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 -

وزارة التعليم العالي والبحث العلمي
جامعة أكلي محند أولحاج
- البويرة -

Faculté des Sciences et des Sciences Appliquées

كلية العلوم والعلوم التطبيقية

Référence : ……………/MM/2021

المرجع:……/م م/ 2021

Master Thesis

Presented to

Department : Electrical Engineering
Domain : Sciences and Technologies
Branch : Telecommunications
Speciality : Telecommunications systems

Presented by:

RAHAL CHRIF

Theme

QoS, Information routing in wireless networks

Presented on:**30/10 /2021**

In front of the jury:

Mr :	Issaouni Salim	President
Bilal SAOUD	Boucenna Lamine	Examinator

University Year: 2020-2021

Acknowledgements

In term of this work:

I would first like to thank ALLAH almighty and master of the universe who gave me the necessary strength, the strong and patience to get this job done. I would like to warmly thank my dear parents. I also thank my promoter: Dr. SAOUD BILAL for the help he gave me and for his availability, as well for his precious advice I would like to express my gratitude to my teachers in the electrical engineering department of the university of Bouira. I would like to express my deeper thanks to the jury members for their participation in the judgment of my work. Finally, I send my thanks to all those who have helped from near or far.

Abstract

Today, wireless networks are very used in our daily life. Among these wireless networks we have Ad Hoc networks (MANET). Ad Hoc network can be defined as a collection of electronic devices. They can be used for many purposes. The most important task to ensure the transmission of data in Ad Hoc network is the routing task. We can find many routing protocols. In our study, we have studied the problematic of routing in Ad Hoc networks. Ad Hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporally-Ordered Routing Algorithm (TORA), Optimized Link State Routing (OLSR) have been chosen in our study. We have evaluated these protocols based on throughput, media access delay, network load, delay and traffic dropped metric. The simulation has been done on Opnet simulator.

Keywords: MANET, AODV, DSR, OLSR, TORA, Routing Protocols.

Résumé

Aujourd'hui, les réseaux sans fil sont très utilisés dans notre vie quotidienne. Parmi ces réseaux sans fil, nous avons les réseaux Ad Hoc (MANET). Le réseau Ad Hoc peut être défini comme un ensemble d'appareils électroniques. Ils peuvent être utilisés à de nombreuses buts. La tâche la plus importante pour assurer la transmission des données dans le réseau Ad Hoc est la tâche de routage. Nous pouvons trouver de nombreux protocoles de routage. Dans notre étude, nous avons étudié la problématique du routage dans les réseaux Ad Hoc. Ad Hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporally-Ordering Routing Algorithm (TORA), Optimized Link State Routing (OLSR) ont été choisis dans notre étude. Nous avons évalué ces protocoles en fonction du débit, du délai d'accès au support, de la charge du réseau, du délai et de la métrique de perte de trafic. La simulation a été faite sur le simulateur Opnet.

Mots clés : MANET, AODV, DSR, OLSR, TORA, Protocoles de routage.

Contents

Chapter 3: Simulation and Results

List of Figures

List of Tables

Acronyms and Symbols List

AODV	Ad hoc on Demand Distance Vector Routing
MANET	Mobile Ad hoc Network
OLSR	Optimized Link State Routing
MPR	Multipoint Relays
WLAN	Wireless Local Area Networks
OPNET	Optimized Network Engineering Tool
RREQ	Route Request
RREP	Route Reply
RERR	Route Error
DSR	Dynamic Source Routing
TORA	Temporally Ordered Routing Algorithm
WSN	Wireless sensor networks
PAN	Wireless Personal-Area Network
LAN	Wireless Local-Area Network
MAN	Wireless Metropolitan-Area Network
WAN	Wireless Wide-Area Network
WISP	Wireless Internet Service Providers
DSDV	Destination-Sequenced Distance-Vector
DYMO	Dynamic MANET On-demand
CBR	Constant Bit Rate
ZRP	Zone Routing Protocol
DAG	Directed cyclic graph
APR	Alternate Path Routing

AOMDV	Ad hoc On-demand Multipath Distance Vector Routing
SMR	Split Multipath Routing
QoS	Quality of service

General Introduction

The network structure is changing rapidly in recent years. The only network available 40 years ago was the cable network. The emergence of wireless networks has come a long way in addressing the growing needs of the service. The focus of research and development has almost changed from wired networks to wireless networks. Wireless network strategy limitations such as high error rates, power limits, bandwidth issues, etc. It has not stopped the growth of wireless networks.

The Ad-hoc mobile network (MANET) is a highly sought after field for wireless networks. MANET has mobile devices or users , referred to as individual nodes equipped with radio transmitter and receiver. MANET is an impermanent organization of wireless nodes with no proper framework. ,no links, No devoted switches passageways and servers. Mobile nodes in the topology can communicate directly with each other or other central nodes play the role of routers between the sender node and the receiver. Therefore, all nodes act as a router for transferring packets to other nodes. One of the main areas of research in the Ad Hoc network is the routing task. Hot topic. Many routing protocols have been made over the years.

In this work, we have been interested in routing problematic in Ad Hoc network. We have studied this problematic by evaluating some very known protocols in Ad Hoc network. We have chosen AODV, DSR, TORA, and OLSR protocols. We have studied each protocol by giving it is mechanism to establish a route between a source and a destination. Then we have compared them based on some metrics. We have used the most important metrics in wireless networks. Throughput, delay, network load, media access delay and traffic dropped have been used in our study. Our study has been done on OPNET Modeler 14.5 simulator.

Our thesis is organized as follow:

- The first chapter presents Ad Hoc networks, the different types and characteristics of Ad Hoc networks.

-In the second chapter, we presented an overview of the different routing protocols.

-In the third chapter, we described the simulation environment, discussed simulation results and finally drawn a conclusion.

Chapter 1: Wireless networks introduction

1.1- Introduction

A wireless network is a flexible data communication system, which uses wireless media as a radio frequency technology to transmit and receive data over the air, reducing the need for wired connectivity. Wireless networks are used to upgrade and replace wired networks. They are widely used to provide the last few stages of communication between a mobile user and a wireless network.

Wireless networks utilize electromagnetic waves to move data from one user to another without the need of any actual physical medium or association. Radio waves are frequently referred to as radio carriers because they simply do the job of bringing power to the remote receiver. The information transmitted is placed at the top of the radio carrier so that it can be accurately extracted from the receiver. Once the info has been modulated to the radio carrier, the radio wave takes quite one frequency, because the frequency or bit rate of modulating information adds to the carrier. Multiple radio carriers are often within the same space at an equivalent time without interruption when radio waves are transmitted on a different frequency . To extract data, the receiving set tunes in one frequency while rejecting all other frequencies. The modulated signal received is then demodulated followed by the extraction of the data from the signal

In this chapter we will give some very important concepts to understand the field of wireless networks. We will start by introducing wireless networks. Then, features of wireless networks will be introduced. Next, classification will be given and we will end the chapter with some applications of wireless networks.

1.2-Definition of wireless networks

A wireless network can be seen as a computer network that procedures wireless data connections between network hosts [1]. Wireless networking is a way which allows homes, telecommunications networks and business installations to avoid the process of using cables into and outside buildings. It avoids also the connection between the different equipment locations [1]. Telecommunications networks are usually instigated and directed by the use of radio communication. This employment takes place precisely at the physical level (layer) of the OSI model network structure [1].

There are many samples of wireless networks. Among these samples we have , wireless local area networks (WLANs), cell phone networks ,wireless sensor networks, satellite communication networks, Ad Hoc networks and terrestrial microwave networks [1].

1.3-Features of wireless networks

As stated earlier, a wireless network allows people to access wireless apps , information, communicate and. This feature provides freedom of movement and the ability to extend applications to different parts of a building, city, or almost anywhere in the world. Wireless networks have many specific features [1]. Among these are the following:

-Increased efficiency: Advanced data communication leads to faster information transfer within businesses and between partners and customers. For example, retailers can remotely check stock rates and prices during sales calls.

-Better coverage and mobility: cables tie you in one place. Wireless means you have the freedom to change your location without losing your connection,

-Flexibility: wireless office workers can be networked without sitting on dedicated computers, and can continue to do productive work while out of the office.

Cost savings: Wireless networks can be simpler and cheaper to install.

-Adaptability: Fast and easy integration of devices in the network, with high flexibility when changing installation.

-New opportunities / applications: Wireless communication allow you to offer new products or services. For example, many train stations, hotels, airports departure lounges, cafes and restaurants have installed wireless hot spots services to allow mobile users to connect their devices to their home offices while traveling.

1.4-Classification of wireless networks

Wireless networks fall under numerous categories, reliant on the dimensions of the physical area that they are able to provide a full coverage on [1]. The resulting types of wireless networks gratify varied user requirements:

- Wireless Personal-Area Network (PAN)
- Wireless Local-Area Network (LAN)
- Wireless Metropolitan-Area Network (MAN)
- Wireless Wide-Area Network (WAN)

These terms are simply an leeway of the more basic methods of wired networks (such as LAN or WAN) that have been in use for years before wireless networks originated about.

Table 1-1 shows a short-term comparison of these types of wireless networks. Each type of wireless network has complementary attributes that satisfy different requirements. The subsequent sections briefly explore each wireless network

Type	Coverage	Performance	Standards	Applications
Wireless PAN	Within reach of a person	Moderate	Bluetooth, IEEE 802.15, and IrDa	Cable replacement for peripherals.
Wireless LAN	Within a building or campus	High	IEEE 802.11, Wi-Fi, and HiperLAN	Mobile extension of wired networks.
Wireless MAN	Within a city	High	Proprietary, IEEE 802.16, and WIMAX	Fixed wireless between homes and businesses and the Internet.
Wireless WAN	Worldwide	Low	CDPD and Cellular 2G, 2.5G, and 3G	Mobile access to the Internet from outdoor areas.

Table 1-1. Classification of wireless networks.

1.4.1-Wireless PANs: As Figure 1-1 shows, this type have moderately short range (up to 50 meters) and are most effective for fulfilling necessities within a small room or personal area [1]. The performance of wireless PANs is adequate, with data rates up to 2 Mbps. These attributes satisfy needs for replacing cables in many situations.

Figure 1.1: Wireless PAN example.

1.4.2-Wireless LANs: Wireless LANs supply high performance within and around office buildings, factories, and homes [1] (See Figure 1.2). Users in these areas typically have laptops, PCs, and PDAs with large screens and processors that support higher-end applications. Wireless LANs efficiently satisfy connectivity requirements for these types of computer devices.

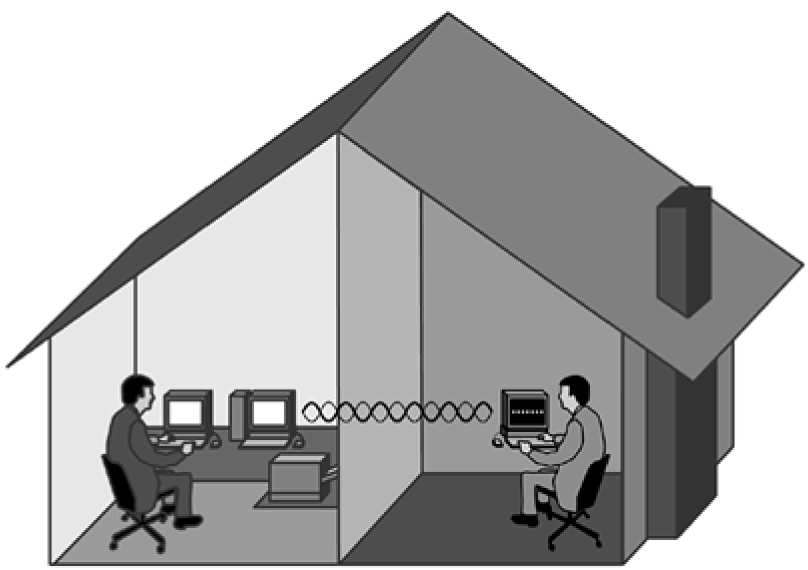


Figure 1.2: Wireless LAN example.

Wireless LANs easily provide levels of performance that enable the higher-end applications to run smoothly. For instance, the users of wireless LAN can stream video from a server or simply view a large e-mail attachment With bitrates of up to 54 Mbps, a wireless LAN can be just enough for any office or home network application.

Wireless LANs are similar to traditional wired Ethernet LANs in their performance, components, costs, and operation. IEEE 802.11 [1] is the most prevalent standard for wireless LANs, with versions operating in the 2.4-GHz and 5-GHz frequency bands.

1.4.3-Wireless MANs: Wireless MANs comprehend areas that are the magnitude of cities [1]. In utmost cases, applications include fixed connectivity, but some operations enable mobility. For example, a hospital can deploy a wireless MAN to provide data communications between the main hospital facility and a remote clinic. Or, a power utility company can install a wireless MAN throughout a city to supply access to work orders from various sites. As a outcome, it can link existing network infrastructures together or allow mobile users to interconnect with an existing network infrastructure.

in cities and rural areas wireless MANs is provided by Wireless Internet Service Providers (WISPs). As Figure 1.3 demonstrates, WISP make available fixed wireless connections for homes and companies. It offers important advantages when it’s impossible to install traditional wired connections (such as Digital Subscriber Line [DSL] and cable modem) [1]. Wireless MANs are effective when right-of-way restrictions make wired systems impossible or too expensive.

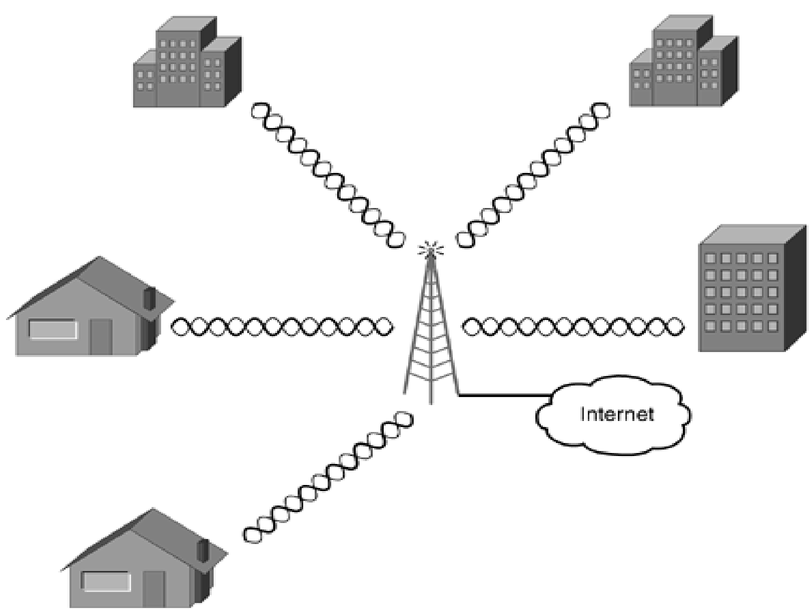


Figure 1.3. Wireless MAN example.

Wireless MAN performance varies. Networks between constructions using infrared light can range 100 Gbps or more; although radio links over a 20-mile distance could offer only 100 kbps. The real performance depends on the choice from a varied mixture of components and technologies.

1.4.4-Wireless WANs: Wireless WANs offer mobile applications covering an outsized area, such as a nation or continent [1]. Because of economies of scale, a telecommunications operator can feasibly deploy the relatively expensive wireless WAN infrastructure to provide long-range connectivity for a large customer base. The expenses like as deployment are often spread across a lot of users, resulting in a diminished subscriber fees.

Wireless WANs, as Figure 1.4 shows, have approximately a worldwide coverage over the collaboration of multiple telecommunications companies. Well-established roaming arrangements amongst telecommunications operators allow continuous connections for instantaneous mobile data communications. By paying only one telecommunications service provider, a user can acquire access to a limited Internet services over a wireless WAN from almost anywhere within the world.

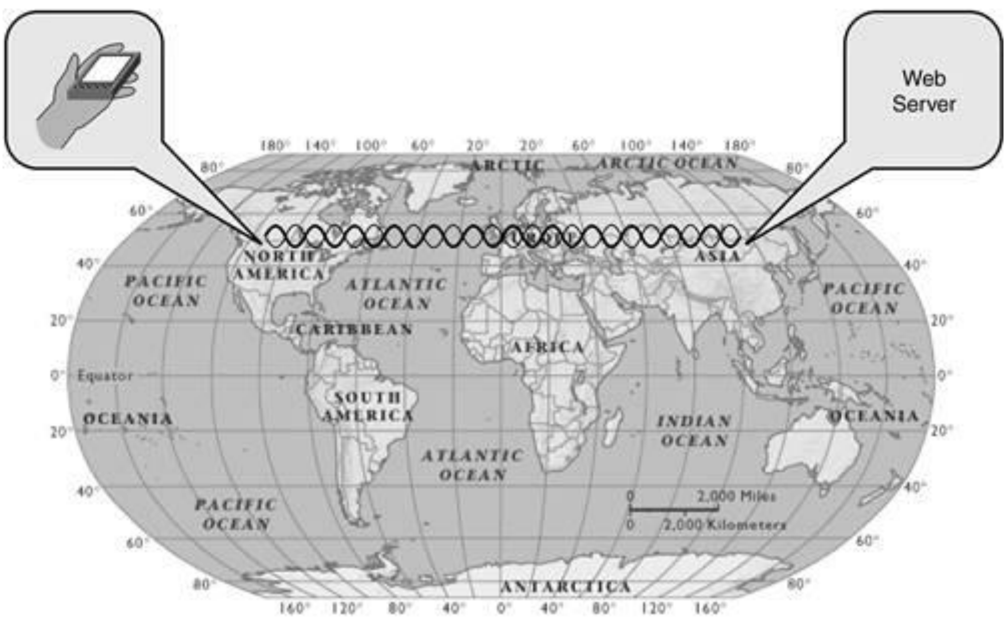


Figure 1.4: Wireless WAN Mobile Application.

1.5-MANET (Mobile Ad Hoc Network)

A Mobile Ad hoc network (MANET) is a sort of wireless ad hoc network, which has self-configuring mobile devices with self-configuration competence and is a collection of mobile routers connected by wireless links forming a network. Network nodes in MANETs are allowed to move freely, randomly and organize themselves indiscriminately [2]. In ad hoc network, nodes do not have a priori knowledge of topology of network around them; the route and all network activities such as discovering the topology and delivering data packets have to be executed by the nodes themselves, either individually or collectively. In MANETs every node is a potential router for other nodes. [3]. In this case, MANET routing protocols should be studied and utilized. Two kinds of routing protocols are more important and popular recently, one is proactive routing protocol. Example of proactive routing protocol is OLSR (Optimized Link State Routing Protocol) [4]. And the other is a reactive routing protocol. Example of reactive routing protocol is AODV (Ad hoc On-Demand Distance Vector Routing Protocol) [5].

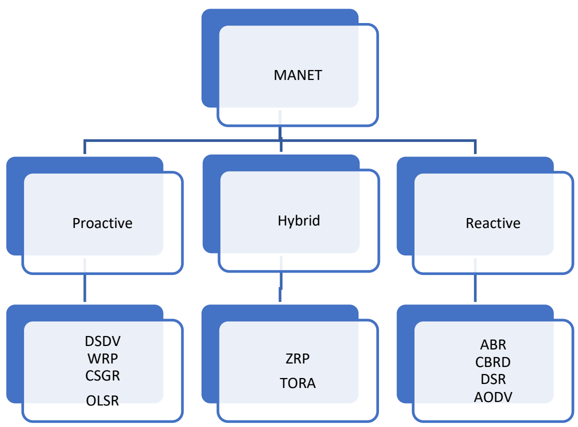


Figure 1.5 MANET protocol structure

1.5.1-Features of MANET

The topology is highly dynamic and arbitrary in mobile ad hoc networks,. Adding, the

distribution of nodes and their ability of self-organizing play an important part.

The main features can be summed up as follow [6]:

- High dynamic network topology and recurrent changes in the organization structure might be hard to foresee.

- Mobile ad hoc networks are built on wireless links, most of the times they have a lower capacity than their wired corresponding item.

- Physical security is imperfect due to the wireless nature of the transmissions.

- they are affected by higher loss rates, and can experience higher delays and jitter than the cable networks due to the nature wireless transmission.

- Their nodes depend on batteries or other exhaustible power materials for their energy.

1.6-Application of MANET

The wireless ad hoc networks and their variations can be applied in different applications, including

mesh networks, opportunistic networks, vehicular networks and wireless sensor networks. In this section, we will present some applications of Ad Hoc network.

1.6.1- Mesh Networks

Unlike pure MANETs, a mesh network introduces a hierarchy in the network architecture, they are built upon a combination of fixed and mobile nodes interconnected via wireless links to form a multihop ad hoc network. [7] The wireless mesh networks are the best solutions to produce both indoor and outdoor broadband wireless connectivity in urban, suburban, and rural environments without the necessity for very costly wired network infrastructure.

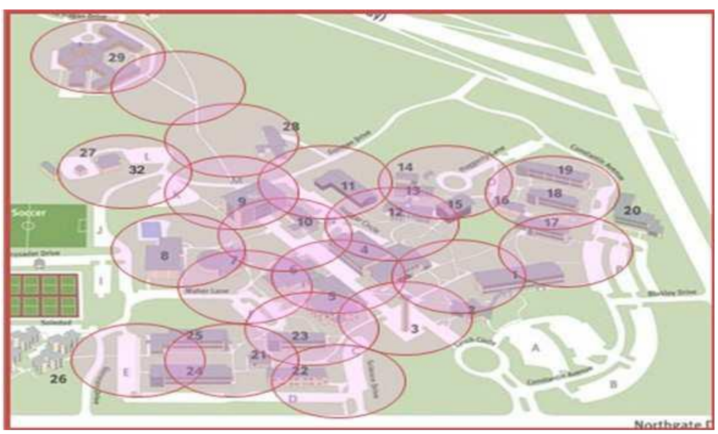


Figure 1.6 presents the coverage of the network in the campus [7]

1.6.2- Opportunistic networks

Opportunistic networks are one among the foremost interesting evolutions of MANETs. In this type of networks, the communication between the mobile node is enabled with one another whether or not a route connecting them never exists. Moreover, nodes aren't presumed to acquire or possess any information about the topology, which is critical in old-style MANET routing protocols [8]. within the network, any possible node is often opportunistically be used as next hop to bring the message closer to the destination.

1.6.3-Vehicular ad hoc Networks

VANETs use ad hoc communications for performing structured driver assistance and car safety. The communications contain data from other cars and from the roadside. The research objectives are to add more information and supply it to the drivers this information involves emergency events and obstacles on the road, mainly due to the limitations of line-of-sight and the delays in the huge processing tasks. VANET are often accustomed communicate premonitions, notification of emergencies, and warnings about traffic conditions. It will be utilized for appropriating data about street conditions and support, climate figures, or other pertinent information dissemination necessities between vehicles. VANET empower the use of cutting edge driver help frameworks (ADAS) and vehicular-to-vehicular (V2V) interchanges, additionally called bury vehicular correspondences (IVC), besides as correspondence with side of the road foundation.. VANET have a plus compared to traditional MANET. They rarely have constraints associated with the capacities of the devices.

1.6.4-Wireless Sensor Networks

It benefits from the leap forward of the computing technology, which led to the gathering of minor,

wireless, smart sensor nodes with battery powered. These nodes are active devices with communication and computing abilities that not only sample world phenomena but also can filter, share, combine, and operate the info they sense [7]. WSN is widely used in Health monitoring, Tracking applications and Intelligent home environment.

1.7-Conclusion

In this chapter we have presented wireless networks in generally. We have started by giving a definition of a wireless network. Then we have presented Ad Hoc networks. Today, wireless networks can be used for different purposes. We have ended our chapter by some examples of application of Ad Hoc networks. To ensure communication between devices in Ad hoc topology we need a routing protocol. There are many routing protocols that have been proposed for MANET. In the next, chapter we will present some of them.

Chapter 2: Routing protocols in Ad Hoc networks

2.1- Introduction

Ad hoc wireless networks accomplish the hard task of multi-hop communications in an environment without a dedicated infrastructure, with autonomous, mobile nodes and changing topology. The lack of infrastructure in Ad hoc networks poses new challenges for algorithms where the network is created by a set of wireless mobile nodes that dynamically make a brief network without the use of any existing network infrastructure or central administration.

There are two main routing protocols widely known : table-based protocols which is called proactive protocols and on-demand protocols called reactive protocols. In reactive protocols, the route is calculated by the nodes only when it's required. Often, caches are used to minimize route discovery. In proactive protocols, each node maintains a routing table that contains routes across all and other nodes in the network. Nodes must periodically exchange messages with routing information to keep routing tables updated regularly.

In addition, other hybrid protocols are proposed. this is because both the reactive and proactive routing has certain advantages and disadvantages that make them suitable for specific situations. Hybrid methods try and take advantage of both of these and achieve better performance.

2.2-Reactive Routing Protocols

Because reactive routing only tries to find a route, when necessary, it's believed that it's more scalable to dynamic, large networks. When a node needs a route to a different node, it initiates a route discovery process to find a route. Generally, it consists of the subsequent two main phases:

2.2.1-Route discovery: it's the procedure of looking and establishing a route between two nodes, whether directly accessible within wireless transmission scope or reachable through one or more intermediate network hops over other nodes.

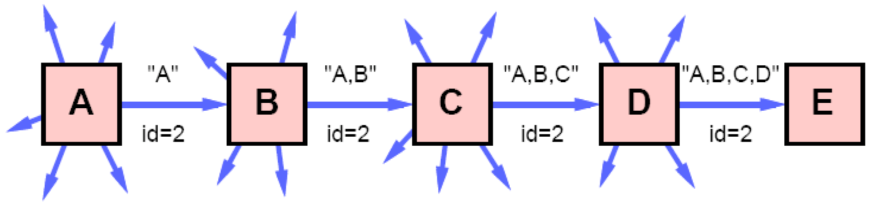


Figure 2.1: Route Discovery example: from Node A to Node E [9]

2.2.2-Route maintenance: it's the method of repairing a broken route or finding a brand-new route within the presence of a route failure. It's a process that monitors the state of the route and notifies the sender of any errors in routing. The DSR and ADOV routing protocols Two of the most extensively used reactive routing protocols are presented.

2.2.3- Dynamic Source Routing

Source routing: it's a routing procedure inside which the sender of the data in form of a packet discovers and fixes the entire sequence of nodes through which to advance the data packet; the sender of a packet regulates the complete sequence of nodes through which to forward the packet; the sender unequivocally record this route inside the packet's header, recognizing each forwarding "hop" by the address of the succeeding node to the terminus host. The DSR [9] is intended to be used in the wireless settings of an Ad Hoc network. there's no periodic router ad messages in the interior of the protocol. As an alternative, when a host needs a route to an alternate host, it dynamically finds one supported cached information and on the results of a route discovery protocol.

2.2.3.1-Route Discovery

When node S originates a brand new packet destined to another Node D, it places within the header of the packet a source route giving the sequence of hops that the packet should follow on its way to D. Normally, S will obtain an appropriate source route by searching it's Route Cache of routes previously learned. But if no route is found in its cache, it'll initiate the Route Discovery protocol to dynamically find a brand new route to D. during this case, we call S the initiator and D the target of Route Discovery. For instance, in Figure 2.1, node A is attempting to find a route to node E .

A diffuses a ROUTE REQUEST message as 1 local broadcast packet, which comprehends a unique exclusive request id. Once another node obtains a ROUTE REQUEST, if it's the goal of the Route Discovery, it sends back a ROUTE REPLY message to the originator. If not, this node adds its own address to the route record and appends it inside the ROUTE REQUEST message and broadcasts it by the transmission of it as a local broadcast packet, till the packet reaches its destination (node E during this example). When the packet gets to the destination, the node will return a ROUTE REPLY message. The way the ROUTE REPLY message is returned are often starting a replacement Route Discovery or simply using the reversed sequence of the nodes depends on the networks situation (unidirectional or bidirectional). When initiating a Route Discovery, the sending node saves a replica of the first packet in a very local buffer called the Send buffer. The Send buffer contains a duplicate of every packet that can't be transmitted by this node because it doesn't yet have a source route to the packet's destination. While a packet remains within the Send buffer, the node should occasionally initiate a new Route Discovery. There are some additional features introduced in [18] to improve the performance of Route Discovery:

• Caching overheard routing information;

• Replying to ROUTE REQUESTs using Cached Routes;

• Preventing ROUTE REPLY Storms;

•ROUTE REQUEST hop limits.

2.2.3.2-Route Maintenance:

When originating or forwarding a packet employing a source route, each node transmitting the packet is accountable for confirming that the packet has been received by the following hop along the source route; the packet is retransmitted (up to a maximum number of attempts) until this confirmation of receipt is received. If the packet is retransmitted by some hop the maximum number of times and no receipt confirmation is received, this node returns a ROUTE ERROR message to the first sender of the packet, identifying the link over which the packet couldn't be forwarded. The source node then removes this broken link from its cache, and use another route within the Route Cache (if it has one), or starts a brand new route Discovery. For DSR, there are several advantages: First, unlike conventional routing protocols, it uses no periodic routing advertisement messages, thereby reducing network bandwidth overhead, particularly during periods when little or no significant host movement is going down. Second, it does not require transmissions between hosts for bidirectional work. And furthermore, it's ready to adapt quickly to changes like host movement, yet requires no routing protocol overhead during periods which such changes don't occur. However, The Route Maintenance protocol does not locally repair a broken link. The broken link is only communicated to the initiator. The DSR protocol is strictly efficient in MANETs with less than 200 nodes. There are also some additional features introduced in [18] to improve the performance of Route Maintenance:

• Packet salvaging;

• Automatic route shortening;

• Increased spreading of ROUTE ERROR messages;

• Caching negative information.

For DSR, there are several advantages: First, unlike conventional routing protocols, it uses no periodic routing advertisement messages, thereby reducing network bandwidth overhead, particularly during periods when little or no significant host movement is going down. Second, it does not require transmissions between hosts to function bidirectionally. And moreover, it's capable off adapting quickly to variations similar to host movements, yet necessitates no routing protocol overhead throughout periods in which such variations don't occur. Nevertheless, The Route Maintenance protocol doesn't have the capacity to locally have a reparation on a broken link. This link is just transferred to the originator. This protocol is basically efficient in MANETs with a size that is less than 200 nodes. Difficulties appear by in a super-fast movements of more hosts so that the nodes could only move around in this instance with a moderate speed. Flooding the network can cause collisions between the packets. Also, there's always a tiny low time delay at the start of a replacement connection because the initiator must first find the route to the target.

2.2.4-Ad hoc On-Demand Distance Vector Routing

AODV [10,11, 12] is an enhancement of Destination-Sequenced Distance-Vector (DSDV) routing protocol the algorithm which contains the characteristics of DSDV and SR. Each node keeps a route table that encompasses routing data yet doesn't automatically uphold routes to each node in the network and greatly minimize the necessities of system-wide transmissions.

2.2.4.1-Route Discovery

Same as in DSR, the route discovery method is started when a source requests a route to a destination and it doesn't contain this specific route in its routing table. The source node will start the flooding operation of the network with a RREQ packet stipulating the destination that is required to have a route . When the destination obtains the RREQ packet, the node creates a RREP packet, which will be distributed again to the source with the reverse path. Every node lengthways the reverse path build up a forward pointer to the node it received the RREP from. This makes up a forward path from the source to the destination as shown in the figure 2.2.

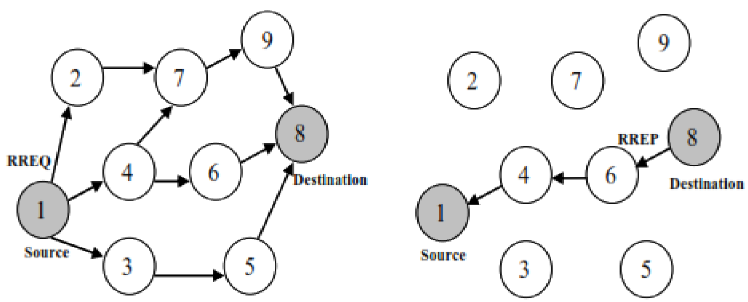


Figure.2.2 AODV route discovery process [11]

2.2.4.2-Route Maintenance:

As soon as a node identifies a broken link in the same time when it's attempting to advance a packet to the next hop, it produces a RERR packet that is directed to all sources utilizing the broken link. The kind of packet deletes all routes using the connection and the links on route. If a source obtains a RERR packet while a route to the destination is been required, it will start a new route discovery procedure. Some of AODV advantages consists in : routing without loops, optional multicast and compact control overhead. But in the same time, delay is caused by route discovery process and bidirectional connections are needed.

2.3- Proactive Routing Protocols

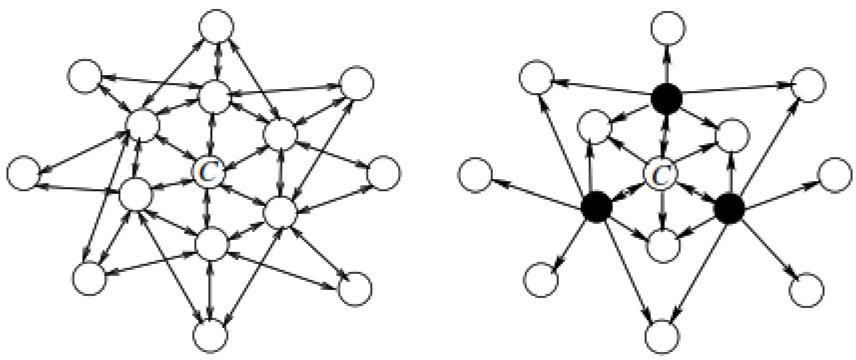
They are also known as table-driven Routing, characterized by every node maintaining an individual routing table which encompasses routing information for every node in the system. All node upholds an updated and a consistent routing information with the use of control messages that are sent periodically among the nodes to keep their routing tables updated. This kind of protocols are known by the usage of link-state routing algorithms which often flood the link data about its neighbors. the disadvantage of this protocol consists on the nodes are constantly maintaining an updated table. a number of the dominant proactive routing protocols are DSDV [11] and OLSR [13,14].

2.3.1-Destination-Sequenced Distance-Vector (DSDV)

Perkins and Bhagwat introduced [15] the Destination-Sequenced Distance-Vector (DSDV), one of Ad Hoc's first routing protocols. like most distance-vector routing protocols, it depends on the Bellman-Ford algorithm. Every single mobile node preserves a routing table that holds possible destinations inside the network and their distance using hop as counts. Every entry similarly retains track of the sequence number allocated by the destination. Sequence numbers are used to identify old entries and thus avoid loops. To maintain flexibility and consistency of the routing table, route updates are periodically transmitted across the network. 2 types of updates are effective; full dump and incremental. The entire route table is sent to the neighbors by the Full dumps and might necessitate numerous network protocol data units (NPDUs). The Incremental updates are smaller (must fit in a sole packet) and are to diffuse those entries from the routing table which have altered since the last full dump update. When a network is stable, incremental updates are forwarded and full dump are usually infrequent. On the opposite hand, full dumps are going to be more frequent in a very fast paced network. Moreover, in regards to the routing table information, every route update packet comprehends a fixed sequence number allocated by the source. The route branded with the utmost fresh (highest number) sequence number is used. The shortest route is chosen if any two routes.

2.3.2-Optimized Link State Routing

Optimized link state routing OLSR [16] is a proactive protocol in which, each node intermittently broadcasts its routing table, allowing each node to create an inclusive view of the network topology. The episodic nature of this protocol creates a large amount of overhead and so as to scale back overhead, it limits the quantity of mobile nodes that can forward network wide traffic and for this purpose it uses multi point relays (MPRs), which are responsible for optimization for flooding operation and advancing routing messages. The Mobile nodes, which are designated as MPRs could send control traffic and decreases the scale of control messages. A node choses MPR’s, in a way that , it must attain to each two-hop neighbor via a least of single MPR, after that it can onward packets, if control traffic gained from a preceding hop has designated the present node as an MPR. Because of mobility, route modification and topology deviations are very recurrent so the topology control (TC) messages are spread through the whole the network. All mobile nodes preserve the routing table that encompasses routes to any or all accessible and nearby destination nodes. This type of protocol does not alert the source instantly after the detection of a broken link. The source node will acknowledge that the route is broken, when the intermediate node broadcasts its next packets. Thus, by determining the trail through the multipoint relays, it's possible to hold away the difficulties experienced during the packet transmission over a unidirectional link.



(a) (b)

Figure 2.3 Illustration for simple flooding and flooding through multipoint relays.[16]

(a) This figure shows simple flooding. Every node that receives the packet initially sent by the central node C broadcasts it again. A double arrow between a pair of nodes indicates the receipt of broadcasts from each other (we have assumed symmetric communication links). (b) The number of packets has been reduced considerably by using the multipoint relay nodes (dark nodes). These nodes are one-hop neighbors of C and collectively neighbors of all the two-hop neighbors of C. The total number of packets is reduced considerably as the one-hop neighbors that are not multipoint relays do not broadcast.

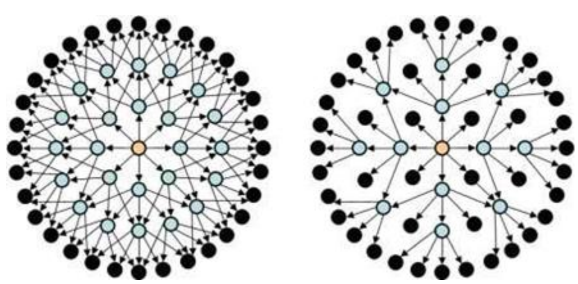


Figure 2.4. Flooding without MPR (left) and with MPR (right) [16]

The protocol functioning includes:

• Neighbor sensing. Each node periodically broadcast its HELLO messages about its neighbor and their link status. These control messages are only one-hop and permit each node to find out the knowledge of its neighbors up to 2 hops.

• Multipoint Relay selection. The MPR set is designed in a style to comprehend a subset of one hop neighbors which shelters all the 2 hop neighbors.

• The declaration of information in MPR. so as to create the intra-forwarding database needed for routing packets, each broadcasts specific control messages called Topology Control (TC) messages. A TC message is scattered sporadically by each node in the network to assert its MPR Selector set. Every node of the network upholds a topology table, through which it collects the info about the topology of the network gained from the TC messages.

• Routing table calculation. Every node preserves a routing table that lets it route the packets for other terminuses in the network. Since the routing table depend on the information confined in the neighbor table and even the topology table, when one of this tables is altered, the routing table is reconsidered to update the route information. The shortest path algorithm is used to induce the route from source to the destination.

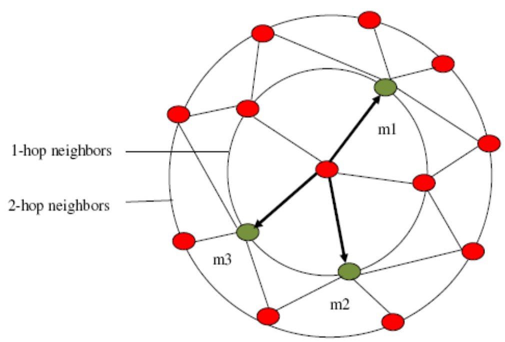


Figure 2.5: -Multipoint Relays of the OLSR network [17]

OLSRv2 OLSR version 2 (OLSRv2) has the identical algorithm and ideas as OLSRv1. Being modular by design, OLSRv2 is formed up from variety of generalized building blocks, standardized independently and applicable also for other MANET protocols. it's simpler and more efficient than OLSRv1, and includes a more modular and extensible architecture:

• RFC 5148 - Jitter Considerations in Mobile ad hoc Networks [21],

• RFC 5444 - Generalized MANET Packet / Message Format [22] and

• RFC 5497 - Representing Multi-Value Time in Mobile ad hoc Networks (MANETs) [23]

are published as RFCs, with the remaining constituent parts,

• MANET Neighborhood Discovery Protocol [24],

• OLSRv2 [25]

being in the final phases of standardization. The multipath and its compatibility that we suggest can also occur as supplementary components in the OLSRv2 framework.

2.4-Reactive Routing vs. Proactive Routing

At the instant, there are two protocols mainly discussed on the IETF standard track:

• Dynamic MANET On-demand (DYMO) [19] routing is the successor to AODV. So, it shares the reactive feature of its ancestor. Compared to AODV, DYMO has TLVs to permit for extensibility and allows a route to be improved by changing in response to superior routing information.

• OLSRv2, as already introduced, is the successor to OLSRv1.

They represent the reactive and proactive protocols respectively within the standardization of MANET routing protocols. The performance evaluation in (20) shows that the traffic load, the mobile node mobility, and therefore the network density all have an effect on the performance of the routing protocol. The proactive protocol offers better performances for CBR (Constant Bit Rate) sources provided that it guarantees lowest delay and jitter. But it consumes more bandwidth. And when the mobility is low, the reactive protocol performances low delay and overhead.

2.5-Hybrid Routing Protocols

Hybrid Protocols [26,27] are the combination of both i.e., Table-Driven and On-Demand protocols. These protocols take the advantage of best features of both the above mentioned protocols. They take advantage of the classified network construction and permit the nodes with near proximity to cooperate to make some sort of backbone, consequently expanding scalability and decreasing route discovery [28]. Nodes in the interior a particular geographical region are supposed to be inside the routing zone of the given node. For routing inside this zone, Proactive i.e., table-driven approach is utilized. For nodes that are situated in the external of this zone, Reactive i.e., an on demand approach is employed. So, in Hybrid Routing Protocols, the route is established with proactive routes and uses reactive flooding for brand new mobile nodes [29]. This protocols, some of the features of proactive and some of the characteristics of reactive protocols are mixed, by upholding intra-zone information proactively and inter-zone information reactively, into one to bring better solution for mobile ad hoc networks [28].

2.5.1-Zone Routing Protocol

ZRP [17] divides the topology into zones and uses different routing protocols within and between the zones depending on their weaknesses and strengths. In ZRP every node integrates a predefined zone centered at itself. A zone is maintained around every node in ZRP which involve of all nodes within ‘k’ hops far-off from that node. Proactive routing is employed within the zone whereas reactive routing is employed amongst zones. For data delivery, it is checked whether the destination node exists within the zone or not. If yes, data is forwarded directly otherwise RREQ packet is directed to border nodes. Border nodes look in their own zones for end point. If found, they will transmit RREP on reverse path else it add its individual address to the packet and send it to its personal border nodes. Procedure remains on going till the packet gets to the destination itself or to a node having destination in its zone. Path within the RREP packet is employed for sending data to destinations. As shown in the figure 2.6 An illustration for the propagation of RREQ in the ZRP. The large circles represent the routing zones of individual nodes. The small solid circles represent border nodes and the empty circles represent other nodes. The solid arrows represent the propagation of the RREQ that succeeds in finding a route. C can send a RREP since the destination D is within its routing zone. The RREQ is propagated from one node to another on its zone boundary. The dashed arrows indicate the propagation of RREQs that are not successful.

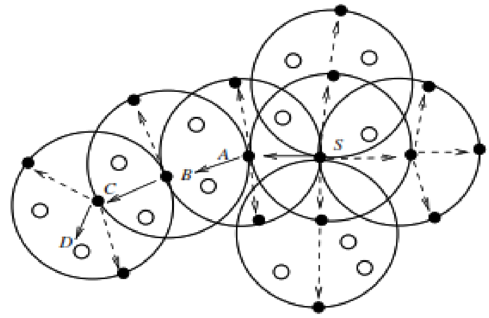


Figure 2.6 An illustration for the propagation of RREQ in the ZRP.[17]

2.5.2-Temporally Ordered Routing Algorithm

Temporally Ordered Routing Algorithm (TORA) [30, 31]: Park and Corson proposed TORA, an adaptive and scalable routing algorithm based on the concept of link reversal. It consists on finding numerous routes from a source to a destination in a extremely dynamic mobile networking setting. In this protocol control messages are limited to a small set of nodes near the topological change. Nodes uphold routing information about their instant one-hop neighbors. The trio elementary functions of the protocol are route maintenance, route creation, and route erasure. Nodes utilize a "height" metric to create a directed cyclic graph (DAG) entrenched at the destination through the route creation and route maintenance stages. The link can be either an upstream or downstream based on the qualified height metric of the adjacent nodes. It's metric holds the unique node ID, the logical time of a link failure, the unique ID of a node that introduced the new situation level, a reflection indicator bit, and a propagation ordering parameter. Establishment of DAG resembles the query/reply process in Lightweight Mobile Routing (LMR) [32]. Route maintenance is critical when any of the links in DAG is broken. Figure 2.7 describes the control flow of route maintenance in TORA.

The key strength of this protocol is its tactic to the management of the link failures. It's reaction to link failures is optimistic: it opposites the links to re-position the DAG for looking for an alternate path. Effectively, each link reversal sequence searches for alternative routes to the destination. This exploration method largely necessitates a single-pass of the distributed algorithm meanwhile the routing tables are customized simultaneously in the outer phase of the search mechanism. Extra routing algorithms like LMR use a two-passes search for the similar task, whereas both DSR and AODV use a three-pass procedure. TORA attains its single-pass technique with the supposition that all the nodes have coordinated clocks (via GPS) to produce a temporal order of topological change of events. The “height” metric is reliant on on the logical time of a link failure.

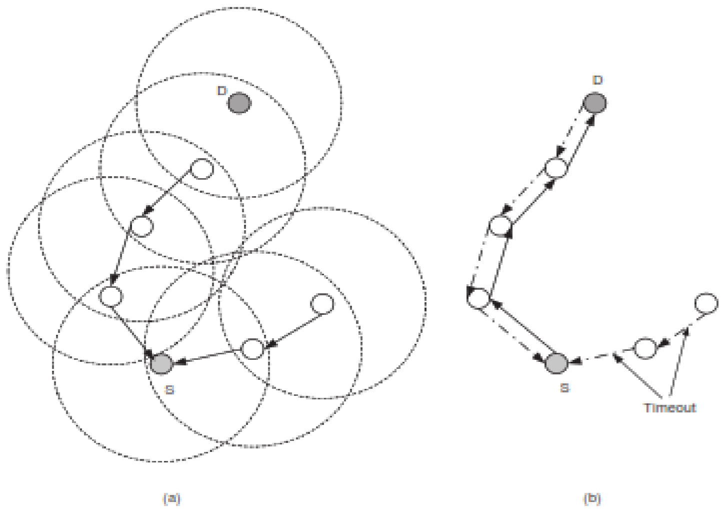


Figure 2.7: the control flow of route maintenance in TORA.[47]

(a) Reverse path formation. the reverse path is set up from all the nodes back to the source through RREQ message traveling in the network. (b) Forward path formation: it is built as the RREP message from the destination node D to source node S. The source node begin to transfer data when it acquired the first RREP message to the sender [47].

2.6-Multipath Routing Protocols

The routing protocols introduced above are uni-path routing. based on those protocols, a lot of multi-path routing protocols are proposed. These protocols consist of finding multiple routes between a source and destination node by exploiting the density of the network. These multiple trails amid source and destination node pairs will be adapted to compensate for the dynamic and random nature of ad hoc networks. The multi-path routing could offer several benefits: load balancing, fault-tolerance, higher aggregate bandwidth, lower end-to-end delay, etc. the remainder of this section goes to introduce several multi-path routing protocols that are proposed.

2.6.1-Alternative Path Routing

In [33], Alternate Path Routing (APR) is proposed. APR had its origins in the traditional circuit-switched telephone networks, where it reduced call blocking by providing multiple network routes for the initial call-setup messaging. The ability of APR's to source a load harmonizing and improved survivability makes it an attractive method for bandwidth-limited MANETs that are intended as packet-radio extensions to the wired Net. But, the APR performance improvements realized on the wired Internet don't unavoidably carry over to MANETs. specifically, the overlapping radio-coverage of neighboring nodes may result in strong interdependence between alternate routes which limits APR's benefits to particular MANET topologies and channel access techniques.

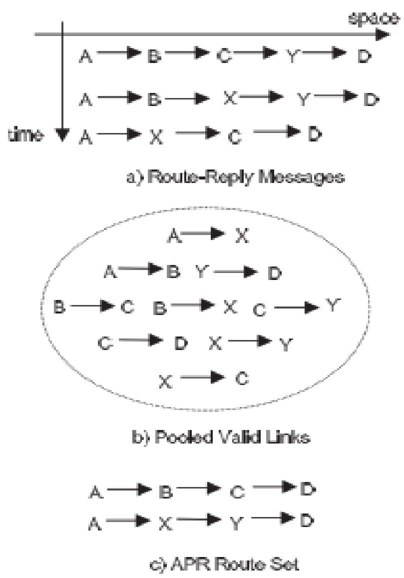


Figure 2.8: APR decomposes route replies into links states in order to reconstruct shorter, more diverse APR routes [33]

APR relies on the ZRP. A link state version of the ZRP's IntrA-zone Routing Protocol (IARP) can deliver every node with newer connectivity in its routing zone. The IntErzone Routing Protocol (IERP) provides routes, as needed, for destinations that lie outside of the routing zone. If a route exists, there'll be a reply explicitly defining a singular path to the destination. The ZRP Route-Reply messages effectively provide a partial snapshot of the network topology. As of the viewpoint of APR route-set structure, the primary worth may be accomplished from the route-replies by disintegrating the reported routes into a set of links. The links returned from the route-query will be pooled with valid links from other route-queries, and the proactively-tracked links form within the source node's local routing zone, in order to maximize the effective routing information, as shown in Figure 2.8. The potential benefits of APR make it appear to be a perfect candidate for the bandwidth-limited and dynamic mobile ad-hoc networks. The investigation of APR within the MANET environment has revealed that APR can, in some circumstances, provide notable improvements to end-to-end capacity. very frequently, nevertheless, the network topology and channel features bound what APR is able to reach.

2.6.2-Ad Hoc On-demand Multipath Distance Vector Routing

It is an on-demand[34], multi route distance vector routing protocol for MANET. It outspreads the AODV protocol to calculate numerous disjoint loop-free routes throughout a route discovery. It has several characteristics in common with AODV. it's grounded on the distance vector idea and the usages of hop-by-hop routing approach. Moreover, AOMDV also finds routes on demand employing a route discovery procedure. the main difference lies within the number of routes found in each route discovery. In AOMDV, the propagation of RREQ it's from the source on the way to the destination creates various reverse paths both at midway nodes extra as the destination. Multiple RREPs pass through these reverse paths back to make manifold forward paths to the destination at the source and intermediate nodes. This protocol also offers intermediate nodes with alternative paths as they are tend to be useful in plummeting route discovery occurrence. The fundamental of the AOMDV protocol consists in guaranteeing that multiple paths revealed are loop-free and disjoint, and in optimally finding such pathways using a flood-based route discovery. It's route update instructions, applied locally at each node, have a key part in preserving loop-freedom and disjointness rules. It depend as much as possible on the routing info already existing in the fundamental AODV protocol, so restraining the overhead sustained in discovering multiple paths. precisely, there is no employment of any different control packets. In fact, extra RREPs and RERRs for multipath discovery and maintenance together with some extra fields in routing control packets (i.e., RREQs, RREPs, and RERRs) constitute the sole additional overhead in AOMDV relative to AODV.

2.6.3- Split Multipath Routing

In [35], It was projected that an on-demand routing structure with the name of Split Multipath Routing (SMR) that exploits and creates multiple routes of maximally disjoint pathways. Provided that multiple routes which supports diminishing control message overhead and route recovery procedure . This protocol utilize a per-packet apportionment structure to issue data packets into numerous paths of active sessions. This traffic distribution efficiently utilizes available network resources and prevents nodes of the route from being congested in heavily loaded traffic situations[48]. Route Discovery The main goal of SMR is to create maximally disjoint multiple paths. It is necessary to construct maximally disjoint routes to stop certain nodes from being congested, and to utilize the available network resources efficiently. The destination must know the complete path of all available routes so it can select the routes. The source routing approach is employed. In the normal source routing approach, the duplicate RREQ packets are discarded. this might cause the multi-paths are mostly overlapped. In order to avoid this overlapped route problem, the author introduces a different packet for- warding approach. rather than dropping every duplicate RREQs, intermediate nodes forward the duplicate packets that traversed through a different incoming link than the link from which the first RREQ is received, and whose hop count isn't larger than that of the first received RREQ. For Route Selection, the destination picks 2 routes which are greatly disjoint. One of the two routes is the shortest delay route; the path engaged by the first RREQ the destination obtains. After this procedure, the destination pauses certain duration of time to receive more RREQs and acquire all possible routes. It then chooses the route that's extremely disjoint to the route that's previously responded. If there's additional than one route that are maximally disjoint with the first route, the one with the shortest hop distance is selected. If there still remain many routes that meet the rule, the path that transported the RREQ to the destination the fastest between them is selected[48]. The destination then directs another RREP to the source through the second route designated. Route Maintenance In SMR, when a node fails to deliver the packet to the subsequent hop, a RERR message is send back to the source, and also the source removes the correspond entry from its routing table. When the source is informed of a route disconnection and the session remains active, it may use one among the 2 policies in rediscovering routes:

- initiates the route recovery process when any route of the session is broken, or
- initiates the route recovery process only if both routes of the session are broken.

The first outline rebuilds the routes more often and produces extra control overhead than the second structure, but the previous offers several routes most of the time and is vigorous to route breaks. SMR outperforms DSR because multiple routes provide robustness to mobility.

2.6.4- OLSR-based multipath routing

The APR and AOMDV are mainly based on reactive topology discoveries. within the literature, there are also some routing mechanisms proposed based on proactive approach. In [36], the authors proved that for OLSR, the broadcasting mechanism based on MPR is important and adequate to provided multiple connectivities between the source and destination. So, several protocols based on OLSR are introduced.

QOLSR In [37], the authors proposed a multipath QOLSR based on the measurement of the bandwidth and therefore the delay. it's an enhancement of the OLSR routing protocol to support multiple-metric routing criteria. Each node calculates the delay and bandwidth information for every of its neighbors. Two approaches are often applied:

- The first approach uses one single metric in route decisions like hop count or delay or

  available bandwidth.
- The second approach treats each metric individually.

The first approach is simple to implement by using Dijkstra algorithm. The second isn't feasible due to the algorithm complexity. the problem of finding a path with an additive and m multiplicative metrics is NP-complete ifn+m >=2 [38]. the most effective path with all parameters at their optimal values might not exist if multiple metrics are included. Queuing delay is more dynamic; therefore, bandwidth is considered into account as more significant. The strategy is to find a path with maximum bandwidth (a widest path), and when there's over one widest path, the algorithm chooses the one with the shortest delay, so called the shortest-widest path algorithm. In the network, every node MPR produces a TC message involving its bandwidth ,MPR selectors and time delay. founded on this info, the routing table is designed. When the most effective path calculated by the shortest-widest path algorithm does not satisfy bandwidth and delay requirements, the multiple paths are calculated.

The futured algorithm calculates several loop-free and node-disjoint paths with a minor association factor founded on the delay and bandwidth metrics. The correlation factor is known as the number of links linking two disjointed paths. it's designed to decrease interference between the multiple paths so as to realize better QoS guarantees to applications and improve network resource utilization. However, the authors didn't prove that the correlation factor can be correctly calculated. Certainly, OLSR nodes can’t have a universal sight of the network, but only links pushed in HELLO and TC messages (defaulting, the advertised link set in TC of the node is restricted to the MPR selector set) [39]. Moreover, this approach assumes a freshness of the measures (bandwidth, delay) which is difficult to get and maintain in practice. Source Routing OLSR [40] propose another version of multipath OLSR using IP source routing. Grounded on Dijkstra algorithm, the node computes several paths to the destination. The designed paths are firmly node-disjoint. the path is implanted within the IP header of the packet beforehand sending. Constructed on these numerous paths, the paper presents an algorithm of load balancing to convey data over the paths founded on the congestion data of all the midway nodes on each path. The congestion information of 1 path is calculated as the highest size of the queue of the intermediate nodes (the queue size of a node is condensed in HELLO packets and pushed in TC messages). The algorithm of load balancing chooses 2 paths to diffuse data following to their congestion information, and stabilities the load on the nominated paths. In [41].This authors similarly suggest an undistinguishable algorithm to compute node-disjoint multiple paths by eliminating used nodes from the topology info base. Though, the pure source routing is challenging particularly with topology deviations which can be examined inside the next section. In both studies, strict node disjoint routes don't seem to be always necessary and also the suppression of nodes in multiple calls of Dijkstra algorithm couldn't work for sparse networks. The node-disjoint multiple paths aren't appropriate for fusion group or partition of nodes that may momentarily suggest a single link for connection. Furthermore, the backward compatibility isn't considered, which might be vital for the deployment of a new protocol.

2.7- Quality of Service

Because the physical characteristic and therefore the dynamic topology of the MANETs, it's a difficult task to offer the guaranteed quality of service (QoS), like delay, jitter, bandwidth and delivery ratio. The routing protocols introduced above mainly focused on finding feasible routes from the source to the destination, and don't take QoS into consideration. To support QoS, the essential problem is to find a route with plenty of available resources to fulfill the QoS constraints and possibly to include optimizations, such as finding all-time low cost or most stable of the routes that meet the QoS constraints. Given these goals, the subsequent are the fundamental design considerations for a QoS-aware routing protocol [42].

• Resource estimation. the main goal is to get information about the available resources from lower layers which helps in performing call admission and QoS adaptation.

• Route discovery. aside from the reactive discovery and proactive discovery, the protocols that support QoS have to determine the mix of reduced latency and reduced overhead.

• Resource reservation. Because the bandwidth is shared by neighboring hosts, the resource reservation scheme must be applied to ensure the QoS.

• Route maintenance. After the building of the routes, those routes still have to be maintained due to the change of the topology.

• Route selection. The more reliable routes must be selected to prevent the frequent route failures within the network.

• Choosing routes with the biggest available bandwidth or minimum delay.

• Providing a call admission feature to deny route requests if insufficient bandwidth is available to support the request.

• Providing feedback to the applying about available bandwidth resources or route delay estimation.

In the following, two QoS-aware routing protocols are introduced.

2.8- Security

The security is a very important issue for network transmission. This subsection tries to provide a summary of the related works of wireless network security, especially ad hoc network security. The security in wireless networks has great difference from the wired networks thanks to the nature of the physical medium. The transmitting signal travels through the air in a wireless network, so any nodes that are within the transmission range of the transmitter can receive the signal. If the node is aware of the frequency and other parameters (modulation, coding, key, etc.), it can potentially decode the signal without permission. Except for the transmission medium, the mobility of the wireless network is another big challenge. Existing technologies often depend on the availability of traffic checkpoints (which most traffic goes through). With the check points, the security devices can inspect traffic of suspicious behavior and implement security policies and respond as needed. However, this is often unachievable in ad hoc networks because such checkpoints don't exist with the mobility of the nodes. the standard security solutions also depend upon some centrally located devices for security of the network, such as key distribution, etc. Such solutions are not applicable for ad hoc networks. Normally a threshold scheme is employed for key management in cryptographic systems [46]. So different security mechanisms must be used for ad hoc networks. One method for the conception of security mechanisms for systems is to look at the threats that the system faces and therefore the possible attacks given the vulnerabilities. The concepted security mechanisms should ensure that the system is secure within the light of those threats, attacks, and vulnerabilities [46]. Menace is the means over which the capability or intent of an agent to unfavorably affect an computerized system, facility or operation can be demonstrated. All the ways or things accustomed exploit a weakness in a system, operation, or facility constitute threat agents. Vulnerability is any hardware, firmware, or software flaw that leaves an information system open for potential exploitation. The exploitation may be of varied types, like gaining unauthorized access to information or disrupting critical processing.

The vulnerabilities of ad hoc network can be within the routing, wireless links or other mechanisms like auto-configuration. An attack is an endeavor to bypass the protection controls on a computer.

The attack may alter, release, or deny data. The success of an attack depends on the vulnerability of the system and also the effectiveness of existing countermeasures.

2.9- Conclusion

In this chapter we have reviewed several protocols for routing in mobile ad hoc networks. We concluded that the routing protocol is required whenever the source has to transmit and delivers packets to the destination.

Many routing protocols have been proposed for mobile Ad Hoc network, they can be divided mainly into two categories: proactive routing and reactive routing. based on those two types, some hybrid routing protocols and multipath routing protocols were also introduced.

Chapter 3: Simulation and results

3.1-Introduction

Simulation is the reproduction of a phenomenon with the goal of verifying theories and hypotheses that explain a given phenomenon then predict the course of this phenomenon.

The simulation process consists of proposing a scenario with various parameters then running the simulation, observing the different output of results.

The analyzing of the results obtained allows us to deduce information and conclusion valuable to our experience. Based on this concept of simulation we have compared some Ad Hoc routing protocols. We will present in this chapter the simulation of AODV, DSR, OLSR and TORA on OPNET 14.5 simulator.

3.2-OPNET modeler

Optimized network engineering (OPNET) tool is used to simulate the performance of the network. It has inbuilt models, protocols and devices that create and simulate diverse networks. It is an open software which has features like applications troubleshooting, protocol modeling, traffic modeling, validation of application, estimating performance of complex network systems. It has discrete event simulation workflow that helps in creation, import, and configuration of topologies as well as network traffic and is also published results with statistics report.

Key features of OPNET are:

(a) Network model.

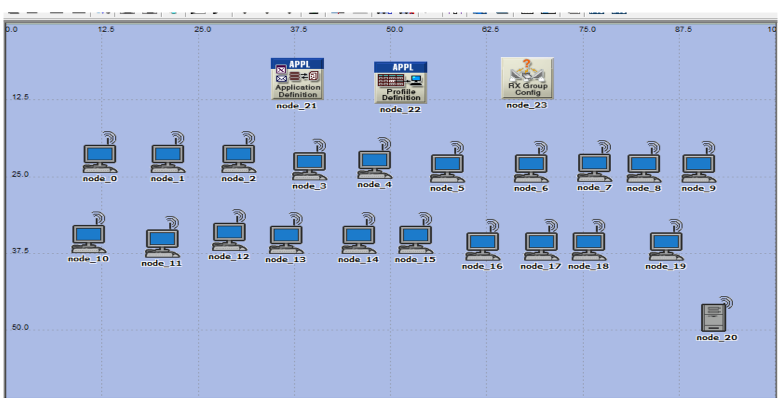


Figure 3.1-OPNET's Network model

(b) Process Modeling

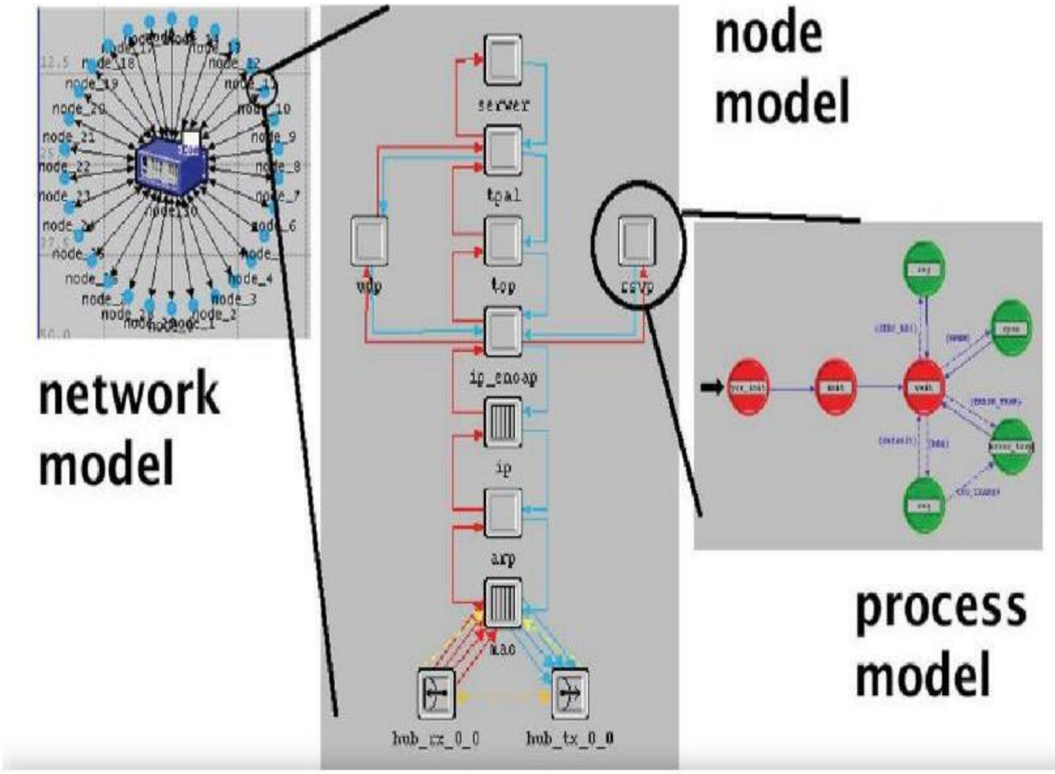


Figure 3.2 - OPNET Graphic Editors for Network, Node, and Process Models

(c) Simulation kernel

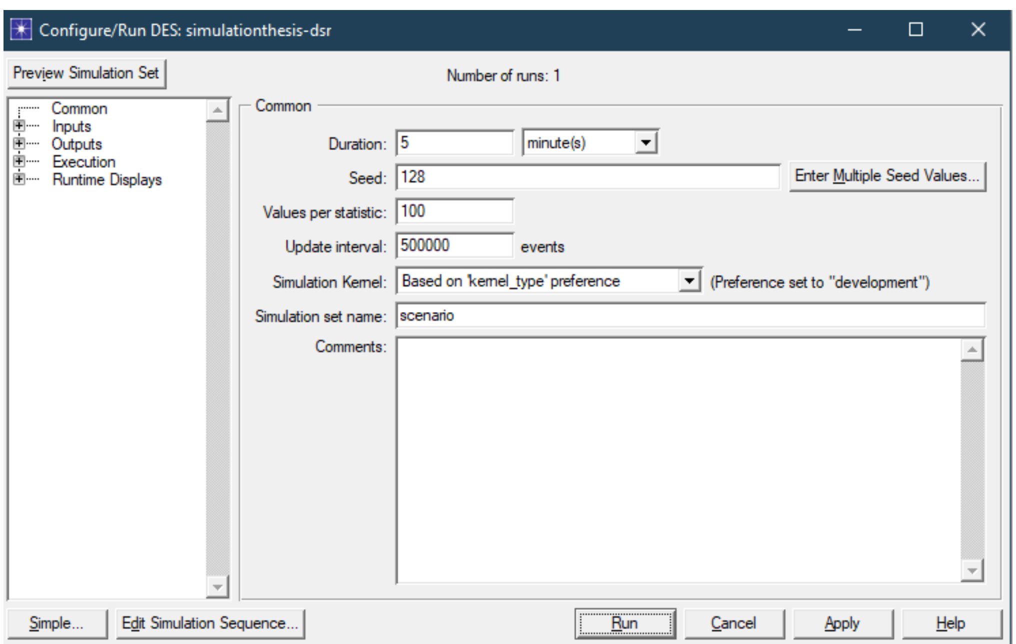


Figure 3.3 – Simulation kernel OPNET

(d) Event based simulation.

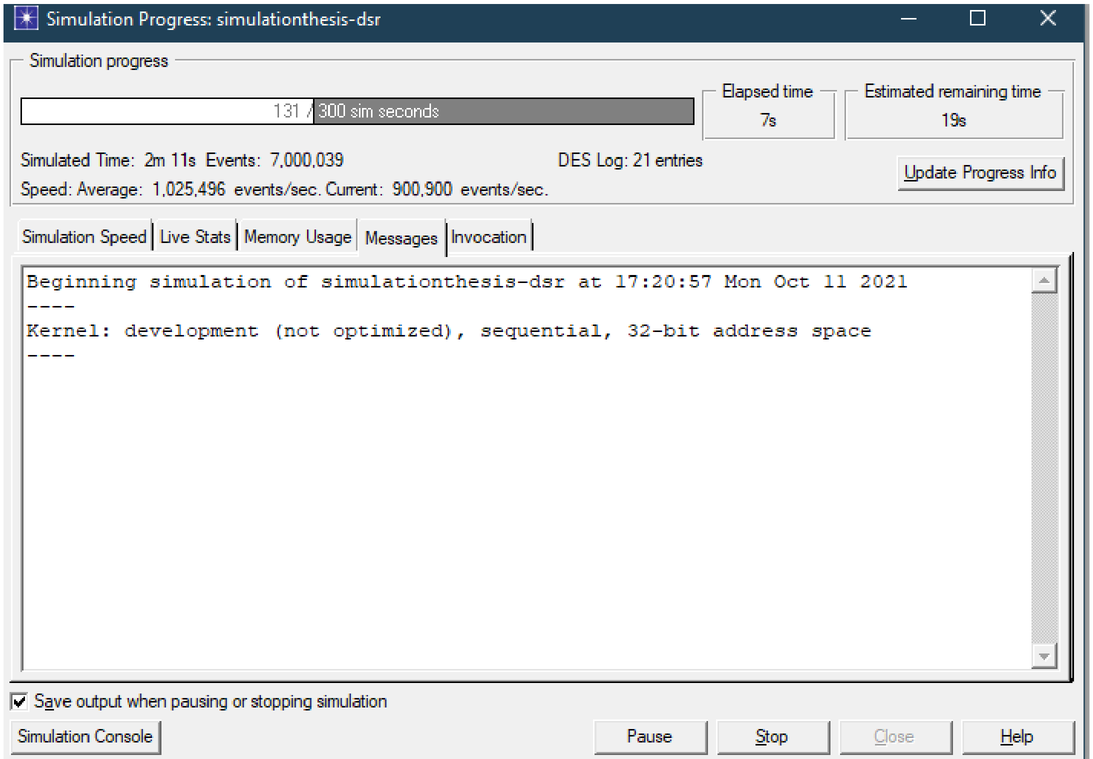


Figure 3.4- Event based simulation in OPNET

(e) Link modeling.

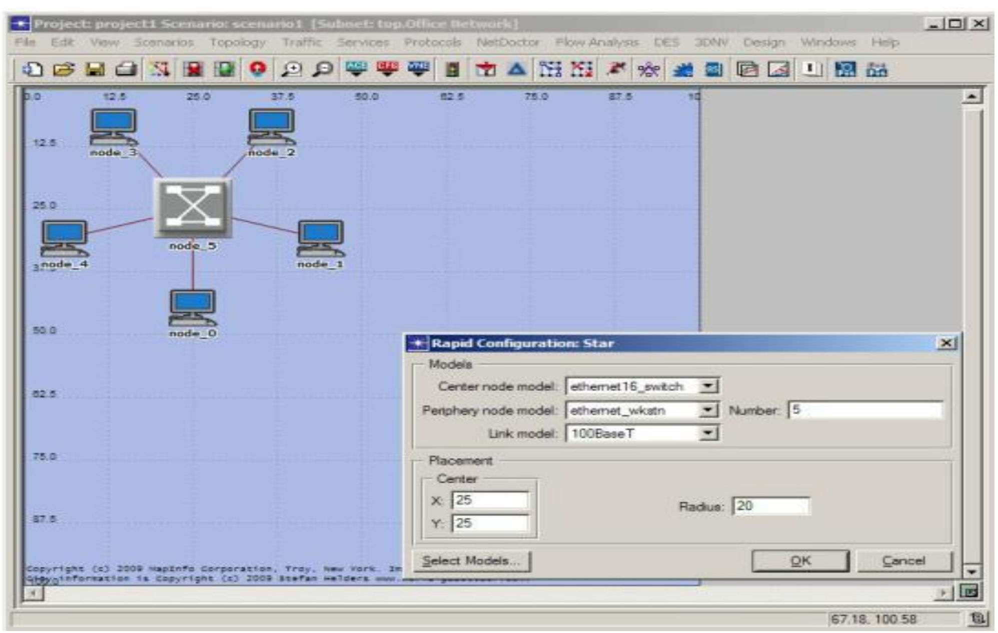


Figure 3.5- Link modeling in OPNET

3.3- scenario of simulation

To monitor various performance matrices related to all four routing protocols we have simulated some scenarios with the help of OPNET modeler 14.5. This scenario consists of 20 nodes enabled with voice application. The area considered for simulation is 100 m X 100 m. For the application designation we have included the Application config and Profile config to set the applications (voice) used by the nodes. Subsequently, we changed the routing protocol of all the nodes to all the routing protocols i.e., AODV, DRS, OLSR and TORA successively. The metrics used for observation are throughput, , network load, media access delay, delay and traffic drop. The seed value considered for simulation is 128.

3.4-Metrics of evaluation

In this session we will give the definition of the metrics which have been used in order to compare the selected protocols.

3.4.1--Throughput

It is the quantity of the number of packets successfully diffused to their last destination per unit of time. It is the proportion among the number of received packets vs sent packets.

3.4.2-Network Load

In computer networks, network load represents the number of processes that a network can handle at a time.

3.4.3- Media Access Delay

The time a node takes to access media for starting the packet transmission is called as media access delay. The delay is recorded for each packet when it is sent to the physical layer for the first time.

3.4.4- Traffic Dropped

traffic dropped shows how many packets successfully sent and received across the whole network. It also explains the number of packets dropped during the transmission due to interference from other devices.

3.4.5-Delay It is the ratio of time difference between every packet sent and received to the total time difference over the total number of packets received.

3.5-Simulation and result

3.5.1-Throughput: figure (3.6) shows the throughput of the network. The simulation runs for the entire duration which generates result in time average mode, specifies AODV has maximum throughput, then OLSR. TORA protocol gives minimum throughput, whereas DSR remains behind to OLSR.

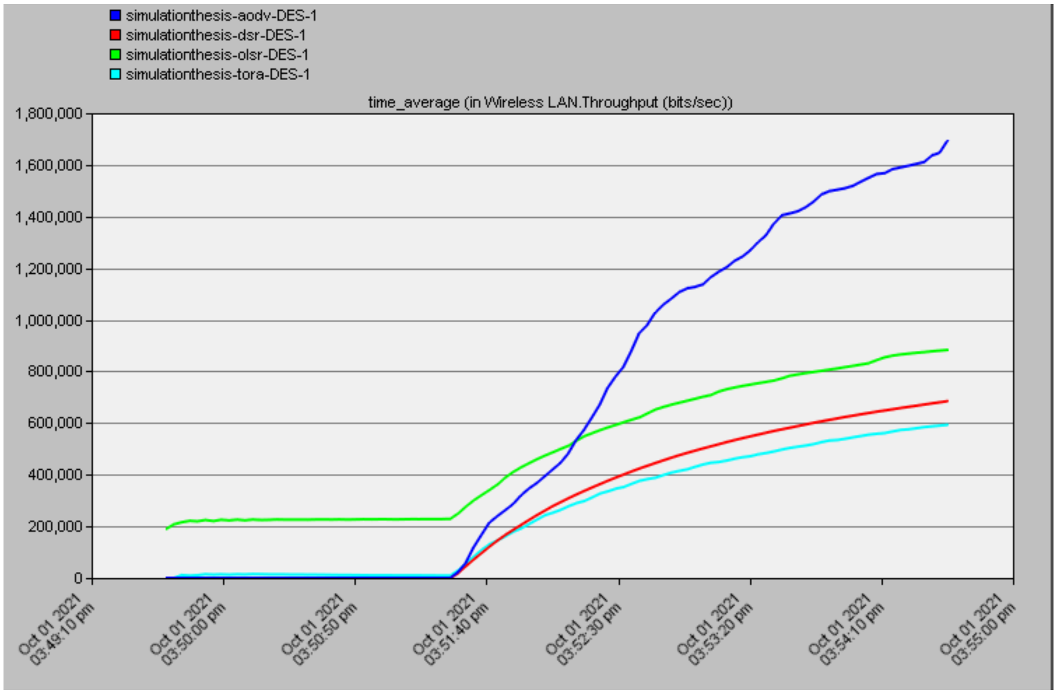


Figure 3.6: Throughput (bit/sec)

3.5.2-Network Load- as depicted in figure (3.7) the network load for all protocols is equal minimum at approx.2 min. of the experiment. Further the network load increases exponentially throughout the execution. The OLSR has maximum network load.

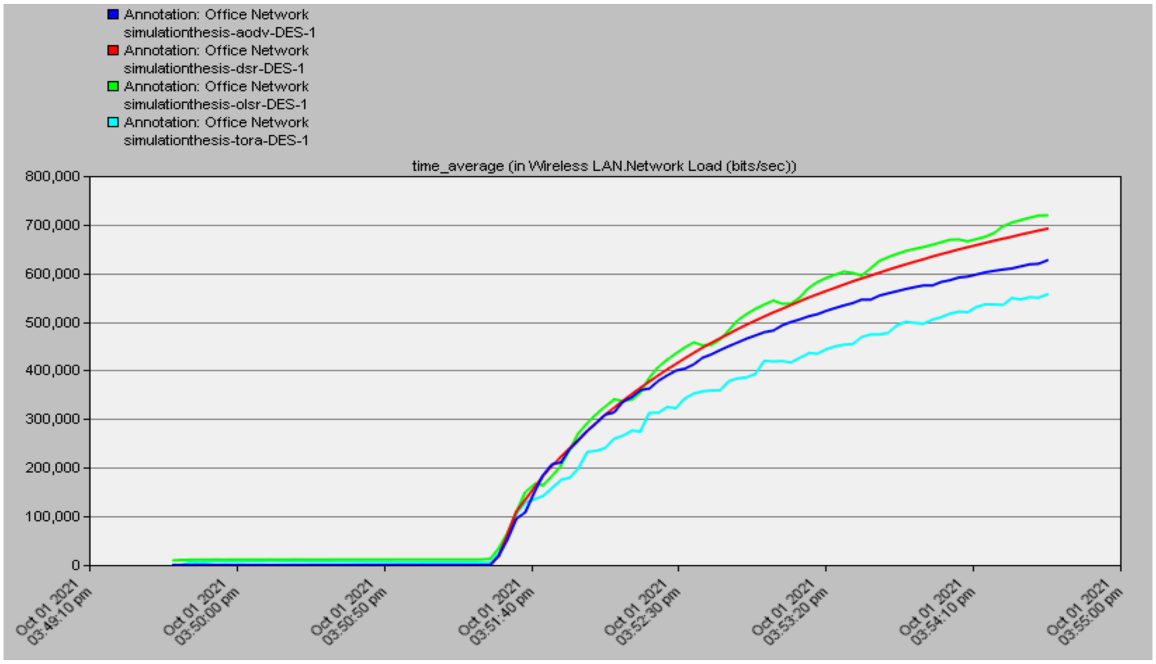


Figure 3.7: Network load(bit/sec)

3.5.3-Media Access Delay- DSR protocol has maximum peak of Media Access Delay at around 50% time of the execution; further the delay keeps increasing followed by AODV slightly below DSR. The OLSR and TORA have gradual increase in their delays. TORA protocol has minimum delay and it remains consistent throughout the experiment, as shown in figure (3.8).

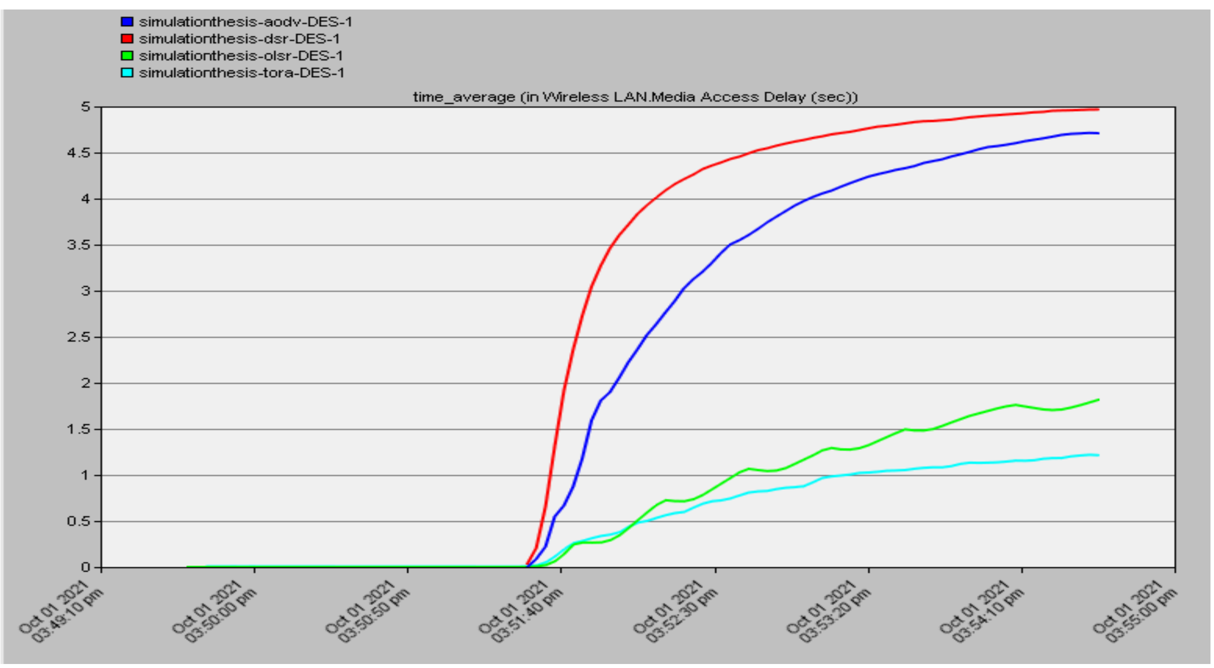


Figure 3.8: Media access delay (sec)

3.5.4-Delay- All protocols have propagation after 25% of execution time, TORA has minimum delay, which remains constant further. DSR and AODV protocols are having much higher delay than OLSR and it remains constant in execution. The DSR protocol has highest delay peak 5 min. as shown in figure (3.9).

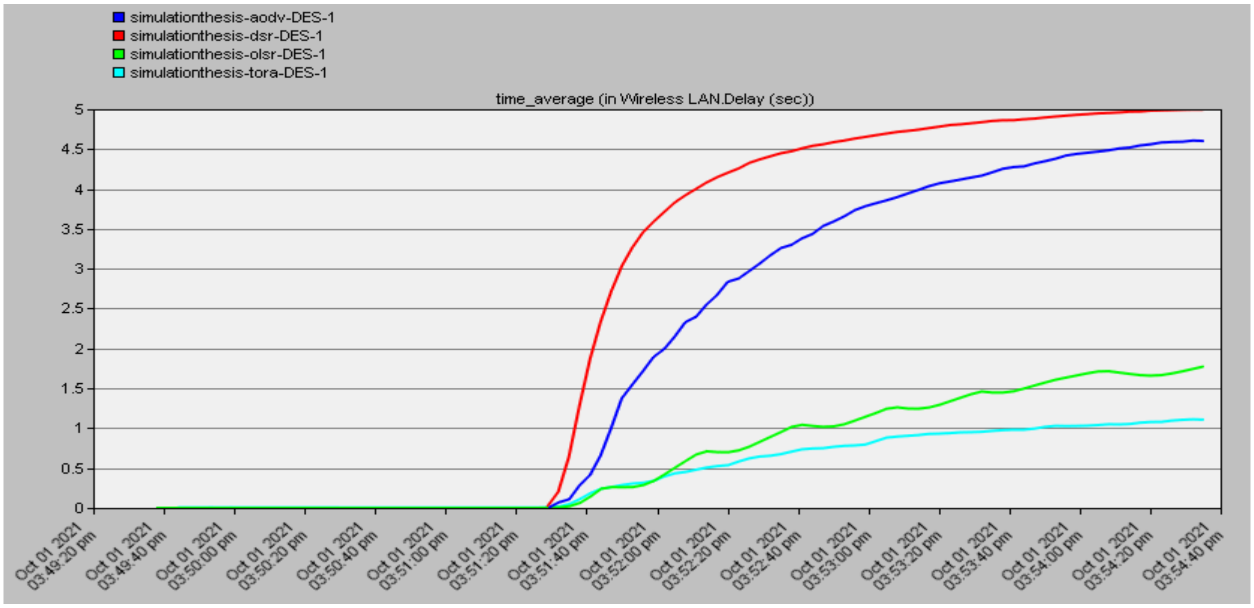


Figure 3.9: Delay(sec)

3.5.5-Traffic Dropped: - Figure (3.10) specifies OSLR protocol has the maximum packets traffic drop. Other protocols AODV, DSR and TORA have minimum packets traffic drop.

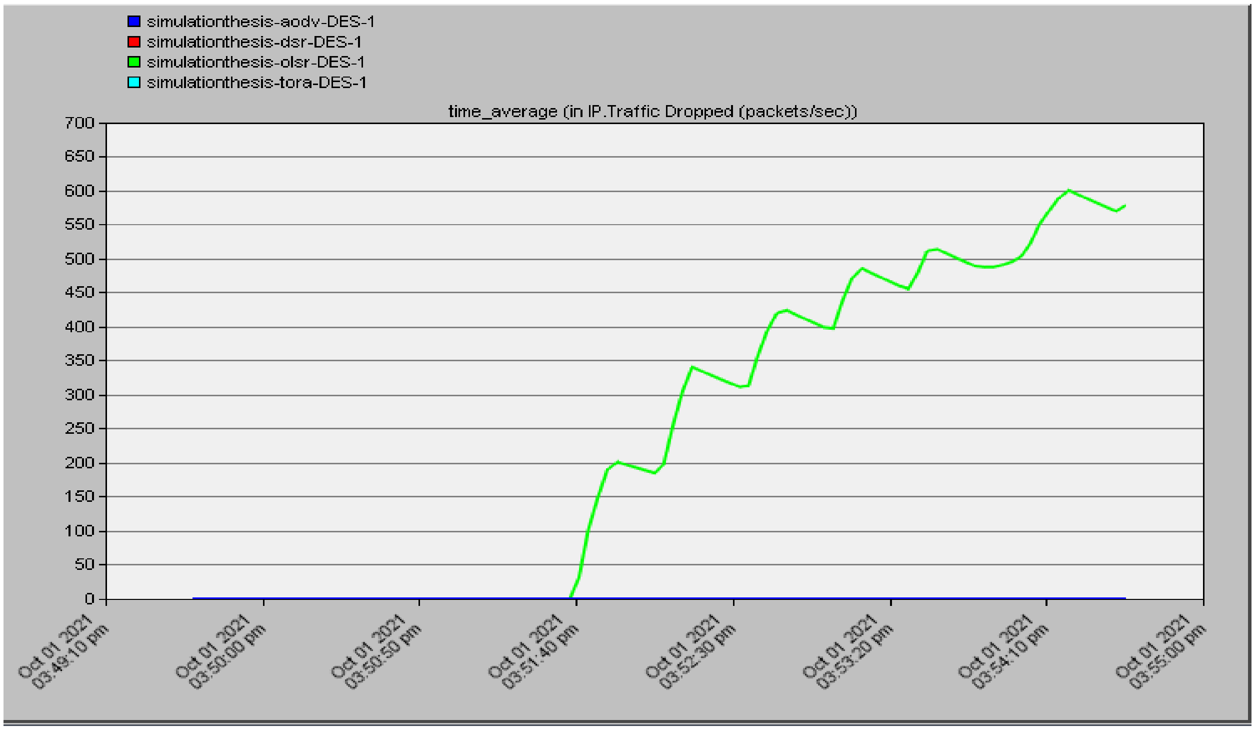


Figure 3.10: Traffic dropped (packet/sec)

3.6-Conclusion

In this chapter simulation-based analysis has been carried out to analyze the MANET routing protocols performances in term of quality of service. As per the research completed, shows AODV has high throughput with low load and low data dropped but shows poor delay. OLSR protocol shows low delay, good throughput but high data dropped and load.

TORA shows poor results in throughput with low load, data dropped and delay the same thing with DSR.

AODV proved to be the best routing protocol for the overall experience, in MANET environment.

General conclusion

MANET Networks is a very broad subject and it's the center of interest for researchers because it has become an essential thing in our life especially with the technological revolution as we are constantly looking to optimize things for the real life of humans. We have compared some routing protocols, AODV, OLSR, DSR and TORA in Ad hoc networks.

We have started our study by introducing wireless networks in the first chapter. Ad Hoc networks and their features with some applications have been presented at the first chapter. The most important task to ensure communication between nodes in Ad Hoc network is routing task. We have presented some routing protocols in the second chapter. AODV, OLSR, DSR and TORA have been selected in our simulation on OPNET. The results of evaluation of these protocols based on some metrics has been shown at the third chapter.

Our next goal will be to propose a new routing protocol by improving an existing routing protocol. This improvement will be made in order to overcome some issues like the delay and packet dropped.

References

[1] Geier, J. T., & Geier, J. (2005). Wireless Networks first-step. Cisco Press.

[2] Youn, J. S., Lee, J., Sung, D. H., & Kang, C. H. (2006). Quick Local Repair Scheme using Adaptive Promiscuous Mode in Mobile Ad Hoc Networks. *J. Networks*, *1*(1), 1-11.

[3] Sumyla, D. (2006). Mobile Ad-hoc Networks (manets).

[4] Clausen, T., Jacquet, P., Adjih, C., Laouiti, A., Minet, P., Muhlethaler, P., ... & Viennot, L. (2003). Optimized link state routing protocol (OLSR).

[5] Perkins, C. E., & Royer, E. M. (1999, February). Ad-hoc on-demand distance vector routing. In Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications (pp. 90-100). IEEE.

[6] NFS Wireless and Mobile Communications Workshop,(March, 1997),Northern Virginia.

[7] Conti, M., & Giordano, S. (2007). Multihop ad hoc networking: The theory. IEEE communications Magazine, 45(4), 78-86.

[8] Pelusi, L., Passarella, A., & Conti, M. (2006). Opportunistic networking: data forwarding in disconnected mobile ad hoc networks. IEEE communications Magazine, 44(11), 134-141..

[9] Maltz, D. A., Johnson, D. B., & Hu, Y. (2007). The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. 2007-tools. ietf. org.Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4.

[10] Klein, A. (2008, May). Performance comparison and evaluation of AODV, OLSR, and SBR in mobile ad-hoc networks. In 2008 3rd International Symposium on Wireless Pervasive Computing (pp. 571-575). IEEE.

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

[12] Perkins, C. E., & Royer, E. M. (1999, February). Ad-hoc on-demand distance vector routing. In Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications (pp. 90-100). IEEE.

[13] Ehsan, H., & Uzmi, Z. A. (2004, December). Performance comparison of ad hoc wireless network routing protocols. In 8th International Multitopic Conference, 2004. Proceedings of INMIC 2004. (pp. 457-465). IEEE.

[14] Park, V. D., & Corson, S. (1998). Temporally-ordered routing algorithm (TORA) version 1 functional specification (Internet-draft). Mobile Ad-hoc Network (MANET) Working Group, IETF.

[15] Perkins, C. E., & Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM computer communication review, 24(4), 234-244.

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

[17] Haas, Z. J. (2002). The zone routing protocol (ZRP). IETF MANET Draft draft-ietf-manet-zone-zrp-04. txt.

[18] Johnson, D. B., Maltz, D. A., & Broch, J. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking, 5(1), 139-172.

[19] Chakeres, I., & Perkins, C. (2010). Dynamic MANET On-demand (DYMO) Routing, draft-ietf-manet-dymo-21. Internet Engineering Task Force: Fremont, CA, USA.

[20] Hamma, S., Cizeron, E., Issaka, H., & Guédon, J. P. (2006, October). Performance evaluation of reactive and proactive routing protocol in IEEE 802.11 ad hoc network. In Next-Generation Communication and Sensor Networks 2006 (Vol. 6387, p. 638709). International Society for Optics and Photonics.

[21] Clausen, T., Dearlove, C., & Adamson, B. (2008). Jitter considerations in mobile ad hoc networks (MANETs).

[22] Clausen, T., Dearlove, C., Dean, J., & Adjih, C. (2009). IETF Request for Comments: 5444. Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format (February 2009).

[23] Clausen, T., & Dearlove, C. (2009). Representing Multi-Value Time in Mobile Ad Hoc Networks (MANETs). RFC 5497, March.

[24] Clausen, T., Dearlove, C., & Dean, J. (2008). MANET neighborhood discovery protocol (NHDP). Internet Engineering Task Force (IETF) draft.

[25] Clausen, T., Dearlove, C., & Jacquet, P. (2009). IETF Draft The Optimized Link State Routing Protocol version 2,".

[26] Pandey, K., & Swaroop, A. (2011). A comprehensive performance analysis of proactive, reactive and hybrid MANETs routing protocols. arXiv preprint arXiv:1112.5703.

[27] Nand, P., & Sharma, S. C. (2011). Comparative study and Performance Analysis of FSR, ZRP and AODV Routing Protocols for MANET. In IJCA Proceedings on International Conference and workshop on Emerging Trends in Technology (ICWET) (Vol. 2, pp. 14-19). [28] Bakht, H. (2011). Survey of routing protocols for mobile ad-hoc network. International Journal of Information and Communication Technology Research, 1(6).

[29] Sahadevaiah, K., & Ramanaiah, O. B. V. (2010). An empirical examination of routing protocols in mobile ad hoc networks. International Journal of Communications, Network and System Sciences, 3(6), 511.

[30] Park, V. D., & Corson, M. S. (1997, April). A highly adaptive distributed routing algorithm for mobile wireless networks. In Proceedings of INFOCOM'97 (Vol. 3, pp. 1405-1413). IEEE. [31] Park, V. D., & Corson, M. S. (1997, April). A highly adaptive distributed routing algorithm for mobile wireless networks. In Proceedings of INFOCOM'97 (Vol. 3, pp. 1405-1413). IEEE. [32] Corson, M. S., & Ephremides, A. (1995). A distributed routing algorithm for mobile wireless networks. Wireless networks, 1(1), 61-81.

[33] Pearlman, M., Haas, Z., Sholander, P., & Tabrizi, S. S. (2000, October). Alternate path routing in mobile ad hoc networks. In MILCOM 2000 Proceedings. 21st Century Military Communications. Architectures and Technologies for Information Superiority (Cat. No. 00CH37155) (Vol. 1, pp. 501-506). IEEE.

[34] Marina, M. K., & Das, S. R. (2006). Ad hoc on-demand multipath distance vector routing. Wireless communications and mobile computing, 6(7), 969-988.

[35] Lee, S. J., & Gerla, M. (2001, June). Split multipath routing with maximally disjoint paths in ad hoc networks. In ICC 2001. IEEE international conference on communications. Conference record (Cat. No. 01CH37240) (Vol. 10, pp. 3201-3205). IEEE.

[36] Viennot, L., & Jacquet, P. (2007, May). Bi-connexite, k-connexite et multipoints relais. In 9ème Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (pp. 9-12).

[37] Badis, H., & Al Agha, K. (2004, May). QOLSR multi-path routing for mobile ad hoc networks based on multiple metrics: bandwidth and delay. In 2004 IEEE 59th Vehicular Technology Conference. VTC 2004-Spring (IEEE Cat. No. 04CH37514) (Vol. 4, pp. 2181-2184). IEEE.

[38] Kuipers, F., Van Mieghem, P., Korkmaz, T., & Krunz, M. (2002). An overview of constraint-based path selection algorithms for QoS routing. IEEE Communications Magazine, 40(12), 50-55.

[39] Clausen, T., Jacquet, P., Adjih, C., Laouiti, A., Minet, P., Muhlethaler, P., ... & Viennot, L. (2003). Optimized link state routing protocol (OLSR)..

[40] Kun, M., Jingdong, Y., & Zhi, R. (2005, October). The research and simulation of multipath-OLSR for mobile ad hoc network. In IEEE International Symposium on Communications and Information Technology, 2005. ISCIT 2005. (Vol. 1, pp. 540-543). IEEE.

[41] Zhou, X., Lu, Y., & Xi, B. (2005, October). A novel routing protocol for ad hoc sensor networks using multiple disjoint paths. In 2nd International Conference on Broadband Networks, 2005. (pp. 944-948). IEEE.

[42] Chen, L., & Heinzelman, W. B. (2007). A survey of routing protocols that support QoS in mobile ad hoc networks. IEEE Network, 21(6), 30-38.

[43] Xue, Q., & Ganz, A. (2003). Ad hoc QoS on-demand routing (AQOR) in mobile ad hoc networks. Journal of parallel and distributed computing, 63(2), 154-165..

[44] Ge, Y., Kunz, T., & Lamont, L. (2003, January). Quality of service routing in ad-hoc networks using OLSR. In 36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the (pp. 9-pp). IEEE..

[45] Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.

[46] Anjum, F., & Mouchtaris, P. (2007). Security for wireless ad hoc networks. John Wiley & Sons.

[47] Perkins, C. E., & Royer, E. M. (1999, February). Ad-hoc on-demand distance vector routing. In Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications (pp. 90-100). IEEE.

[48] Lee, S. J., & Gerla, M. (2001, June). Split multipath routing with maximally disjoint paths in ad hoc networks. In ICC 2001. IEEE international conference on communications. Conference record (Cat. No. 01CH37240) (Vol. 10, pp. 3201-3205). IEEE.