network topology. To achieve this, AODV incorporates various mechanisms that enable nodes to promptly respond to link failures and topology changes, ensuring efficient and reliable routing. Unlike some other protocols, AODV prioritizes timely adaptability, facilitating dynamic route repairs and the exploration of alternate routes when necessary.

Similar to the Dynamic Source Routing (DSR) protocol, AODV comprises two core components: route discovery and route maintenance. The route discovery process is triggered when a node requires a route to a specific destination, utilizing broadcasting of route request messages to identify a suitable path. The route maintenance component monitors the connectivity of established routes and facilitates repairs or updates as needed.

3.2.2.1. Route discovery in AODV:

In the AODV routing protocol, the process of route discovery is initiated by the source node through the broadcast of a Route Request packet (RREQ) to its neighboring nodes. The RREQ packet contains the requested destination sequence number, which serves as a means to differentiate between fresh and stale routes and avoid potential looping issues. when the packet reaches the destination, it replies with Route Reply. Route reply messages (RREP) are only generated by the destination or hosts who are in possession of information regarding the destination host being connected. [31]

This process of route discovery in AODV allows nodes to dynamically and efficiently establish routes in response to communication requirements. By broadcasting RREQ packets and receiving RREP packets, nodes can collaboratively build and maintain routes within the network, ensuring effective communication between source and destination nodes. [41,42]

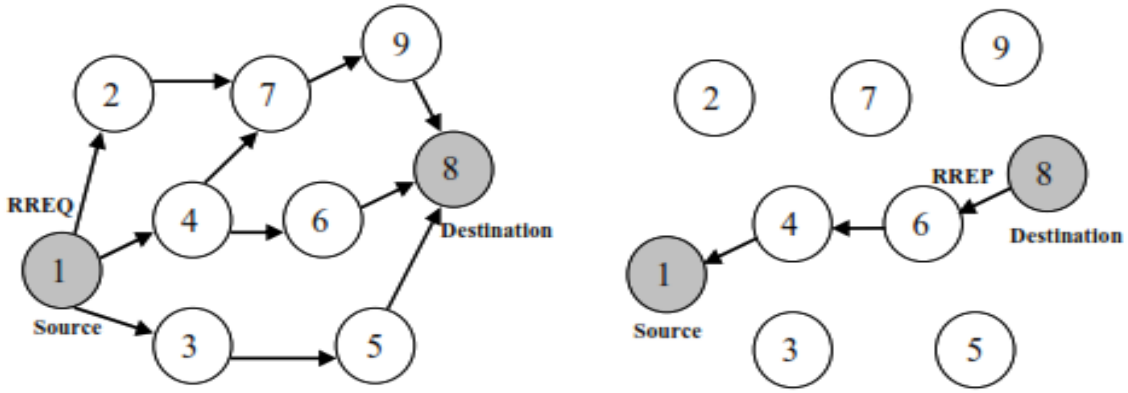

Figure 2.6: Process of route discovery in AODV [43]

3.2.2.2. Sequence numbers in AODV:

Sequence numbers in AODV are crucial for maintaining the integrity and freshness of routing information in the network. Each originating node in AODV maintains its own sequence numbers, which serve multiple purposes to enhance the routing protocol's performance. Can be used to prevent the routing protocol from loop problems by getting rid of invaluable old information or routes, or it is used by other nodes to determine the freshness of routes for example. [43]

The destination sequence numbers can be updated in the routing table when the host receives a message with a greater sequence number which gives the information that this message is the new fresh one. The sequence number can be changed in case of link failure or if the host is proposing a new route to itself.

3.2.2.3. Generating Route Requests (RREQs), and Route Replies (RREPs):

When a node has no valid route and needs a route to destination, it broadcasts a route request message throughout the network, this message will include the last known destination sequence number, along with the source sequence number, RREQ ID, and the hop count will be set to zero.

Type = 1	J	R	G	D	U	Reserved	Hop count
RREQ ID							
IP Address of the destination							
Destination Sequence number							
Source IP Address							
Source sequence number							

Table 2.1: RREQ message format. [42]

- **Type**: 1
- **J**: Join flag; reserved for multicast
- **R**: Repair flag; reserved for multicast
- **G**: Gratuitous RREP flag; indicates whether a gratuitous RREP should be unicast to the node specified in the Destination IP Address field.
- **D**: Destination only flag; indicates only the destination may respond to this RREQ.
- **U**: Unknown sequence number; indicates the destination sequence number is unknown.
- **Reserved**: Sent as 0; ignored on reception.
- **Hop count**: The number of hops from the originator IP address to the node handling the request.

In addition, there's a limit of how much a source node can generate RREQ messages per second, before trying to retransmitting RREQ message for route discovery, the node must wait for an RREP message or any control message regarding route information, if such message is not received, the node may broadcast another RREQ message up to a limited number of times, after each retry the request ID is updated. The data packets are buffered beforehand, after reaching maximum attempts of route discovery with no RREP message received, the data that was supposed to be sent to that destination will be dropped from the buffer. to prevent unnecessary spreading of RREQ messages, AODV uses the expanding ring search technique.

After a node receives an RREQ message, that node will compare the sequence number of the destination in its own table to the sequence number in the recently received RREQ message, if that

node has a route with a sequence number that is equal or greater than the one in the RREQ it will be able to generate a route reply message and unicast it to the node it received the RREQ from.

The RREP will then travel through the reverse path, and is generated only by a node if it is the destination or if it is an intermediate node that has a valid route to destination (a greater sequence number than in the RREQ received), when the RREP message is created, it is unicasted to the next hop in the reverse path (towards the originator), while the RREP is traveling, the hop count is incremented by one every hop, and the number of hops will be the distance.[31,41,42]

Type = 2	R	A	Reserved	Prefix size	Hop count
IP address of destination					
Sequence number of destination					
Source IP address					
Lifetime					

Table 2.2: RREP message format. [42]

- **Type**: 2
- **R**: Repair flag; reserved for multicast
- **Reserved**: Sent as 0; ignored on reception.
- **Hop count**: The number of hops from the originator IP address to the node handling the request.
- **Size of prefix**: if not 0, the 5-bit prefix size specifies that the indicated next hop may be used for any nodes with the same routing prefix as the requested destination.

  - Lifetime: route validity time, measured in milliseconds, determines the duration for which nodes that receive RREP consider the route to be valid.

3.2.2.4. Route maintenance in AODV:

Outdated routes and breakage of links happens often, and in AODV, when a node detects any link failure, it will mark the route as invalid in the routing table and try to determine which neighbors can be affected by the breakage of link. The host must send a route error message (RERR), this message can be unicasted if one neighbor is in need of that message, or broadcasted if multiple nodes are affected. [31,42]

Before sending the RERR message, the destination sequence numbers for the unreachable destination must be incremented or copied in some cases, and the unreachable destination entry will

be marked as invalid and the lifetime is updated. When the source nodes are informed of the broken link, it can start a new route discovery if a route to destination is still in need, if the node has recently sent packets to destination, it will try to locally repair the failure instead of initiating the discovery process.

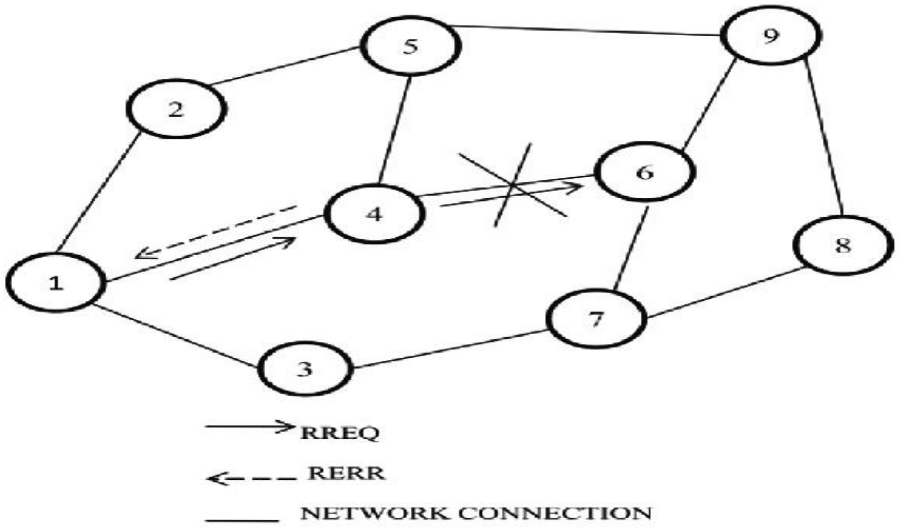

Figure 2.7: Illustration of route maintenance in AODV [44]

3.2.2.5. Route repairing in AODV:

AODV employs a local repair mechanism to handle disruption that is caused by link failures, to do so, the destination sequence number is increased to one higher than in the failed route entry and is sent through a Route Request to the host.

The node trying the repair will wait for RREP message in response to its RREQ message, if no RREP is received, the route entry will be set as invalid, if the opposite happens an it receives the RREP message it will compare the hop count, if the hop count of the new route is greater than the one in the previous route, the node then send an RERR message for the destination with the 'N' bit set up which means that the route should not be deleted and that it has been locally repaired.

Type =3	N	Reserved	DestCount
IP address of the unreachable destination			
Sequence number of the unreachable destination			
Additional unreachable destination IP address if needed			
Additional unreachable destination sequence number if needed			

Table 2.3: RRER message format. [42]

- **Type:** 3
- **N:** No delete flag; set when a node has performed a local repair of a link, and upstream node should not delete the route.
- **DestCount:** The number of unreachable destinations included in the message; must be 1 at least.
- **Unreachable destination sequence number and IP address:** the destination sequence number and IP address of the destination that became unreachable due to link failure.

3.2.2.6. Hello messages:

Hello messages in the AODV routing protocol serve as a means for nodes to maintain connectivity [45], even though AODV is a reactive routing protocol. These messages are periodically broadcasted to neighboring nodes, providing information about the liveliness of the route. It's important to note that Hello messages have a Time-to-Live (TTL) value of 1, which means they are not forwarded beyond the immediate neighbors.

When a node receives a Hello message, it updates the lifetime of the node information associated with that neighbor. If a node stops receiving Hello messages from a particular neighbor for a specified duration, the link to that neighbor is considered lost.

It's worth mentioning that the routes used exclusively for transmitting Hello messages are independent of other routes established in the network. Therefore, if a link failure occurs within these Hello routes, it does not trigger the generation of route error messages.[42]

3.2.2.7. Advantages and disadvantages of AODV routing protocol:

The Ad hoc On-Demand Distance Vector (AODV) routing protocol offers several advantages in the context of mobile ad hoc networks (MANETs):

AODV enables fast route discovery when a source node needs to communicate with a destination node. It establishes routes on-demand, avoiding the need for maintaining routes to inactive destinations. This efficiency is especially beneficial in dynamic and rapidly changing network topologies, Also Unlike proactive routing protocols (e.g., DSDV), AODV operates reactively, establishing routes only when needed. This reduces control message overhead and conserves network resources. AODV also performs route maintenance by monitoring link liveliness through Hello messages. This helps detect link failures and enables timely route repairs or route rediscovery. However, being a reactive routing protocol reducing the overhead and discovering routes only when it’s needed can come at the cost of increased latency and delay.[41]

3.3. Hybrid routing protocols:

Hybrid routing protocols offer a combination of both reactive and proactive approaches to routing, leveraging the benefits of both. By combining these two approaches, hybrid routing protocols optimize routing efficiency and adaptability in networks with varying characteristics. They provide the advantages of proactive protocols in stable regions and the benefits of reactive protocols in dynamic regions. This flexibility allows the protocol to adapt to the specific requirements of different areas within the network.[46]

Examples of hybrid routing protocols include the Zone Routing Protocol (ZRP), which defines a proactive zone surrounded by a reactive zone, ZHLS, and many more.

Overall, hybrid routing protocols aim to strike a balance between proactive and reactive approaches, utilizing the most suitable routing strategies based on the geographical characteristics of the network.

3.3.1. Zone routing protocol (ZRP):

In the Zone Routing Protocol (ZRP) [47], a hybrid routing protocol, the advantages and characteristics of reactive and proactive protocols are combined. The protocol operates based on the concept of zones, where different routing approaches are employed within and outside these zones.

In ZRP, each node in the network serves as the center of a predefined zone. The size of these zones is determined by the number of hops. The network topology is divided into multiple zones, which can vary in size and can be configured accordingly. Each node can belong to multiple zones simultaneously. [48]

Within a zone, two types of nodes exist: peripheral nodes and interior nodes [49]. Peripheral nodes are defined as nodes that are located at a distance equal to the radius of the zone from the center node. In contrast, interior nodes refer to nodes that have a minimum distance from the center node that is less than the zone radius.

The ZRP combines proactive and reactive routing strategies to optimize routing efficiency. Within the zone, a proactive routing approach is used to maintain up-to-date routing information. This enables quick availability of routes and minimizes the delay in establishing connections within the zone. Outside the zone, a reactive routing approach is employed. When a route is needed to a destination outside the zone, a route discovery process is initiated to find the path. This reactive approach conserves network resources and reduces control overhead in areas where route changes are less frequent.

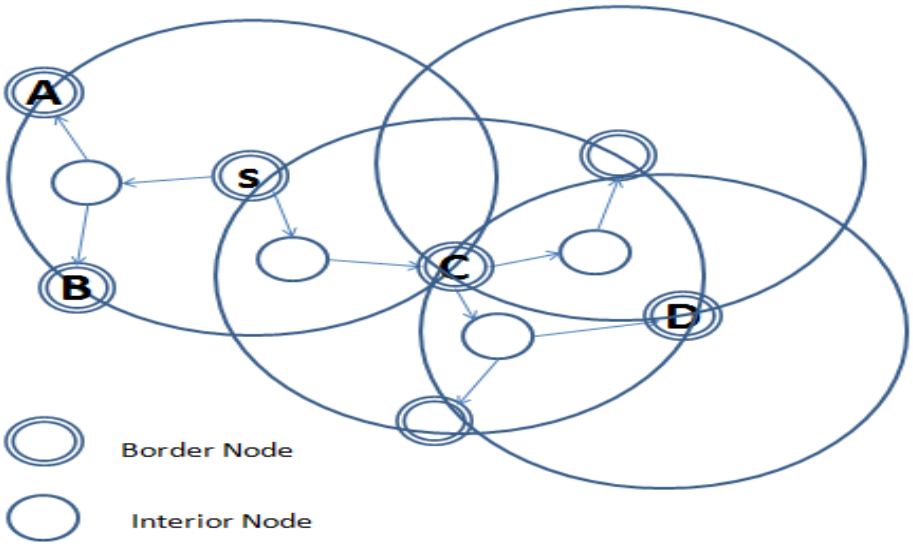

Figure 2.8: Zone routing in ZRP [50]

In the Zone Routing Protocol (ZRP), the routing process involves two distinct protocols: IntrA-zone Routing Protocol (IARP) and IntEr-Zone Routing Protocol (IERP). These protocols serve different purposes within the network. [47]

The IntrA-zone Routing Protocol (IARP) operates proactively within the same zone, also known as the Routing Zone (RZ). Its main responsibility is to maintain and update routes within the RZ. By continuously exchanging routing information with neighboring nodes, IARP ensures that up-to-date routing tables are available within the zone. This proactive approach allows for efficient and timely routing within the RZ, reducing latency and improving overall network performance.

On the other hand, the IntEr-Zone Routing Protocol (IERP) comes into play when the destination node is not found within the local zone. In such cases, IERP is responsible for initiating route discovery to locate the destination outside the current zone. It functions as a reactive protocol, similar to other reactive network protocols. When a route discovery is needed, the source node generates a route query packet.

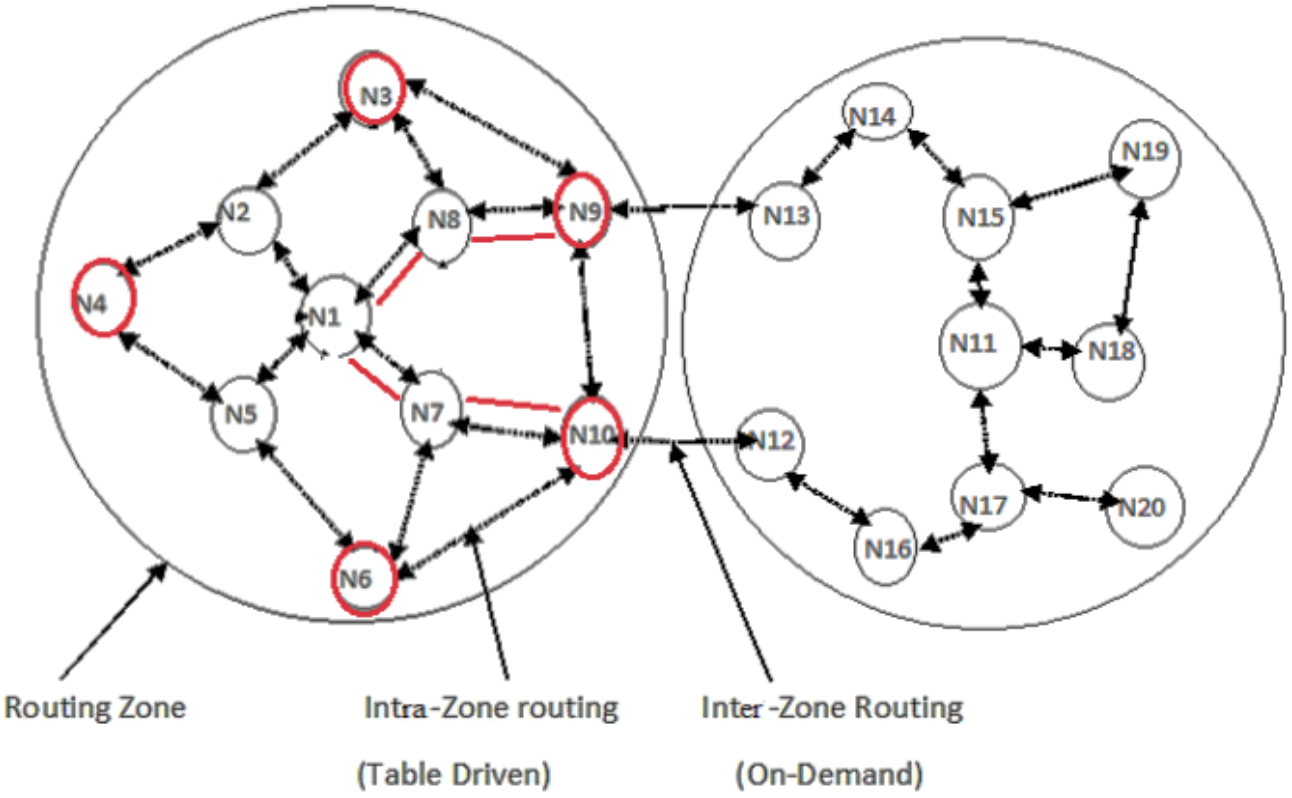

Figure 2.9: Intra-zone routing, and inter zone routing in ZRP [51]

To optimize the route discovery process, ZRP employs a mechanism called Bordercast Resolution Protocol (BRP) [47]. Unlike traditional broadcasting where route queries are sent to random neighbors, BRP directs the route discovery towards peripheral nodes that do not belong to the routing zone of the initiating node. This targeted approach increases the efficiency of the route discovery process by reducing unnecessary broadcast traffic.

The Bordercast Resolution Protocol (BRP) plays a crucial role in ZRP by facilitating the distribution of route queries to the appropriate border nodes for route discovery. It ensures that the route queries are efficiently propagated towards the zones where the destination might be located, enabling effective inter-zone routing.

By combining proactive routing within the zone (IARP) and reactive route discovery outside the zone (IERP) through the Bordercast Resolution Protocol (BRP), ZRP provides a comprehensive and adaptive routing solution for mobile ad hoc networks. This approach allows for efficient utilization of network resources and timely establishment of routes both within and between zones.

3.3.1.1. Route discovery in ZRP:

In the Zone Routing Protocol (ZRP), the process of route discovery is determined based on if the destination node is located within the local zone or outside of it. [47]

When sending data packets, the source node first checks if the destination node is within its own zone. If the destination is within the zone, the source node can directly find a route to the destination and send the packet accordingly. However, if the destination node is outside the local zone, a reactive routing mechanism is employed for route discovery. The route discovery process begins with the source node initiating a route request by sending route request packets (RREQ). These RREQ packets contain information such as the source node's address, destination address, and a request number. The route request packets are then sent to the peripheral nodes within the network through the Bordercast Resolution Protocol (BRP). Each peripheral node checks its own local zone to determine if the destination is present. If the destination is not found within a node's local zone, the packet is forwarded to other neighboring nodes following the bordercast algorithm. [47,49]

As the route request packets traverse the network, nodes along the path append their IDs and addresses to the packets, creating a record of routing information. This process continues until the packet reaches the destination node or a node with a valid route to the destination. Upon reaching the destination or a node with a valid route, a route reply packet is generated and sent back through the reverse path of the accumulated route recorded in the route request messages. This route reply packet provides the necessary route information to establish a path from the source node to the destination node.

3.3.1.2. Route maintenance in ZRP:

In the Zone Routing Protocol (ZRP), route maintenance plays a crucial role in ensuring the reliability and stability of routes in the network. The way this mechanism works in ZRP:

- Local Zone Route Maintenance: Nodes in a local zone have knowledge of the routes within their zone. This information is utilized during route maintenance. When a node detects a route failure within its local zone, it can either notify the source node about the failure or attempt to repair the route. The notification message contains details about the route failure, including the hop where it occurred. Alternatively, the node can initiate a repair process by conducting a repair discovery to find an alternate route. During the repair process, packets may experience delays until a new valid route is established. [52]
- IntEr-Zone Route Maintenance (IERP): IERP is responsible for maintaining routing tables and monitoring changes and updates in the network. It takes on the responsibility of repairing route failures that extend beyond the local zone. When a node detects a route failure, it can notify the source node or initiate a repair process. The repair process involves searching for an alternative route until a new valid route is discovered. Depending on the situation, the successful repair may or may not be reported to the source node to maintain connectivity without compromising network performance.

3.3.1.3. Advantages and drawbacks of zone routing protocol:

ZRP improves scalability in large networks by dividing the network into smaller zones. Each zone operates independently, reducing the overall routing overhead and improving network performance. Being a hybrid routing protocol, ZRP also combines the benefits of both proactive and reactive routing protocols [53]. Within a zone, proactive routing is used, which reduces control overhead as routes are continuously maintained. Outside the zone, reactive routing is employed, conserving network resources by only establishing routes when needed. However, the reactive of approach of the zone routing protocol can also be a drawback in the sense of When a node needs to communicate with a destination outside its local zone, the route discovery process involves broadcasting requests to neighboring zones. This can lead to increased control overhead at zone boundaries and potential delays in establishing routes. Adding to that, the complexity of the protocol compared to other routing protocols, it requires accurate and careful configuration of zone sizes and other parameters to optimize performance.

3.4. Overall comparison between proactive, reactive, and hybrid routing protocols:

Proactive, reactive, and hybrid routing protocols each have their own characteristics, advantages, and drawbacks:

Proactive Routing Protocols:

- Characteristics: Proactive protocols maintain routing information continuously by exchanging routing updates among network nodes. Each node keeps a routing table with pre-established routes to every destination in the network.[54]
- Advantages: Low latency for data transmission as routes are already established, reduced delay in delivering data packets since routes are readily available.
- Drawbacks: High control overhead due to continuous routing updates, which can lead to increased network traffic, increased resource consumption due to the continuous maintenance of routing tables

Reactive Routing Protocols:

- Characteristics: Reactive protocols establish routes on-demand when a node needs to communicate with a destination. Route discovery is initiated only when required, reducing control overhead and conserving network resources.
- Advantages: Reduced control overhead as routes are established only when needed, Efficient utilization of network resources in dynamic or mobile networks.
- Drawbacks: Longer delay for route establishment as route discovery is required, increased latency for data transmission due to the route discovery process.

Hybrid routing protocols:

- Characteristics: Hybrid protocols combine proactive and reactive approaches to leverage the benefits of both. They divide the network into zones and employ different routing strategies inside and between zones. [54]
- Advantages: Faster route establishment within zones using proactive routing, Efficient resource utilization through reactive routing outside zones.
- Drawbacks: Increased complexity in configuration and management compared to single-mode protocols, dependence on accurate zone configuration and location information.

4. Conclusion:

Throughout this chapter, we delved into various routing types and explored several routing protocols employed in mobile ad hoc networks. Each protocol was thoroughly examined, outlining their route discovery and maintenance processes. Furthermore, we discussed respective strengths and weaknesses of these protocols, culminating in a comprehensive comparison of proactive, reactive, and hybrid routing techniques.

Chapter 3:
Simulation and Results

1. Introduction:

Simulation is a valuable process that allows researchers to recreate or model real-world processes or systems. It finds extensive use in educational settings and serves various purposes. Researchers benefit from simulation as it enables them to experiment with different scenarios and test hypotheses in a controlled environment. However, it is important to acknowledge that simulations are representations and may not always reflect real-life situations accurately. Simulations are conducted using specialized software tools that generate output data. This data is then analyzed and observed by researchers who draw deductions and conclusions based on the results.

In line with this concept, we aimed to study the performance of Mobile Ad Hoc routing protocols in a realistic environment. To achieve this, we conducted a comparative simulation of AODV, OLSR, and DSDV protocols using different scenarios and parameters. We used the Network Simulator 3 (NS-3) software for this purpose. By simulating these protocols, we aimed to gain insights into their performances and make informed observations and evaluations.

2. Network Simulator 3 (NS-3) :

Network Simulator 3 (NS-3) is a renowned open-source discrete-event network simulator that enables the simulation of network behavior. It offers a comprehensive collection of modules and models for various networking technologies and protocols, with most of its components implemented in C++ and few in Python.

NS-3 has gained substantial popularity among students and researchers in the field of networking due to its high credibility and its effectiveness in developing and testing new technologies and protocols. It provides a reliable platform for conducting simulations and evaluating the performance of networking solutions.

For our simulation, we utilized the latest version of NS-3, specifically version 3.38. We performed the simulation on a Linux Ubuntu operating system using a virtual machine (VBox) setup. This configuration allowed us to leverage the capabilities of NS-3 effectively and carry out our study in a controlled and efficient manner.

3. Simulation parameters and metrics :

We simulated three routing protocols, AODV, OLSR, and DSDV using the parameters presented below:

Parameters	Values
Simulation time	50 seconds
Packets size	64, 128, 256, 512, and 1024 bytes
Simulation surface	500x500 meters
Wi-Fi Operation Mode	Ad Hoc Mode
Number of sink nodes	10, 25 source nodes
Mac Standard	802.11B
Data type	UDP packets
Data rate	2048 Kbps
Position allocator	Random rectangular

Table 3.1: Parameters of the simulation.

3.1. Simulation parameters:

During the simulation, we conducted experiments for a duration of 50 seconds, starting with the first packet transmission occurring randomly between 50.0 and 51.0 seconds. The Wi-Fi configuration was set to ad hoc mode, operating at a rate of 2 Mb/s. source nodes will be sending packets at a rate of 4 UDP packets per second at an application rate of 2.048 Kbps.

Designing a simulation involves carefully selecting and manipulating various parameters to simulate different scenarios and obtain reliable and consistent results. Some important parameters we opted for are:

Propagation loss model: In Network Simulator 3 (NS-3), the wireless channel for the 802.11b standard is configured using propagation loss models and propagation delay models. By default, NS-3 utilizes the constant speed propagation delay model, which was also employed in our simulation. Additionally, NS-3 employs the log-distance propagation loss model as the default choice. However, NS-3 provides a range of other propagation loss models, including the two-ray ground loss model and the Friis propagation loss model, among others. These alternative models can be selected and used based on the specific requirements and characteristics of the simulated wireless network scenario.

- **The Two-ray ground propagation loss model:** The Two-ray ground propagation loss model is a model highly used in wireless communication systems. It considers various factors such as the distance between the transmitter and receiver, the height of antennas, and the reflection

coefficient of the ground. This model takes into account the phenomenon of both direct path propagation and ground-reflected path propagation. By considering these factors, the Two-ray ground propagation model provides an estimation of the signal strength and characteristics of wireless signals in outdoor environments, where the ground reflection plays a significant role in signal propagation.

- **The Friis propagation loss model:** The Friis propagation loss model is a commonly used model in wireless communication systems. It assumes that the transmitted signal propagates in free space without considering the effects of obstacles or reflections. This model provides a simplified estimation of the signal strength based on the distance between the transmitter and receiver, the frequency of the signal, and the antenna gains. The Friis model is often used in scenarios where the focus is on studying the fundamental characteristics of radio wave propagation in a clear and unobstructed environment, without considering the complexities introduced by obstacles or multipath effects. This makes the Friis propagation loss model suitable for situations where the objective is to analyze the basic performance of wireless communication systems without incorporating additional variables that may unpredictably affect signal propagation.

The equation below is used for the Friis propagation loss model:

$$P_r = \frac{P_t + G_t + G_r + \lambda^2}{(4\pi \times d)^2} \text{ L} \qquad (3.1)$$

- P_t is the transmission power (watts)
- P_r is th reception power (watts)
- G_t *is transmission gain*
- G_r *is the reception gain*
- λ *is the wavelength*
- d being the length of the link, and L, is the system loss

Mobility model: In our simulation, we utilized the "Random Mobility Waypoint" model to represent the mobility of nodes in mobile ad hoc networks. This model, implemented through the "ns3: RandomWayPointMobilityModel" command, allows nodes to move randomly within the simulation area. The nodes move at a constant speed, determined by the specific scenario being simulated, without any pauses in their movement.

The Random Mobility Waypoint model captures the inherent mobility and unpredictability of nodes in mobile ad hoc networks. By simulating random movement, we can study the dynamic nature

of the network and evaluate the performance of routing protocols under varying node positions. This model is well-suited for scenarios where nodes have no specific pattern or predefined routes, and their movements are governed by randomness, reflecting real-world scenarios more accurately.

Transmission power: the transmission power of a Wi-Fi router usually ranges from 3 dBm to 17 dBm, in a 500x500 meters area, we decided to use 7.5 dBm transmission power to have close results to reality.

When comparing simulations to the real word, several differences can be found, simulation often make simplifying assumptions to make the modeling process manageable and ca omit certain details or factors present in the real world, and since real world models involve very complex interactions and parameters that are challenging to replicate in a simulation, all that conclude into limitations and inaccuracy in simulations, the real word parameters are actual characteristics and properties, they are based or actual measurements and observations from the physical system

3.2. Metrics of evaluation:

In order to compare the performance of the AODV, OLSR, and DSDV routing protocols, we considered several metrics to analyze their effectiveness in different scenarios. These metrics provide insights into the network's behavior and performance. The metrics used for comparison are:

- ***Throughput:*** Throughput measures the amount of data transmitted over the network within a given time period. It indicates the network's capacity to handle data traffic. Higher throughput implies better utilization of network resources and efficient data transfer. Throughput is calculated using the following equation:
- ***Packet Delivery Ratio (PDR)***: it represents the ratio of the delivered packets to the total packets sent to destination, expressed in percentage, a higher PDR means a larger proportion of packets is sent successfully.
- ***Packet loss:*** refers to the totality of packets that were not successfully delivered to their intended destinations in a network communication scenario. It represents the count of packets that were either dropped, discarded, or unable to reach their destination, a higher Packet loss indicates a larger proportion of packets that were not successfully transmitted or received, which is generally undesirable as it indicates poor network performance.
- ***Average delay***: refers to the average time interval between sending a packet from a source node to the reception of it from the destination node.

4. Simulation and results interpretation:

Below are the results of the simulation for the three routing protocols (AODV, OLSR, and DSDV) based on different scenarios involving variations in node speed and the number of nodes in the network. The packet size used for the simulation was fixed at 64 bytes.

4.1. Variation in number of nodes:

In Figure 3.1, the bar graph illustrates the comparison of throughput among the three routing protocols (AODV, OLSR, and DSDV) under different network densities.

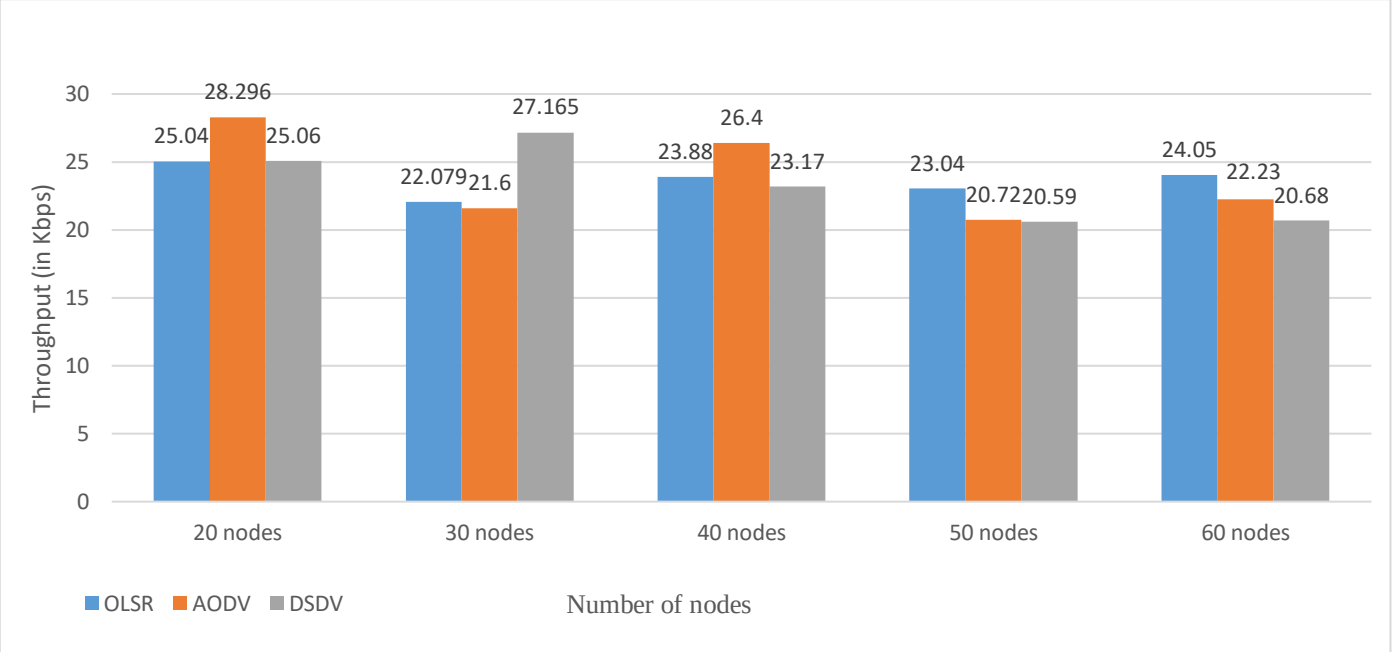

Figure 3.1: Throughput vs number of nodes.

When the network density is moderate to low, AODV exhibits slightly higher throughput compared to OLSR and DSDV, indicating its effectiveness in such scenarios. However, as the network density increases, a slight decrease in throughput can be observed for all three protocols. This reduction may be attributed to factors such as increased interference. In terms of individual performances, DSDV also demonstrates good throughput in low-density networks, but AODV outperforms the other protocols when the network density is average to low. On the other hand, OLSR remains relatively stable in terms of throughput across different densities and even outperforms the other two protocols in denser networks.

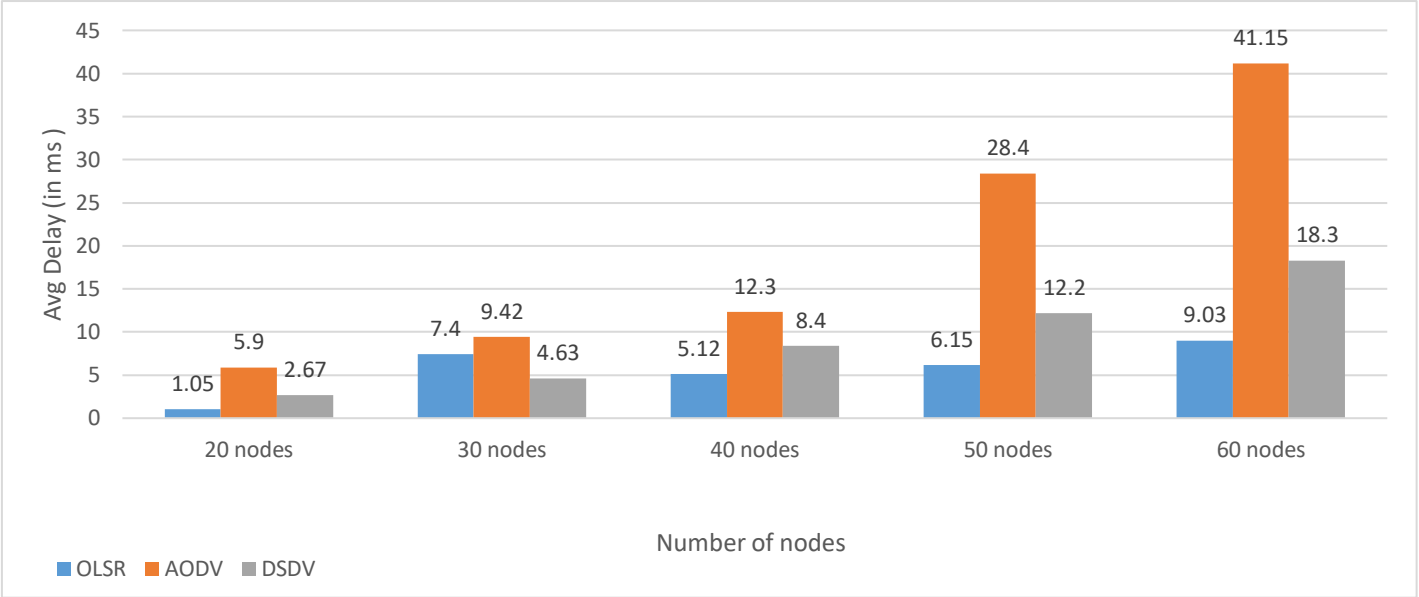

Figure 3.2: Average delay vs number of nodes.

In Figure 3.2, the bar graphs depict the end-to-end delay for the three routing protocols (AODV, OLSR, and DSDV) as the number of nodes in the network varies.

The analysis of average delay reveals further insights into the performance of the routing protocols. OLSR demonstrates a consistent delay across different network sizes, with a slight increase as the density increases. This suggests that OLSR maintains a relatively stable average delay and performs well regardless of the network size. In comparison, DSDV challenges OLSR in low-density networks but experiences a higher increase in delay as the nodes number grows.

On the other hand, AODV performs less optimally compared to the other two protocols due to its reactive nature. However, it shows a good performance in less dense networks. As the network density increases, AODV experiences a higher rate of delay increase compared to OLSR and DSDV.

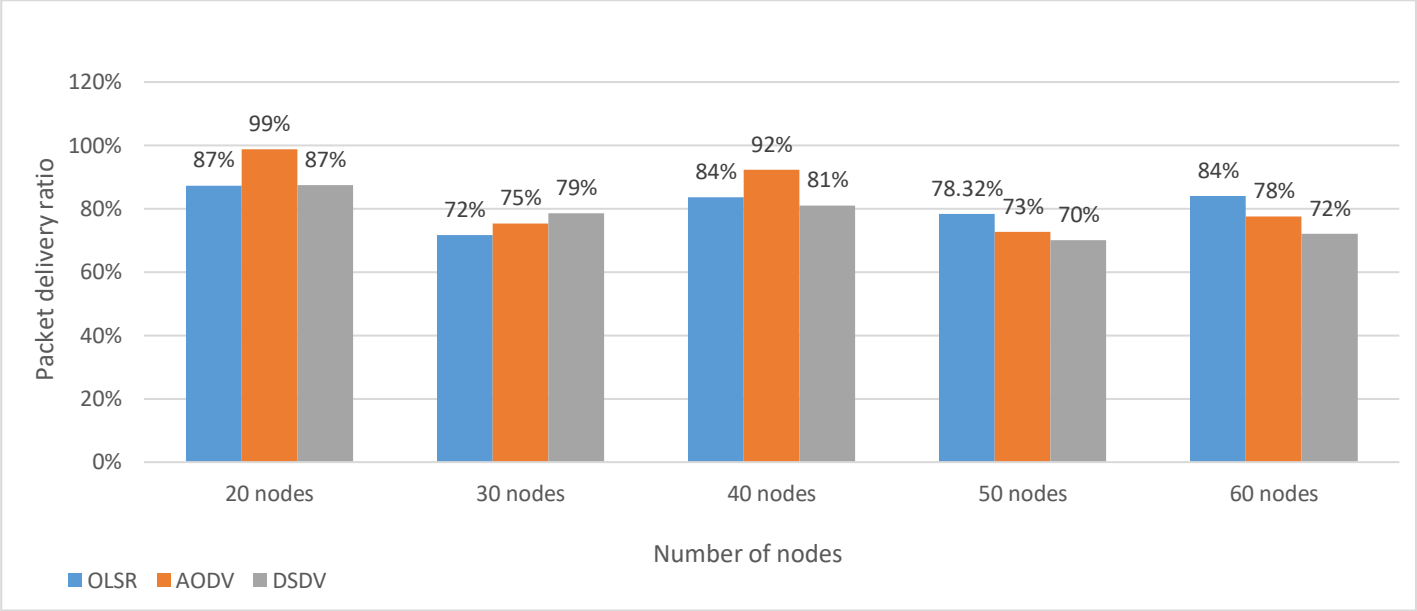

Figure 3.3: Packet delivery ratio vs number of nodes.

Based on the analysis of Packet Delivery Ratio (PDR) for the OLSR, AODV, and DSDV routing protocols in figure 3.3, we noticed the following:

AODV exhibits a high Packet Delivery Ratio (PDR) that gradually decreases as the number of nodes increases. It demonstrates superior performance compared to the other two protocols, namely OLSR and DSDV, in low-density and medium-density networks. Although OLSR shows a lower PDR than AODV, it shows improvement as the network size expands. Similarly, DSDV performs adequately in low-density networks with a medium to low number of nodes, but it exhibits the poorest overall performance, albeit by a small margin. Therefore, based on these findings, it can be concluded that AODV delivers packets more effectively than the other protocols, especially when number of nodes is not very high.

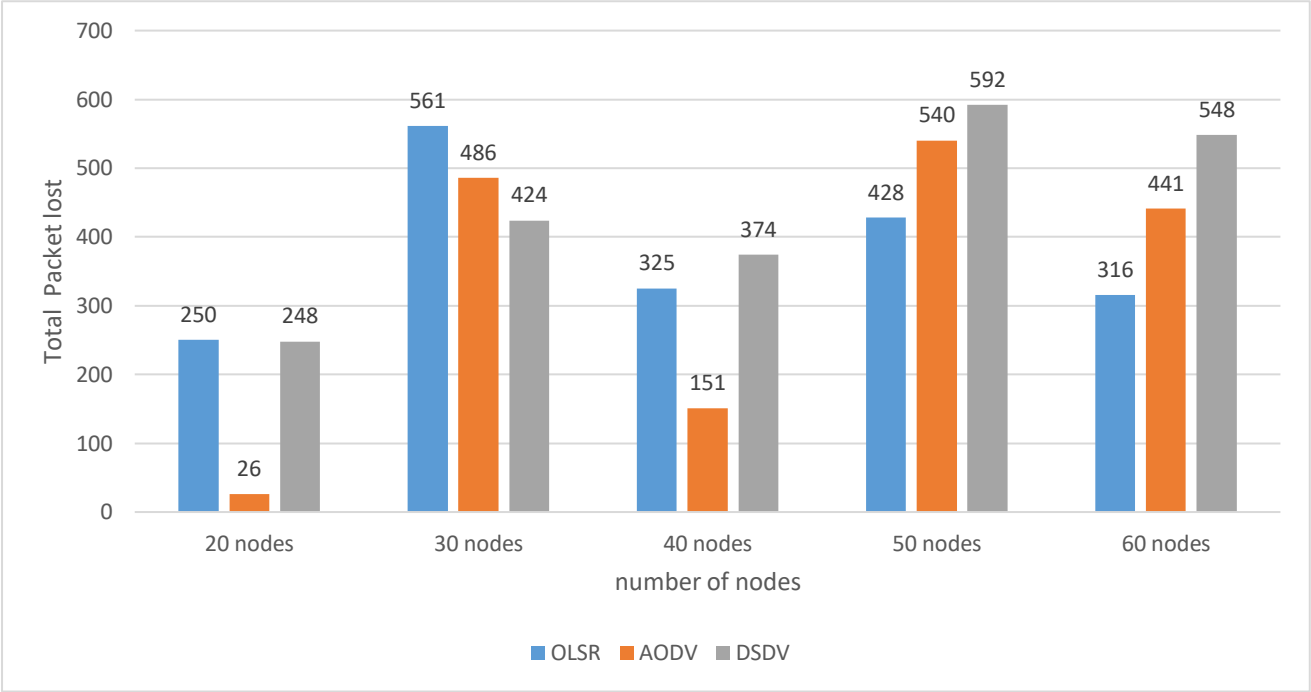

Figure 3.4: Total packet lost vs number of nodes.

The analysis of Figure 3.4 examines the impact of varying the number of nodes on packet loss in AODV, OLSR, and DSDV. The results reveal notable differences in performance among the protocols. AODV consistently outperforms the other two protocols, exhibiting lower packet loss rates, particularly in networks with lower density.

In comparison, OLSR and DSDV demonstrate similar levels of packet loss in networks with similar density. However, an interesting observation is that DSDV shows improved performance as the number of nodes increases, surpassing both AODV and OLSR. Despite this, AODV stands out as the most reliable protocol overall, consistently losing fewer packets and demonstrating superior performance.

4.2. Variation of nodes speed:

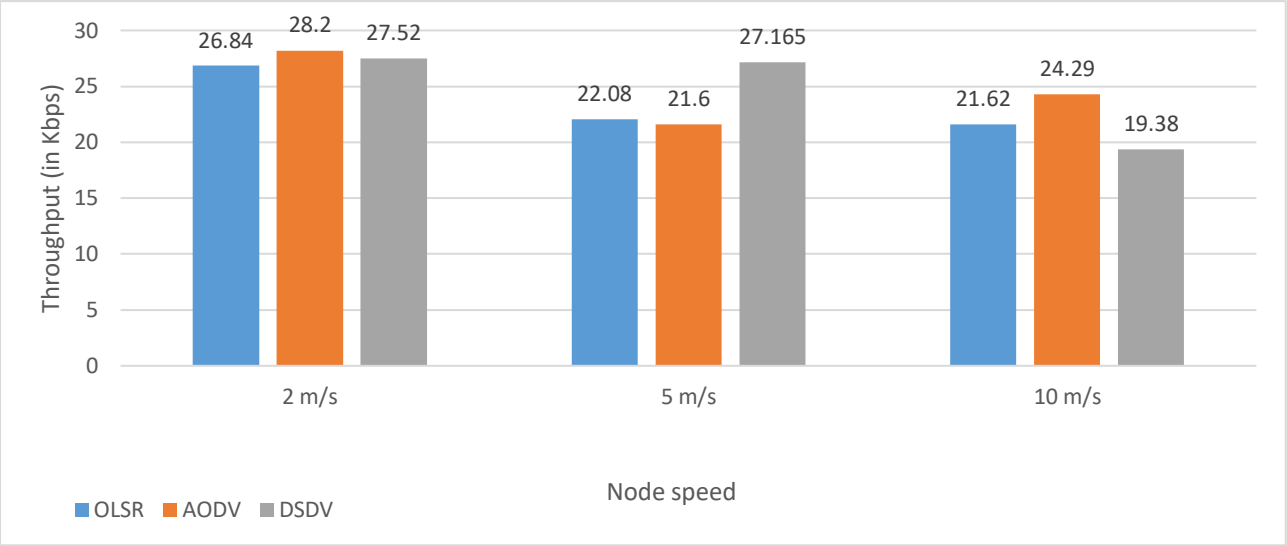

Figure 3.5: Throughput vs node mobility.

The analysis of Figure 3.5 focuses on the throughput performance of the OLSR, AODV, and DSDV routing protocols under varying speeds. At low speeds, the performance of the three protocols appears to be relatively similar, with comparable throughput levels. However, as the speed increases, a decrease in throughput is observed across all three protocols.

Notably, DSDV exhibits a slightly better throughput performance compared to AODV and OLSR under these conditions. When the speed reaches its maximum value of 10 m/s, OLSR and DSDV experience a slight further decrease in throughput, while AODV demonstrates relatively better throughput performance.

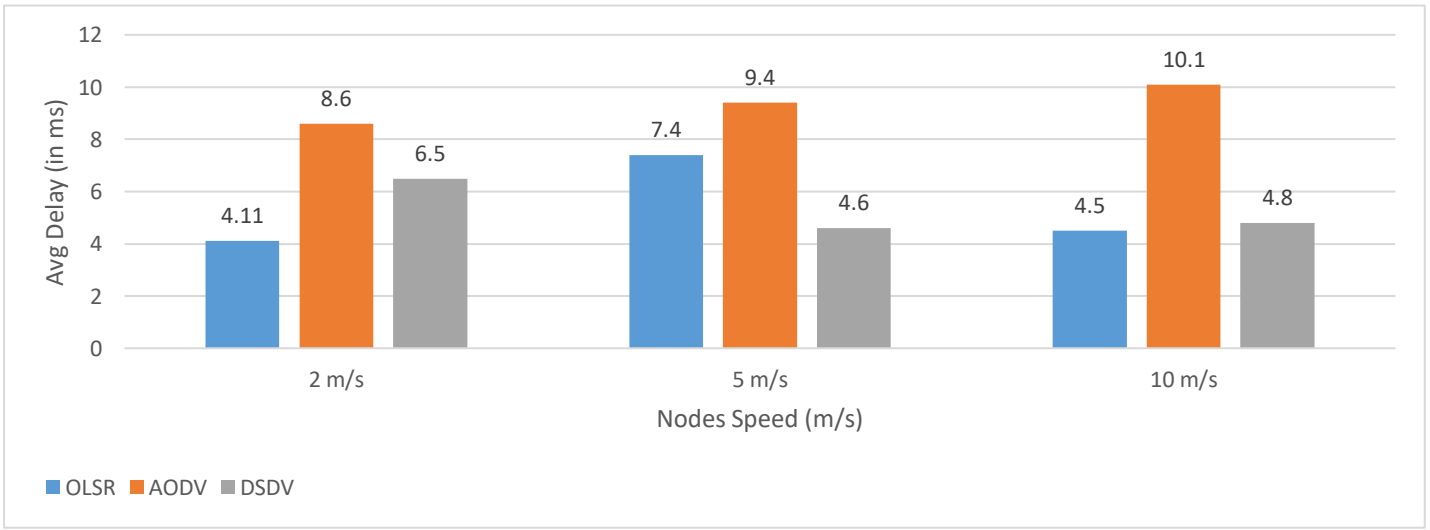

Figure 3.6: Average delay vs nodes mobility.

Figure 3.6 highlights the average delay of the OLSR, AODV, and DSDV routing protocols as the speed increases. AODV exhibits the highest delay among the three protocols.

Conversely, OLSR demonstrates the lowest delay when the speed is low, followed by DSDV. Notably, DSDV exhibits a decreasing delay trend as the node's speed increases, indicating its improved performance in highly mobile scenarios.

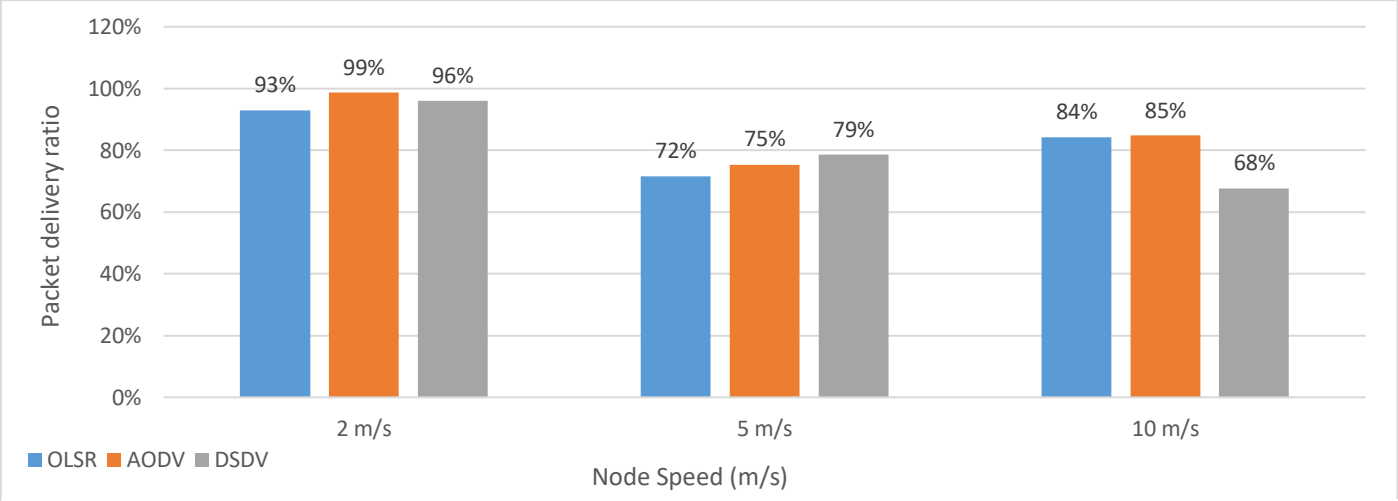

Figure 3.7: Packet delivery ratio vs Nodes speed

In Figure 3.7, the bar graphs illustrate the packet delivery ratio (PDR) across different node speeds for the OLSR, AODV, and DSDV routing protocols. The PDR performance is relatively similar among the three protocols, with AODV slightly outperforming the others. However, as the node speed increases, there is a noticeable decline in PDR for all protocols. At the maximum speed, DSDV exhibits the lowest PDR compared to the other two protocols.

5. Problem identification:

The purpose of our comparative study was to evaluate the performance of three MANET routing protocols: OLSR, AODV, and DSDV. By analyzing key metrics such as packet delivery ratio (PDR), throughput, and delay. We aim to gain insights into the strengths and weaknesses of these protocols under various network conditions.

One significant challenge in MANETs is network saturation and congestion. Network saturation occurs when the available network resources, such as bandwidth and processing capacity, are fully utilized, leading to a degradation in overall network performance. Congestion, on the other hand, specifically refers to the situation where there is a high demand for network resources that exceeds their capacity, resulting in severe performance degradation and packet loss.

Several factors can contribute to network saturation and congestion. Increasing the density of the network and Data potentially leads to higher traffic loads. As the number of nodes and packets size grow, the network's resources become more constrained, and the probability of congestion increases. Additionally, factors such as high data transmission rates, and frequent route updates can

also contribute to network saturation. Network saturation and congestion can have detrimental effects on MANET performance, including reduced throughput, increased packet loss, and higher delays.

To further investigate the performance of AODV in saturated networks, we conducted additional simulation. In this simulation, we employed 25 sink nodes and 70 regular nodes while gradually increasing the packet size. By varying the packet size, we aimed to emulate higher network traffic and evaluate how the two protocols would cope with network saturation.

The choice of 25 sink nodes and 70 regular nodes allowed us to simulate a realistic scenario with a considerable number of nodes in the network. This setup enabled us to observe the behavior and performance of AODV under higher traffic conditions. By monitoring key performance metrics such as packet delivery ratio, and overall transmission delay, we will able to assess the effectiveness of AODV in handling network saturation. These metrics provide valuable insights into the protocols' ability to maintain efficient packet delivery, sustain high data rates, and minimize delays in challenging network conditions.

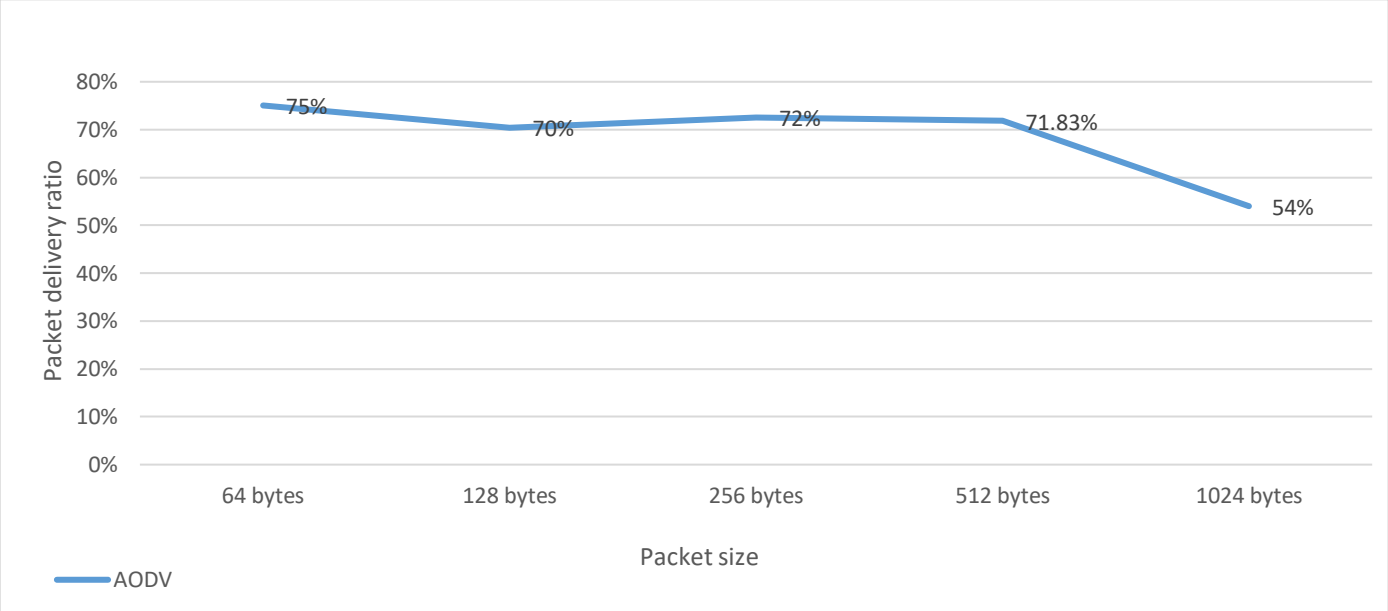

Figure 3.8: Packet delivery ratio vs packet size.

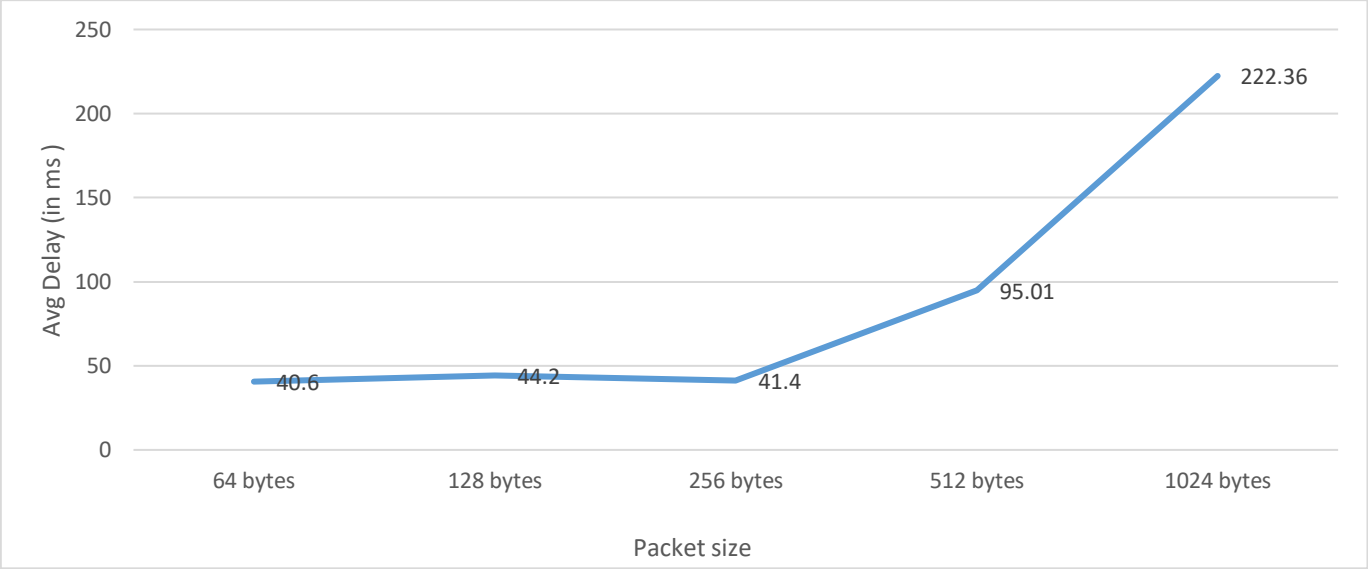

Figure 3.9: Avg delay vs packet size.

The analysis presented in Figures 3.8 and 3.9 provides insights into the performance of the AODV routing protocol in terms of packet delivery ratio (PDR) and transmission delay. These graphs demonstrate a relatively stable performance of AODV as we vary the packet size. However, a significant deviation occurs when the packet size reaches 1024 bytes, leading to a notable drop in PDR and a substantial increase in delay, the PDR dropped from 70% to 54%, and the delay spiked from 100 ms to 222 ms. This observation suggests that the network reaches a critical point where congestion and saturation become prominent issues.

The observed threshold of congestion and network saturation at the packet size of 1024 bytes highlights the limitations of the network in handling larger packets effectively. The substantial drop in PDR indicates a higher rate of packet loss, compromising the successful delivery of data. Additionally, the considerable spike in delay indicates increased latency, which can adversely affect real-time applications and overall network responsiveness.

These findings emphasize the need for further optimization and management strategies to address congestion and saturation issues.

6. Problem solution:

6.1. Optimized AODV [55]:

To address the issue of network congestion, similarly to authors in [55], an optimized version of the AODV routing protocol is proposed. In this enhanced version, the routing decisions are based on the minimum queue charge rather than the traditional minimum hop count metric.

The key idea behind this approach is to prioritize routes that have the least amount of congestion in terms of queue occupancy. By considering the queue charge as a routing metric, the

optimized AODV aims to distribute traffic more evenly across the network, and to ensure the equilibrium in the network, regarding the concept of the Game theory, thereby alleviating congestion hotspots and improving overall network performance.

In the traditional AODV, routes are selected based solely on the minimum hop count, which may not necessarily reflect the actual state of congestion in the network. By taking into account the queue charge, the optimized AODV can intelligently steer traffic away from heavily congested nodes and towards nodes with lighter traffic loads.

By dynamically adapting the route selection process based on the queue charge metric, the optimized AODV protocol ensures that the network resources are utilized more efficiently. This can lead to improve throughput, reduce packet loss and latency, ultimately enhancing the overall quality of service experienced by network users.

The introduction of the optimized AODV protocol provides a promising solution to mitigate congestion in ad hoc networks. By incorporating queue charge as a routing metric, the protocol intelligently manages network traffic and balances the load across different nodes. This approach can significantly enhance the network's ability to handle high traffic volumes and improve the overall stability and performance of the ad hoc network.

The work could be done following the steps below:

- Calculating the cost of each network node based on its load.
- Updating the routing table periodically by the nodes.
- Modifying the metric of the route discovery algorithm to prioritize cost over the number of hops.

6.2. Protocol switch:

Our approach involves initially deploying the standard AODV routing protocol in the network. We then leverage the threshold values obtained from the previous graph analysis, which indicate the point of congestion and degraded performance. Once the network reaches this threshold, we dynamically switch to the optimized AODV protocol. This switch allows us to address the congestion issue by utilizing Optimized AODV that selects routes based on the minimum queue charge rather than the minimum hop count. By implementing this protocol switch mechanism, we aim to improve the network's performance and alleviate congestion-related problems, ensuring efficient and reliable communication in the MANET environment.

To further explain the idea, made a simple flowchart and algorithm of the proposed protocol and protocol switch for data transmission from source node S to destination node D:

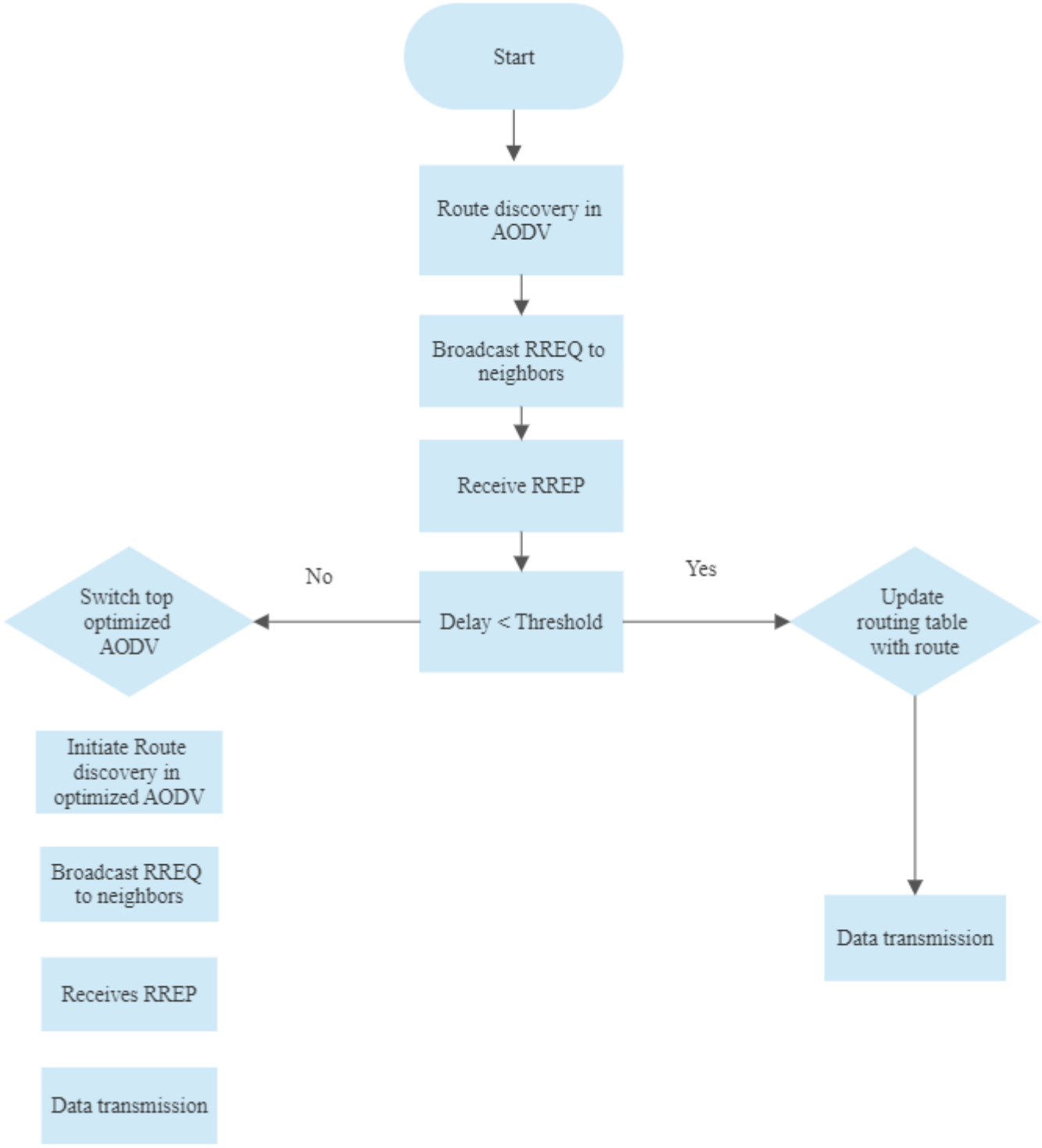

Figure 3.10: Flowchart of switch from AODV to Optimized AODV.

#Source node perspective

Start

Source node S has data packets to send to destination node D

If S has a valid route to D:

Begin data transmission directly to D

Else:

Initiate route discovery process

Create a route request (RREQ) packet with S as src node and D as dest node

Initialize the cost ($C_p = C(S)$)

Initialize Hop count ($Hop\_count = 0$)

Broadcast RREQ to neighboring nodes

Set up a timer for RREP packets

Evaluate transmission delay

While data in transmission:

If a RREP packet is received in S **then:**

If delay < predefined threshold **then:**

Update routing table with route to D

Begin transmission

Else switch to optimized AODV

End If

Else if RERR packet is received **then:**

Update routing table to remove invalid route

Restart route discovery

Else if Timer for receiving RREP expires:

Re-broadcast the RREQ packet

End If

End while

#Intermediary node perspective

Start

Intermediary node I receives Route request (RREQ)

If nodes I has a route to D, **then:**

If sequence number = max **then**

Send route reply (RREP) to the source

Else discard RREQ

Else

Accumulate the cost: $C_p = C_p + C(I)$

Accumulate the cost : $Hop\_count = Hop\_count + C(I)$

Update routing table

Update *Cp* et Hop_count in the RREQ

Broadcast RREQ to neighboring nodes

End If

End If

End.

#Destination node perspective

Start

Node D receives route request (RREQ)

If destination IP address in RREQ is the node IP address **Then**

If sequence number = max **then**

If min ($Min(C_p)$ **Then**

Send RREP to source node S

Else If Routes have equal cost, **then**

$(Min(Hop\_count)$

Send RREP to source node S

Else discard RREQ

Else discard RREQ

Else Intermediary node algorithm

End

The above algorithm is a simple high-level overview of data transmission using AODV protocol. It explains the idea that could achieve congestion control in AODV and achieving equilibrium through discovering route based on the minimum charge in queue instead of minimum hop count by switching from the standard AODV to the O-AODV, when certain predefined threshold value is already met (delay, throughput, or packet loss).

7. Conclusion:

In this chapter, we conducted simulations to evaluate the performance of three routing protocols: AODV, OLSR, and DSDV. Through a comparative analysis using various scenarios and metrics, we examined the behavior of each protocol under different environmental conditions and parameter variations. Additionally, we investigated the performance of AODV in a saturated network to understand its congestion behavior. To mitigate congestion and achieve equilibrium, we proposed an approach using an optimized version of AODV. This involved switching from AODV to optimized AODV when a predetermined congestion threshold is reached. The findings from these simulations provide valuable insights into protocol performance and offer a potential solution to alleviate congestion in such networks.

General Conclusion

The present thesis provides a comprehensive analysis of various routing protocols in Mobile Ad Hoc Networks (MANET). Through an exploration of the characteristics, strengths, and limitations of different routing protocols, we have gained valuable insights into their performance in dynamic and self-configuring wireless environments.

The study commenced with an exploration of ad hoc networks, elucidating their distinctive features and application domains. Subsequently, the focus shifted to routing and the diverse strategies employed in mobile ad hoc networks, classified as proactive, reactive, and hybrid protocols. A meticulous examination of these protocols encompassed their mechanisms, attributes, advantages and drawbacks.

The research objective encompassed gaining insights and conducting a comparative study of MANET routing protocols, culminating in the analysis of three specific protocols: AODV, OLSR, and DSDV. The aim was to comprehend how these protocols ensure effective data routing between source and destination nodes. To facilitate a comprehensive evaluation and comparison, simulation modeling using ns-3 was employed, enabling an in-depth assessment of protocol performance under varying network conditions. This simulation-based approach facilitated the identification and analysis of key performance metrics such as Packet Delivery Ratio (PDR), throughput, and delay, thus enabling a robust comparison of the routing protocols.

Additionally, this thesis addressed the critical issue of congestion in ad hoc networks. A potential solution was proposed to alleviate congestion by modifying the operation of the routing protocol, introducing the concept of cost based on the traffic load in a node's queue. This approach aimed to mitigate congestion-related challenges such as increased end-to-end delay and decreased throughput, thereby enhancing overall network performance and efficiency. The insights gained from this research contribute to a deeper understanding of MANET routing and serve as a foundation for the design and implementation of efficient and reliable wireless communication networks across various domains.

We will continue working on this issue by making a more efficient and complete switch process that could be really employed in practice. Related work needs a deep and smart changes in protocols scripts that make the switch fast and reliable.

Bibliography

[1] Ali AK, Kulkarni U. Characteristics, applications and challenges in mobile Ad-Hoc networks (MANET): overview. Wireless Networks. 2015 Dec;3(12):6-12.

[2] Dr.S.S.Dhenakaran and Dr.S.S.Dhenakaran, "An Overview of Routing Protocols in Mobile Ad-Hoc Network", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, pp. 251-259, February 2013.

[3] Kumar M, Mishra R. An overview of MANET: history, challenges and applications. Indian Journal of Computer Science and Engineering (IJCSE).;3(1):121-5. 2012 Feb

[4] Hanafy IM. Using Biological Techniques for MANet security based on fuzzy classification (Doctoral dissertation, Banha University).2013

[5] Shiny SJ. A Review on Application of MANET-IoT. i-manager's Journal on Mobile Applications and Technologies.;9(1):28. 2022

[6] Jayakumar G, Gopinath G. Ad hoc mobile wireless networks routing protocols–a review. Journal of Computer science.3(8):574-82. 2007 Aug

[7] Ahmed DE, Khalifa. An overview of MANETs: applications, characteristics, challenges and recent issues. 2017

[8] Raja L, Baboo SS. An overview of MANET: Applications, attacks and challenges. International journal of computer science and mobile computing. 2014 Jan;3(1):408-17.

[9] Swati AJ, Priyanka R. Wireless sensor network (WSN): Architectural design issues and challenges. Int. J. Comput. Sci. Eng. 2010;2(9):3089-94.

[10] Maraiya K, Kant K, Gupta N. Wireless sensor network: a review on data aggregation. International Journal of Scientific & Engineering Research. 2011 Apr;2(4):1-6.

[11] Akkaya K, Younis M. A survey on routing protocols for wireless sensor networks. Ad hoc networks. 2005 May 1;3(3):325-49.

[12] Sohraby K, Minoli D, Znati T. Wireless sensor networks: technology, protocols, and applications. John wiley & sons; 2007 Apr 6.

[13] Misra S, Misra SC, Woungang I, editors. Guide to wireless mesh networks. London, UK: Springer; 2009 Feb 19.

[14] Redwan H, Kim KH. Survey of security requirements, attacks and network integration in wireless mesh networks. In2008 New Technologies, Mobility and Security 2008 Nov 5 (pp. 1-5). IEEE.

[15] Rejina Parvin J. An Overview of Wireless Mesh Networks [Internet]. Wireless Mesh Networks - Security, Architectures and Protocols. IntechOpen; 2020.

[16] Goyal P, Parmar V, Rishi R. Manet: vulnerabilities, challenges, attacks, application. IJCEM International Journal of Computational Engineering & Management. 2011 Jan;11(2011):32-7.

[17] Nissar N, Naja N, Jamali A. A review and a new approach to reduce routing overhead in MANETs. Wireless Networks. 2015 May; 21:1119-39.

[18] Ahmed DE, Khalifa. An overview of MANET: applications, characteristics, challenges and recent issues.2017

[19] Muchintala PR, Hash L. Routing protocols for Manet.(2016)

[20] : Kaur H, Sahni V, Bala M. A survey of reactive, proactive and hybrid routing protocols in MANET: a review. network. 2013;4(3):498-500.

[21] Mohseni S, Hassan R, Patel A, Razali R. Comparative review study of reactive and proactive routing protocols in MANETs. In4th IEEE International Conference on Digital ecosystems and technologies 2010 Apr 13 (pp. 304-309). IEEE.

[22] Palaniammal M, Lalli M. comparative study of routing Protocols for MANETs. International Journal of Computer Science and Mobile Applications. 2014 Feb;2(2):118-27.

[23] Clausen T, Jacquet P, editors. RFC3626: Optimized link state routing protocol (OLSR).(2003)

[24] He G. Destination-sequenced distance vector (DSDV) protocol. Networking Laboratory, Helsinki University of Technology. 2002 May 6;135:1-9.

[25] Narra H, Cheng Y, Cetinkaya EK, Rohrer JP, Sterbenz JP. Destination-sequenced distance vector (DSDV) routing protocol implementation in ns-3. InSIMUTools 2011 Mar 21 (pp. 439-446).

[26] Gupta SK, Saket RK. Performance metric comparison of AODV and DSDV routing protocols in MANETs using NS-2. International Journal of Research and Reviews in Applied Sciences. 2011 Jun;7(3):339-50.

[27] Abd Rahman AH, Zukarnain ZA. Performance comparison of AODV, DSDV and I-DSDV routing protocols in mobile ad hoc networks. European Journal of Scientific Research. 2009 Jun;31(4):556-76.

[28] Baraković S, Kasapović S, Baraković J. Comparison of MANET routing protocols in different traffic and mobility models. Telfor Journal. 2010;2(1):8-12.

[29] Shah S, Khandre A, Shirole M, Bhole G. Performance evaluation of ad hoc routing protocols using NS2 simulation. InConf. of Mobile and Pervasive Computing 2008 Aug 7.

[30] Rao, B. P., & Murthy, M. B. Investigating Quality Metrics for Multimedia Traffic in OLSR Routing Protocol. International Journal of Electronics and Communication Engineering,2012. 6(9), 949-952.

[31] Huhtonen A. Comparing AODV and OLSR routing protocols. Telecommunications Software and Multimedia. 2004 Apr 26;26:1-9.

[32] Palta P, Goyal S. Comparison of OLSR and TORA routing protocols using OPNET Modeler. International Journal of Engineering Research and technology. 2012 Jul;1(5):984-90.

[33] Kannhavong B, Nakayama H, Kato N, Nemoto Y, Jamalipour A. Analysis of the node isolation attack against olsr-based mobile ad hoc networks. In2006 International Symposium on Computer Networks 2006 Jun 16 (pp. 30-35). IEEE.

[34] Tarek Sheltami and Hussein Mouftah "Comparative study of on demand and Cluster Based Routing protocols in MANETs", IEEE conference, pp. 291-295, 2003.

[35] Dhenakaran SS, Parvathavarthini A. An overview of routing protocols in mobile ad-hoc network. International Journal of Advanced Research in Computer Science and Software Engineering. 2013 Feb;3(2).

[36] Johnson D, Hu YC, Maltz D. RFC 4728: The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4.(2007).

[37] Johnson DB, Maltz DA, Broch J. DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking. 2001 Jan 8;5(1):139-72.

[38] Salem AO, Samara G, Alhmiedat T. Performance analysis of dynamic source routing protocol. 2017 Dec 13.

[39] Raju SR, Runkana K, Mungara J. ZRP versus AODV and DSR: A comprehensive study on ZRP performance. International Journal of Computer Applications. 2010 Feb;1(12):1-6.

[40] M.Asim and A.J. PullinM.Asim and A.J. Pullin, Comparison analysis of MAODDP with some other prominent wireless ad hoc routing protocols, in IBITE Computing., Liverpool Hope University. 2005

[41] Bakht H. Survey of routing protocols for mobile ad-hoc network. International Journal of Information and Communication Technology Research. 2011 Oct;1(6).

[42] Perkins C, Belding-Royer E, Das S. RFC3561: Ad hoc on-demand distance vector (AODV) routing. (2003)

[43] Lee, K. C., Lee, U., & Gerla, M. (2010), "Survey of Routing Protocols in Vehicular Ad Hoc Networks", Advances in Vehicular Ad-Hoc Networks: Developments and Challenge, Watfa, M. (Ed.), (pp. 149-170), 2010

[44] Sameswari V, Ramaraj E. Shortest route discovery using hybrid (AODV and OLSR) routing protocols in manet. InUGC sponsored national conference on data science and engineering-proceedings 2014 (pp. 273-279).

[45] Maurya PK, Sharma G, Sahu V, Roberts A, Srivastava M, Scholar MT. An overview of AODV routing protocol. International Journal of Modern Engineering Research (IJMER). 2012 May;2(3):728-32.

[46] Kaur H, Sahni V, Bala M. A survey of reactive, proactive and hybrid routing protocols in MANET: a review. network. 2013;4(3):498-500.

[47] Beijar N. Zone routing protocol (ZRP). Networking Laboratory, Helsinki University of Technology, Finland. 2002 Apr;9(1):12.

[48] Amouris KN, Papavassiliou S, Li M. A position-based multi-zone routing protocol for wide area mobile ad-hoc networks. In1999 IEEE 49th Vehicular Technology Conference (Cat. No. 99CH36363) 1999 May 16 (Vol. 2, pp. 1365-1369). IEEE.

[49] Kaur S, Kaur S. Analysis of zone routing protocol in MANET. International Journal of Research in Engineering and Technology. 2013 Sep;2(09):3.

[50] Chudasama JJ, Nayak A, Patel B. Performance comparison of ZRP Bordercasting using Multiple Unicasting vs Broadcasting. International Journal of Computer Applications. 2016; 975:8887.

[51] Bhoopathy, V.M., Frej, M.B., Amalorpavaraj, S.R., & Bhoopathy, A.M. Zone Routing Protocol (ZRP) - A Novel Routing Protocol for Vehicular Ad-hoc Networks. (2016)

[52] Pearlman MR, Haas ZJ, Mir SI. Using routing zones to support route maintenance in ad hoc networks. In2000 IEEE Wireless Communications and Networking Conference. Conference Record (Cat. No. 00TH8540) 2000 Sep 23 (Vol. 3, pp. 1280-1285). IEEE.

[53] Sinha S, Sen B. Effect of varying node density and routing zone radius in ZRP: a simulation-based approach. International Journal on Computer Science and Engineering. 2012 Jun 1;4(6):1069.

[54] Meenakshi VK, Singh K. Simulation & Performance Analysis of Proactive, Reactive & Hybrid Routing Protocols in MANET. International Journal of Advanced Research in Computer Science and Software Engineering, vol2. 2012 Jul.

[55] M.H. Badji, M.N. Badji. Etude des réseaux Ad Hoc par la théorie des jeux. Bouira university. (2020).

ملخص

أحدثت الشبكات اللاسلكية ثورة في الاتصال من خلال تمكين الاتصال دون الحاجة إلى الكابلات المادية. أنها توفر وصولاً مرنًا ومريحًا للمعلومات والخدمات، وتدعم مختلف الأجهزة والتطبيقات. من بين الشبكات اللاسلكية، تبرز الشبكات المخصصة كشبكات ذاتية التكوين مكونة من أجهزة لاسلكية دون الحاجة إلى بنية تحتية موجودة مسبقًا. ولتقديم البيانات، نستخدم بروتوكولات التوجيه.

حيث قمنا بتقييم هذه البروتوكولات بناءً على مقاييس مختلفة من خلال سيناريوهات مختلفة AODV OLSR,

.,DSDV

الكلمات المفتاحية: ةصصخملا تاكبشلا ، OLSR ، DSDV ، AODV ، هيجوتلا تلاوكوتورب

Résumé

Les réseaux sans fil ont révolutionné les communications en permettant une connectivité sans câbles physiques. Ils offrent un accès flexible et pratique à l'information et aux services, prenant en charge divers appareils et applications. Parmi les réseaux sans fil, les réseaux ad hoc se distinguent en tant que réseaux autoconfigurants formés par des appareils sans infrastructure préexistante, et pour établir la communication, nous utilisons des protocoles et des algorithmes de routage. Dans notre étude comparative, nous avons analysé certains de ces protocoles de routage, notamment Ad hoc On-Demand Distance Vector (AODV), Destination-Sequenced Distance Vector (DSDV) et Optimized Link-State Routing (OLSR), en évaluant ces protocoles selon différents critères à travers différents scénarios.

Mots clés : Protocoles de routage, AODV, DSDV, OLSR, Réseaux ad hoc.

Abstract

Wireless networks have revolutionized communication by eliminating the need for physical cables and providing flexible access to information and services. Ad hoc networks, specifically, are self-configuring networks formed by wireless devices without a pre-existing infrastructure. To establish communication in ad hoc networks, routing protocols and algorithms are used. In our study, we compared routing protocols such as Ad hoc On-Demand Distance Vector (AODV), Destination-Sequenced Distance Vector (DSDV), and Optimized Link-State Routing (OLSR) using various metrics and scenarios to evaluate their performance and effectiveness.

Key Words: Routing protocols, AODV, DSDV, OLSR, Ad hoc Networks.