T.C.

ALTINBAS UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

USING THE SUMO WITH NS3 TO EVALUATE THE OLSR, DSDV AND AODV FOR ROUTING PROTOCOLS OF REAL-TIME WITH DIFFERENT SCENARIO

Master of Science

Ali Muwafaq Shaban SHABAN

Supervisor

Asst. Prof. Dr. Sefer KURNAZ

Istanbul, 2021

USING THE SUMO WITH NS3 TO EVALUATE THE OLSR, DSDV AND AODV FOR ROUTING PROTOCOLS OF REAL-TIME WITH DIFFERENT SCENARIO

by

Ali Muwafaq Shaban SHABAN

Electrical and Computer Engineering

Submitted to the Graduate School of Science and Engineering

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2021

The thesis titled **"**USING THE SUMO WITH NS3 TO EVALUATE THE OLSR, DSDV AND AODV FOR ROUTING PROTOCOLS OF REAL-TIME WITH DIFFERENT SCENARIO**"** prepared and presented by "Ali Muwafaq Shaban SHABAN" was accepted as a Master of Science Thesis in Electrical and Computer Engineering.

Asst. Prof. Dr. Sefer KURNAZ

Supervisor

Thesis Defense Jury Members:

Asst. Prof. Dr. Sefer KURNAZ	School of Engineering and Architecture, Altinbas University	_____
Prof. Dr. Osman Nuri UÇAN	School of Engineering and Architecture, Altinbas University	_____
Prof. Dr. Mesut RAZBONYALI	Faculty of Engineering and Architecture, Maltepe 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.

Ali Muwafaq Shaban SHABAN

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 go to my father and my mother. Every success is a direct consequence of them influence in my life and their love. Also, I don't forget to thank "Asst. Prof. Dr. Sefer KURNAZ" for his advice, In the end, I have to mention All my brothers and my friends for their support and love.

ACKNOWLEDGEMENTS

I thank everyone who stood beside me, my family, my friends and my teachers who stood with me in my academic career.

ABSTRACT

USING THE SUMO WITH NS3 TO EVALUATE THE OLSR, DSDV AND AODV FOR ROUTING PROTOCOLS OF REAL-TIME WITH DIFFERENT SCENARIO

SHABAN, Ali Muwafaq Shaban,

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Dr. Sefer KURNAZ

Date: 08/2021

Pages: 48

Vehicle communication is a major research topic for academics and the automotive industry. In order to test various routing protocols in a vehicle scenario, the NS3 network simulator was employed. The BSM PDR and average good are measurement metrics that measure performance. AODV may be effective in low-traffic settings, but in high-traffic environments, OLSR provides significant benefits.

Keywords: Routing Protocol, Basic Security, Message Package Delivery Ratio, Average Good Put.

TABLE OF CONTENTS

Pages

ABSTRACT ..... **vii**

LIST OF TABLES ..... **xii**

LIST OF FIGURES ..... **xii**

LIST OF ABBREVIATIONS ..... **xiii**

1. INTRODUCTION **1**

1.1 INTRODUCTION 1

1.2 BACKGROUND FOR VANET 2

1.3 PROBLEM STATEMENT 2

1.4 COMMUNICATION IN VANET 3

1.5 WIRED AND WIRELESS NETWORKS 3

1.6 OBJECTIVES 4

1.7 THESIS OUTLINE 4

2. LITERATURE REVIEW **5**

2.1 RESEARCH TOPIC 5

2.2 WHAT IS VANET? 5

2.3 APPLICATIONS OF VANET 6

2.4 A MAP FOR SIMULATION OF VANET 7

2.5 PROTOCOL ARCHITECTURE IN VANET 7

2.6 KEY ACADEMIC AREAS 8

2.7 COMMUNICATION PARADIGMS 10

2.8 ROUTING PROTOCOLS 11

2.8.1 AODV 13

2.8.2 DSDV 14

2.8.3 OLSR 15

2.9 CHALLENGE OF THE MOBILE AD-HOC NETWORKS EXPLAINED AS FOLLOWS 16

2.10 ON DEMAND ROUTING PROTOCOLS (REACTIVE PROTOCOLS) 17

2.11 TABLE DRIVEN ROUTING PROTOCOL (PROACTIVELY PROTOCOLS) 18

2.12 SECURITY ISSUES 19

2.13 ON DEMAND OR REACTIVE PROTOCOLS: 20

2.14 PROACTIVE PROTOCOLS 21

2.15 HYBRID PROTOCOLS 22

2.16 STEADY STATE RANDOM WAYPOINT 22

2.17 PACKET FORWARDING SYSTEMS IN VANET 23

3. METHODOLOGY 26

3.1 INTRODUCTION 26

3.2 JUSTIFICATIONS FOR CHOOSING NETWORK SIMULATOR (NS3) 26

3.3 SIMULATION SETUP 27

3.4 PERFORMANCE EVALUATION PARAMETERS 28

3.4.1 Average Goodput 28

3.4.2 Basic Safety Message Packet Delivery Ratio (BSM PDR) 29

3.5 SUMMARY 29

4. SIMULATIONS 30

4.1 SIMULATION FOR THE PDR-BSM 30

4.2 SIMULATION FOR THE AVARAGE GOODPUT 34

5. CONCLUSION 37

5.1 FUTURE WORK 30

REFERENCE 38

LIST OF TABLES

Pages

Table 3.1 Simulation Parameters for First Scenarios..... 28

Table 4.1 Simulation Parameters for First Scenarios..... 30

Table 4.2 Simulation Parameters for First Scenarios..... 32

Table 4.3 Simulation Parameters for First Scenarios..... 33

LIST OF FIGURES

Figure 1.1: Vehicular Ad-Hoc Networks. 1

Figure 2.1: Applications of VANET 7

Figure 2.2: Types of Routing Protocols. 13

Figure 2.3: Example of a AODV Routing Protocol 14

Figure 2.4: Example of a DSDV Routing Protocol 15

Figure 2.5: Example of an OLSR Network. 16

Figure 3.1: Methodology 26

Figure 3.2: NS3 Simulator Design 27

Figure 4.1: Cars in SUMO. 31

Figure 4.2: BSM-PDR for CARs 31

Figure 4.3: Cars in SUMO. 32

Figure 4.4: BSM-PDR for CARs and BUS 33

Figure 4.5: BSM-PDR for CARs, BUS and TRAIN. 34

Figure 4.6: BSM-PDR for CARs, BUS and TRAIN. 35

Figure 4.7: BSM-PDR for CARs, BUS and TRAIN. 35

Figure 4.8: BSM-PDR for CARs, BUS and TRAIN. 36

LIST OF ABBREVIATIONS

MANETs	:	Mobile Ad-Hoc Wireless Networks
WLAN	:	Wireless Local Area Network
CPU	:	Central Processing Unit
PDAs	:	Personal Digital Assistants
VANETs	:	Vehicular Ad-Hoc Networks
AODV	:	Ad-Hoc On Demand Distance Vector Routing Protocol
DSR	:	Dynamic Source Routing Protocol
DSDV	:	Destination Sequenced Distance Vector Routing Protocol
IGRP	:	Interior Gateway Routing Protocol
RIP	:	Routing Information Protocol
OSPF	:	Open Shortest Path First
ISIS	:	Intermediate System To Intermediate System
IETF	:	Internet Engineering Task Force
RREQ	:	Route Requests
RREPs	:	Route Replies
RERRs	:	Route Error Messages
NAM	:	Network Animator
NS-3	:	Network Simulator Version Three

PDR : Packets Delivery Ratio

E2E : Average End to End Delay

1. INTRODUCTION

1.1 INTRODUCTION

Numerous researchers, car industries and carriage departments of different countries are interested in developing reliable and stable vehicle-to-vehicle communication systems. Vehicular Ad hoc networks (VANET) is an emerging park that connects vehicles for private and commercial purposes [1]. VANET can be divided into vehicle to vehicle (V2V), vehicle to infrastructure (V2I) and mix. Vehicular messages are exchanged amid vehicles shown in Figure 1.1.

Figure 1.1: Vehicular Ad-Hoc Networks.

There are issues for VANET such as regularly disconnected network, fast moving vehicles, interactive topology, etc. Vehicular communication began with DSRC which was built on IEEE 802.11a physical and MAC layer. VANET based standards of 802.11p and IEEE 1609 are appropriate for vehicular environments. A whole range of VANET programs are being implemented to provide a speedy solution to traffic issues

The most obvious consequences of air pollution and climate change are to be found. CODECs, ROADART, MAVEN, and Adaptive are all a part of current projects that explore connected vehicle concepts, all of which include federal transportation organizations. Many types of VANET technology are used, with Wi-Fi IEEE 802.11b/g, Bluetooth, ZigBee, and Wi-MAX

IEEE 802.16, in directive to avoid severe traffic congestion and potential damage. Intelligent transportation system (ITS) monitoring traffic density and speed will influence traffic transportation. It uses a base station to connect to the local area network, where it then processes the controlled traffic. This network keeps running efficiently thanks to sensors and data centers that use them. Since iPads, laptops, and cell phones will be able to detect VANET implants hidden in the vehicles, the use of these devices will become prevalent. During the last decade, technological advances have been occurring at an accelerated pace. Simplified duties and functions have been developed because of this. Several new software tools have been developed in the past few years, among them NS-2 and SUMO. In light of terrorism being a global crisis, security is a high priority. In terms of enhancing the security of their nation and territories, each state has developed strategies tailored to its particular needs.

1.2 BACKGROUND FOR VANET

A wireless communication network in which vehicles armed with radios are able to communicate with apiece other, as well as with roadside infrastructure, is known as vehicular ad hoc network. The idea is to divide the non-safety and safety functions. V2V and roadside infrastructure communication (V2I). Vehicle-to-vehicle (V2V) communication exists. Every vehicle in the V2V communications network is mobile. V2I refers to road communication Side Unit (RSUs). This connection is also used for access to other networks such as Internet. V2I technology, such as Wi-Fi, Dedicated Short Range Communications (DSRC), WiMAX, cellular, and satellite are applicable.

1.3 PROBLEM STATEMENT

These interdependencies between the nodes are challenging for the routing protocols. The timing to find path between the destinations depends on the process of routing to send the packet. The inability of a network of MANETs that a node in the network could move freely to another. There are several routing protocols and we prefer OSPF, DSDV and DSR because of different conditions. A literature review that refer to the effectiveness of such protocols. Based on research results, we can compare various types of networks.

1.4 COMMUNICATION IN VANET

There are five main types of communications in VANET: oral speech, written speech, visual speech, signed speech, and computer speech. This beaconing is useful in roadside receiving systems. To help other vehicles find our location, to warn others about our location. Beaconing is standard point-to-point transmission. Geo-Broadcasting: This is a common method of communication between countries. The sender adds a destination to the post, so that it will be sent to the next user on the list. This is used for vehicle to vehicle communication, where the dispatcher wishes to communicate only with a vehicle. Internet of vehicles has many uses, such as vehicular social network. The concept is intended to enable vehicles to set up a secure network. Unicast is crucial in this form of application. A message can only be sent if the sender and recipient are both physically close to each other. Advanced information dissemination strategies. The role of information dissemination in VANETs is another challenge as there is a high velocity for vehicles network topology and change occur frequently. The aim of these patterns is to ensure that which vehicle is arrived late or not received the message.

This method is called information aggregation. The aim of this method of communication is to reduce messaging overhead and improve data reliability. Jam reporting has higher accuracy because of aggregation of traffic information.

1.5 WIRED AND WIRELESS NETWORKS

The goal of serves in the wireless network to allowing all the people to connect with each other, for getting the acquaintance without need any substantial contact such as cable among them. These types of wireless give ours good usefulness of applications such as connecting between commune or devices that called areas cement movement for free connection. The common upshot of networks that varied the period of wireless intercourse example E- mails, Bluetooth and internet. We can have called that as WLAN or a computer network but the connect physical or using the cable to connect they are not desired. to decrease the cost, the wireless networks are using the wave radio instead of cable. The work can be interpreted as follows. We can explain that by take the two nodes A and C the computer connection between them or any device that can be do that to arrow the information or data. Every node already has a network modifier and the communication has a router use it to join. When node transmits the data after encoded the

data by binary form with radio frequency and push the data during the router of the lattice. The node C will received data from the antenna and make a decode to the information into binary shape to convert a data to original data[2].When we talk about the existence of wires causes many problems in any network. This is clear when we want to add the new gear with new filament with wire technique supposedly required at several step. that mean probably we cannot do that add or maybe it be very difficult or impossible because that need cost equal when we want to establish a new network, it may not be contingent to make widespread scale changes. Further, tied lengths of wires influence the amplitude of the infrastructure. Second hitch is the limited combination with wireless technology, principally with mobile devices.

1.6 OBJECTIVES

We have two great research objectives for this thesis:

1. To conduct a genealogical analysis of three VANET routing protocols: constructive, reactive, and hybrid.

2. 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.

1.7 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 INVESTIGATION TOPIC

The current research on the Vehicle ad hoc network (VANET), its mechanism, its procedures, its limitations, and delimitations, and how they can also be accepted, is examined in this chapter. VANET has been duly recognized and technical advancements for better performance and reliability have been added more and more recently. However, efficient routing protocols for route data between vehicles are difficult to design and to formulate, which creates further implementation challenges. The problem is further compounded by frequent disconnection and rapid technological changes. In order to meet a daily traffic scenario, existing VANET-enabled routing protocols, such as vehicles-to-vehicle (V2V) and roadside organization (V2I), are not highly functional. There has been considerable effort and testing to develop an effective VANET protocol.[3]

2.2 WHAT IS VANET?

VANET, also known as a Mobile Ad-hoc Network (MANET). Using moving cars as the building blocks, the technology creates a mobile network. Every vehicle is a network node. These cars are also wireless routers. The estimated range between the moving vehicles should be between 100 and 300 meters. when one system experiences a breakdown, the next system becomes part of the network It is feasible to assume that some kind of fixed infrastructure would be necessary to support VANETs since nodes have movement restrictions. with the aid of VANET, cars are kept informed about road conditions, weather conditions, or any other potential pitfalls or complications encountered along the route. The nodes communicate with each other using the help of the North America DSRC that makes use of the IEEE 802.11p form of wireless networking. passing on messages to other nodes when the cars are out of radio range (multi-hop communication). it produces a number of technical issues because of its mobility models VANETTING is simply a communications technology that uses moving vehicles as a node to construct a mobile network A vehicle in VAN is thought of interacting with its neighbors and other vehicles in the network is regarded as intelligent. With VANET, each moving vehicle is transformed into a wireless node. The criteria of connection are extended, as long as one vehicle

fails, the rest will take its place and hence the connection never breaks. Many vehicles are internet-connected. An individual vehicle has an IP in the same way as a machine does.

The first models to employ this VANET have been fire and police vehicles communicating with each other for protection. During the previous years, the project has gotten excellent results, and now it is used all over the developing world. This network assisted them in providing each other with timing-related details as well as traffic and other transportation-related facts[4].

2.3 APPLICATIONS OF VANET

For safety warnings, VANET is commonly used. Messages will be sent via VANET FIRE VEHICLES, POLICE, AMBULANCE, etc. within a certain location. And that too. Contributes to each other's correspondence helps. For drivers, VANET is also used. VANET can be used to alert drivers of this traffic when there is a heavy traffic bottleneck, so that they can take a separate path in order to get out of this jam. It can also be used to alert drivers who rush or violate traffic laws. VANET can be used to enable passengers and drivers in moving vehicles to access the internet. VANET will reduce charges for telecommunications. You can use the internet and use SKYPE. You can use it. Free to contact other people GOOGLE TALK etc. The drivers are warned about the working zones and about the incorrect way to drive. Figure 2.1 Classic road safety application in VANETs. With the assistance of VANET, maps can be revised and downloaded. Parking can be found through VANET as well. VANET may be used to carry out correspondence between auto mobiles. VANET enables the communication between the vehicles (IVC) and RVC (Roadside to Vehicle Communication).

Figure 2.1: Applications of VANET.

VANET connectivity is a very technological approach. The relation of VANET must take the physical propagation and a particular situation into account. We must ensure that the distance between the cars is not wider than the gearbox. That's not true in the real world. However, the application of the ADHOC network in the real world has certain drawbacks, in comparison to the theoretical spectrum of transmission. To explore networking we choose two areas. You are in the district and you are uphill [5]

2.4 A MAP FOR SIMULATION OF VANET

There are three things used in networking when sending a packet to a destination from the source. First of all, when the data is transmitted from the source to the destination, any path requests are also broadcast. Second, we must know that, if the routes answered unicast will find a way back and finally if the sent data packet will fly over a path. This is the way to bind VANET.

2.5 PROTOCOL ARCHITECTURE IN VANET

VANET protocol is designed to allow communications between nodes on a network. The architecture is presented as two-layered and unaltered. For the OSI and TCP/IP versions, functionality has been optimized to satisfy non-particular requirements. Multi-hop VANET utilizes multiple and single-hop communication modules. these protocols are configured to ensure that easier-to-to-access metadata is blocked at different layers Despite this, however, some VANETs are not conducive to modeling because of their control and stability layers.

Unlayereden VANETs allow users to build their style sheets as they please, and thus are safer than those that use a predetermined style. Since all communications and applications are captured within a single logical block with sensors, it follows that they are in complete harmony with each other and interchangeable Interaction with other structures makes it more difficult and unwavering in order to safeguard the VANET from unauthorized users getting access, VANET personalization is required. This demonstrates the difference between a layered and an un-layered model. lots of different links the various communication methods, such as general web browsing, industrial control loops, cell phone protocols, utilize a protocol dependent on the communication mechanism, which is commonly found in most communication networks. When it comes to the channel, the MAC protocol decides who is the recipient. A multitude of protocols is available, from which you can select according to dispute-free and contention-free operations. TDMA and FDMA are two examples of conflict-free protocols (FDMA). As protocols go, they are usually implemented with a central feature, such as a base station or an access point, to which the other devices in the network connect to share resources. Resentment-based protocols, such as Aloha and CSMA, are samples of contention-based protocol.[6] The Aloha protocol has the simplest implementation in which each transmitter sends its packet as soon it is generated locally. In the Aloha protocol, the transmitter begins by listening for the channel before transmitting, thus preventing unwanted transmissions. Reducing the likelihood that many transmitters immediately sends when the channel becomes available is accomplished by implementing a random back off period for each transmitter. The disadvantage is that it is possible for multiple transmissions to collide, and this can result in packets with bounded delays.

2.6 KEY ACADEMIC AREAS

The contact between vehicles uses autonomous, self-organized wireless MANET operates on the communications network, which is the basic type of VANET used in the wireless communication network of vehicles & vehicles. Information is shared and transmitted via VANET nodes between clients and servers. The VANET system's net architecture, pure ad hoc, cellular, WLAN, and hybrid, is also specified in three categories. Appropriate VANET applications include vehicular accident alerts, co-operative driving, map position, distribution of road information, driver support, driverless cars, co-operative cruise control, automated parking,

security distance warning and Internet access. As I have shown previously, VANET is the focus and continuous

Research to improve productivity and reduce the technological obstacles attached to it has been carried out in the past. There are also many other obstacles that must be overcome. To understand the requirements of an advanced and developed VANET protocol, we will discuss the advantages and disadvantage of already established protocols and concentrate on studies to investigate and rectify these and other advantages and disadvantages in VANETs. Several research projects in the field of VANETs are conducted worldwide: COMCAR, CarNet, NoW (Wheels Network), DRIVE etc. etc. Government and the private sector work together to synchronize latest VANET technologies, academia is aimed at detecting system breaches and, ultimately, joint effort by both will improve system efficiency [7]. Thanks to its high performance and QoS delivery, the proposed cross-layer design is common with wireless devices. Only where several layers are present, more importantly, on Multi-Hoc, function in the cross-layer systems. It provides a specialized interface for information flow across layers. The following figure illustrates how the method works[8].

It is worth noting that safety applications are normally critically retarded to notify other vehicles instantly of any accident on the lane. One-hop MAC-layer broadcasting, known also as beaconing, is special cases for this transmission. The beaconing method is used to disseminate information among the neighbors across a contact range. By beaconing efficiently, position and speed of the car can be shared. All information will support security users in scenarios such as colliding cooperative warning[9]. Business applications: Internet access, advertising and entertainment communications services such as communications apps are offered. For example, vehicle diagnosis, map download for browsing and video streaming are such applications. Unlike above-mentioned applications, commercial applications rely primarily on unicast communication. In commercial applications, far greater bandwidth than two other applications is required.

2.7 COMMUNICATION PARADIGMS

If we consider all three network applications, then we may claim that GeoCast, unicast communications and beaconing are key paradigms for all three applications. Bai[10]claimed that broadcasting could further be shared into scheduled, on-demand and event-driven fractions. Letter is used in situations of way hazard warning through delay-critical usage where information is spread over several hops through specific geographical areas. Scheduled transmission is used for co-operative collision warning and other applications

Applications for traffic control. These applications share information on a regular basis and are transmitted in the form of MAC transmission. This knowledge is only disseminated to close-knit neighbors. To solve the limitation bandwidth problem, applications that involve the distribution of multi-hops must apply some effective methods and protocols of aggregation. For entertainment and business applications, Unicast is powerful and important[11]. Requirements Analysis: VANETs are subject to different requirements with special network characteristics and a wide range of applications. These specifications have been reduced from previous paragraphs and outlined below. Scalability: Broadcast protocols have to deal with very dense networks in order to correctly run security applications in traffic jams and other such scenarios. Effectiveness: ensuring that knowledge disseminated efficiently by all nodes or fractions of nodes is defined in a particular area. Efficiency: Due to the limited usable bandwidth, the broadcast protocol normally has to remove message redundancy. To do this, forwarding rates are minimized, but all nodes in the same geographic area still receive an informative post. This significantly helps to prevent the issue of broadcast storms and allows several VANET applications to coexist.

Delay in dissemination: immediate knowledge exchange Dissemination time: the basic necessity for safety applications is immediate transmission of information and that is without delay too.

Dissemination of delayed tolerance: Vehicle networks are generally subjected to routine partitioning and thus caching information in such scenarios is desirable. Important information might otherwise be lost if the network in the destination area is not completely connected. Robustness: communication is prone to error through the wireless media, but packet losses are necessary for the broadcast to work correctly with critical security applications. Some

specifications can be inconsistent, so all requirements are extremely unlikely to be completely met., the requirement robustness is no longer working, because there is only a single failure point at propagation nodes. Thus, when a message cannot be transmitted to the dissemination node, the overall receiving rate drops dramatically (Wireless communication Channel is likely the reason). In such cases an elaborate compromise is necessary between these requirements.

2.8 ROUTING PROTOCOLS

A major consideration for VANET in advance of its extensive real-world implementation is its speed of exchange of information while respecting the safety and security of data transfer. In 2010 Asif et al. presented in a communications software and network conference a method to maintain these two factors in VANET without compromise. Previously, the techniques suggested by others have been used to scary one element for the other, mainly by increasing the exchange speed of information, but unfortunately also by reducing the transmission security level. Currently as shown in (Figure 2.2), in the VANET community the standard security system is recognized as the security framework for PKI/ECDSA. Asif 2010, he criticized this, since computational costs are too high, thus reducing its practical use in emergencies in which information exchange, especially between nodes in the vehicle, must be fast. The idea behind a study[12]is based on the fact that vehicles and nodes in close proximity form a trustworthy group connection which improves group communication with standards of security. This is a hardware-based architecture and the trusted community relationship is built on a large node, which is coined as a Trusted Platform Module (TPM) for short. Group entities may be established on the basis of which cells a vehicle node belongs to in the geographical location.

The hardware used is a TPM chip, which is integrated into each vehicle, as suggested by the study[13]in the grouping process. This chip not only includes a central TPM, but a supplementary four sub-modules, a symmetric module, a random number generator or RNG, an asymmetric module or ECC and a hash module. The TPM module ensures the safety of messages sent and that any aspect has not been tempered. By creating a digital signature, the ECC module works. There is a public and a private key in this signature. During the production stage, the private key is incorporated into the TPM chip. In a VANET scheme, the public key is freely available to users. The random number generator produces the number of seeds for the keys. The

Hash module with Secure Hash Algorithm or SHA1 gives the hash value. When choosing a group leader within a trusted vehicle group, the hash value is used. Similarly, every external node can be connected with the trusted group and can be a member of the trusted group at any time in the vicinity. It is imperative that this study[14]conducts simulations and presents its outcomes in the future in the order to verify if the trustworthy community technique applied in the real physical world. The Vehicular Mesh Network, or VMESH for a short term, which was proposed by Zang, is another form of cellular group-style wireless network. Vehicles within the transmission line are here in VANET, also known as the mesh, as a group-type structure. If one of the nodes on a mesh contains information, then the same information will be conveyed by all other nodes on that mesh by broadcasting information from the initial node to other nodes. This is a useful networking tool that saves resources. For instance,

A provisional event in VANET, such as the appearance of an obstruction on the road that is supposed to be cleared after a certain date, is known as a temporary event of interest or shortly EOI. Moreover, in the form of a region of interest or short ROI, the information stored on a node within a web that has an EOI meeting is. ROI determines the physical area that covers the EOI, e.g. the exact position and height of the obstacle in coordinates. Information stored in a grid may be moved to a different grid if all grids are within d distance. This distance is not a stone distance but can be tuned. This distance d is, however, determined on the basis of the position of the obstacle, for example, if the information itself is about the obstacle. If in the area of distance d no other mesh exists, information loss takes place if the first mesh the EOI has flowed from the field. Thus if a mesh exists in the region, the EOI information still exists if the initial mesh which first encounters the obstacle has moved beyond the EOI region.

The VANET Routing Protocol can be roughly grouped into two, namely the topology-based routing protocol, as outlined by [15]. There are two sub-categories within the protocol which are based on topology: each node maintains a table of information on the other nodes connected to it. This is another constructive routing protocol name, referred to as the Fisheye State Routing (FSR). However, there is a limitation here: the load on the network is substantial. Additionally, routing tables take a long time to process. With reactive routing, you can avoid any problems that you may encounter when using constructive routing. Once information is required or communication with another node is required, the discovery of the route only begins at that

point. As a result, the network load is significantly reduced. This is an example of a constructive routing protocol, which happens to be on-demand distance vector routing. This protocol can be used to perform unicast or multicast routing. This protocol has the disadvantage of creating initial links taking longer on average. Even when the GPS signal is present, however, it may be unable to find your location in a tunnel, as the density of the air above the tunnel interferes with the GPS signal. The Delay Tolerant Network (DTN) is a framework which can be used to deal with this problem. the data packet in this system, which will be re-calculated after nodes are disconnected, will be sent to other nodes, and will be used by the rest of the nodes. Another approach is to remove the node from any of the contact lists that the neighboring nodes share. At each node, there is a beacon that sends a short data packet out to other nodes at a specific time interval. If after a given amount of time, no data is available from a node, it is considered non-operational and does not appear near other nodes. To merge the benefits of both geography-based steering and topology-based routing, Lecher suggested a new protocol famous as the Geographical-Source Routing-Protocols (GSR).

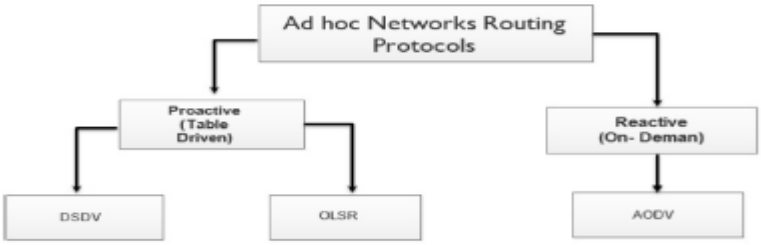


Figure 2.2: Types of Routing Protocols.

2.8.1 AODV

Hop-by-hop reactive routing is utilized by OSPF. The cars here are vehicles in VANET. Vehicle movement and travel at various speeds are completely random. The AODV method empowers mobile nodes that want to create and sustain a network to be proactive about it. The mobile nodes of AODV can rapidly grow in number for destinations that have not been communicated successfully however, AODV nodes are not required for routes that have not been communicated effectively. For AODV route requests, route answers, and route errors, route message is a

suitable synonym. spoken communication (RERRs). Nodes maintain a record of the node that sends the query when they are received via AODV routing (RREQ). The method of creating recordings while reversing time is known as backward learning. another packet in response to the query (RREP) is sent when received at the destination. The node records its previous hop once it stops and thus creates the forward path. The path is supported while the source is using the path. The path is supported. The source will be notified of a connection failure and then a new route will be generated with different question answers. as shown in Figure 2.3

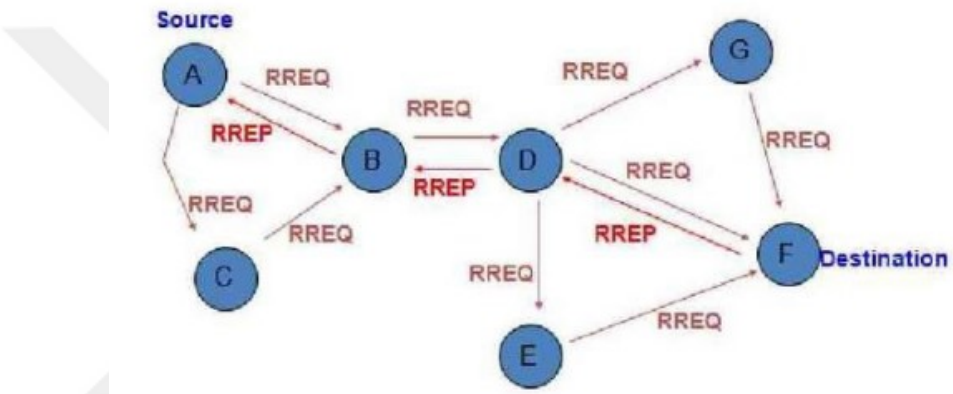


Figure 2.3: Example of a AODV Routing Protocol.

2.8.2 DSDV

is the sequenced vector of the destination? A proactive DSDV

A routing protocol that makes routing choices using facts stored in the routing table. Each node on DSDV maintains a route in tabulation form to all known destinations. The table consists of destination, next hop, and the cost metric records, the destination sequence number allocated to prevent loops, number of hops, and install time. Time used to delete the stalking entries when the entry has been entered. The changes in topology are reorganized with immediate messages to neighbors. The tables are fully revised.

Update where a node sends all the information to a different node, where the node sends only modified nodes. The benefits and drawbacks of DSDV. The route does not have loops because it uses a number series and no path is latency as the path is DSDV protocol. as shown in Figure (2.4) Taken from the node-kept routing table. The drawbacks are, however, overwhelming

because some of the information is never used and the tables must be modified with a large bandwidth to upgrade the amount consumed.

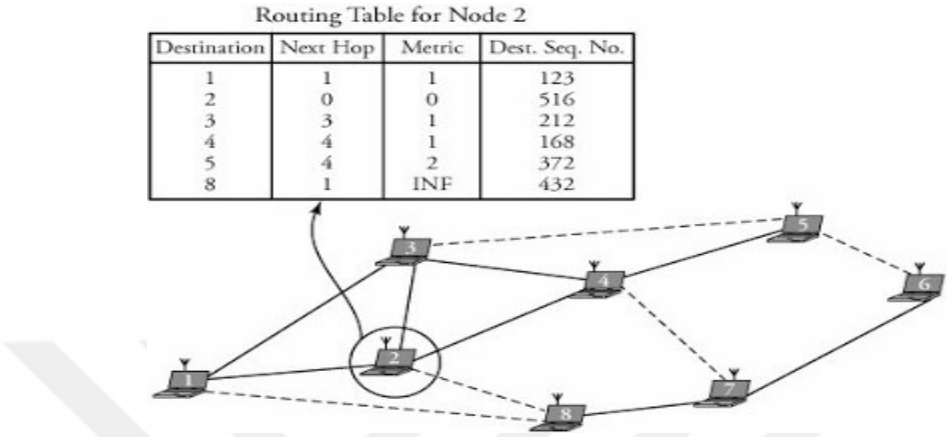
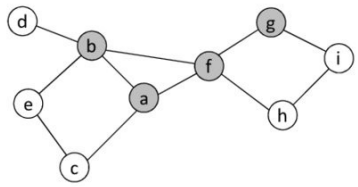


Figure 2.4: Example of a DSDV Routing Protocol.

2.8.3 OLSR

The Optimized Link State Protocol is derived from its RFC 3561 in this section [16]. OLSR is a pro-active routing protocol so routes are always available immediately when needed. OLSR is a pure connection state protocol optimization version. Thus the topological changes cause all hosts in the network to flood topological knowledge. Multi-point relays are used to reduce the potential overhead for the network protocol (MPR). The idea of MPR is to eliminate broadcast flooding, by limiting broadcasting in some areas in the network and later in this chapter you can find more information on MPR. The shortest path is another reduction. The reduction in time for the transmission of control messages will increase reactivity OLSR uses dual kind of control message: Hi and Control Topology (TC). Hello messages are used to find the connection status information and neighbors to the host. Hello gives a Hello message that describes which neighbors choose this host to be used as MPR and host can calculate its own MPRs set from this information. Hello messages are transmitted only one hop forward, but TC messages are transmitted all over the network. TC message is used to broadcast information on the MPR Selector List of own advertised neighbors. The transmission of TC messages is normal and only MPR hosts can transmit the transmission messages.[17]. The improved OLSR are constructive routing protocols that provide guidance, if necessary. Link Statement Transmission Protocols OLSR is an improved state protocol for plain correlation that enables topological information

across all network hosts to be exchanged as a result of changes in topology. By increasing the average time frame for sending daily reports, OLSR will improve interaction with topological changes. OLSR actually offers information on all network vulnerabilities and traffic flow protocols are beneficial, since a wide section of the nodes connecting a wide range of nodes and pairs shifting over time. OLSR is appropriate for use as it is not long overdue for the packets. as shown in Figure 2.5. OLSR has a dynamic network with the greatest number of links across a range of nodes. OLSR reduces control loads, allows MPR to adjust its correlation status and improves efficiency when the established MPR group is as low than the standard correlation status procedure. In the downside, the routing table must be held on all possible paths in order to prevent differences in LAN, but the number of mobile hosts is increasing with increasing growth in the control messages. [18]



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

Figure 2.5: Example of an OLSR Network.

2.9 CHALLENGE OF THE MOBILE AD-HOC NETWORKS EXPLAINED AS FOLLOWS

1. Scaffolding: You should publish an in detailed number of nodes to extend the network, which may be a challenge to the ad hoc mobile system, as the growth of your infrastructure might be necessary, such as the need to establish where you have the service, the routes and the key exchanges for encryption. This requirement needed a large bandwidth overhead with the network increase. On the other hand, these separate nodes mean that a particular and restricted transmitter is used so that every node depends on the neighboring node for sending the information and using it as a route and host. The new routing protocols must also be implemented This challenge[19]to be overcome.

2. Routing: Due to a changing network topology in the laptop environment, there is therefore no prediction about network topology. Therefore, there is no provision for the interchange between

the nodes with network information It is one of the main obstacles facing the MANETs. In order to prevent errors, the network ultimately had to adjust and find routing between nodes very rapidly.

3. Class of service: The class of service of any network depends on several factors including the likelihood of a packet loss, delay and bandwidth, so that a good network output will occur by controlling this factor. Algorithms, protocols, routing schemes are the key factors of network quality[19].

4. Security: Because of its multiple impromptu system like a military or secret set, it is therefore the most significant challenge that MANETs face, because there is no centralized administrator to save the data from hacker[19].

5. Interpolation: The integration of two MANET networks is of concern because it is too dangerous for us to discuss saving the data without losing it. This is an interference that the network is already trying to adapt. Maybe one of them has used the various methods of synchronization. Protection like this atmosphere is actually a matter of concern due to the existence of network work (MANET) under which this scenario operates, such as military or sensitive meetings[19].

2.10 ON-DEMAND ROUTING PROTOCOLS (REACTIVE PROTOCOLS)

In this type of convention, the systems do not always hold the data for all the node, but only if they want it will submit the request and receive it when the node wants to send the data and it does not have the appropriate information to send the text to the destination, so if the source node wishes to send a message, it will send a request to at least the next hop to the destination to receive sufficient information after that message is sent. This problem is also caused by congestion, which also has an impact on the throughput, as the node broadcasts the pack to all the surrounding nodes that cause the flood. However, if we don't have enough details about our next step we can find the way between the node in this way. Indeed, when the source node is broadcast towards the destination, some of the middle node that has routing information returns to the source or gets a node during the middle node between its source and the destination. In the first instance, the broadcast is limited to neighbor hops, until the broadcast is widespread across the network. The routing request must pick the best route before you send the message in this

form of protocol. This method will therefore be followed If the paths unknown to the nodes are unknown, the defects for reactive protocols will postpone sending the message. Most protocols use the temporary memory to save the routing that was built to reduce this delay.

However, because information in cache memory will be old in short time, the route is invalid because of the node mobility in this environment. Old cache data must be avoided. The program that uses the on-demand routing protocol must be tolerant to potential delays when first paths are detected. The wireless channel does not have to have much routing knowledge for paths because it is not used in traffic or high-mobility nodes, this measured benefit for the on-demand routing protocol[19].There are several protocol examples like ABR: Associativity-based routing DREAM: Distance Routing Result Algorithm aimed at Mobility, DSR: Dynamic Source Routing Protocol: Ad Hoc on Request, CEDAR: Distributed Ad Hoc Routing Core Extraction,

2.11 TABLE-DRIVEN ROUTING PROTOCOL (PROACTIVELY PROTOCOLS)

On the other hand, such routing protocols will continue to try to keep on all routing details, for every node, the protocols known as proactive routing protocols that are divided into two types, namely the first event and the second protocol, which is regularly modified. The event-driven protocols remain and do not route if the topology of the network is not changed, and what the mean of change topology here means can be changed as changes in the neighbor set. There is some reception or modification Each message implies that there is a node shift or a link/node failure; sending a message to another node depends on the routing protocol strategy. Then protocols with updated information about changing topology will send this update to the other node at regular intervals, and we should also consider the far-reaching nodes, whereby the interval is needed for frequent updates than the nodes, in this respect we know that we find traffic higher than nodes far away in the closer nodes, so that in any change in topology we do not have to flood the whole network. The proactive protocols to keep routing tables would make the enforce subclass a fixed overhead, not depending upon the number of entries used, but the benefit of the one-time routing of proactive protocols without any set-up delay. This type of protocols is desirable in the low or moderate networks because there are a number of mobility nodes with numerous data sessions in such networks[20].Proactive (Event driven) routing protocols are: CBRP: The protocol of cluster routing CGSR: Switch Routing Cluster head

Gateway The following are regularly updated protocols: DSDV: Destination Sequenced Distance Vector Routing Protocols

2.12 SECURITY ISSUES

when installing wireless networks, problems such as authentication and encryption must be dealt with inappropriate or reckless driving instructions may be issued to the vehicle as a result of corrupt data in a vehicle information channel The VANET security objective consists of five key criteria or components: authentication, confidentiality, credibility, availability, and repudiation of the data.

Article in 2013 states that the authentication requirements state that links in a communication have the correct identities verified as being correct Registration is required for this to happen, so that each vehicle must be individually marked before being driven on the road. The reason that data must remain private and confidential is because of the sensitivity of the information that is contained in it. disclosure of this information can leak important information about the

communication links. Disasters will occur if the hackers intend to overwrite the instructions and nodes would act in an unlawful manner.

the principle of data validity defines the aim of data validation is to ensure that every piece of data received has been confirmed to be the same as the original data given by a source, which has been permitted to do so. Changes to the data, such as compression or loss compression, have no effect on the data's readability. data should be always being readily available Checks must be done to ensure the batteries generating the signal power must not be recharged or supplied. In addition, the routing protocol should be protected from unauthorized modification.

Sender authentication is described by the non-repudiation criteria in the form of Matthew and Kumar [21].states that the vehicle data must recognize it as originating from itself. Likewise, the vehicle node is not permitted to deny having received the data. There are many kinds of VANET attacks, including those by Matthew and Kumar [21].Sybil assault, distributed denial of service (DDoS), resource denial (Drowning), and role misbehavior A Sybil attacks may be brought on by a single person mischievously inventing several identities. There is only one or one vehicle in the digital world, but in the real world there are several of these. Thus, other nodes, which

receive this information, may think that there is congestion ahead and go to alternate routes. In this case, the greedy node takes the full path and no other nodes are near it, so it has no competitors. in order to avert a Sybil attacks, one must be aware of Sybil's, one must monitor other Sybils for a certain amount of time interval, and the data obtained from neighboring nodes are compared to each other Any possible inconsistencies from the comparison results will be identified as a possible malware. in a distributed denial of service attack, the objective is to prevent nodes from accessing network services and resources This can be achieved by flooding the network like a mailing system. Therefore, the nodes will go offline, leaving them unable to communicate, which can lead to accidents. The DoS attack is different from a DDoS attack, but shares the same purpose. If the attacker's node is in the path, all data must pass through it. Due to this capability, the attacker now has the ability to influence the traffic flow of information or to build harmful packets to be sent to other devices, traffic may be misdirected. This type of cyber-attack occurs when the malicious node manipulates a signal before sending it out to other nodes. In turn, the malicious node's traffic appears to be nonexistent, but the traffic from its neighbor nodes can be seen in other words, Lu mentioned that the azimuth could be adjusted. Azimuth knowledge is the collection of lines of sight linking two nodes, which can be thought of as imaginary angles. One of the VANET rules is to follow the rule of right hand of protocol, which is employed in the GeoGPC to give azimuth information from the source node to the destination node. When an adversary launches a malicious attack, the concept of the hand disappears. In other words, the information is sent to another set of nodes that are not part of the laws of right, and one of those nodes is the malicious.

2.13 ON DEMAND OR REACTIVE PROTOCOLS

Because of the nature of an on-demand protocol, a network built using it does not have all time routing information stored on all nodes, but it is created on demand. A node needs the requested information if it doesn't have enough information to send a message to the destination or if it does not wish to relay a message. Reactive Protocols do not store routing information persistently, but rather collect the information as it flows through nodes. The node must know the next hop of the packet for it to function. (including its neighbors). Although the node will only send the packet to all its neighbors, this in many situations leads to severe congestion which usually affects the performance negatively. However, if no next-hop information remains

available, such broadcasts can be used in a path discovery operation. This normally consists of a message from the source node that indicates the intended destination. Knots that have the desired routing information will refer to the node that decides on a path from the responses that they receive. The broadcast may only spread to only a few hops until a net broadcast is broadcast (which would flood the whole network). Before sending a post, you must complete the route request and selection process. This leads to initial messages configuration delays if the node is unaware of their path. The delay in data transmission is normally higher since it is due to the initial route discovery process. Many protocols use a route cache for already known routes, in order to limit the effect of this delay. The knowledge in this cache is time-out because, due to nodes and changes in topology, the routes are invalid in a mobile environment after some time. This is done to prevent blocked data from the path cache. Applications using an on-demand routing protocol obviously must tolerate the initial configuration wait. On demand routing protocols have the advantage that the wireless channel doesn't need to hold much overhead routing details for routes that are not usually even used. High traffic mobility scenarios may provide significant efficiency improvements such as throughput or Latency with low overhead path set-up. Examples of protocols on request are as follows: The Distance Routing Effect Algorithm for Mobility, the DSR (dynamic source routing protocol) Associativity based Routing [22]; the Ad Hoc on Demand Distance Vector Routing Protocol , and the CEDAR: Distributed Ad Hoc Routing Core-Extraction [22].

2.14 PROACTIVE PROTOCOLS

Proactive routing protocols will often aim to keep right details on all network nodes. This can be done in various ways and is thus divided into two main subclasses: event-driven and protocols regularly modified. If no change in topology occurs, event-driven protocols can no longer send update packets. It will only then be recorded to other nodes in accordance with the updating Strategy for the routing protocol if a node detects a change in topology (usually a change to the neighbor collection, a receipt of a message suggesting a change in any other neighbor nodes, or a link/node failure). Protocols that are regularly modified often send topological data to other nodes at regular intervals regardless of changes in topology. Many state links function in this way. The maximum distance of an update message can be different with the length of the interval so that nodes further away are updated more often than near nodes and the load on the

network may thus be balanced. This is founded on the fact that traffic is increased at closer nodes and that the entire network is not inundated if changes occur. Proactive protocols of each sub-class need a fixed overhead, even though several of the entries are not used. The main benefit of this is that the routes can be used at once and no set-up time exists. In networks with low to moderate mobility, fewer nodes and more data sessions, proactive protocols are generally best done.

Proactive routing protocols powered by events are as follows: CBRP: Cluster-based Routing Protocol [22], CGSR , DSDV: Destination Sequenced Distance Vectors Routing Protocol (DSDV) Cluster-based Gateway Switch Routing . The following protocols are regularly updated: FSR: State Routing of Fisheye State Routing OLSR Optimized connection.

2.15 HYBRID PROTOCOLS

These are the protocols use both proactive and on-demand routing, and seek to exploit on-demand routing' Programmatic routing is done at nodes (active receivers), but the frequency and size of the updates are controlled. If no aggressive path exists, a passive route exploration mechanism is used instead. Other possible examples include: since it is the recommended mesh protocol for 802.11, it is required that users run HWMP (Hybrid Wireless Mesh) to ensure compatibility. AODVHWGPS is built on tree-based routing standards (RFC 3561). To detect what information is missing in your Excel workbook before publishing it is essential before you release it to the world, so users' data can't be expected to change without you knowing. Anchored Geodesic Packet Forwarding (Packet-directed routing) (Terminode Local Routing, TLR). Banned substance does not exist in nature and cannot be obtained from plants, animals, so animals that ingest or otherwise come into contact with it cannot suffer as a baneful effect. a program It also incorporates an active intra-zone routing protocol (IARP) and an on-demand inter-zone routing protocol (IERP) Steady-State Random Waypoint

2.16 STEADY-STATE RANDOM WAYPOINT

This is a method to increase the accuracy of RPW simulations, and thus to improve it would lead to SS-RP. the RWP model is a plain, memoryless representation, as compared to other models such as random walk. The ad hoc network model is the most widely used mobility model [in

simulations] A node selects a random location in the region as its destination, and travels at a constant velocity towards it until it reaches that point. After every finish line, a new destination is picked from the interval uniformly. the machine pauses for a certain period of time before moving to the next location Keep in mind the selection of speed and destinations is unrelated to previous movements. Mobility in both ns-2 and ns-3 is handled by all nodes being placed at their starting points. The big issue here is that the mobility models are slow to converge. The long-term convergence efficiency metrics are heavily influences of the mobility simulation results Since it takes about 20% of the overall simulation time to warm up. The SSRWP model alters the RWR model such that the motions of the nodes are tracked to steady-state starting from the beginning of the simulation. Some nodes start in a stopped state while other nodes are started based on a random probability distribution. Wide acceptance is due to ease of implementation and analysis. However, due to its simplicity, the RWP model might not be able to represent realistic movement. As the node movement speed diminishes, the average movement time will increase. Studies conducted in the past have shown that the concentration of a node's position around the midpoint of its region [have discovered that] is higher. Additionally, people who are suffering from poor memory are prone to severe mobility shifts in attitude and behavior.

2.17 PACKET FORWARDING SYSTEMS IN VANET.

An effective packets forwarding algorithm is essential for the design of available VANET routing protocols, and certain related workings are provided in this section. [22] AODV employs each node's routing database to identify the next hop, although route discovery in that protocol incurs significant overhead on the network. Choosing the next hop in the packet header where the whole route list is contained when forwarding a data packet However, route scaling issues arise with the complete node-based route overhead. The geographical forwarding technique is used to get around data delivery issues by solving issues of scalability and dependability. Preceding studies have relied on the previous node's neighbor list and geographic location to determine where future transmissions will be sent. [9].The next step is to select a forward path in such a way that forwarding progress is maximized (e.g., typically, this is the neighbor closest to the destination). The above process is used until the packet's end. If the neighbor list of each node is accurate, each one will be able to select the optimal hops in the sequence. And if the list is inaccurate, a node that is outside the range will be chosen as the next hop

This node and the target node both. Both. If the target node is on the next table but the new location provision shows that during the data packet transferring phase the target node might be out of its contact range, the node nearest to the new position of the target is then selected as the next hop. If the destination node is not located in the next table, it will consult the packet travel time and determine if the destination node can possibly be reached in one hop transmission. If yes, the data packet will be transmitted directly to the target node.

If no reply is received (from the destination or node which has the target node in its table and is closer than the current forwarding node to the destination node), then the next node is selected nearest to the intended destination node and the procedure is repeated. However, in addition to two geographical transmission algorithms, data packets often fall into local limits and then start repairs, which in urban scenarios do not work well because they use a distributed algorithm for graph planning.

Utilizes a limited transmission algorithm to resolve the maximum local problem. In this algorithm, the data packet should be transmitted to a node at intersections greedily instead of to a node that is the most distant from but within its contact range from the current forwarding node. Moreover, there have been recent reports on some link-aware routing schemes, but the link length between nearby vehicles is very limited because of high mobility. In addition, GeOpps uses the spatial method of selecting the next hop on a trajectory basis. In this approach the suggested routes are followed.

In its own destination, neighboring nodes determine first the point closest to the destination of the data packet and then use a function expression (based on the nearest point and digital map information) to estimate the minimum time required for this data packet to reach them.

Expiration time for the previous hop is reached, and the sender is notified that the next hop is the highest. this methodology is only calculating one factor in the calculation of wait time, which is the distance between the next possible hop and the destination, which performs well when it is assumed that all of the information needed to travel to the final destination is stored on a disk drive (for example, the wireless channel is model and the transmission range is a circle of a fixed radius). Additionally, many studies have demonstrated that wireless radios, contrary to the unit disk assumption, are far from following it. Numerous buildings exist in a VANET, but other

physical barriers stop the spread of radio waves. Maximum transmission progress is enhanced by picking one person who will do the work. It is not possible to guarantee the best possible range of the next hop. To successfully address a Challenge, there will be many options to find the next hop selection approach based on recipient parameters. Adoption of these approaches does not take into consideration the wireless channel model, interfering signals, and transmission models.

3. METHODOLOGY

3.1 INTRODUCTION

This chapter highlights the methods in the three-stage study (Figure 3.1). Phase one is the literature review of simulation configuration, which will include the rationale of network simulator selection (NS3), and performance metrics competition, phase two is simulation execution, stage two is analysis of outcomes.

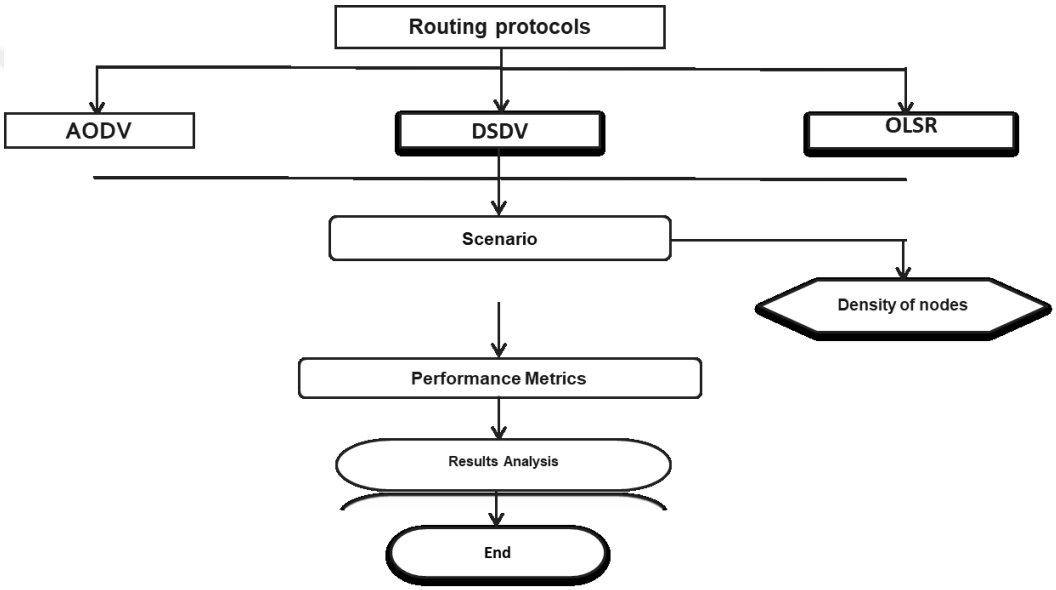


Figure 3.1: Methodology.

3.2 JUSTIFICATIONS FOR CHOOSING NETWORK SIMULATOR (NS-3)

Some of the reasons for using NS-3 include studying the actions of a system in a highly regulated and reproductive environment, which is harder or impossible with real systems, and how networks function. In the field of network science and education, s-3 was created to provide a free and extensible network simulation platform. In short, ns-3 offers templates for the functioning and performance of the packet data network and the simulation engine for users. Some of the reasons for using NS-3 include studying the actions of a system in a highly Two regulated and reproductive environments: one, much tougher, even impossible, and the other, just like a real-world system. This is especially important when studying network systems. Due to the fact that users will be able to use the model in NS-3, but they may also apply it to non-

Worldwide systems, many users will see that the model in NS-3 is useful. Some users of Ns-3 are now using Ns-3. Network simulation tools are many. Here are several features that set ns-3 apart from other tools. - Ns-3 is a library that contains several other software libraries that can be integrated with other external libraries. With regard to this aspect, ns-3 is more modular. The main benefit of the Ns-3 solution is that it enables the use of external animators and data and visualization software. Users can, however, plan to use C++ and/or Python software development tools on the command line as shown in the (Fig 3.2).

-Ns-3 is used mainly for Linseed or macOS systems, while BSD systems and Windows frames, such as Windows Subsystem or Cygwin, are supported. Native Windows Visual Studio is not funded at the moment but there is potential support for a developer. The users of Windows can use a virtual machine for Linux too.

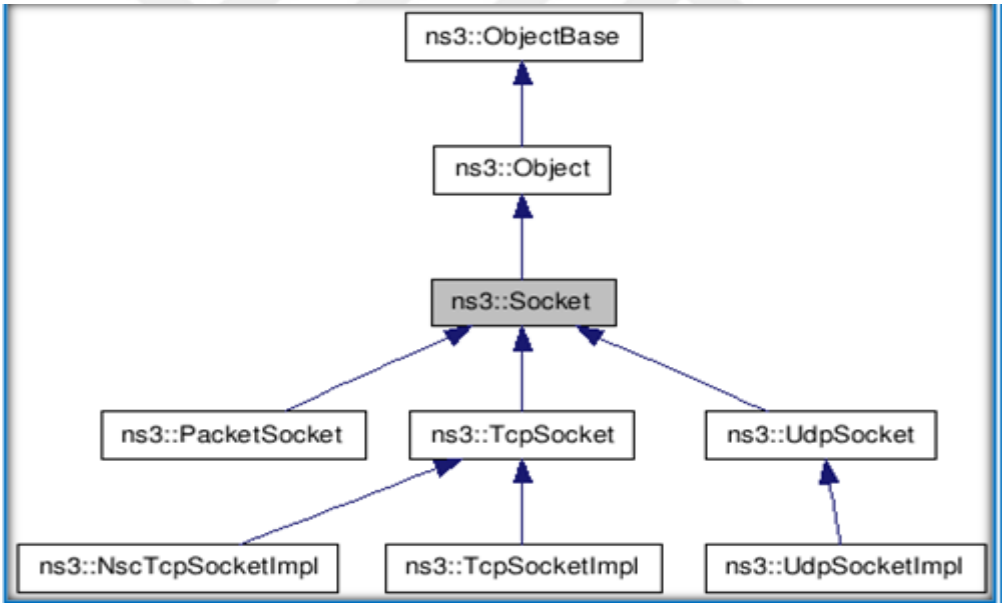


Figure 3.2: NS3 Simulator Design**.**

3.3 SIMULATION SETUP

In this point, we will demonstrate first how to build various appropriate environments, which have been explained in detail in Chapter 2, to simulate the DSDV, AODV, and OLSR routing protocols, by explaining all of the following steps, the first of which is to identify the parameters which will be used to create the DSDV, AODV, and OLSR routing protocols.

Table 3.1: Simulation Paramete For First Scenarios.

802.11	MAC Protocol
Parameter Value	Parameter Name
AODV ,OLSR,DSDV	Protocols
Random	Source/Terminus
102	Number of Vehicle
Speeds of nodes	30K/m
20s	Total Simulation

under this parameter in the table 3.1. In the NS3 simulation scenarios, these parameters were used to evaluate three protocols: DSDV, AODV, and OLSR. The second step would be to define the performance metrics for each routing protocol, such as DSDV, AODV, and OLSR.

3.4 PERFORMANCE COSTING PARAMETERS

The routing performance of the different protocol used was analyses on the basis of Average good practice and Basic Safety Paced Delivery Rate (BSM PDR)

3.4.1 Average Good put

As a VANET performance assessment parameter, only information that is valuable as fundamental safety messages is taken into consideration. To arrive at a data file's data percentage, how long does it take to move the data file itself needs to be taken into consideration. Performance at the application layer is also taken into consideration. An acceptable place may be denoted as "bps" (bits per second), "kbps" (kilobytes per second) or "mbps" (megabytes per second) (Mbps)

3.4.2 Basic Safety Messages Packet Distribution Ratio (PDR-BSM)

Each node transmits each second ten BSM in this work. For individual BSMs the total packet delivery ratio for a complete simulation period is calculated. A high PDR offers more secure network-wide connectivity.

3.5 SUMMARY

The methodology of the research is described in this chapter. We have outlined each stage in detail in order to ensure that the verification of the results is completed successfully. The result and review of the DSDV, AODV and OLSR directory conventions to show the best Convention in various situations will be given in the next chapter.

4. SIMULATIONS

This section clarifies the performance of the three routing protocol in each setting and evaluates that the BSM-PDR and Average Good put have three protocols by performance measures.

4.1 SIMULATION FOR THE PDR-BSM

The first scenarios: 102 Cars were selected with the SUMO parameter in Figure 4.1, as illustrated in Table 4.1.

Table 4.1: Simulation Parameter for First Scenarios.

PARAMETER NAME	PARAMETER VALUE
Number of Vehicle	102
Protocols	DSDV, OLSR, AODV
Speed of node	30K/m
Source/Destination	Random
Total Simulation	20s
MAC Protocol	802.11

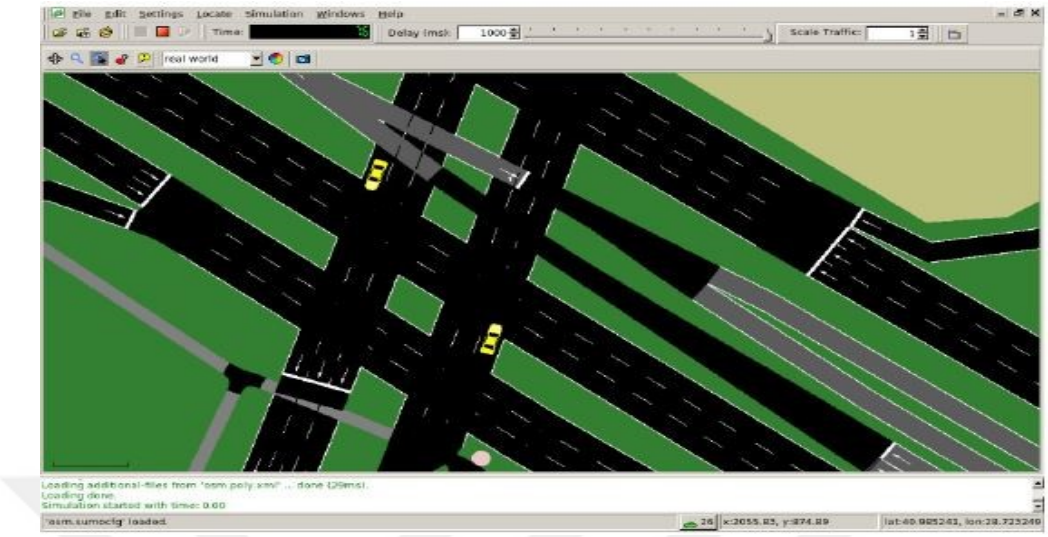


Figure 4.1: Cars in SUMO.

In Figure 4.2, the effects show that for the three focal routing protocols, the PDR for all 10 basic security messages is same similar. The highest PDR is achieved for all 10 posts, and the lowest PDR is shown in the OLSR. Output of DSDV between OLSR and AODV.

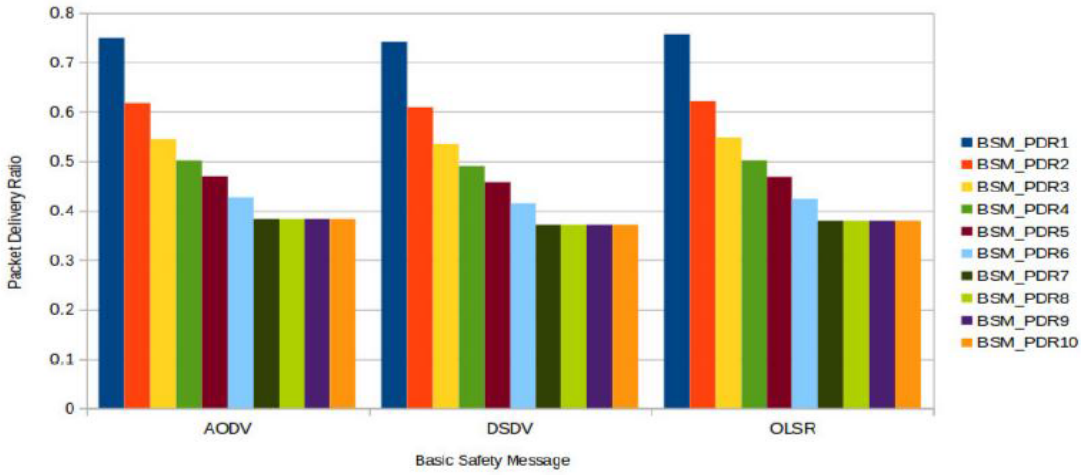


Figure 4.2: BSM-PDR for CARs.

The secede scenarios: select 146 Cars and Bus by means of SUMO in Figure 4.3 the table parameter as shown in Table 4.2.

Table 4.2: Simulation Parameter for First Scenarios.

PARAMETER NAMES	PARAMETER WORTH
Protocol	AODV ,OLSR,DSDV
Source/Terminus	Random
Speeds of nodes	30 K/m
MAC Protocols	802.11
Over-all Simulation	20.s

Figure 4.3: Cars in SUMO.

Third scenario: Used SUMO in Figure 4.4 to find 205 Cars, Buses, and Trains by finding their total in Table 4.3 The results in Figure 4.5 show that all 10 of the basic safety messages have very similar PDR values for the three routing protocols tested. In fact, the AODV performs the best for all 10 messages, while OLSR performs the worst. between AODV and OLSR during DSDV's concert.

Table 4.3: Simulation Parameter for First Scenarios.

PARAMETER NAME	PARAMETER WORTH
Protocol	AODV, OLSR ,DSDV
Source/Terminus	Random
Amount of Vehicle	205
Speed of nodes	30K/m
Overall Simulation	20s

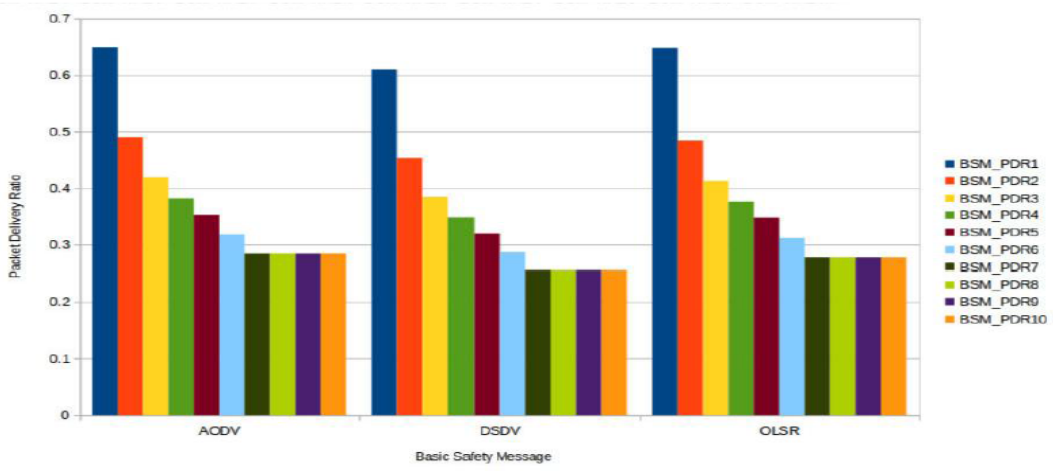


Figure 4.4: BSM-PDR for CARs and BUS.

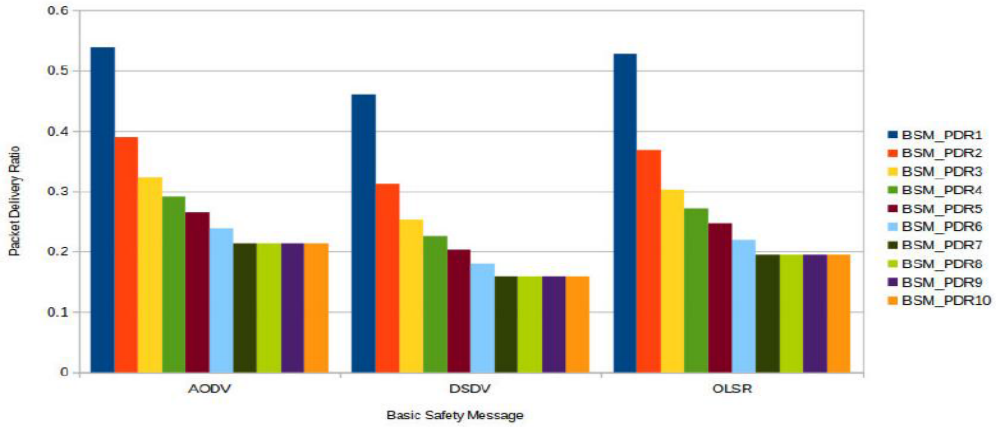


Figure 4.5: BSM-PDR aimed for CARs, BUS and TRAIN.

4.2 SIMULATION AIMED AT THE AVARAGE GOODPUT

This research is conducted with simulations close to those of analysis 1 with velocity shifts from 10 m/s to 20 m/s and 30 m/s the average good position is based on the three protocols

1- For the vehicles: AODV is the best protocol to demonstrate all three vehicle speed scenarios to a general audience. However, being better than two protocols, DSDV positioning is superior to 10K/m vehicle speed. Lowest level of AODV and DSDV: AODV and DSDV have similar OLSR value results in Figure 4.6

2- For the cars, as well as the bus: the findings of the AODV research demonstrate that the protocol is the right choice for all three vehicle speed scenarios. Still, OLSR is more successful than two protocols that achieve 30,000km/h for the vehicle. Figure 4.7 shows the best-case scenario for OLSR.

3- For cars, bus, and train: The OLSR well-constructed visuals depict the different vehicle speed values over time in the best way possible. However, success placed by DSDV in terms of 30km/m vehicle speed is higher than two protocols. The minimum amount obtainable with the OLSR and DSDV model is depicted in Figure 4.8.

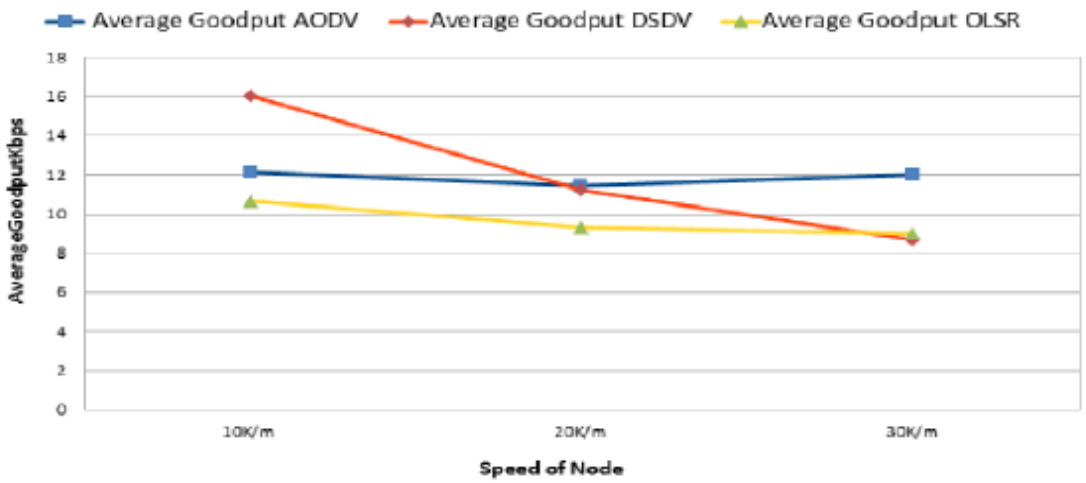


Figure 4.6: BSM-PDR for CAR, BUS and TRAIN.

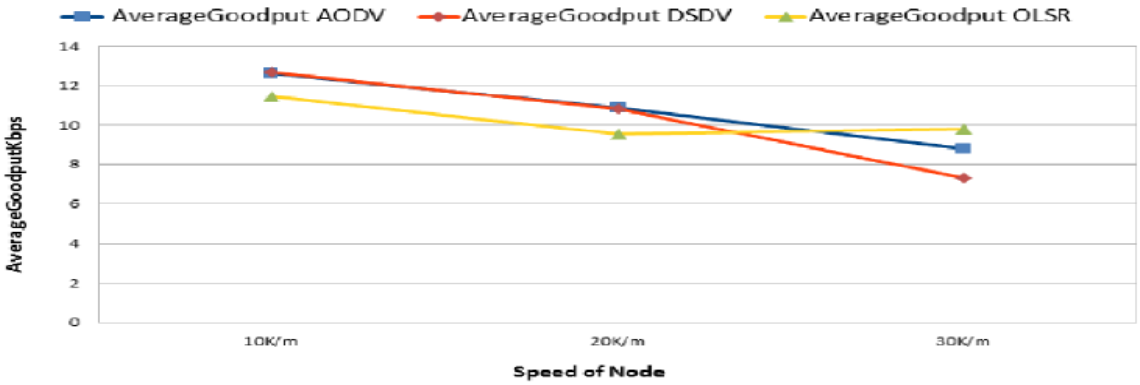


Figure 4.7: BSM-PDR for CAR, BUS and TRAIN.

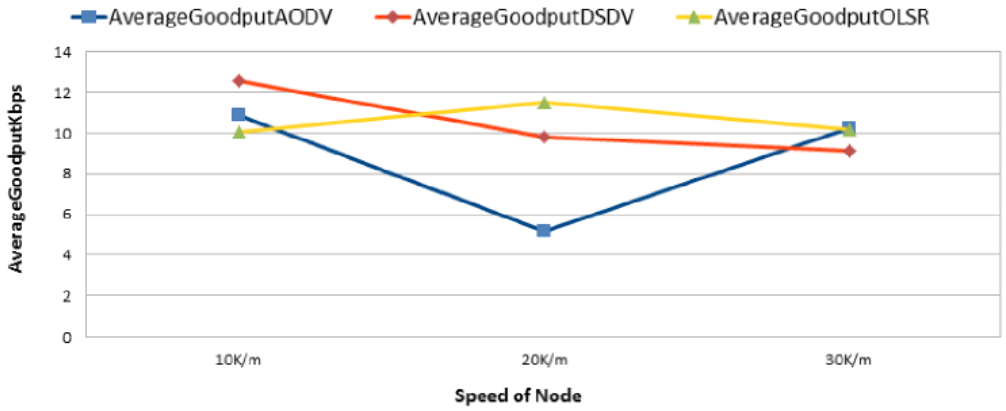


Figure 4.8: BSM-PDR for CARs, BUS and TRAIN.

5. CONCLUSION

To study the DSDV, OLSR, and AODV system's relative performance in VANET scenarios, we used a simulation model. Sharing critical information requires vehicle-to-vehicle (V2V) communication. Every second ten messages can help drivers and other motorists stay informed. The calculated performance assessment ratio of simple safety messages is the norm. When vehicles are going at speeds of 10 km/h and 20 km/h at 30 km/h, results from AODV are better. AODV can operate at a higher throughput than OLSR. In densities between the lowest and highest vehicles, AODV and DSDV perform better than the BSM PDR.

5.1 FUTURE WORK

We suggest in the future work to give more scenarios and in different areas and change the number of nodes participating throughout the network to understand how the changes in the work of the protocols also compare these protocols with other protocols to understand the properties of the protocols more deeply and choose the best among them.

REFERENCE

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

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

[12] 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.

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.