T.C.

ALTINBAS UNIVERSITY

Institute of Graduate Studies

Information Technologies

USING THE NETEDITOR TO EVALUATION THE DSR AND OLSR ROUTING PROTOCOLS FOR VICHER AD-HOC NETWORKS IN NS3

Muhmmad Shihab Muayad SHIHAB

Master of Science

Supervisor

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Istanbul, 2021

USING THE NETEDITOR TO EVALUATION THE DSR AND OLSR ROUTING PROTOCOLS FOR VICHER AD-HOC NETWORKS IN NS3

by

Muhmmad Shihab Muayad SHIHAB

Information Technologies

Submitted to the Institute of Graduate Studies

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2021

The thesis titled **“**USING THE NETEDITOR TO EVALUATION THE DSR AND OLSR ROUTING PROTOCOLS FOR VICHER AD-HOC NETWORKS IN NS3**”** prepared and presented by “Muhmmad Shihab Muayad SHIHAB” was accepted as a Master of Science Thesis in Information Technologies.

____

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Supervisor

Thesis Defense Jury Members:

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	School of Engineering and Architecture, Altinbas University	_________________
Asst. Prof. Dr. Sefer KURNAZ	School of Engineering and Architecture, Altinbas University	_________________
Assoc. Prof. Dr. A. Mohammed ABUBAKAR	Faculty of School Economics, Administrative and Social Science, Antalya Science University	_________________

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Approval Date of Institute of Graduate Studies: ____/____/____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Muhmmad Shihab Muayad SHIHAB

DEDICATION

First and foremost, I would like to thank Allah Almighty for giving me the knowledge, ability and opportunity to undertake this research study and to persevere and complete it satisfactorily. Heartfelt thanks goes to my father and my mother. Every success is a direct consequence of their influence in my life and their love. At the end I have to mention my brother and sister for their support and love.

ACKNOWLEDGEMENTS

All praises are to ALLAH Subhanahu wa ta'ala for bestowing me with health, opportunity, patience, and knowledge to complete this research. May the peace and blessings of ALLAH Subhanahu wa Ta'aala be upon Prophet Muhammad (Sallallahu alayhi wa sallam).

My profound gratitude goes to my supervisor Asst. Prof. Dr. Abdullahi Abdu IBRAHIM, for his invaluable guidance, excellent supervision, continuous encouragement and constant support in making this research possible. His cooperation, tolerance, constructive criticism and useful suggestions have been of immense encouragement to me and enabled me to develop a deeper understanding of this research. I also thank Dr. Alaa Hamid Mohammed I sincerely thank him for the time spent in proofreading and correcting my mistakes.

Finally, I extend my gratitude to all those who were directly or indirectly involved by either encouraging, praying and offering constructive advice in this thesis.

Thank you.

ABSTRACT

USING THE NETEDITOR TO EVALUATION THE DSR AND OLSR ROUTING PROTOCOLS FOR VICHER AD-HOC NETWORKS IN NS3

SHIHAB, Muhmmad Shihab Muayad,

M.Sc., Information Technologies, Altınbaş University,

Supervisor: Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Date: 06/2021

Pages: 41

Ad hoc vehicle networks (VANETs) have recently gained popularity due to their ability to improve vehicle safety and convenience. The unique characteristics and features of VANETs, on the other hand, made designing routing protocols extremely difficult. In comparison, the literature indicates a complex series of routing protocols. We will compare the DSR and OLSR routing protocols in three scenarios using the overhead, Goodput, and Packet Receives Rate efficiency metrics in this paper.

KEYWORDS: Pouting Protocols, Methodology, Overhead, Good Put, Packet Receives Rate.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

LIST OF ABBREVIATIONS

CDR	:	Cup-to-Disc Ratio
DR	:	Diabetic Retinopathy
DRIVE	:	Digital Retinal Images for Vessel Extraction
MESSIDOR	:	Methods to Evaluate Segmentation and Indexing
OD	:	Optic Disc
STARE	:	Structured Analysis of the Retina

1. INTRODUCTION

1.1 INTRODUCTION

The fact that there are still an increasing number of cars on the road has increased the need for modern car technologies that can boost safety and customer loyalty. VANET will provide protection, ambulance and entertainment services. A VANET is a dynamic network that turns out to be a router for any node. The VANET also added new technical features, such as road-mode restrictions, unlimited network capability, fluid topology, convergence models and unrestricted power and data/information localization capabilities. These characteristics make VANET difficult to create. VANET is divided into V2V and VANET infrastructure (V2I). Our focus is the previous model. VANET is comprised of different layers of V2V routing protocols that are divided into four main parts: Instead of sending private IP addresses, nodes send their unique vehicle coordinates regularly to each other. Distributed GPS technologies and petition-based guidance are used to create or keep a direct connection between all nodes. However, this requires a cluster header in the terminal node to communicate with the other cluster head. [1] Vehicular communications using spatial geo-cast and mobiles calls. Another aim of this category is to communicate with individuals located within a given geographic location called zOR. If the goal node belongs to the other ZOR zone, then HSLA is implemented. ZOR (Zone of Function) transmittal to other ZORs for data packets. The routing algorithm accommodates structure of the network. Topological protocols may be categorized as followed: Positive protocols, Mutual protocols and Mixed protocols. Both good directions in route to the target are now in sight. To keep the path information updated, the node must constantly send control messages. The key benefit of Routing Algorithm is to find the paths to all possible destinations without any human input. It is regrettable to lose bandwidth and network expenses. Vehicular Ad-Hoc Network (VANET) has been structured in a mobile network format. Vehicle-to-vehicle contact is important because it can improve road safety. The VANET technologies are mounted inside vehicle to provide comfort and protection to those on board. Small electronic devices can be used in the Ad-Hoc Network for the passengers in the same car. A server communication is not necessary in VANET network installation. The computer and other electronic devices on a van can be linked to each other inside the vehicle [2]. VANET is a self-organizing traffic information system. In VANET, each vehicle is regarded as a router and each of them is capable of transferring information from itself to another router. Path is the way to locate nodes in networks via routing protocols. The stability of a path in VANET is critical because each node is most likely a moving vehicle and not a stationary car. When cars are moved quickly, a road can be cut when vehicles are too far apart. The integration of people and technology enables systems to become more collaborative and effective. For a long time, wired connections have been used to receive missions, but because of the increasing need of wireless connections, users can receive information, such as sending e-mail messages to someone else or connecting to the Internet. In protocols in (Fig1.1) we used the OLS and DSR as an example of the two families.

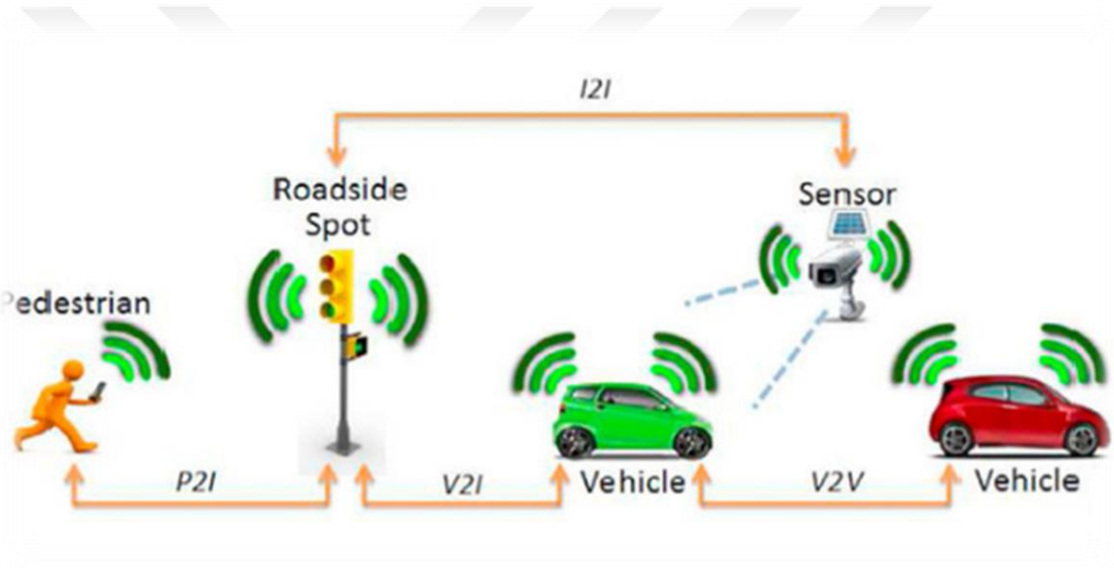


Figure 1.1: Communication Scheme Between Nodes in a VANET.

1.2 GENERAL BEHAVIOR FOR THE NODE IN THE MOBILE AD-HOC NETWORKS

The term Ad-hoc mean for difference topological network, independent and infrastructure less, which can provide dependable access. These hubs will use features of the ad hoc organization and have revelation if the way harmed, and will navigate and robotically make decision to participate or separate. This node is under contract and therefore it has an obligation of performing maintenance and self-healing to other nodes.

1.3 PROTOCOL ARCHITECTURE IN VANET

VANET protocol architecture facilitates collaboration between network nodes. The architecture is divided into two sections, the logic and the practical layer. For layered models, the OSI and TCP/IP models were used as foundations to fulfill all the requirements of a specific task or the user. Layered VANET system uses multi-hop and single-hop communication protocol whereby each layer is an individual module or common component. These layers are established to restrict valuable information from leaking to others. At this moment some of VANETs cannot be used as models in OSI model because of security and stability of its layers. VANET systems can be more trusted by users as they have adjustments and customizations as per users' needs. All applications and communication processes are integrated and provided as a single logical block along with sensors. This makes it more complicated and inflexible. This allows the consumer to personalize the VANET so all others are prevented from accessing it. There are clear differences between layered and un-layered versions. [3].

1.4 TRANSPORT LAYER

The cars are designed to store data that the vehicle can transfer to other cars and traffic lights. These vehicles would be able to communicate with each other in real time so that the user can create requested services. By utilizing this vehicular network system will allow Internet access or inter-vehicular peer applications. Many of these applications depend on Transport Layer Protocols (TCP).

There has been much discussion about the issues surrounding TCP in wireless environments. The researches prove that output of TCP isn't good. TCP packet loss means that you're experiencing network congestion. There are too many instances of congestion in wireless networks, such as bad channel conditions or collisions. If there is a loss, TCP can decrease congestion window size, effectively decreasing network throughput. Besides this problem, the usefulness of VANET is hindered by an absence of symmetry in VANET networks. This can decrease packet loss by incorrect RTT calculation, which results in unwanted retransmissions.

1.5 WIRED AND WIRELESS NETWORKS

The aim of serving in a wireless network is to allow everyone to communicate with each other and get to know each other without needing any substantial communication such as a cable between them. These types of wireless provide us with a wide range of applications, including connecting communes or devices that are known as cement movement areas for free connection. E-mails, Bluetooth, and the internet are examples of networks with varying periods of wireless intercourse. We can refer to this as a WLAN or a computer network, but the physical link or the use of a cable to connect them are not ideal. Wireless networks, rather than using cable, use wave radio to save money. The following is a potential interpretation of the work: Consider the two nodes A and C, as well as the computer link between them or any other device capable of arrowing information or data. Every node has a network modifier, and the connection has a router that uses it to connect to the network. When a node transmits data through radio frequency after encoding it in binary form, the data is pushed through the lattice's router. The node C will receive data from the antenna and decode it into binary form in order to convert it back to its original form [4]. When we talk about wires, they trigger a slew of issues in every network. This is obvious when we want to add a new gear with a new filament using the wire technique, which is supposedly needed at multiple steps. That implies that we will most likely be unable to do so, or that it will be extremely difficult or impossible to do so, since the cost of establishing a new network must be comparable, and widespread scale changes might not be feasible. Furthermore, the amplitude of the infrastructure is influenced by the lengths of wires that are connected together. The second stumbling block is the limited compatibility with wireless technology, especially mobile devices.

1.6 THE AADVANTAGEOUS OF WIRELESS

i. This makes the technology more useful and portable.

ii. Like, the meetings where these three people can touch each other only when necessary and spontaneously. This helps to collect relevant knowledge and improves method from it.

iii. We can connect to other computers within our network whenever we wish.

iv. Here, we concentrate on the costs and the difficulties of adding new hubs or relocating hubs in wireless networks, but that's different in wired network, so easy to do that and without spend a lot of money.
v. Possibility of visitor access: mercantilism within an entity is needed in circumstances where you'd like to share your system access with certain guests, such as clients or partners. Within a remote device, this would be necessary.

1.7 PROBLEM STATEMENT

Since the links between the nodes are complicated and challenging because they are complex, routing protocols face a challenge. The mechanism of routing to send the packet is used to determine the direction between the sources and the destination. The topology of the VANET network is variable also because the mobility of all the hubs in the system is variable; such hubs can freely enter and exit the system, so the routing between the nodes in the network is variable to maintain the network's stability.

1.8 OBJECTIVES

We have two great research objectives for this thesis:

i. To conduct a genealogical analysis of three VANET routing protocols: constructive, reactive, and hybrid.
ii. In this research on proactive and reactive using simulation, the impact of routing protocols in VANET in terms of density of nodes and different areas on those protocols will be discovered by comparing them to each other.

1.9 PROJECT SCOPE

i. We will choose one of two reactive routing protocols, DSR. To test these routing protocols in VANET, one protocol from constructive routing, OLSR, was used. In simulation, we can test network parameters such as node density and different areas.
ii. We will evaluate routing protocols using three efficiency metrics Average Throughput, Packet Delivery Ratio (PDR), and Average End-to-End Delay.

1.10 THESIS OUTLINE

Chapter 1 We go over the project presentation, problem statement, objectives, and finally project scope in it.

Chapter 2 contains a review of the literature on routing protocols, including their characteristics, challenges, and applications, as well as a classification of VANET routing protocols.

Chapter 3 explain how the methodology of the project to ensure the achievement of the desired goals and determine the parameters and metrics.

Chapter 4 include the simulation setup and discussion the results of the project.

Chapter 5 include the summary of the research (conclusion) and the future work.

2. LITERATURE REVIEW

2.1 INTRODUCTION

Developing VANET applications is difficult, although developing specific VANETs is not. The short summary is below: Not only does it describe in technical terms how the program structures itself, but it also attempts to approximate the human behaviour. It influences the Analogy. Two cars traveling at the same speed would also yield the same radio spectrum. The issue is not that people are moving around, it's that people aren't moving around enough. Traffic conditions such as traffic, vehicle activity, the rate of speed of accumulation, and the road itself all help to form a moving vehicle's pattern. The Frequency Disconnected Network: Information is shared in dynamic topology is often becomes disconnected. We also observed this dissociation in sparse networks. up to 14GB of dedicated memory and 3,000mAh of extra power Traditional cars are less able to store and supply power than modern cars are. Due to the high number of legacy systems used in VANET, processing capacity was reduced. Modern vehicles equipped with VANETs can assist in contact routing decisions. In terms of network topology, you can claim that dense networks have numerous communications while sparse networks have sparse communication [5]. A variety of objects, such as trees, houses, as well as other elements, block dense networks (sparse networks). Different methods for dense and sparse networks it will greatly assist in knowing where the nodes are located and movement detection by using a GPS and other onboard sensors. And when we succeed in attaining that, successful communication will be ours. VET apps and inter-vac contact several research studies concentrate on the broadcast processes of VANETs. These applications and techniques were researched and applied in different ways to identify them. Vehicle Communications Project imagined a variety of VANET applications, each of which ranged between 75 and 75 possibilities. Creative usage: A successful use of these tools may yield high benefits. Research into “VANET” was carried out by “Automotive Networks and Applications” and the analysis concluded that the results were negative. Although the aim of this method is to make life on the road more pleasant and facilitate driving, different methods are being used to assist in traffic management. Most efficiency applications distribute knowledge about road and traffic conditions to drivers in an effort to improve traffic flow distribution. Constant vehicle-to-to-to-vehicle networking occurs. The data obtained from their own sensors could be pooled and distributed to vehicles in the vicinity [6]. Travel time estimation is accomplished for various segments of the lane, and each is useful for different applications of traffic management. Drivers should plan for traffic congestion or use alternatives ahead of time. As a result, this would make a big difference in their travel time. Effective implementation and jobs of such applications would also lead to substantial reductions in fuel consumption and other cost reduction. Comfort software program assistance can be offered in a variety of different ways. Such an example is the discovery of available parking spaces and optimizing for traffic flow are great examples." These applications can tolerate a delay of any duration. Nonlimiting restrictions or threats do not face tight time demands. When one sector wants to collaborate with another, there is usually a need to redirect the flow of information [7]. Active protection is by far the most significant vehicle safety application. Our application goal in making the road safer is to decrease the number of casualties in the event of a crash. Accessing injury data over the longer period of time when use of safety equipment was lower allows one to infer that the number of injuries has decreased. This application offers a great opportunity for improvement and this could be done by distributing information about all kinds of dangerous conditions in the aftermath of an accident, including personal injury and defective road signs. Vehicles will greatly benefit from this app Thus, this type of application relies on data disseminating geographically and broadcasting the data specifically to particular locations. An excellent example of how [and tool] to use is geocaching, and geocaching [8] is both [useful and profitable].

2.2 COMMUNICATION PARADIGMS

All three networks are key if we include beaconing and unicast applications. Although on-demand and event-driven-oriented video were mentioned above, Bai [9] said that broadcasters could be separated into schedule-based, on-demand, and on-demand. Distribution of written materials. Scheduled transmission is useful for such applications as alarm in the interest of promoting safe and efficient running ahead of other vehicles as well as avoiding collisions as far as traffic control went, it had been as smooth as glass until they started painting the road white. These programs exchange information frequently and are sent as part of a MAC frame. People who live in the same town would hear about this if they talk to the other people in the same town. Effective methods and protocols for the delivery of multi-hop applications are required. For both pleasure and commercial purposes, unicast is extremely valuable. Criteria, requirement or criterion: Which do you think we should base our decisions on? Connectivity: VANs have various specifications for different and extensive uses [10]. These earlier requirements have been reduced to below, followed by more complex ones. Security applications have to scale when dealing with high-volume or complex networks, but fail if the network becomes dense. Usefulness: Ensuring that all members of the network understand the relevant information has been disseminated in the region. It's still a problem when you just have a small amount of bandwidth. To do this, the forward rate is avoided, but information is still sent to all nodes within the same geographic region it effectively stops broadcast storms, allowing for many broadcast applications to occur concurrently. Means that if anyone sees an item of value today, they should be able to see the same, or something very similar to it tomorrow. In order to preserve protection, apps must transmit information as quickly as possible, which is called 'dissemination time'. It is therefore recommended that the vehicle network disseminate routine information about delayed tolerance rather than partition the networks. Connectivity in the destination area can otherwise deteriorate the importance of the data All transmission is susceptible to error over the wireless, but packets are required for broadcasts to function correctly. A criterion can vary, so all the specifications are highly unlikely to be met. As in this example, when we achieve the desired or highest transmission rate, there are only a single failure points. When an individual message cannot be sent to the receiving unit, the rate of transmission to the whole system plummets (Wireless communication Channel is likely the reason). There needs to be a balance between these conflicting conditions in cases like this. [11].

2.3 ROUTING PROTOCOLS

Boxes make a road more manageable by organizing it into segments and splitting it into parts. There will be a number of group members and a group leader in each group. The leader can be chosen by placing it in the centre of the party. Symmetric module is used mainly in events shown in (Fig 2.1) driven transfers, however.

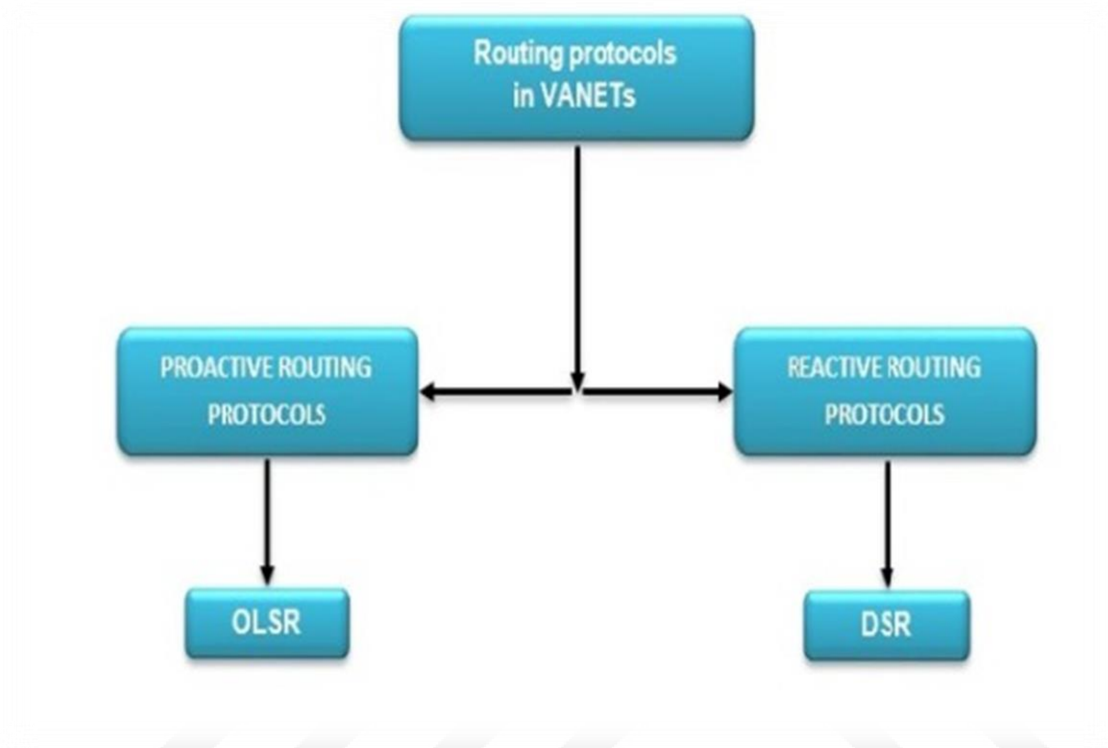


Figure 2.1: Types of Routing Protocols.

Node-event information is also warning other nodes about hazards that the group encounters to aid group coordination. Information transmission of this sort consists of details about the node like the speed, position, and direction is a nonstop. Due to the slower generation of digital signature generation and verification, this will be transferred using the EEC module. It's not restricted to any nodes in the trusted network. It's possible for any node to exit the network, for example, if a particular node leaves the party that defines the network. Also, any external nodes may join the trusted group at any time, and any time in which they are located near the trusted group will be counted as being part of it. To ensure the success of the group research, the researcher must perform simulations and include their findings in a future report. Vehicular cellular networking describes VMN for short, which was suggested by the Chinese professor Ye Zang [12]. Vehicles that are similarly situated will join forces to form a collection known as VANET. if one of the nodes in a mesh has information, it must immediately send the data to all other nodes in the mesh in order to get the information. It's a productive and money-saving networking approach. For eg, if A is a rope. It will encounter an obstacle on the path, but if a plane with B and C as the edges intersecting points passes over the rope, it will not. intelligence is provided on an obstacle, and a plan is devised to resolve it, for example, by slowing down or fully diverting from their original course. Since B and C have never met each other, it is not appropriate that they have seen what A has done. Vanity: The study conducted a VANET test in 2010 and ran a simulation with the VMESH protocol. Three hours is what it simulated. Several assumptions were made which were required to create the data that was fed into the model. As in the example, a Poisson distribution also illustrated the trip time it took for a vehicle to travel from one place to another. It was expected that this would take place with free flow of traffic. Thirdly, it is possible that an EO will spontaneously shows up. Furthermore, it is possible to instantly disseminate knowledge about an EOI to other nodes in a mesh. The Nagel-Schreckenberg vehicle simulator is used by Liu et al to simulate the movement of the nodes; this model was first presented in 1992 by Nagel and is still accurate today. The simulation's results were based on an analysis of mean knowledge loss times. [13] "This is known as the average amount of time, or time interval, before a financial return can be lost" The measurement was performed by taking the difference between the capture time of the EOI and the last vehicle and the time the first node's closest registered location to the captured EOI. They found that the average time to the knowledge loss on one-way roads inversely associated with the travel speed. The mean time needed to loss of information for two-way traffic was almost two times that of one-way traffic. An analysis revealed that it was possible for vehicle nodes on the opposite side of a two-way highway to store ROI because the intersection wasn't in the given lane of interest. In VMESH, a route is significantly more stable when driving in the right direction than when driving the wrong way. An OSPF Topology-based routing protocol can be roughly placed into two categories: a topology routing, as defined by topology can be further broken down into constructive protocols and reactive routing protocols for each vertex, the vertex routing table maintains a database of other vertices to which it is connected. There is an expression in academia which describes the Fished State Routing, called the "constructive routing." The only problem is that the network load is heavy. The routing method often takes a long time to process. Using a reactive routing protocol prevents the network from suffering from malfunctioning. There will be no new nodes in the network when information is required, and no new nodes will be added when nodes are in this protocol are communicating. As a result, the load on the network has been reduced. It is a relatively new type of distance vector routing protocol. The router may be configured to do unicast or multicast routing. Using this protocol, the amount of time to set up a connection between two nodes is slightly increases. When the car is in the tunnel, however, GPS signal is often hampered by the density of the surrounding matter. Delay-avoidance Network (DAN) can be employed to help us with this issue. When a node disconnects, the data packet will be re-issued. Another technique is to remove the communication record from any nodes adjacent to it. Additionally, each node has a beacons which pass on short bits of data at specified time intervals. If no new data is found after a specified amount of time has passed, the node is considered to be disconnected. Instead of applying the new Geographical Routing Protocol (GPR) proposed by Lochert [14], one could combine the geographic-based routing method with the topology-oriented method. Source routing and a-based routing are also used in the Dynamic Source Routing (DS) protocol. It consists of two phases, as shown in (Fig.2.2). Namely phase one is route exploration and phase two is route maintenance. DSR doesn't use route messages on a set time scale. There will be an error message printed if there are any broken links. These ID values for the intermediate nodes are included in the DSR packet. If multiple routes lead to the destinations, DSR can handle more. Two of the main differences are: In AODV, only the address of the destination node is used when a packet is sent. In the case of AODV, a node must send all of the relevant routing information, which causes a significant increase in packet-forwarding time. AODV, a node must send all of the relevant routing information, which causes a significant increase in packet-forwarding time. [15]

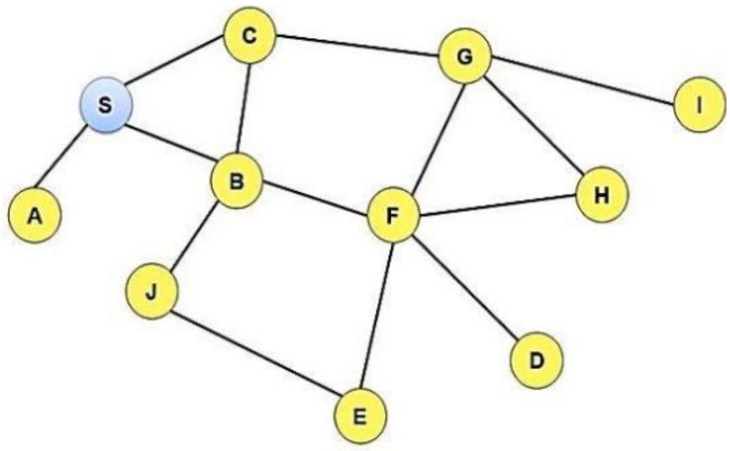
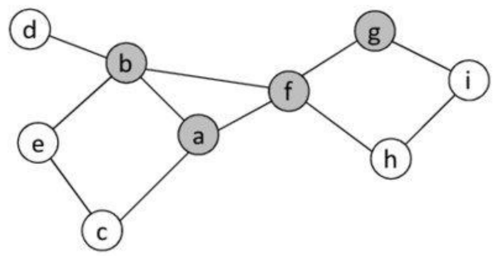


Figure 2.2: Example of a DSR Routing Protocol.

Optimized Connection State Routing (OLSR): Proactive Connection State routing protocols provide guidance to the algorithm in the form of heuristics. More out-of-of-the-the-the-the-box results mean topological information can be shared due to network topology changes. For maximizing interaction with topological changes, routine messages can be increased to get a better distribution of messages over time. At a deeper level, as shown in (Fig 2.3) OLS also offers information on how the total connectivity of various segments of the network shifts over time. OLS is correct for this situation, since the packets have not been overdue for a long time." The OLS has a highly interconnects a wide range of nodes. OLS reduces control workload, using less MPR status updating procedures while the correlation defined LOWER than the normal one. When you raise the number of mobile nodes, you still have to retain the routing table on all possible routes, so that they don't deviate. In this section, the Optimized Link State Protocol is extracted from its RFC 3561[16]. OLSR is a pro-active routing protocol, so routes are often available immediately when necessary. OLSR is a pure state communication optimization protocol version. As a result, topological changes cause all hosts in the network to inundate topological information. Multipoint relays are used to reduce the possible overhead for the network protocol (MPR) [17]. The idea of MPR is to prevent broadcast flooding, by restricting broadcasting in some areas of the network, and later in this chapter you will find more information on MPR. The shortest path is a further reduction. Decreased time for the transmission of control messages would increase reactivity. OLSR uses two types of control messages: Hi and Control Topology (TC). Hello messages are used to find out about the state of the link and neighbors to the host. Hello gives a Hello message describing which neighbors choose this host to be used as an MPR, and the host can calculate its own MPR set from this information. Hello messages are transmitted only one hop forward, but TC messages are transmitted throughout the network. The TC message is used to broadcast information on the MPR Selector List of its own advertised neighbors. Transmission of TC messages is common and only MPR hosts can transmit messages. [17]



MPRs	Selector Set
a	b, c, f
b	a, e, f, d
f	a, b, h, g
g	f, i

Figure 2.3: Example of an OLSR Routing Protocol**.**

2.4 DEFINITION AND DRAWER THE CHARACTERISTICS OF MANETS CLARIFIED AS FOLLOWS

1. Non-Party nodes: The hubs in the specially designed portable systems are self-sufficient in their simplicity, and the end points are not simple, and these nodes act as routers and hosts (the node and the neighbour node in the network (in any environment) [18]

2. Distributed to you work: The aim of these networks is to permit the increase in quantity of usage; since the existence of an infrastructure precludes the use for that purpose, thus each one is strictly limited to that one.

3. Architectural and implementation: When we discuss the architecture and implementation, which rely on specialist systems and variables, they are single or multi-staged. The multi-staged one is more time consuming and more elaborate than the single-staged type.

4. Dynamic topology: the fast and eccentric portability of the lapped hubs can influence to a different type of connectivity with the topology to cope with the traffic challenges, the VANET must attempt to adapt to different network environments and mobility patterns. therefore, using the network protocols among the nodes for any use [19]

5. Node: Since in the impromptu systems, no foundation and each node has its own batteries, but all nodes are connected to the portable transmitters, there is no way for it to maintain its stored content, resulting in a link between transmitters and receivers. Thus, the only way to do that is to employ an appropriate algorithm.

2.5 ON-DEMAND ROUTING PROTOCOLS (REACTIVE PROTOCOLS)

Convention conventions do not necessarily hold the data unless they desire it; rather, when they want it, the systems request it and send, and if they don't have the right information, the node sends, unless it receives the data from the system. Since the source node wants to send information, it must send a request at least one hop before receiving the answer. Both of these problems stem from the same source - the flooding of the nearby nodes which also reduces network throughput. So long as we have the specific information, we will find our way to the next step using this method. In general, the middle node that has routing information can return to the source or get a node in the middle. The first iteration of the broadcast is restricted to the immediate neighbours until it is found to be of interest to all the network hosts on the network. Before you send the message, the protocol must choose the best route. It will be done that way. If the unknown paths are unknown to the nodes, the faulty links can slow down delivery of reactive packets. In most cases, temporary memory is employed to lessen the amount of time it takes to get the connection established.

Due to the fact that information in memory will be slow to change, thus, the route in this setting will be incorrect for a short period of time. Avoid using old cached data wherever possible to be tolerant of delays when on-demand protocols are being used, it must be able to cope with unpredictable time-to-to- build routes. The on-demand route channel has limited routing expertise because it is for traffic and not a high-power path requirement there are many protocols like ABR: The protocols have associativity. As a critical feature the ability to extract and offer paid advertisement related to mobility in the (DSR: Dynamic Source Routing Impact, CED: Distributed Ad hoc Routing Core).

2.6 TABLE-DRIVEN ROUTING PROTOCOL (PROACTIVELY PROTOCOLS)

in the case of proactive routing, this kind of protocols is anticipated to keep details for all the nodes which are introduced when two or more networking protocols are required If there are no changes to the neighbour settings in the network, the event based protocols persist and do not route packets, regardless of what is specified here. is there been some effect or does it produce an effect? If there is a shift in the node or a mistake on a connection, the protocol will transmit a message to another. Often, if a shift occurs in the topology occurs at regular intervals, the modified information is propagated to other nodes and the nodes that must be checked constantly will also receive these changes at equally timed intervals, so the more away they are from the adjustment, the less often we can they should receive them. This idea seems logical if the closer nodes are of greater bandwidth/traffic capacity than faraway ones. It will be a waste of resources to still overwhelm the network with information just to benefit those far away from the topology update. Routing tables have the benefit of maintaining their own overhead without depending on the amount of entries in them, but do not require frequent upkeep. This is appropriate in networks with a few or moderate nodes as there are in that form of networks with numerous data sessions The event-driven protocols are, among others, the following: A cluster-based routing protocol that does not need peer agreement for each update Popular Gateway Services - Gateway Routing Appropriate and appropriate updates to the DSDV: Destination Sequenced Distance Routing Protocol regularities: Two roads meet in at an imaginary right angle on a gradient of 1/3 with a turn in the third lane. A Classless Optimized Interior Gateway Routing.

2.7 SECURITY ISSUES

To secure a wireless network such as VANET, threats and vulnerabilities need to be recognized and solutions must be implemented. If information is tampered with, it could cause accidents on the road. Generally speaking, VANETs security requirements can be divided into five principal components: authentication, confidentiality, availability, and non- repudiation of data, plus some other considerations such as personal safety and productivity. A research paper that was released in 2013 identified the authentication criterion as being a confidence that the nodes in a connection chain are actually belong to the same database. Therefore, in order for this to occur, each car must be registered with an authority in advance of driving it. We use strict data protection rules so all data must remain private and confidential. Exposure of this information may lead to leaks and tampering with other nodes. The results of one or two careless or malicious mistakes can be disastrous if the hackers plan to overwrite the data with new instructions that will allow the nodes to misbehave. The data integrity requirements state that all data retrieved has been examined by an authenticated node to ensure that it is precisely the same as that was sent out. Nothing can be done to the data until it is out on the wire. A working framework must guarantee data availability Receiver checks should be performed to make sure that none of the batteries have power going to the transmitter. Often, it should be assured that the routing protocol cannot be jeopardized by any hackers. This criterion from Matthew and Kumar is used to define non-repudiation in their definition of the vehicle: the vehicle must accept responsibility for having transmitted the data. Similarly, the recipient node is obliged to admit they have accepted the data. There are many and diverse kinds of security attacks on VANET. Any network attacks target mainly a few sites or a certain user class of people with particular goals in mind, while others want to impede the network, cause chaos or subvert perceptions for reasons of their own. Examples of the latter include trolling, downhole denial of service (kudos), bog hole assault, load distributor, and misbehaving nodes. A Sybil is a scammer sets up some fake identities of itself. In the real universe, one node equals one car; but, in the digital world, several nodes may be mapped to the same vehicle. The data from these duplicates may be causing other nodes to misjudge the network congestion, causing them to go elsewhere to get to their intended destinations. This heretical node is acting selfishly, because no other nodes can be in close proximity to it. A node can stop a Sybil attack by keeping track of other nodes for a certain amount of time. There are differences in data between the interval stretches over (connecting nodes), and it is contrasted with the data seen at its neighbours'. Any deviations from the expected results would be investigated and potentially exploited. During a Distributed Denial of Service (DDoS) attack, the aim is to prevent nodes from accessing the VANET. Jamming the network works just the same as it does with email. Nodes would be unable to keep talking to other nodes while under DDoS attack, which can lead to accidents. It uses various methods but has the same end goal: to the Denial of Service attack. This attack passes through the attacker node, leaving no alternative path open. If an attacker controls the records, it might be possible to reroute the other vehicles, or make malicious data appear on the road, which will increase the danger of an existing on the road. [20]

A dishonest node can manipulate a vehicle's original signal before broadcasting it to other nodes. Therefore, other adjacent nodes perceive only a transitory, or virtual, but not a real, link. Another of Lu said that the azimuth could be adjusted. The azimuth is the relative angle between two points on the path. To relay azimuth, protocols like VANET and GeoDNT use the rule of hand. When a wrong is done, the rules of the hand are broken. However, in accordance with the rule of the right, the information is sent to other nodes, some of the non-injected nodes aren't there and one of the injected nodes is.

2.8 PROTOCOLS FOR LINKING STATES AND DISTANCE VECTORS

The best path from the source to the target in the Ad-hoc arranges will be determined by the steering conventions. In this way, the conventions are so essential in the VANET. We may also characterize the relation state and the separation vector conventions. We'll go over it in more detail later.

1. Distance vector protocols: The word distance refers to the context, where these protocols rely on to choose the best path between the source and the destination, and choosing the best path is based on the shorter path or the fewer hops from the source to the destination. As a consequence, hops serve as a unit of distance measurement, with packets lost and delays to the destination Any time a packet is sent from the source to the destination in the VANET. The (fig 2.4) explain the operation of the distance vector protocols. [21]

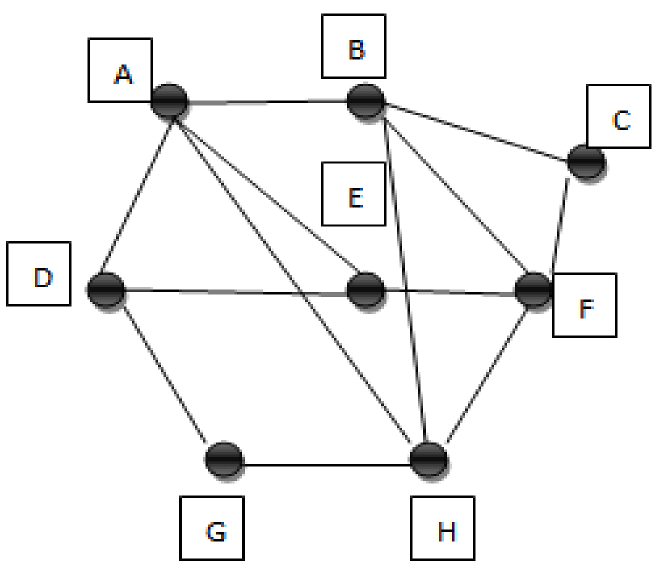


Figure 2.4: Activity of the Distance Vector Protocols.

The node routes are represented by black dots labelled S, T, V, W, X, Y, &Z. The distance routing protocol's approach works as follows: Each node in the network contributes to the distribution of distance vectors for other nodes, which is dependent on the information available from the nodes. And we'll clarify how those nodes select the easiest or shortest path to their destination.

After completing the computation for each node as shown in the table, take the best or shortest path in the network, and then take node Z and compute the routing table for it as shown in the table above. As a result, route Z will know from the routers X&T that route U is just one of their two routers X&T, and route H will know that the routers X&T are a neighbour of it. As a consequence, it must hop away from it through its route neighbours (X&T) in order to reach the U.

2. Link state protocols: In this way, the protocols have a full understanding of the network, and it is also referred to as the shortest path. As a result, it has three tables to give you a complete picture of the network: the first table contains full details about the neighbors' directions, the second table contains full details about the network's topology, and the third table contains full details about the main routing table. When they connect, they share all the information between the hubs in the system. (OSPF) Open the narrowest path first, followed by (ISIS) a transitional framework to the middle framework.

Each node in the network has those three tables, and the node that activates connection state begins to discover its neighbors' node tables, bandwidth and delay for all neighbors' nodes, and also sends the routing update information. Finally, use the Dijkstra calculation to determine the best or shortest path [22].

2.9 DISTANCE FROM DESTINATION TO DESTINATION PROTOCOL OF VECTOR ROUTING

This protocol employs the Bellman Ford in an ad hoc networking environment, and it belongs to the proactive protocol community, which systematically updates knowledge. When we talk about mobility nodes in an environment, at the point when the hub needs to send the information to another hub should that node have information about that node to avoid the loop, they add the sequence number to the directing table that table has a rundown of all goal, the new idea in the protocol when we want to incorporate routing mechanism to work with a variable topology when we talk about mobility nodes in an environment at the point where the hub needs to send the information to another hub should that node has information about This number (sequence number) was calculated from the destination and sent along with the update. All of this in order to stop a network loop, choose the correct path, and cancel the route that has no purpose. Both stations (nodes) relay it table routing to the neighbors on a regular basis with new changes if there is a change in topology, which means moving any node out of the network or disconnecting. In general, we can assume that the update is event-driven as well as time-driven.

When we find a space in a packet, we can use it to provide modified routing data, but most importantly, we can prevent extra traffic when the network is secure. As a result, we employ gradual updates. Full dumps are rare since there are few changes and the data sent will be excessive. But, in a rapidly evolving network, the gradual packets will grow large and must be precise in one packet, making full dumps more likely.

Clamped the routing packet update with steering table information in addition to the succession number. All of this is done to prevent the occurrence of loops in networks and to avoid routes that have no purpose, and if two courses have a similar number (sequence number), it will choose the best course or the most restricted course based on previous history. The assessment station can measure the time settling of routes for each destination by keeping a probable weighted average over the most recent updates.

The length of the settling period they can delaying the broadcast the mobile will decrease the moving of the network traffic and increase the routing that will be due to the destruction of that broadcast if there is any new best route discover.

2.10 TABLE DRIVEN AND ON DEMAND ROUTING PROTOCOLS ARE HYBRID

To take advantage of all of the features, this type of protocol incorporates on-demand and proactive routing. So, routes are maintained from constructive protocols, but only for some of the nodes that essentially share the network (active receivers), and the regulation for the size and repetition that depends on the network division, such as into zones of the zrp protocol. They will discover the reactive route in the network using the reactive protocols [23]

3. METHODOLOGY

3.1 INTRODUCTION

In Figure 3.1, three phases of study were formalized selecting an appropriate network simulator (setup and simulation details), and then conducting the simulation (execution); the study portion of the report is conducted after the simulation has been completed.

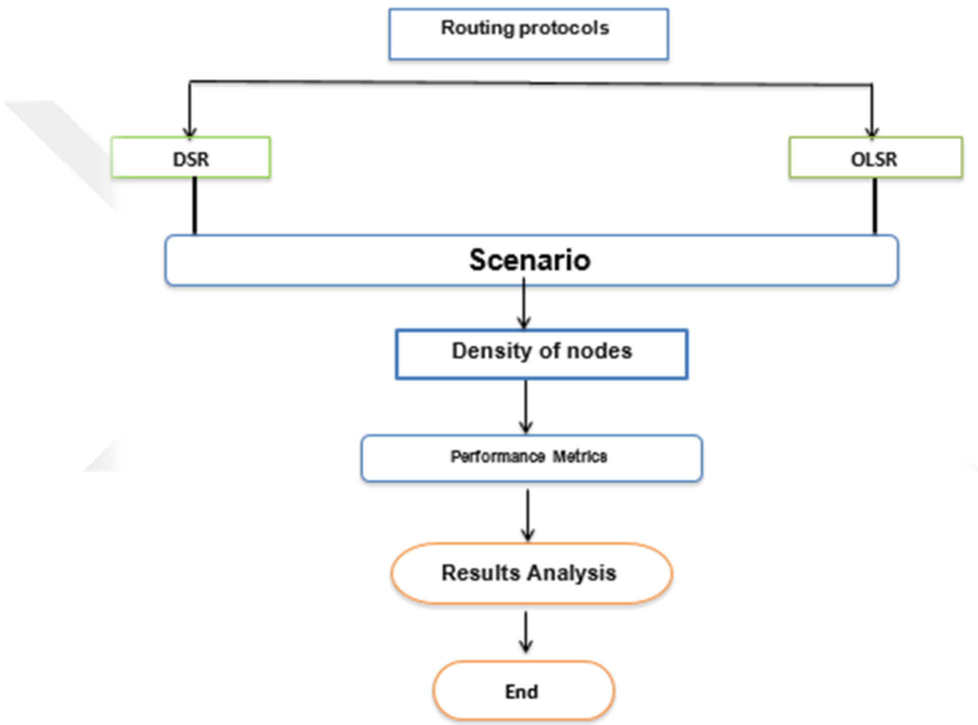


Figure 3.1: Methodology.

3.2 JUSTIFICATIONS FOR CHOOSING NETWORK SIMULATOR (NS-3)

Reasons for using ns3 include studying systems with complex behavior, to understand more about network behavior in a controlled context, and to do experiments that aren't realistic in the real world, to research or verify in a live condition. The network is designed to be accessible and extendable, so that it can be used for science and education. In essence, ns-3 models how packet networks operate and offers a simulation engine for users to conduct experiments. Ns-3 can be used to conduct experiments that would be too complex to perform on actual systems, to examine system behavior in a regulated, reproducible context, and to research how networks function. The accessible ns-3 model range encompasses protocols and non-based structures.

Many simulation tools exist for network simulation studies. Below are a few distinguishing features of ns-3 in contrast to other tools.

i. Ns-3 is intended to be a set of libraries which can be integrated with other external software libraries. Although some simulation systems offer users an integrated, single graphical user interface environment in which all activities are performed, ns-3 is more modular. Several external animators and data and viewing software can be used.

ii. Ns-3. Ns-3. Users can however prepare to work with C++ and Python software development tools on the command line.as shown in the (Fig3.2).

iii. Ns-3 mostly applies to Linux or Mac OS systems, while BSD systems and Windows frameworks that can develop Linux code, like Windows Subsystem for Linux and Cygwin, can be supported. Native Windows Visual Studio is not funded at the moment even though a developer works on potential assistance. Windows users can use a virtual Linux computer, too.

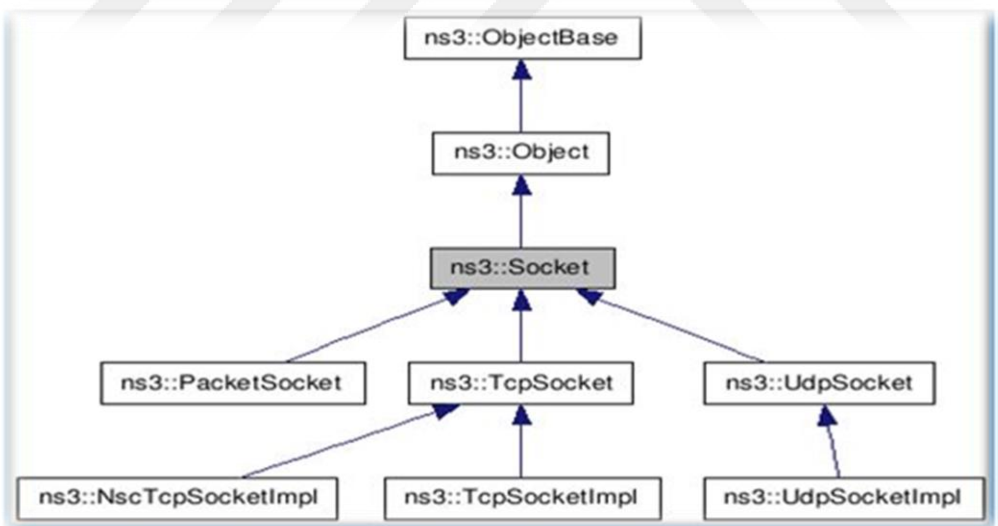


Figure 3.2: NS3 Simulator Design.

3.3 SIMULATION SETUP

This chapter describes various appropriate environments, which have been laid out in detail in chapter 2, and here we shall describe all the following procedures step in the Table 3.1 in the simulation scenarios, going through one key step at a time: This is where we test DSR, OLS, and OLSR by applying these settings to the three simulations. And the second step for evaluating OLS and DSR would be to collect protocol efficiency measurements for each routing protocol.

Table 3.1: Performance Evaluation Parameters.

Parameter Name	Parameter Value
Protocols	OLSR,DSR
Nodes	20,40,60
NS2 Version	NS3.27
No. of sources	rundown
Time of simulation end	20seconds
Node speed	20m/s

3.4 A. GOOD PUT

The portmanteau of "nice" and "performance" is that the network use of useful bits to supply a specified target. Anything that needs to be transmitted through the upper and lower protocol layers is called part of the total amount of data. The sum of time required from the very beginning of the first packet to the very end.

3.5 B. PACKET RECEIVES RATE

The packet is designated for the destination only.

3.6 C. OVERHEAD

Networking overhead happens to be the same for data packets almost all, because they are known to be routing packets. This overhead is referred to as overhead [1] or overhead [11].

3.7 SUMMARY

We discussed the analysis methods in this chapter. We went through - stage in great detail to ensure that the results verification went smoothly and that the desired outcomes were achieved. The results and interpretation of the guiding conventions will be presented in the following sections OLSR and DSR to demonstrate the best convention in the various situations.

4. SIMULATIONS RESULTS

In this article, we have three seniors to test the (OLSR and DSR) protocols in each of the seniors that we submitted, for example, tow the 20 nodes as illustrated in (Table 4.1) and compare the results using the efficiency metric, and check which protocol is the better protocol between them in (Figure 4.1)

Table 4.1: Parameters For The Nodes.

Parameter Name	Parameter Value
Protocols	OLSR,DSR
Nodes	20,40,60
NS2 Version	NS3.27
No. of sources	rundown
Time of simulation end	20seconds
Node speed	20m/s

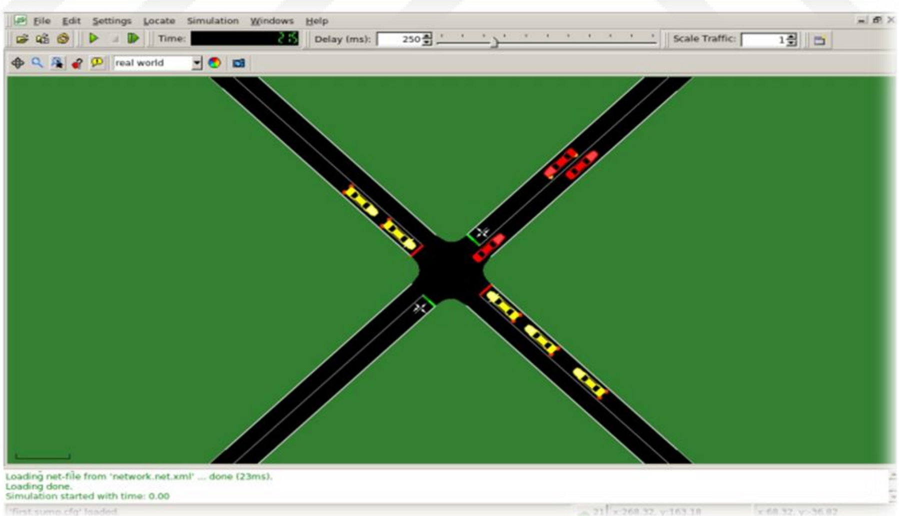


Figure 4.1: Seniors of the Vehicle.

A. The scenario of the 20 vehicles: In this case, the protocols were extended to 20 nodes with 20 seconds on both protocols (OLSR and DSR) and the effects were seen in Figure 4.2 and Figure 4.3 Despite the overhead, a significant improvement in the OLSR protocol was observed, showing positive results in the case of packet receiving rates. This, in comparison to the DSR protocol, is a simple decrease when compared to the OLSR protocol, as it did not provide significant results for Packet receives a rate as compared to the OLSR protocol.

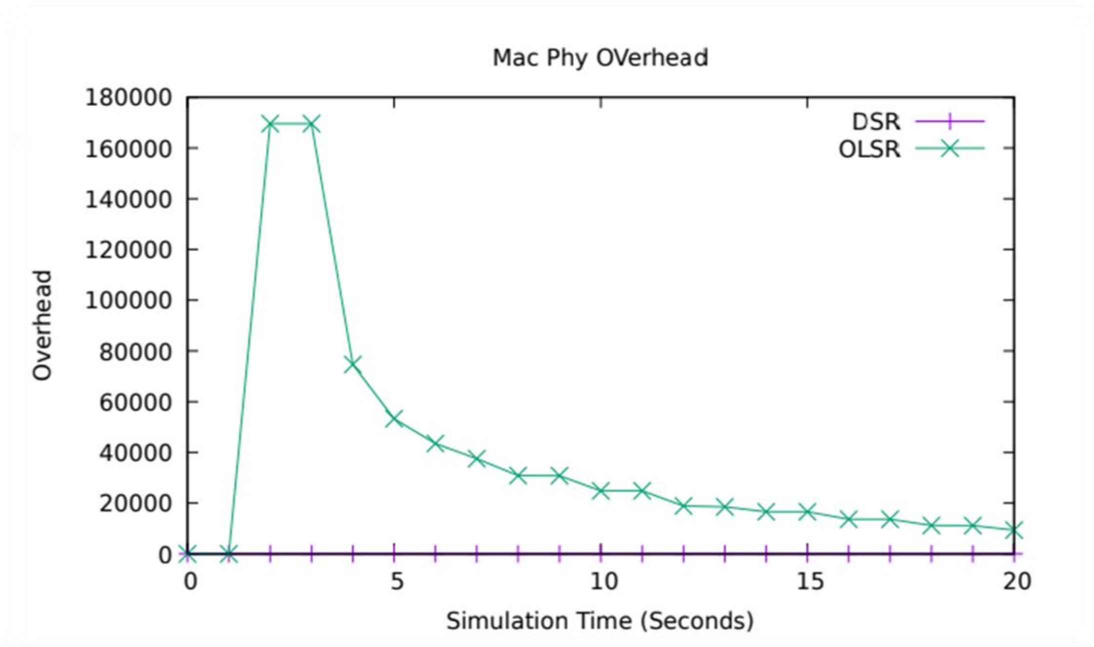


Figure 4.2: Seniors of the Vehicle.

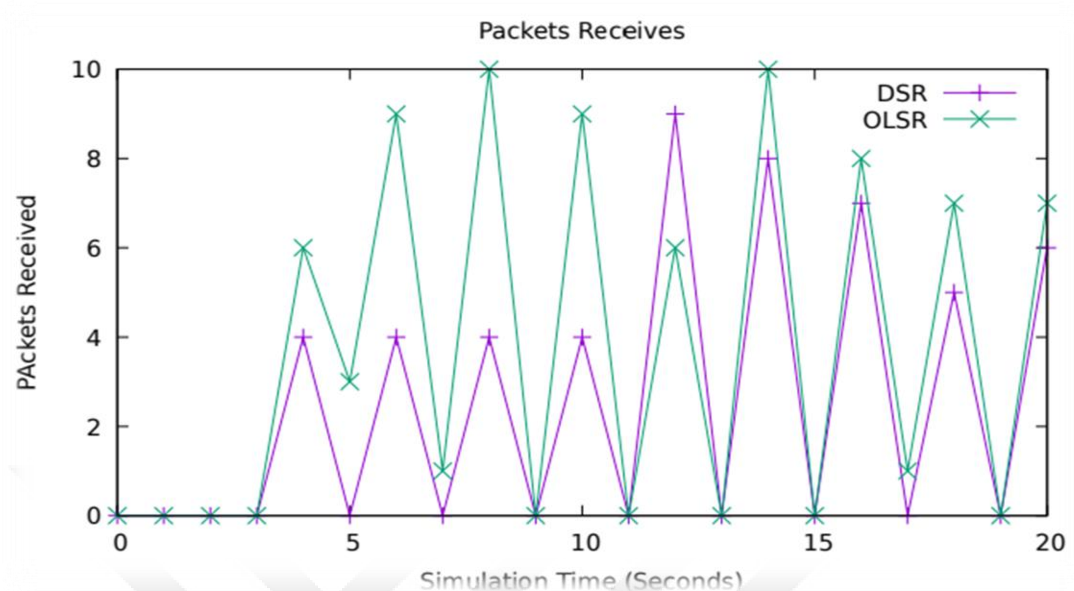


Figure 4.3: Seniors of the Vehicle.

B. the scenario of the 40 vehicles: In this case, the protocols were extended to 40 nodes with 20 seconds on both protocols (OLSR and DSR) and the effects were seen in (Figure 4.4) and (Figure 4.5) A significant increase in the OLSR protocol was found amid overhead, showing positive results in the case of the packet receiving rate, but there was a notable gain from overhead, as well as the packet receiving rate. This, in comparison to the DSR protocol, is a simple decrease when compared to the OLSR protocol, as it did not provide significant results for Packet receives a rate as compared to the OLSR protocol.

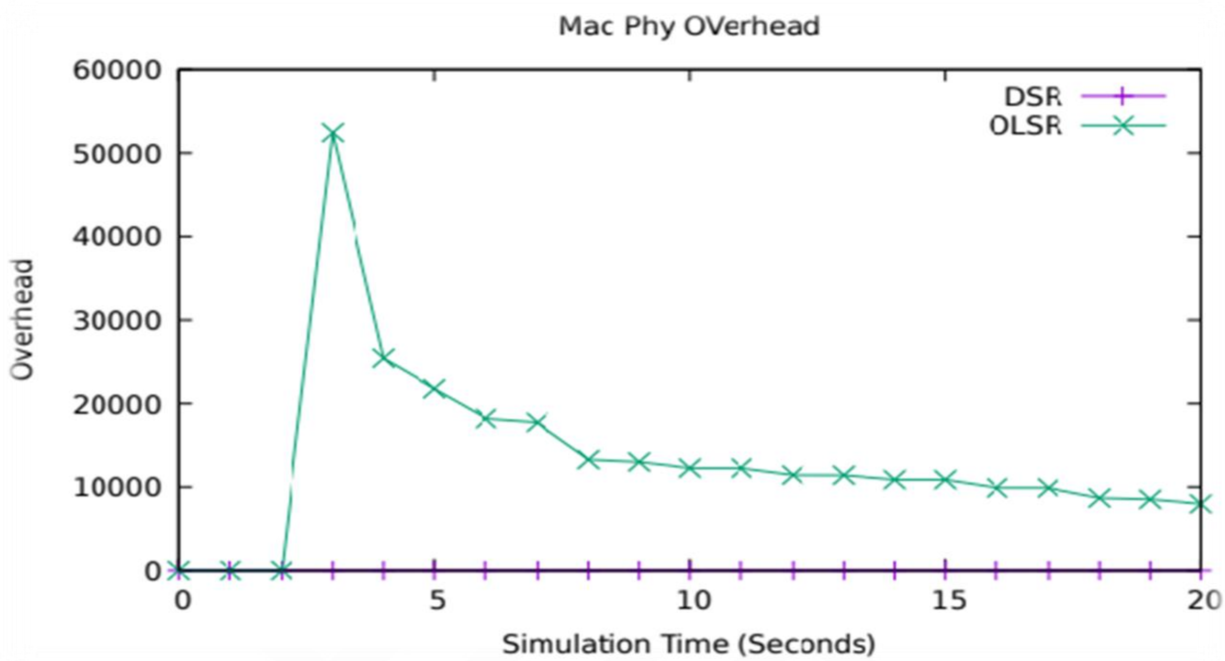


Figure 4.4: Seniors of the Vehicle.

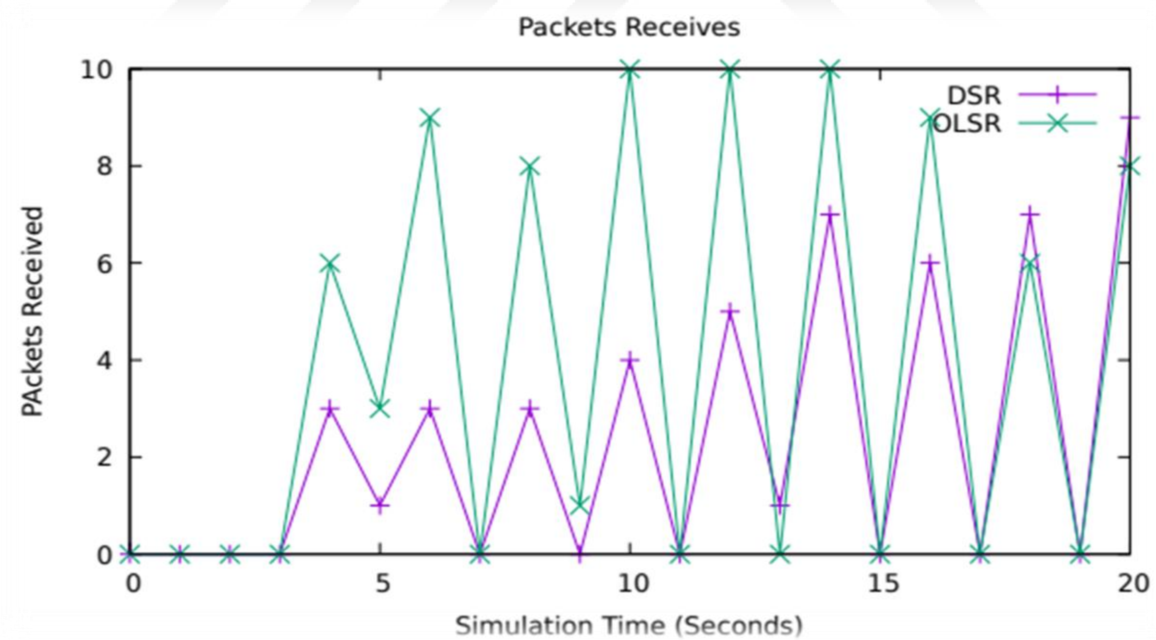


Figure 4.5: Seniors of the Vehicle.

C. the scenario of the 60 vehicles.

In this case, the protocols were extended to 60 nodes with 20 seconds on both protocols (OLSR and DSR) and the effects were seen in (Figure 4.6) and (Figure 4.7.) A significant increase in the OLSR protocol was observed amid overhead, showing positive results in the case of Packet receives rate, but there was a notable change from overhead, just as Packet receives rate when we compare with ourselves in the 20 and 40. This, in comparison to the DSR protocol, is a simple decrease when compared to the OLSR protocol, as it did not provide significant results for Packet receives a rate as compared to the OLSR protocol. Good placed the two protocols in three scenarios of 20, 40 and 60 nodes in 20 seconds. Here, the DSR protocol is stronger than the OLSR protocol in (Figure 4.8.) This can be seen in all the scenarios chosen. While the DSR protocol struggled in the amount of packets received, it demonstrated a very strong condition in all environments as well as overhead relative to the OLSR protocol.

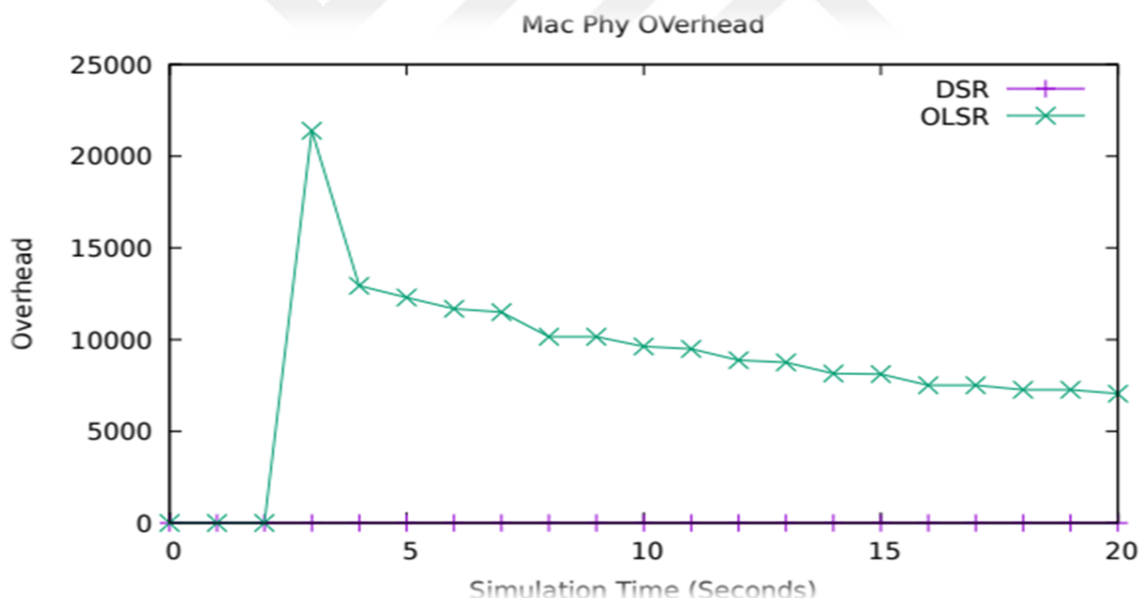


Figure 4.6: Seniors of the Vehicle

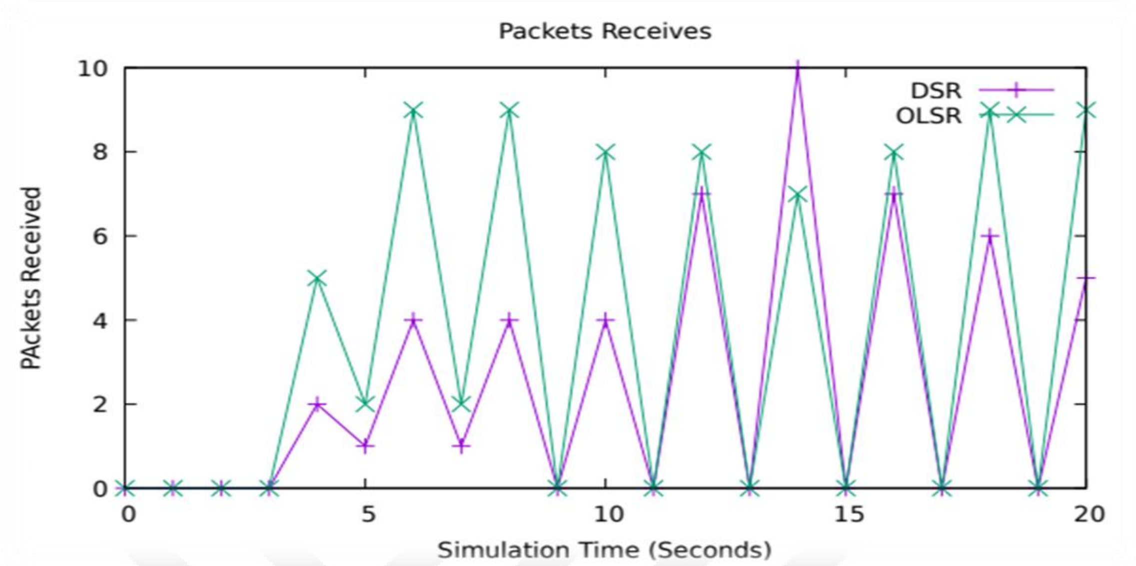


Figure 4.7: Seniors of the Vehicle.

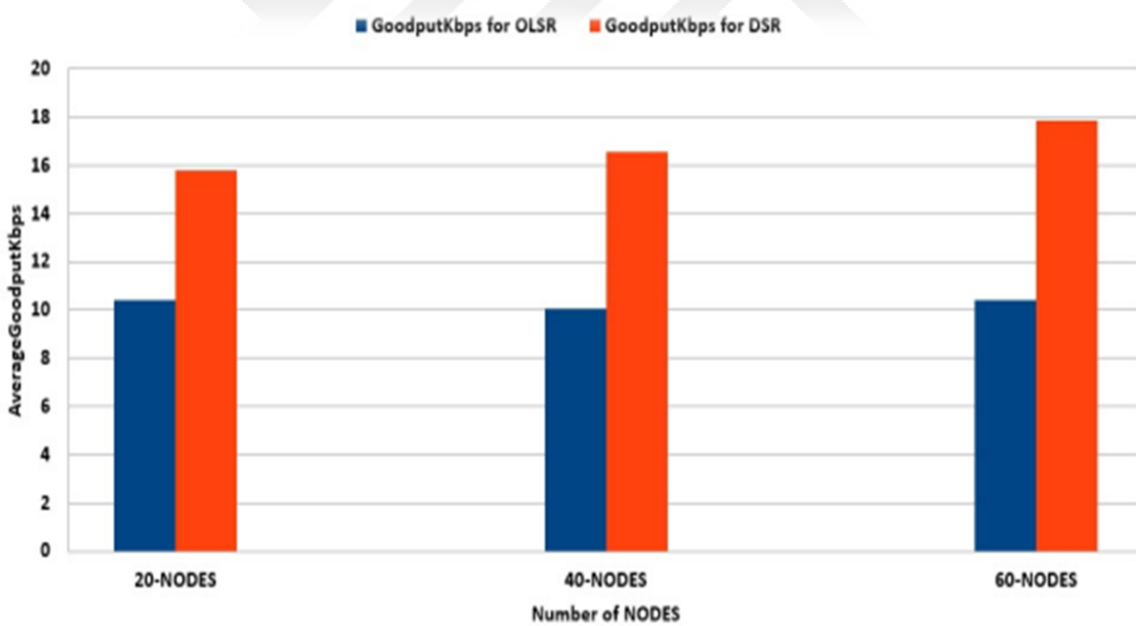


Figure 4.8: Seniors of the Vehicle.

5. CONCLUSIONS AND FUTURE WORK

5.1 CONCLUSIONS

In this analysis, the protocols (OLSR and DSR) were tested in three separate situations in order to assess the characteristics of each protocol under different circumstances. The outcomes were shown in the Despite the overhead, a large increase in the OLSR protocol was observed, with good results in almost all cases of Packet receives rate. However, it showed a substantial change from the overhead, as well as Packet receives rate in 60 nodes as compared to 20 and 40 nodes. This is in contrast to the DSR protocol, which showed a strong decrease in when compared to the OLSR protocol, despite the fact that it did not produce statistically significant results for packet receives rate when compared to the OLSR protocol. As compared to the OLSR protocol, the DSR protocol failed in the number of packets received rate, but it performed admirably in all other environments and in terms of overhead.

5.2 FUTURE WORK

Putting these protocols together with other protocols in different environments to know more details and characteristics about the nature of these protocols work in changing circumstances, taking into account other measures to reach the closest path between the sender and the recipient and keeping data in record time.

REFERENCES

[1] P. G. Shinde and M. M. Dongre, “Traffic congestion detection with complex event processing in VANET,” in 2017 Fourteenth International Conference on Wireless and Optical Communications Networks (WOCN), 2017, pp. 1–5.

[2] A. N. Hassan, O. Kaiwartya, A. H. Abdullah, D. K. Sheet, and R. S. Raw, “Inter vehicle distance based connectivity aware routing in vehicular adhoc networks,” Wirel. Pers. Commun., vol. 98, no. 1, pp. 33–54, 2018.

[3] M. Dixit, R. Kumar, and A. K. Sagar, “VANET: Architectures, research issues, routing protocols, and its applications,” in 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016, pp. 555–561.

[4] B. Vidhale and S. S. Dorle, “Performance analysis of routing protocols in realistic environment for vehicular Ad Hoc networks,” in 2011 21st International Conference on Systems Engineering, 2011, pp. 267–272.

[5] A. Sahoo et al., “Performance Evaluation of AODV, DSDV and DSR Routing Protocol for Wireless Adhoc Network,” in 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2018, pp. 348–351.

[6] M. S. M. Shihab, A. A. Ibrahim, and A. M. Shantaf, “Evaluate the DSR and OLSR Routing Protocols in different scenarios under NS3 and SUMO Using the NETEDITOR in VANETs,” in 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2020, pp. 1–5.

[7] C. Gautam and A. Patel, “Improving Route with Automatic MPR Selection Using OLSR Routing Algorithm in Mobile Adhoc Network,” 2019.

[8] A. Ayoob, G. Khalil, L. Yingzhuang, M. Chowdhury, and T. Al, “Efficiency Broadcast Base Safety Message BSM Through VANET Based on Transmit Packet Coding (TPC),” in 2020 IEEE 2nd Global Conference on Life Sciences and Technologies (LifeTech), 2020, pp. 383–387.

[9] S. Ali and P. Nand, “Comparative performance analysis of AODV and DSR routing protocols under wormhole attack in mobile ad hoc network on different node’s speeds,” in 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016, pp. 641–644.

[10] Y. Ben Chigra, A. Ghadi, and M. Bouhorma, “New Metrics to Evaluate the Impact of High Mobility on AODV Routing,” in The Proceedings of the Third International Conference on Smart City Applications, 2018, pp. 902–911.

[11] C. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vector routing,” in Proceedings WMCSA’99. Second IEEE Workshop on Mobile Computing Systems and Applications, 1999, pp. 90–100.

[12] Y. Zang, L. Stibor, B. Walke, H.-J. Reumerman, and A. Barroso, “A novel MAC protocol for throughput sensitive applications in vehicular environments,” in 2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring, 2007, pp. 2580–2584.

[13] B. Jarupan and E. Ekici, “A survey of cross-layer design for VANETs,” Ad Hoc Networks, vol. 9, no. 5, pp. 966–983, 2011.

[14] A. M. Shaban, S. Kurnaz, and A. M. Shantaf, “Evaluation DSDV, AODV and OLSR routing protocols in real live by using SUMO with NS3 simulation in VANET,” in 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2020, pp. 1–5.

[15] S. A. Ade and P. A. Tijare, “Performance comparison of AODV, DSDV, OLSR and DSR routing protocols in mobile ad hoc networks,” Int. J. Inf. Technol. Knowl. Manag., vol. 2, no. 2, pp. 545–548, 2010.

[16] S. Mohapatra and P. Kanungo, “Performance analysis of AODV, DSR, OLSR and DSDV routing protocols using NS2 Simulator,” Procedia Eng., vol. 30, pp. 69–76, 2012.

[17] E. Spaho, M. Ikeda, L. Barolli, F. Xhafa, M. Younas, and M. Takizawa, “Performance evaluation of OLSR and AODV protocols in a VANET crossroad scenario,” in 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA), 2013, pp. 577–582.

[18] E. M. Belding-Royer, S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, “Routing approaches in mobile ad hoc networks,” Mob. ad hoc Netw., vol. 1, no. 1, pp. 275–300, 2004.

[19] B. Paul, M. Ibrahim, M. Bikas, and A. Naser, “Vanet routing protocols: Pros and cons,” arXiv Prepr. arXiv1204.1201, 2012.

[20] S. Biswas, J. Mišić, and V. Mišić, “DDoS attack on WAVE-enabled VANET through

synchronization," in 2012 IEEE Global Communications Conference (GLOBECOM), 2012, pp. 1079–1084.

[21] P. Fazio, F. De Rango, C. Sottile, P. Manzoni, and C. Calafate, "A distance vector routing protocol for VANET environment with Dynamic Frequency assignment," in 2011 IEEE Wireless Communications and Networking Conference, 2011, pp. 1016–1020.

[22] J. Xu, X. Li, Y. Ding, and Y. Chen, "A comparative study of the link-state-aware routing in typical wireless sensor network models for home automation," in 2017 36th Chinese Control Conference (CCC), 2017, pp. 8890–8894.

[23] A. Sharma and R. Kumar, "Performance comparison and detailed study of AODV, DSDV, DSR, TORA and OLSR routing protocols in ad hoc networks," in 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2016, pp. 732–736.