Performance Analysis of Routing Protocols and TCP Variants under HTTP and FTP Traffic in MANETs

Ghassan A. Qas Marrogy

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirements for the Degree of

Master of Science
in
Electrical and Electronic Engineering

Eastern Mediterranean University
June 2013
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Prof. Dr. Elvan Yılmaz
Director

I certify that this thesis satisfies the requirements as a thesis for the degree of Master of Science in Electrical and Electronic Engineering.

Prof. Dr. Aykut Hocanın
Chair, Department of Electrical and
Electronic Engineering

We certify that we have read this thesis and that in our opinion it is fully adequate in scope and quality as a thesis for the degree of Master of Science in Electrical and Electronic Engineering.

Assoc. Prof. Dr. Ahmet Rizaner
Co-Supervisor

Assoc. Prof. Dr. Ali Hakan Ulusoy
supervisor

Examining Committee

1. Prof. Dr. Hasan Amca
2. Prof. Dr. Aykut Hocanın
3. Assoc. Prof. Dr. Hasan Demirel
4. Assoc. Prof. Dr. Ahmet Rizaner
5. Assoc. Prof. Dr. Ali Hakan Ulusoy

ABSTRACT

MANET stands for mobile ad-hoc network that has multi-hop and dynamic nature, where each station changes its location frequently and automatically configures itself. Nodes can move freely in MANET while transmitting and receiving the data traffic by using wireless radio waves. Hence, nodes mobility in MANET requires a routing mechanism to communicate with each other. Additionally MANET experiences several types of delays and losses which may not be related to congestions. Appropriate precaution has to be taken for assessing such losses and distinguishing them from congestion losses, so that TCP can be sensitive while invoking the congestion control mechanism. In this thesis, four routing protocols that are optimized link state routing (OLSR), geographic routing protocol (GRP), dynamic source routing (DSR), and ad-hoc on-demand distance vector (AODV) are discussed along with three TCP variants that are SACK, New Reno and Reno. The main focus of this thesis is to study the impact of high, medium and low traffic load on routing protocols and TCP variants. The thesis also analyzes the performances of routing protocols and TCP variants on other environmental conditions such as scalability and mobility. The results of the thesis show that the proactive protocols OLSR and GRP outperform the reactive protocols AODV and DSR with the same nodes size, nodes speed, and traffic load. On the other hand, regarding the TCP variants, the results of the research reveal the superiority of the TCP SACK variant over the other two variants in case of adapting to varying network size, while the TCP Reno variant acts more robustly in varying mobility speeds and traffic loads.

Keywords: MANET, routing protocols, TCP variants, performance evaluation, network load.

ÖZ

Mobil tasarsız ağlar anlamına gelen MANET dinamik bir yapıya sahip olup, her istasyonun sık sık yer değiştirdiği ve otomatik olarak düzenlendiği bir yapıya sahiptir. Düğümler kablosuz radyo dalgalarıyla iletim ve alış veri trafiğini sağlarken MANET içerisinde serbestçe hareket edebilirler. Bu nedenle, düğümlerin MANET içerisindeki hareketliliğinden dolayı birbirleri ile iletişim kurabilmeleri için bir yönlendirme mekanizmasına ihtiyaç vardır. Ayrıca MANET'de tıkanıklık ile ilişkili olmayabilen birçok gecikme ve kayıp yaşanabilir. TCP'nin duyarlı bir şekilde tıkanıklık kontrol mekanizmasını sürdürebilmesi için bu kayıpların değerlendirilmesi ve tıkanıklık kayıplarından ayırt edilmesi için uygun özenin gösterilmesi gerekmektedir. Tezde en uygun bağlantı durumu yönlendirme (OLSR), coğrafi yönlendirme protokolü (GRP), dinamik kaynak yönlendirme (DSR), ve anlık talep üzerine mesafe vektörü (AODV) olarak adlandırılan yönlendirme protokolleri ile birlikte SACK, Yeni Reno ve Reno olarak adlandırılan TCP türevleri incelenmiştir. Tezin ana inceleme alanı yönlendirme protokolleri ve TCP türevleri üzerinde, yüksek, orta ve düşük trafik yükünün etkisini incelemektir. Tez ayrıca ölçeklenebilirlik ve hareketlilik gibi diğer çevresel koşullara göre yönlendirme protokollerinin ve TCP türevlerinin başarımlarını analiz etmektedir. Tezden elde edilen sonuçlar neticesinde, proaktif yönlendirme protokolleri OLSR ve GRP'nin ayni düğüm boyutu, düğüm hızı ve trafik yükü altında reaktif protokoller AODV ve DSR'den daha iyi başarımlar verdiği gösterilmiştir. Diğer yandan, TCP türevleri ile ilgili olarak yapılan araştırma sonuçları göstermiştir ki, TCP Reno türevi farklı hızlarda hareket ve trafik yükünde daha sağlıklı davranmasına rağmen, TCP

SACK türevi değişik ağ boylarına uyum sağlama açısından diğer iki türevden daha iyi başarım göstermektedir.

Anahtar Kelimeler: MANET, yönlendirme protokolleri, TCP türevleri, başarımlarının değerlendirme, ağ yükü.

This thesis is dedicated to my lovely Father, Mother, Wife, Three Sisters, and to all my Friends.

ACKNOWLEDGMENTS

My sincere appreciation goes to my supervisors Assoc. Prof. Dr. Ali Hakan Ulusoy and Assoc. Prof. Dr. Ahmet Rizaner for their endless patience, support, motivation, knowledge and guidance of my master study. Their supervision in this thesis assisted me through studying, writing and preparing it. I never imagined better supervisors for my master education.

My deep gratitude goes to god who helps and facilitates the way to fulfill my dream. Special thanks to my father AMANUEL and mother WIJDAN for their patience, pain, effort, support, and prayers were the success of my life I own to them. Exceptional thanks go to my precious wife RAGHDA with her continuous love, encouragement, support, who stands with me in this dream. I also thank all the support and help from my family and friends.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACK	Acknowledgements
AODV	Ad-hoc On-Demand Distance Vector
AP	Access Point
BPS	Bits per second
CPT	Client Processing Time
DSR	Dynamic Source Routing
GRP	Geographic routing protocol
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
LAN	Local Area Network
MANET	Mobile Ad-Hoc Network
MPR	Multipoint Relay
NS-2	Network Simulator 2
OLSR	Optimized Link State Routing
OPNET	Optimized Network Engineering Tool
PRNG	Pseudo Random Number Generator
PRP	Proactive Routing Protocol
RERR	Route Error

RREP	Route Reply
RREQ	Route Request
RRP	Reactive Routing Protocols
RTO	Retransmission Timeout
SPT	Server Processing Time
SSThresh	Slow Start Threshold
TCP	Transmission Control Protocol
WAN	Wide Area Network

Chapter 1

INTRODUCTION

In the recent years, the requirement for exchanging data information over the wireless environments is rapidly growing. There is an increasing demand on connections to access the Internet for browsing, downloading and sending e-mails, contacting friends, and connecting in social media. Wireless networks are much more preferred in those connections due to the simplicity, low-price installation and the ability of joining new hosts to the network at no or low charge. Therefore there is a need for reliable and effective routing protocols to transmit the information across the wireless networks. The fixed infrastructure devices, such as access point (AP) and wireless base station permit any device with wireless adapter card to attach the local network and access the internet. There are solutions for the need of connecting in cases of no AP, routers or base stations available. In this case the mobile ad-hoc network (MANET) steps in where the hosts can join, move or leave the ad-hoc network at any time without any limitation.

1.1 Thesis Aims

The main objectives of this thesis are to get accurate perception and finding the best behavior of the MANET reactive, and proactive routing protocols under heavy, medium and low hypertext transfer protocol (HTTP) traffics, and transmission control protocol (TCP) variants under a combination of heavy, medium and low file transfer protocol

(FTP) and HTTP traffics. The thesis also discusses the performance evaluations of the routing protocols and TCP variants under other environmental conditions, such as the mobility, and scalability.

1.2 Research Challenges

The key problem in MANET is to find and choose reliable, effective and accurate routing protocol among the three MANETs routing categories that plays optimal role for selecting the best route. Challenges revolve on finding which routing protocol provides a better performance regarding the effect of scalability, mobility and varying traffic load over heavy, medium and low HTTP traffics by analyzing and observing mainly the end-to-end delay and throughput. Another challenge is to find the best TCP variant over heavy, medium and low HTTP and FTP traffic loads that ensure the best performance for MANET environments by analyzing and observing mainly the page response time and retransmission attempts.

1.3 Thesis Scope

Basically, routing protocols in MANET are categorized into three groups as reactive routing protocols, proactive routing protocols and the combination of both protocols known as hybrid protocols. The study in this thesis discusses two reactive routing protocols (RRPs) namely, ad-hoc on-demand distance vector (AODV) and dynamic source routing (DSR), and two proactive routing protocols (PRPs) namely optimized link state routing (OLSR) and geographic routing protocol (GRP). The thesis also discusses three TCP variants namely, Reno, New Reno and SACK in MANETs. Extensive simulation studies are carried out to discuss the performance analysis of routing protocols and TCP variants on different MANET environmental conditions. The design issues of RRP, PRP and the energy consumption of the routing protocols are not considered in the content of the thesis.

1.4 Thesis Outline

The first chapter presents the thesis content, aims, and challenges of the research. The second chapter covers both background and related work. The third chapter describes the ad-hoc routing protocols. Fourth chapter explains the HTTP, and FTP traffic models and TCP variants. Chapter five discusses the performance parameters of routing protocols and TCP variants together with the software environment. Sixth chapter presents the results of simulations, and explains the performance analysis of routing protocols and TCP variants in terms of mobility, scalability, network traffic load. Finally, the conclusion is given in the chapter seven along with the future work.

Chapter 2

BACKGROUND AND RELATED WORK

Pervasive computing surroundings are expected to support the recent computing and communication technologies advances and progresses. The upcoming generation of wireless and mobile communications may involve prestigious infrastructure wireless networks and novel infrastructureless MANETs.

This chapter presents a general introduction about networks, with a brief outline about wireless networks, and their types and the relation between ad-hoc networks and the MANETs. Then, an overview about the routing protocols and the TCP variants is presented. This chapter also discusses the types of network simulators used in similar researches to present the performance results of MANETs. Finally a literature review about the protocols and variants are given to show some related work.

2.1 Introduction to Networks

Generally, a network is an infrastructure group of computers, software, and hardware that provides connectivity and interacts to each other or to multiple autonomous computers, for sharing resources, such as information data, hardware, software and other resources. Any network can be connected by wire or wireless medium, arranged and controlled by software and devices that manage and control the exchange of information. There are two main types for the networks, client/server and peer-to-peer networks. The first type uses single or multiple dedicated nodes as a server to exchange the data and share the resources such as printers, and applications, while the second type allows any node to share the information with any other node without any central devices, or dedicated server. There are different types of networks but the most common types are local area networks (LANs) that connect a group of devices within a small geographic position, such as homes buildings or office, and wide area networks (WANs) that extends to various countries or cities, using cables or satellite links.

2.2 Introduction to Wireless Networks

Wireless networks are preferred because of their easy installation without any cabling, and providing easy access to the network for anyone. The wireless networks use the radio signals and/or microwaves for communicating among the devices. Sometimes a wireless network is also referred as Wi-Fi network, or WLAN. The IEEE 802.11 standards define two kinds of operating modes as infrastructure and ad-hoc mode. Infrastructure mode connects wireless devices by the help of AP. Ad-hoc mode connects wireless clients directly with each other, without any need for a wireless router or AP.

2.3 Types of Wireless Networks

As mentioned above networks, depending on wireless component can be separated into two categories where one is the infrastructure wireless and the other is the infrastructureless or ad-hoc networks.

2.3.1 Infrastructure Networks

The basic term in infrastructure networks is the fixed topology. It is an interconnected set of computer systems linked together by AP or base station, which is connected to the main network by backbone physical cable, wireless links or combination of both.

2.3.2 Ad-Hoc (Infrastructureless) Networks

Ad-hoc network can be installed and set up anywhere without needing any type of external infrastructure or APs. All of the nodes behave as AP, and are directly connected to each other to exchange and pass data from one to another. They also engage in discovering and maintaining the routes to other nodes in the same network. That is why it is called as ad-hoc network or infrastructureless network.

Generally ad-hoc networks are closed and network nodes cannot connect to Internet. However, if one of the nodes is directly connected to the Internet, the connection is shared through other nodes and the users are allowed to access the Internet. One of the major reasons for using this type of network is the flexibility and facilities of deployment.

2.4 Mobile Ad-hoc Networks

A MANET is an independent set of wireless mobile devices that can dynamically form a network connected by wireless links to exchange information without using any pre-existing fixed network infrastructure. The network topology always changes rapidly and unpredictably, since the devices are free to move randomly and arrange themselves arbitrarily.


(a) Initial topology (b) Changed topology

Figure 1.1: MANET Changing Topology

Such networks can operate independently or can also connect to larger networks such as Internet. Due to the dynamic topology of MANET as shown in Figure 1.1, with no AP and no prerequisites of fixed infrastructure, quick propagation and self-configuration of MANET nodes in cases as catastrophic situations makes them more suitable. Many areas makes MANET needed to be used. It can be used as an extender for the infrastructure networks coverage such as cellular networks [1, 2], or other operations such as, search and rescue, collecting information, virtual conferences and classes using tablets, laptops, or other wireless equipment in wireless communication [3].

Mobile hosts in a MANET forward the incoming traffic of the neighbor to destination host acting like a router [3]. So there is no need for AP, base station or any physical wired infrastructure. Each wireless node communicates with other wireless nodes within its wireless range with their smart antennas. That is the main reason why such a network structure is called as MANET. Due to the mobility and the joining and leaving processes in a wireless network, the nodes waste high amount of energy [4]. The leading aim for developing routing protocols for the ad-hoc networks is to conquer MANET’s dynamic nature. The ad-hoc routing protocols efficiency can be specified by the consumption of the battery power.

2.5 MANET Protocols

Many routing protocols were proposed for ad-hoc networks [5]. They can be categorized in to three types, namely PRPs (table driven), RRPs (source-initiated or on-demand-driven) and HRPs (hybrid) that use the advantage of both PRP and RRP.

2.6 TCP Variants used in MANETs

TCP is required to be responsible for reliable transmission of the end-to-end data packet. In MANET, TCP is still required due to its commonly used for achieving the integration very smoothly through the current global Internet. The traditional TCP does not perform well on MANETs and it raises serious performance issues. Therefore, several TCP variants such as TCP SACK, Tahoe, New Reno, Reno, and Vegas were designed for MANET applications. For the static global Internet, researchers’ interest increased to find the best TCP variant that is suitable for MANET. Many studies evaluated the TCPs through the selection of one routing protocol, or many routing protocols evaluated with single specific TCP variant.

2.7 Simulators for MANETs

There are many popular network simulators to simulate different network environments, such as the OPNET modeler simulator [6], the NS-2 simulator [7] or the GloMoSim simulator [8]. All these simulators offer advanced environments for the simulation to run, debug, and test all types of protocols and applications for wireless networks.

2.8 Literature Review about the Routing Protocols

Several routing protocols for MANETs have been applied and implemented to achieve higher throughput, lower overheads per packets and low consuming of energy. Many research studies have been carried out for the performance evaluation of routing protocols regarding scalability, mobility and different traffic loads by the use of network simulators such as NS-2 and OPNET. Studies have shown that routing protocols have different benefits and drawbacks over specific circumstances. The main requirements of routing protocols has been discussed in [5] which included the delay of the least route acquisition, routing speed re-configuration, loop-free routing, process of the distributed routing, scalability and leased overhead control.

During the past few years, many simulation studies regarding MANET routing protocols have been done with route discovery and maintenance, memory overhead, communication complexity, time complexity and control overhead [5, 9], but still there is serious absence in functionality and MANET’s routing protocols operational experiences. Mobility kinds have been specified and implemented in [10] where the mobility of node affects total performance of the routing protocols. The research in [11] analyzed TORA, OLSR and GRP, in term of routing overhead and delay. The results of the research show that OLSR has the highest throughput and lowest delay, with the expense of a high routing load cost. Research in [12] integrated a discussion on protocols of DSR, AODV, TORA and OLSR, regarding scalability and mobility, where

OLSR was the most favorite PRP, while AODV has been designated as the most effective on-demand protocol for MANET scenarios. The performance of DSR, AODV and OLSR routing protocols has been evaluated and measured by taking into account metrics like route length and control traffic overhead, packet delivery ratio using the simulator NS-2 in [13, 14]. Similarly TORA, DSR, AODV and OLSR performance were again examined by OPNET simulator with packet delivery ratio metrics, throughput, media access and delay end-to-end delay in [15, 16]. These protocols do not have similar properties, and their behaviors are different for different network environments, so it becomes indispensable to simulate and examine their performance in an ideal environment network.

MANET TCP optimization has been investigated in many studies [15, 17, 18]. Due to intolerance mechanisms of TCP in dealing with link failures, this leads to incapability of distinguishing the difference between network congestions and link failures in MANET. Many research addressed the TCP performance problems due to route failures in MANETs [19, 20]. For improving the TCP performance in MANET a new feedback based scheme has been proposed, which declared the use of feedback mechanism that offers noteworthy gains in throughputs, for saving the unnecessary data packet transmissions. A study conducted in [21] regarding the Westwood, TCP Reno, and BIC-TCP demonstrated the superiority of Reno variant over the others. However it lacked in recognizing different realistic scenarios with one source of TCP traffic was simulated in this research. The research in [22] discussed the performance evaluations of Reno, Tahoe, New Reno and SACK in different MANET realistic scenarios under the conditions of fading, signal attenuation, and multipath. It was shown here that TCP

Reno version overcame the other congestion control algorithms regarding throughput, congestion window, and goodput.

Four different MANET routing protocols, namely DSR, AODV, OLSR and GRP are simulated under HTTP traffic in this thesis by OPNET Modeler 14.5 educational version [6]. Reno, New Reno and SCAK TCP variants are also analyzed to observe their behavior under different MANET environments.

Chapter 3

AD-HOC ROUTING PROTOCOLS

In order to facilitate communication within the network, different network management routing protocols are used. Generally the routing protocols are used to determine the best routes from the sender/source node to the receiver/destination node, to connect two or more nodes to transfer data with each other where a set of rules must be followed. In this chapter detailed description of MANETs routing protocols are classified, discussed and compared.

3.1 MANET Routing Protocols

Routes in ad-hoc networks are enabled using multi-hop between the nodes in a limited wireless radio propagation range. When the nodes are busy in traversing packets over MANET, they are not aware of the network topology. Discovery of the network topology is done with the routing protocols by receiving the broadcast messages from the same network neighboring nodes. Routing protocols as shown in Figure 3.1 are categorized as reactive, and proactive, depending on the routing information update time, and hybrid that is the combination of both.

Based on the content of the routing table, there are two other classes of routing protocol which are defined as distance vector class and link state class [23, 24]. The distance vector protocols spread the distance lists to the destination node, while the link state protocols involve in maintaining the network topology. Generally, the link state protocols exhibit more stability and robustness than the distance vector protocols though they are found much more complex to use in MANETs.

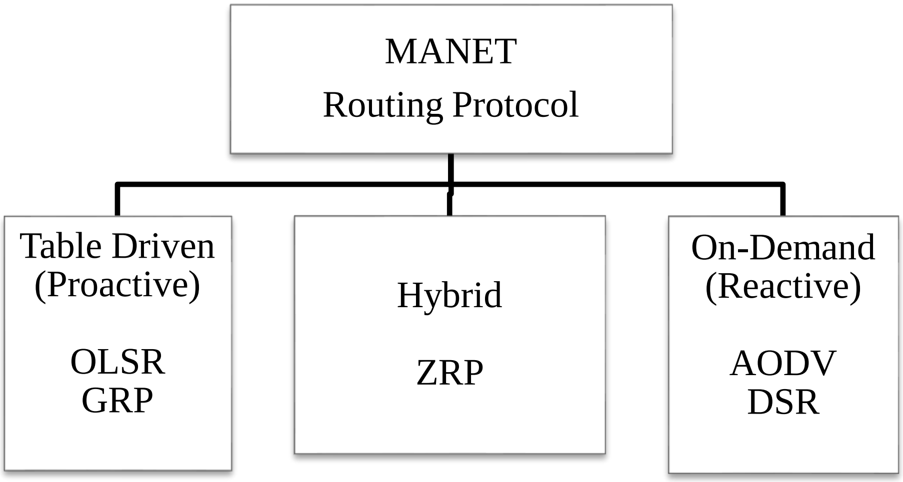


Figure 3.1: Types of MANETs Routing Protocols

3.2 Reactive (On-demand) Routing Protocols

Another name of RRP is on-demand routing protocols, where there is no pre-defined route between the nodes for routing. Whenever a transmission is required a source/sender node demands for the route discovery mechanism to define a fresh route. The mechanism of route discovery depends on the flooding technique, where the source/sender node broadcasts only its data packet to all of its neighbor nodes, and intermediate nodes simply forward the same data packet to their neighbors. This is constantly a repetitive technique till it reaches the receiver/destination node. Briefly reactive techniques have higher latency but shorter routing. AODV and DSR routing protocols are discussed in more details as examples of reactive routing protocols in the following sections. The DSR protocol executes source routing from the acquired query packet addresses, while the AODV protocol uses the information of the next hop saved in the route nodes.

3.2.1 Ad-hoc On-demand Distance Vector

AODV’s reactive approach indicates that it requests and sets up a route to destination only when it requires one to transmit data, and it does not maintain the initiated route after the transmission is finished. AODV protocol starts a broadcast route discovery mechanism to find the recent effective route to destination by using a route request (RREQ) route reply (RREP) query cycle. An AODV sender broadcasts an RREQ packet to all nodes in the network, and after receiving this packet the nodes update their information in the routing table for the sender node and initiate a route back to the sender node through the RREQ path. The RREQ packet contains the sender Internet protocol (IP) address, destination’s IP address and broadcast ID. Then nodes unicast a RREP packet to the sender if the receiver node has an active route to the destination, otherwise, the RREQ packet is forwarded to other nodes. When there is a reply transmitted, all the nodes in that route can record the route to the destination in this packet. Because other paths can be found between the sender and the destination, the sender can receive the RREQ packet multiple times. In case of route failure, due to mobility or link disconnection a route error (RERR) packet is sent to the neighbors to inform about the broken paths, and activate the route discovery mechanism.

A destination sequence number is also used for avoiding routing loops, and guaranteeing the recent routes to be selected, where the larger the number is the fresher the route is. The sequence number is included in both RREQ and RRER packets, where in RREP the number must be larger or equal to the number included in the corresponding RREQ packet, to ensure that the sender node does not choose an old route. In case of many routes available by different RREP packets, the effective route should be with the largest destination sequence number, and if many routes have the same sequence number, the lowest hops route to destination is chosen. AODV protocol is used in relatively static networks, with low byte overhead and loops free routing using the destination sequence numbers.

3.2.2 Dynamic Source Routing (DSR)

DSR’s reactive approach uses source routing mechanism for transmitting data, meaning the sender must know the complete sequence of hops to reach the destination. DSR also sets up a route only when required and does not maintain routes after the transmission is finished. It consists of two parts: route discovery and route maintenance. Every network node preserves a route cache that stores all known routes, and if a desirable route cannot be found in the cache, it starts a route discovery mechanism to lower the RREQ packets broadcasted. As each node receives the RREQ packet and sees the request identifier from the sender it discards it. Otherwise it includes its address to the request list and rebroadcasts it. After RREQ reaching to the destination node, it sends back a RREP packet to the sender, including accumulated list addresses from the request. Finally after receiving the RREP packet, it caches the new route in its route cache. If a link break is detected, the sender starts route maintenance mechanism, where a RERR packet is transmitted back to the sender for maintaining the information of the route. When the sender receives the RERR packet, it starts again a route discovery mechanism, then the failed routes has to be deleted from the intermediate nodes route cache after sending the

RERR packet to the sender. The sender must determine the sequence of hops that each packet should be transmitted through. This involves that each packet’s header must include the sequence of hops that a packet should across. By this way each intermediate node can specify and learn the route to the destination depending on the source routes in the received packet. The advantage of this technique is the decrease in the overheads of the control packets of the route discovery with using route cache. On the other hand the disadvantage is that source routing can lead increase in the packet header size with route length.

3.3 Proactive (Table-Driven) Routing Protocols

The PRPs are also called table-driven protocols. In the PRPs the routes between the nodes are maintained in routing table and the packets of the source/sender node are transmitted over the route that is predefined in the routing table. During this phase, the packets forwarding are done quicker, however the routing overhead is larger. As a result, before transferring the packets, all of the routes need to be defined and maintained at all the times. Therefore PRPs have smaller latency. OLSR and GRP protocols are considered and explained as examples of PRPs in the following sections.

3.3.1 Optimized Link State Routing (OLSR)

OLSR’s proactive approach updates and stores at all-time its routing table. It always maintains its routing table to provide routes when required. All network nodes broadcast periodically their routing tables to permit all nodes for knowing the topology of the network. As a disadvantage of this, it generates an overhead to the network. To decrease this overhead, it limits the number of the network nodes that can pass the traffic of the network by using multi point relays (MPRs). The responsibilities of MPRs are to pass the routing packets and enhance the control flooding and its operations. MPRs selected nodes can decrease the control packet size and pass the control traffic. All network nodes select MPR group from one away neighbor hop, where each chosen MPR can reach other two hop neighbor by minimum one MPR. Each network node broadcasts periodically its selected MPR list rather than the all neighbors list. In case of broken links due to mobility, topology control packets are broadcasted over the network. All network nodes preserve the routing table that includes routes to all reachable destination network nodes. OLSR protocol does not inform the sender when there is a route failure immediately. Therefore the sender comes to know about the broken links when the intermediate node broadcasts its next packet.

3.3.2 Geographic Routing Protocol (GRP)

GRP is a position based protocol, where each node in the network knows its geographic location, its immediate nodes and the sender knows the destination position. Each node updates the location of its immediate neighbors periodically by using Hello messages. The destination node geographic location is used for routing the data packets through the network without needing network address. GRP functions without the need for routing tables. Therefore, it can reach the destination node by using the information of the physical position concerning its neighbor’s nodes. Each network node defines its position by using Global Positioning System (GPS) or other positioning services, and flooding that information by quadrants nodes. The node can also return the data packet to the last previous node when the route becomes unavailable to the destination node. GRP divides the MANET network into various quadrants for decreasing the route flooding, where every node in the quadrants knows the initial position of every reachable node after the initial flooding is finished in the network.

3.4 Comparison of Routing Protocols

Table 3.1 presents a comparison of four MANETs routing protocols in terms of routing mechanism, loop freedom, routing updates, advantages, disadvantages.

Table 3.1: Comparison of Routing Protocols

Parameter	AODV	DSR	OLSR	GRP
Routing mechanism	Reactive	Reactive	Proactive	Proactive
Network information maintenance	Route table	Route cache	Route table	Position data
Routing method	Broad cast or flooding	Broadcast	Flooding	Flooding
Update of routing information	As required	As required	Periodically	Periodically
Multicasting possibilities	Yes	No	No	Yes
Drawbacks	Scalability and large delay problem	delays in large network, source routing mechanisms	The MPR sets could be overlapped	complexity and overhead required
Advantages	efficient to dynamic topologies	Provide multiple routes and avoid loop formation	Trim down the number of broadcasts	does not require maintained of routing tables

Chapter 4

INTERNET TRAFFIC AND TRANSMISSION CONTROL PROTOCOL

Internet traffic models are required for the purpose of architecture refinement and network dimensioning. Currently, in residential and backbone access networks most of the traffic is World Wide Web (WWW), where mostly HTTP and FTP protocols are used to exchange or transfer hypertext and files together with TCP. In this chapter, the discussions about the Internet traffic and TCP are explained.

4.1 Internet Traffic

Internet traffic transports a widely range of various information resources and data services, such as HTTP, FTP, e-mail, media streams. In this thesis, the HTTP and FTP traffics as the most widely traffic types used in the Internet are simulated for MANETs.

4.1.1 HTTP Traffic

HTTP is the foundation of data communication for WWW. It plays a key role of web browsers communication with the web servers. By avoiding counterfeits and eavesdroppers, it certifies and guarantees the security of communication. The standard of HTTP is not only restricted to the exchange of the fixed information, nevertheless it can exchange and store all kinds of information. A group of rules has been offered by the hypertext markup language (HTML) to create a web page, whereas, HTTP is expert for converting multimedia objects, program files, and remote printing instructions [25]. The performance evaluation of routing protocols in this thesis is carried out under different amount of HTTP traffic such as low, medium and high.

4.1.2 FTP Traffic

FTP is a protocol that transfers files from any node through the Internet and other networks. The performance evaluation of TCP variants in this thesis is carried out under different amount of FTP traffic such as low, medium and high together with HTTP traffic.

4.2 Transmission Control Protocol

The responsibilities of the transport layer are to transmit data packets, provide error and flow control and divide application data parts into appropriate blocks for below layers. TCP is executed at the fourth layer (transport layer) of MANET, and transports nearly 90 percent of the traffic in the Internet in recent various wired and wireless networks [26]. It is also commonly used as a connection oriented transport layer protocol that enjoys the advantage of reliable data transmission in the Internet over unreliable links. Generally connections on TCP are virtual which implies setting up a logical connection before data transmission. TCP does not count on the layers of the underlying network. Therefore different TCP variants initially designed for the wired networks properties. TCP works with the end systems at a higher level like web servers and web browsers. The applications included with TCP are HTTP, e-mail, FTP, and streaming media. Requests are used by TCP when transmitting the data for the packet loss to minimize the network congestion and rearrange the out of order packets. Although TCP is an efficient packet delivery mechanism, it sometimes leads to long delays by the use of requests for lost packets [27]. The algorithms of the TCP congestion control cannot execute efficiently in diverse networks.

The standard TCP always uses more than one of the four congestion control algorithms, namely: slow start, congestion avoidance, fast retransmit and fast recovery, during the connections. The slow start algorithm is used after the connection is set-up. During this algorithm, the congestion window is incremented by a single packet for each new received ACK. Till specific conditions occur [28] the connection stays in the slow start mechanism. After receiving the new ACKs, additive increase phase is used for adjusting the congestion window. After congestion occurs, multiplicative decrease phase is used for adjusting the congestion window. These two parts form the congestion avoidance algorithm. When transmitting packets, the fast retransmit algorithm is used once a three duplicate ACKs is received concerning the same packet. Then the sender retransmits immediately the lost packet, for avoiding the waiting for the timeout timer to expire. The algorithm of fast retransmit is designed to avoid waiting the timeout to go off before transmitting the lost packet. If the packet is lost, the congestion avoidance multiplicative decrease phase is used to update the slow start threshold (ssthresh), and then the congestion window is set to the new ssthresh value. After decreasing the window size, the congestion avoidance additive increase phase is used to renew the congestion window.

Even though TCP ensures reliable end-to-end message transmission over wired networks, a number of existing researches has showed that TCP performance can be substantially degraded in MANETs. Along with the traditional difficulties of wireless environment, the MANET includes further challenges to TCP. In particular, challenges like route failures and network partitioning are to be taken into consideration. Furthermore, MANET experiences several types of delays and losses which may not be related to congestions, though TCP considers these losses as a congestion signal. These non-congestion losses or delays mostly occur due to the inability of TCP's adaptation to such mobile network. Appropriate cares have to be taken for assessing such losses and distinguishing them from congestion losses, so that TCP can be sensitive while invoking the congestion control mechanism.

4.3 TCP Variants

The original design of the TCP was reliable, but unable to provide acceptable performance in a large and congested network. The development of the TCP has therefore been made progressively since its original incarnation in 1988. Although there are TCP variants called Dual, FACK, Vegas, Vegas+, Veno and Vegas A at the experimental status, three standard TCP variants namely Reno, New Reno, and SACK that are given in Table 4.1 are discussed in this thesis.

Table 4.1: Standard TCP Variants [14]

TCP Versions	**Changed /Added Features**
Tahoe	Slow start, congestion avoidance, fast retransmit
Reno	Fast recovery
New Reno	Multiple losses resistant for fast recovery
SACK	Feed-back messages extended information

4.3.1 TCP Reno

The current three TCP variants are constructed upon the TCP Tahoe mechanisms. TCP Reno is the most widely deployed TCP variant that most operating systems used. It is similar to TCP Tahoe, but with more mechanisms for detecting the lost packets earlier. When three duplicate ACKs are obtained by the TCP Reno sender, it retransmits one packet and decreases its ssthresh by half. Then it increases it for each received duplicated ACK. After receiving an ACK for a new data by the sender, it exits the fast recovery mechanism. The TCP Reno fast recovery mechanism is enhanced for the losses of one packet from the data window, but it does not execute well in case of multiple packets losses, where in this scenario the retransmission timer expires and causes the congestion avoidance mechanism to start with a lower throughput.

4.3.2 TCP New Reno

TCP New Reno attempts to enhance the problems of Reno. It eliminates TCP Reno’s waiting retransmission timer during multiple lost packets by the use of the information included in the partial ACKs differently. Partial ACKs acknowledge several packets in the sender’s window but not all the unacknowledged packets. The partial ACK in TCP Reno makes the sender exit the fast recovery mechanism. The received partial ACK through the fast recovery mechanism in TCP New Reno indicates the loss of the packet that follows the partial ACK and needs to be retransmitted. Therefore, in case of multiple packet losses partial ACKs guarantee the retransmission of the lost packets without waiting the retransmit timer to expire. After all transmitted packets are acknowledged during fast recovery phase, TCP New Reno exits the fast recovery mechanism. New Reno needs one round trip time (RTT) to sense the lost packet.

4.3.3 TCP SACK

The TCP SACK was built over TCP New Reno. It contains more functions for quicker data recovery in case of multiple packet losses. When an out of order data block is received by the receiver, it makes a hole in the buffer of the receiver. It leads the receiver to create for the packets received a duplicate ACK before the hole. It also contains the packet’s first and last sequence numbers that are delivered out of order. This data information is known as selective acknowledgments (SACKs). Therefore, every ACK has a block that indicates which packets are acknowledged ensuring that the sender knows which packets are still outstanding. This TCP mechanism permits the sender to recover from the losses of multiple packets in the data window during one loss detection RTT. When the TCP sender receives three duplicate ACKs it senses a lost packet. Then it retransmits the single packet, reduces the congestion window by half, and starts the fast recovery mechanism, similar to Reno, and New Reno. A variable known as pipe is used by SACK to estimate the number of outstanding packets in the path. The pipe decreases for received duplicate ACK having a new SACK and increases for each transmission. Depending on the received SACK, the sender has a list for the lost packets, and it retransmits these packets when the pipe is lower than the congestion window. In the end, once receiving partial ACKs, the SACK sender decreases the pipe by half. SACK also runs the fast recovery mechanism once every packet in the window during fast recovery mechanism is ACK. One important disadvantage of SACK is to have no selective acknowledgment option at the receiver.

Chapter 5

PERFORMANCE PARAMETERS AND SOFTWARE ENVIRONMENT

In this chapter, an overview of different metrics such as delay, throughput, page response time and retransmission attempts regarding the performance parameters of the routing protocol and the TCP variants is presented and discussed. This chapter also describes the simulation environment, the network model design and the necessary parameters to configure the network model used in this thesis. Finally, the simulation scenarios and the network conditions are presented at the end of this chapter.

5.1 Performance Metrics of Routing Protocols

In order to study and analyze the overall network performance, two parameter metrics are presented for MANET environment in OPNET simulator. These parameters play a key role for the evaluation of routing protocols in a communication network. They present the effectiveness of MANET protocols in finding the best route to the destination, such as the average throughput and the end-to-end delay where they can be described as follows:

5.1.1 Delay

The end-to-end average packet delay of the data packet is the time (in seconds) required as the source/sender node to generate and transmit a data packet across the network, until it is received by the destination node. Therefore, the entire network delay that includes the transmission time and buffer queues is called end-to-end average packet delay. It is also known as latency. Real time traffic such as video or voice applications is sensitive to the data packet delays, and needs delay as low as possible. However, the FTP and HTTP traffic is tolerant to a specific level of delay.

5.1.2 Throughput

The average network throughput refers to the amount of the data packets in seconds that are transmitted over a communication channel to the final destination node successfully. In other words it is the time in bits or bytes per second that the receiver node needs to receive the last message [29]. There are many factors affecting the throughput, such as frequent network topology changes, unreliable nodes communication, limited bandwidth and power source [29]. In every network it is desirable to have a high throughput. In this thesis throughput is defined as in equation (1):

$$\text{Throughput} = \frac{\text{Number of delivered packet} \times \text{Packet size} \times 8\ \text{bit}}{\text{Total duration of simulation}} \tag{1}$$

In (1) the number of delivered packets does not only include the HTTP or FTP data but also routing protocol’s Hello, control packets and topology information.

5.2 Performance Metrics of TCP Variants

The performance of different TCP variants also appears to be sensitive to metrics such as a page response time and retransmission attempts. Any communication network considers these parameters as an excessive effect for the selection of an efficient TCP variant and routing protocol. The performance metrics used for measuring the TCP variants are descripted in the following sections.

5.2.1 Page Response Time

Page response time can be defined as the time that a web page needs to be displayed completely on the user's browser. The page response time can be represented as in equation (2) [30]:

$$\text{Page Response Time} = \frac{\text{Page Size}}{\text{Minimum Bandwidth}} + (\text{RTT} \times \text{Turns}) + \text{SPT} + \text{CPT} \qquad (2)$$

where page size is the size of the transmitted page measured in Kbytes, minimum bandwidth is the lowest transmission line bandwidth between the web page and the end user, RTT is the latency between sending a page request and receiving the first bytes, turns is the number of TCP connections needed to fully download a page, SPT is the server processing time and CPT is the client processing time needed to assemble and view the required page.

Web page response time mostly relies on the size of the HTTP objects, number of the objects, and the underlying throughput [31]. In order to receive an optimal response time, web pages must hit the optimum balance between the content served and perceived end user response time.

5.2.2 Retransmission Attempts

Retransmission attempts occur when the transmitted data packets are not successfully delivered to the final destination node, due to dropping or losing the packets in the network. Then the sender retransmits the data packets again. Therefore, the number of times for retransmitting the packets through the network can be defined as the retransmission attempts

5.3 Simulation Environment

In this thesis, OPNET v14.5 is used as the simulation software. OPNET software is a discrete event network simulator [6], which provides many different solutions for controlling and managing applications and networks, such as network planning, performance management, research and development, network engineering and operation. The OPNET simulator is commonly used in simulating technologies, protocols, wireless mobile devices, and modeling performance of these technologies. OPNET also offers academic research solutions, such as Wi-MAX, Wi-Fi, UMTS and seamless communication, MANET protocols assessment and design, optical and core network design and enhancement, such as MPLS, IP-v6, and schemes of wireless sensor network power management [6]. OPNET has verified and accredited many simulation packages that have been done in several previous MANET studies. Widespread support also ensured for routing protocols, multi-cast protocols and TCP over both wired and wireless networks [6, 32]. These features make it desirable more from other simulation tools, such as OMNET [24] and NS-2 [7]. Also due to the efficiency, measurability, and the creditability of the OPNET simulator, in addition to its remarkable characteristic, such as inclusive graphical user interface, supporting various devices and protocols, and its flexibility for simulate and analysis, it becomes very useful and important tool in the research fields. Furthermore, it offers open source code model and object oriented modeling, which brings an easier understanding of the system.

The usability of OPNET can be divided into four basic steps. Modeling is the first step in OPNET. Then choosing and selecting the statistics is the second step. By third step, the network is simulated. And finally the fourth step is to analyze and view the simulation outcomes. The four mentioned steps are schematically presented in the Figure 5.1.

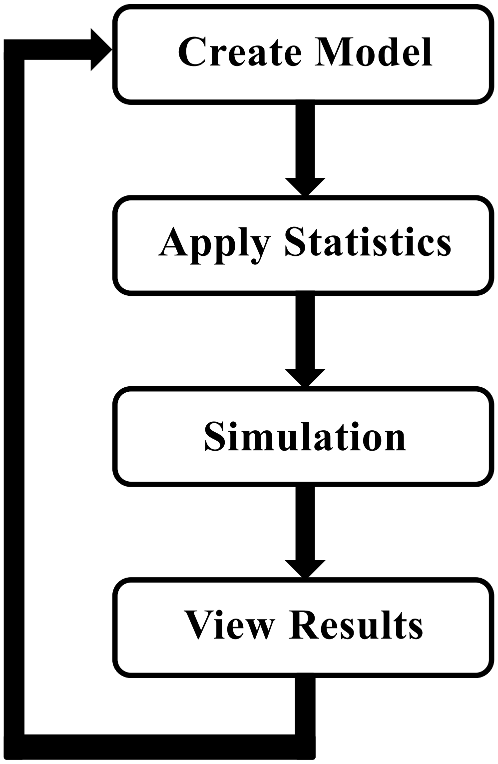


Figure 5.1: The Four Steps of OPNET Simulator

In this thesis a network with a common size of 1,000×1,000 m^2 is modeled with OPNET as shown in Figure 5.2. The number of nodes in the network is selected as 20, 40, 60 and 100 where one node is specified as server and the connections between the nodes are established by the help of four routing protocols AODV, DSR, OLSR, and GRP. There are also some other model objects used in the analysis of the network. These objects of the model are general component settings of the network that allows tuning and definition to the attribute that can be described as the follows:

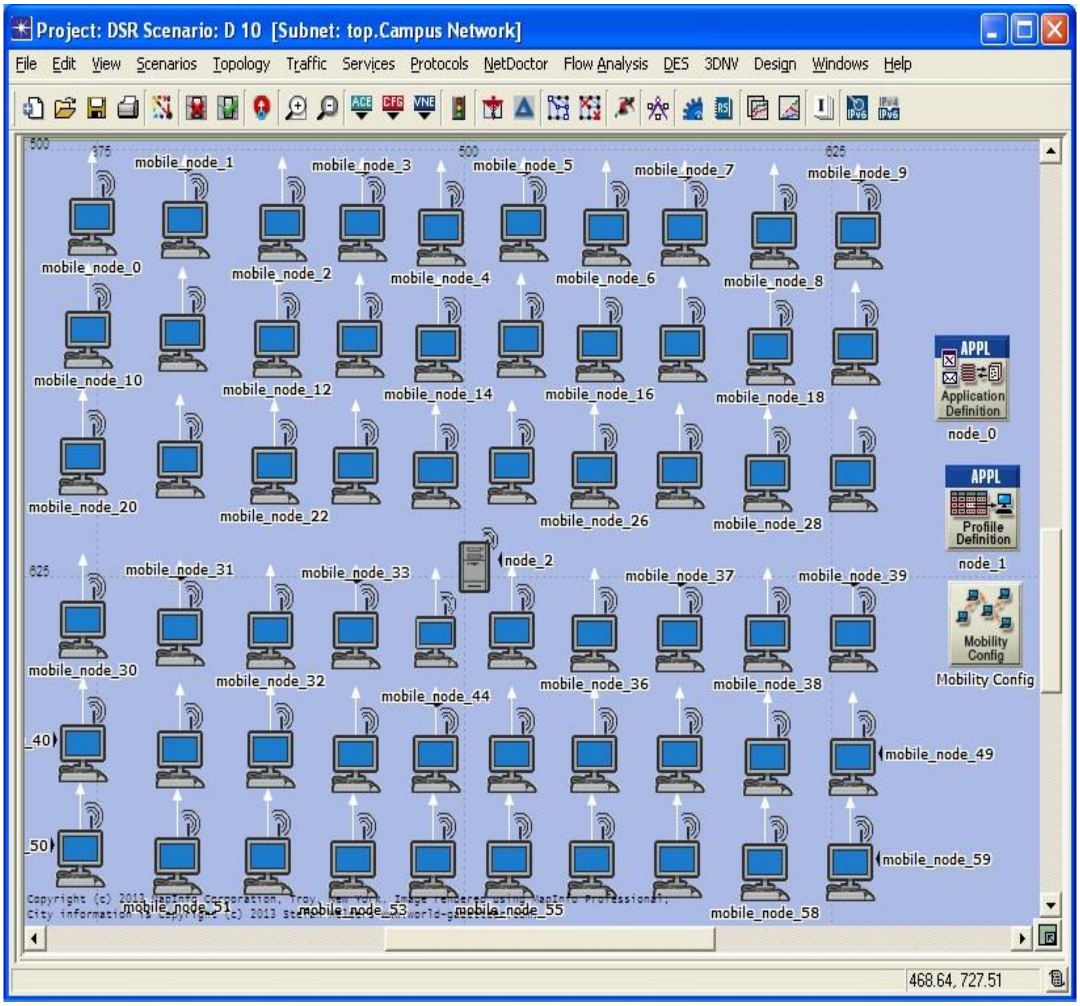
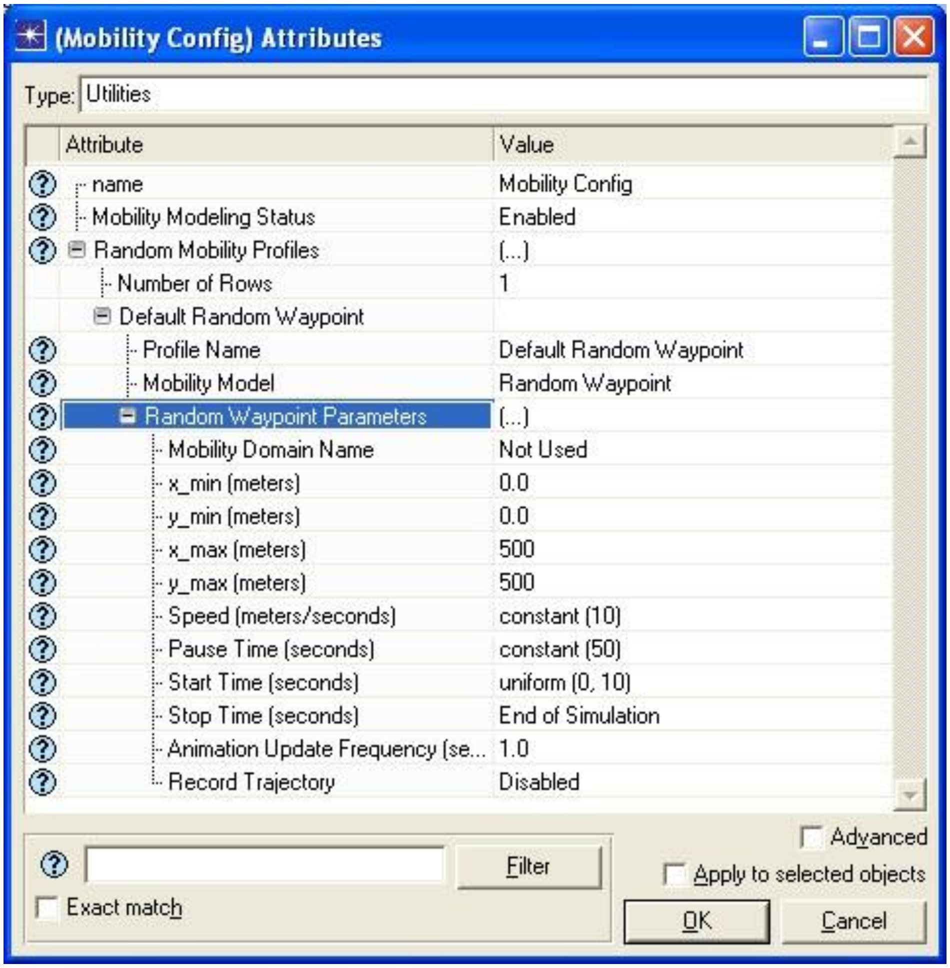


Figure 5.2: An Example of Network Model

5.3.1 Mobility Configuration

Mobility configuration is used to determine the nodes mobility. It includes many parameters to select such as start, pause and stop time and speed to control accurately the nodes mobility of the network. One of many reasons that the mobility object are inserted in the simulation, as shown in Figure 5.3, is to permit the nodes to move in the network within specific allocated 1,000×1,000 m^2 network area. All the traffic generated outside the specific range is not considered. Nevertheless, for configuring the mobility option in the network nodes, a widely used mobility model called random waypoint mobility is used [30]. The random waypoint model permits the nodes in the network to keep moving in random directions until they reach any random destination defined by its algorithm.



Type: Utilities

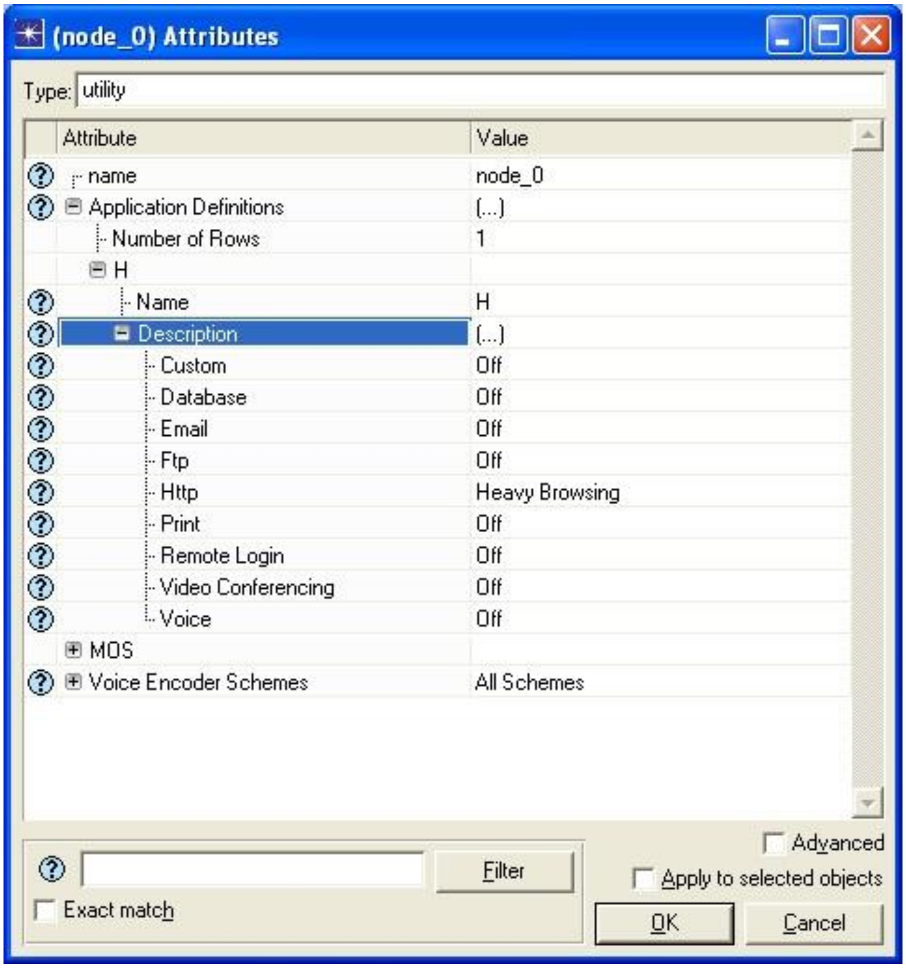
Attribute	Value
name	Mobility Config
Mobility Modeling Status	Enabled
⊟ Random Mobility Profiles	(...)
Number of Rows	1
⊟ Default Random Waypoint	
Profile Name	Default Random Waypoint
Mobility Model	Random Waypoint
⊟ Random Waypoint Parameters	(...)
Mobility Domain Name	Not Used
x_min (meters)	0.0
y_min (meters)	0.0
x_max (meters)	500
y_max (meters)	500
Speed (meters/seconds)	constant (10)
Pause Time (seconds)	constant (50)
Start Time (seconds)	uniform (0, 10)
Stop Time (seconds)	End of Simulation
Animation Update Frequency (se...	1.0
Record Trajectory	Disabled

Figure 5.3: Mobility Configuration Parameter

As the nodes reach to the random destination, they stop for a specific period of time that is called the pause time. After the pause time expires, a new movement is created again with a random destination. To analyze the effect of node mobility on the network performance, different node speeds are used as 10 m/s, variable in the range of 10-20 m/s and 30 m/s with a pause time of 50 seconds.

5.3.2 Application Configuration

Application configuration is the most important object in OPNET software that defines the type of transmitted data, the size of the data or file, and the type of the traffic load.



(node_0) Attributes

Type: utility

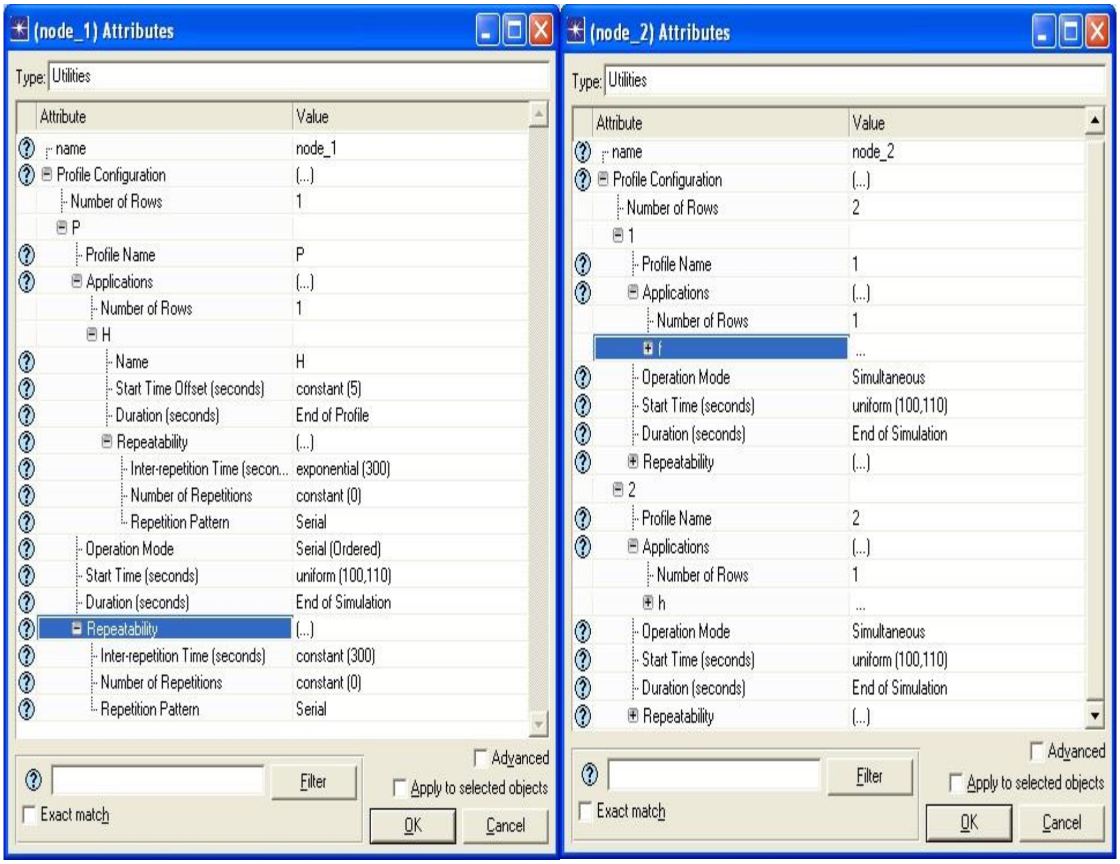
Attribute	Value
name	node_0
⊟ Application Definitions	(...)
Number of Rows	1
⊟ H	
Name	H
⊟ Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	Off
Http	Heavy Browsing
Print	Off
Remote Login	Off
Video Conferencing	Off
Voice	Off
⊞ MOS	
⊞ Voice Encoder Schemes	All Schemes

Figure 5.4: Application Configuration Parameter

It supports many common applications, like FTP, voice, HTTP, e-mail, and database. HTTP application is chosen for the data traffic analysis for the routing protocols, and FTP and HTTP applications together are chosen for the data traffic analysis of the TCP variants scenarios, as shown in Figure 5.4 with three type of traffic as heavy, medium and low load for the requirement of bandwidth utilization.

5.3.3 Profile Configuration

Profile configuration determines from where the data of file has been received by determining the relationships between the clients and the server. It creates a user profile that is employed in the network nodes to generate the application traffic.



(node_1) Attributes

Type: Utilities

Attribute	Value
name	node_1
Profile Configuration	(...)
Number of Rows	1
P	
Profile Name	P
Applications	(...)
Number of Rows	1
H	
Name	H
Start Time Offset (seconds)	constant (5)
Duration (seconds)	End of Profile
Repeatability	(...)
Inter-repetition Time (secon...	exponential (300)
Number of Repetitions	constant (0)
Repetition Pattern	Serial
Operation Mode	Serial (Ordered)
Start Time (seconds)	uniform (100,110)
Duration (seconds)	End of Simulation
Repeatability	(...)
Inter-repetition Time (seconds)	constant (300)
Number of Repetitions	constant (0)
Repetition Pattern	Serial

(node_2) Attributes

Type: Utilities

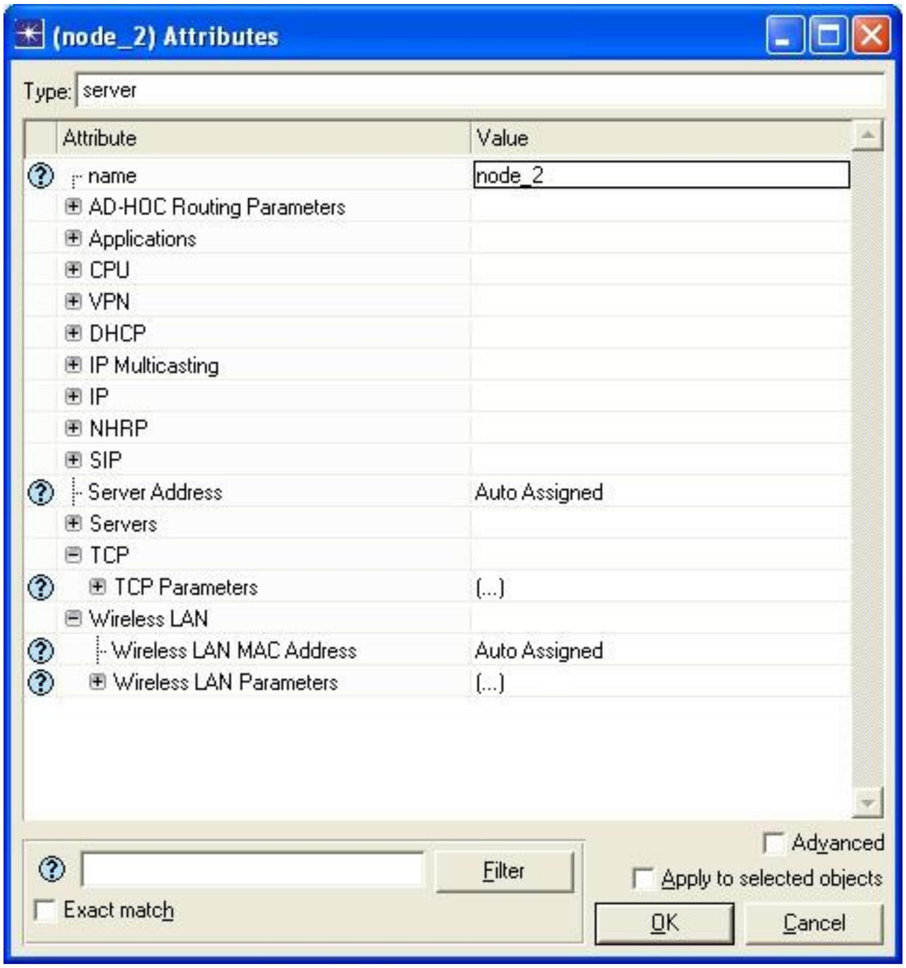
Attribute	Value
name	node_2
Profile Configuration	(...)
Number of Rows	2
1	
Profile Name	1
Applications	(...)
Number of Rows	1
f	...
Operation Mode	Simultaneous
Start Time (seconds)	uniform (100,110)
Duration (seconds)	End of Simulation
Repeatability	(...)
2	
Profile Name	2
Applications	(...)
Number of Rows	1
h	...
Operation Mode	Simultaneous
Start Time (seconds)	uniform (100,110)
Duration (seconds)	End of Simulation
Repeatability	(...)

Figure 5.5: HTTP and FTP Profile Configuration Parameter

Figure 5.5 shows the application configuration objects profile that created for the routing protocol and TCP variants in the profile configuration object to support HTTP and FTP traffic.

5.3.4 Server Node

Server node is configured to control and support the application services, as shown in Figure 5.6 such as HTTP application that depends on the user profile. This node is basically a WLAN server that specifies what type of routing protocol and TCP variant can be selected.



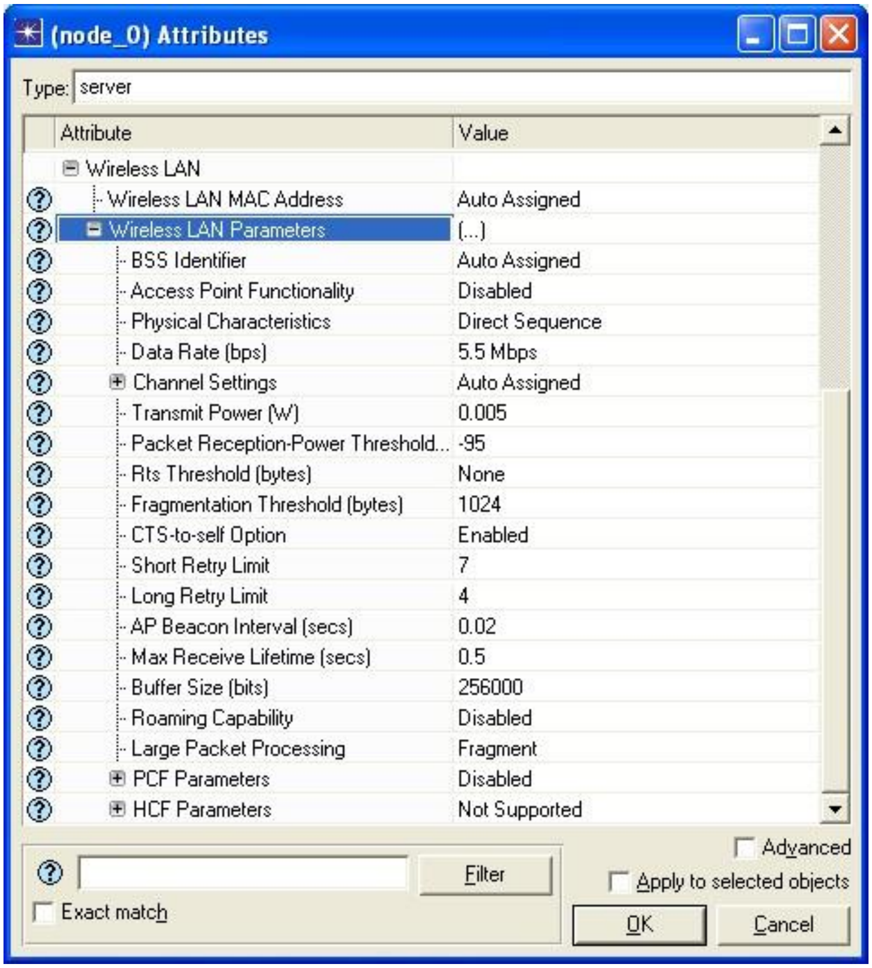
Type: server

Attribute	Value
name	node_2
⊞ AD-HOC Routing Parameters	
⊞ Applications	
⊞ CPU	
⊞ VPN	
⊞ DHCP	
⊞ IP Multicasting	
⊞ IP	
⊞ NHRP	
⊞ SIP	
Server Address	Auto Assigned
⊞ Servers	
⊟ TCP	
⊞ TCP Parameters	(...)
⊟ Wireless LAN	
Wireless LAN MAC Address	Auto Assigned
⊞ Wireless LAN Parameters	(...)

Figure 5.6: Server Node Configuration Parameter

5.3.5 Workstation Nodes

Workstation nodes are configured with the client server application, as shown in Figure 5.7 that runs over TCP/IP. It supports the underlying WLAN connection at many data rates. The data rate for all nodes is set to 5.5 megabits per second (Mbps) for all the simulations.



Type: server

Attribute	Value
⊟ Wireless LAN	
Wireless LAN MAC Address	Auto Assigned
⊟ Wireless LAN Parameters	(...)
BSS Identifier	Auto Assigned
Access Point Functionality	Disabled
Physical Characteristics	Direct Sequence
Data Rate (bps)	5.5 Mbps
⊞ Channel Settings	Auto Assigned
Transmit Power (W)	0.005
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	1024
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000
Roaming Capability	Disabled
Large Packet Processing	Fragment
⊞ PCF Parameters	Disabled
⊞ HCF Parameters	Not Supported

Figure 5.7: Workstation Nodes Configuration Parameter

The design attributes and their values are presented in a tabular format, which are configured through the execution of the proposed network model. All these tables are provided in Appendix. Finally, all the scenarios are described under three categories as shown in Table 5.1.

Table 5.1: Description of the Experimental Categories [12]

Simulation Investigations	
Category Types	**Description**
Scenario 1 (Scalability)	Scenario 1 is configured to analyze the scalability. A 1,000×1,000 m^2 network that has different number of nodes as 20, 40, 60, 80 and 100 with a fixed WLAN server running low HTTP application for routing protocols and HTTP together with FTP for TCP variants is set up. The page inter-arrival time is selected as exponential 720 seconds. The object size is set to 500 bytes that includes 5 small images. The speed of nodes is used as 10 m/s with a pause time of 50 seconds. Four types of MANET routing protocols and three TCP variants are employed in the network and their performances are evaluated for the different-sized networks based on the analysis of the performance metrics.
Scenario 2 (Mobility)	Scenario 2 analyzes the mobility. It presents a medium-sized network with a node size of 60. The speed of nodes is set as 10 m/s, 10-20 m/s and 30 m/s. All other configurations remain the same as explained in Scenario 1. The purpose of scenario is to observe the performance of the routing protocols and TCP variants under different node speeds.
Scenario 3 (Traffic Size)	Scenario 3 analyzes different traffic sizes. A medium-sized network with 60 nodes that have speed of 10 m/s is set up. The same configuration settings are used as explained in Scenario 1 except for the traffic size. Three different traffic sizes such as HTTP low traffic (page inter-arrival time of 720 s, object size of 500 bytes and 5 small images), medium traffic (page inter-arrival time of 270 s, object size of 800 bytes, 5 medium images) and heavy traffic (page inter-arrival time of 60 s, object size of 1,000 bytes and 5 medium images) for routing protocols scenario and HTTP together with FTP low, medium and high for the TCP variants scenario. The purpose of this scenario is to monitor the change in the performance of the routing protocols and TCP variants and under different traffic size.

Chapter 6

SIMULATION RESULTS AND ANALYSIS

This chapter presents the experimental results for three different MANET scenarios as explained in chapter 5. The first part of the chapter discusses the performance analysis of the routing protocols under different MANET environments. The second part of the chapter presents the analysis of the TCP variants.

6.1 Simulation Results of Routing Protocols

This subsection analyzes the performances of the AODV, DSR, OLSR and GRP routing protocols under different MANET environments. In this section, the end-to-end delay and the average throughput of the network under different conditions are analyzed by simulating the model for a duration of 10 minutes. The start time of application and profile generation is set to 5 s and 100 s, respectively. This can be observed from the results as there is no transmitted application traffic up to 105 s of the simulation time. The no traffic period is often known as the warm up time. A warm up period permits the queues and other aspects in the simulation to enter the conditions which are typical of normal running conditions in the system [23]. However, for OLSR and GRP protocols it can be observed that the graph lines start before the warm up period finishes since OLSR and GRP protocols need to transmit the control messages in the network for making the routes available before the data transmission starts during the warm up period. For achieving the most accurate OPNET results, the simulations are repeated ten times for each scenario in all categories for the routing protocols performance, with different constant seeds of the pseudo random number generator (PRNG) [32]. The x-axis represents the simulation time in seconds while the y-axis represent the delay in seconds or the throughput in bps in the presented simulation results.

6.1.1 Impact of Scalability on MANET Routing Protocols

Five simulation environments for the node size of 20, 40, 60, 80 and 100 over low HTTP traffic are developed for the four MANET protocols. The speed of nodes is set to 10 m/s with 50 s of pause time, and 0 s as the start time.

As it can be notice from Figure 6.1, the OLSR and GRP have lower end-to-end average delay on average, while the end-to-end average delay for the DSR is the highest among all the routing algorithms. When the simulation time increases, the results of all protocols enter into a steady state and remain there till the end of the simulation time. In the large size network case (80 – 100 nodes), the end-to-end average delay for OLSR and AODV initially rises dramatically, unlike the delays of GRP and DSR which decrease, and then become flat almost at 120 s and 220 s of the simulation time, respectively.

By analyzing the end-to-end average packet delay with respect to different network size given in Figure 6.2, it is shown that the OLSR and GRP protocols set up quick connections between network nodes without creating major delays. Unlike the other routing protocols, the OLSR and GRP protocols do not need much time in a route

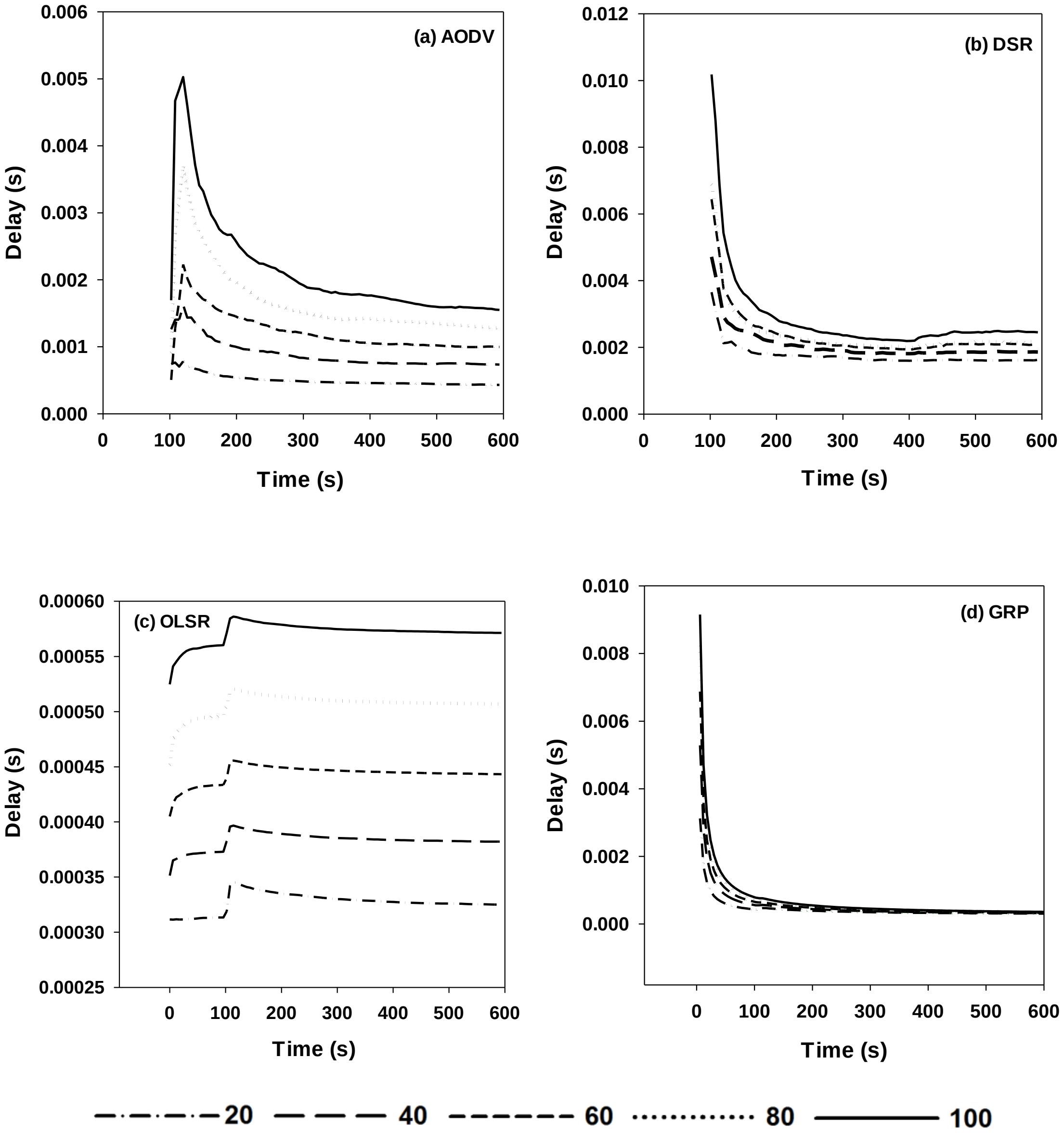


Figure 6.1: Average End-to-End Delay with Varying Node Size for (a) AODV, (b) DSR, (c) OLSR and (d) GRP

discovery mechanism, because the routes are available in advance, resulting lesser end-to-end packet delay when the data information packet exchange is needed. Mainly this advantage in OLSR protocol is due to the utilizing of the MPR nodes, to permit the control messages to be forwarded to other nodes.

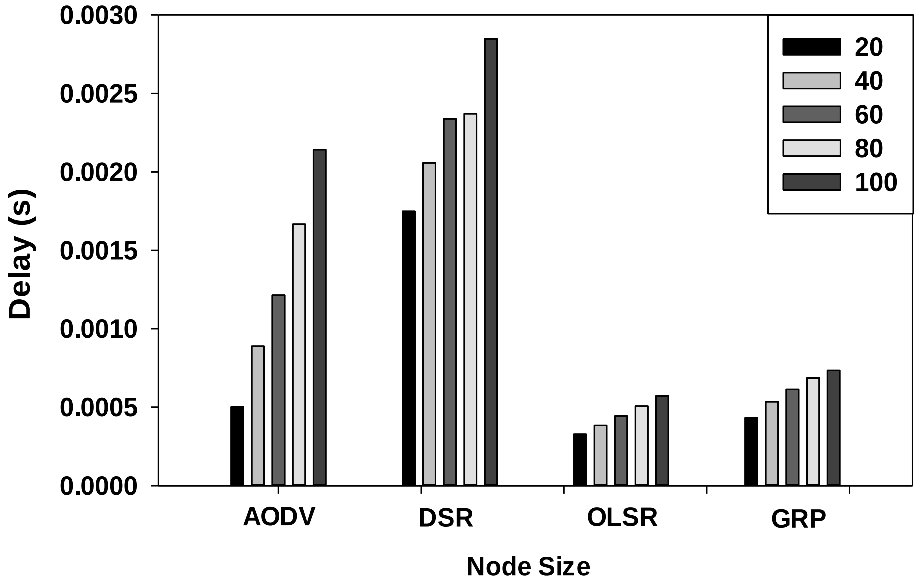


Figure 6.2: Routing Protocols Performance in terms of End-to-End Delay with Varying Node Size

Eventually this helps to minimize the overhead and maximize the throughput of the network. While the information in GRP is gathered rapidly at a source node without spending a large amount of overheads, the source node still has to wait until a route to the destination node can be discovered, increasing the response time. On the other hand, both AODV and DSR protocols cannot set up the node connection quickly and create larger delays in the network. Due to the reactive approach nature of the DSR protocol, it is highly possible that the data packets wait in the buffers, till it discovers a route on its way to the receiver/destination node. In time a RREQ packet is transmitted for the purpose of route discovery, the destination node replies back to all nodes for the same route request packet that it receives. Therefore, DSR protocol needs large time to determine the lowest congested route. The DSR also follows a source routing mechanism where the information of the complete route is included in the header of the data packet, causing an increase in the length of the data packet, and resulting also an increase in the delay experienced by the network data packets. Thus, it can be concluded that when the network is denser, the experienced end-to-end average delays will be probably higher within the network while utilizing the DSR protocol.

The average throughputs of the routing protocols are analyzed as the second metric in Figure 6.3. As explained before, throughput indicates the total data packet successfully received by any receiver/destination node. The efficiency of the route can be predicted by monitoring the overall throughput received by the network nodes. The figure shows the average throughput of the protocols for different network sizes when low HTTP traffic is transmitted. It is clear from the results that the OLSR protocol performs better compared to the other three routing protocols, receiving the highest throughput.

Considering the AODV and the DSR as reactive protocols, the AODV offers better performance. The data packets received for AODV is found to be higher than DSR. The performance of DSR tends to fall after some seconds, whereas AODV is found to be more stable at the same time. As the size of the network is increased, the overall throughput increases since more nodes are available to route the data packets to the destination nodes. It is obvious that the OLSR protocol keeps overtaking other three routing protocols by achieving the highest throughput. In a large network (80 – 100 nodes), OLSR protocol continues to be dominating over AODV, DSR and GRP. The higher performance achieved by the OLSR protocol is due to the proactive characteristics approached by this protocol. The OLSR protocol constantly sets up,

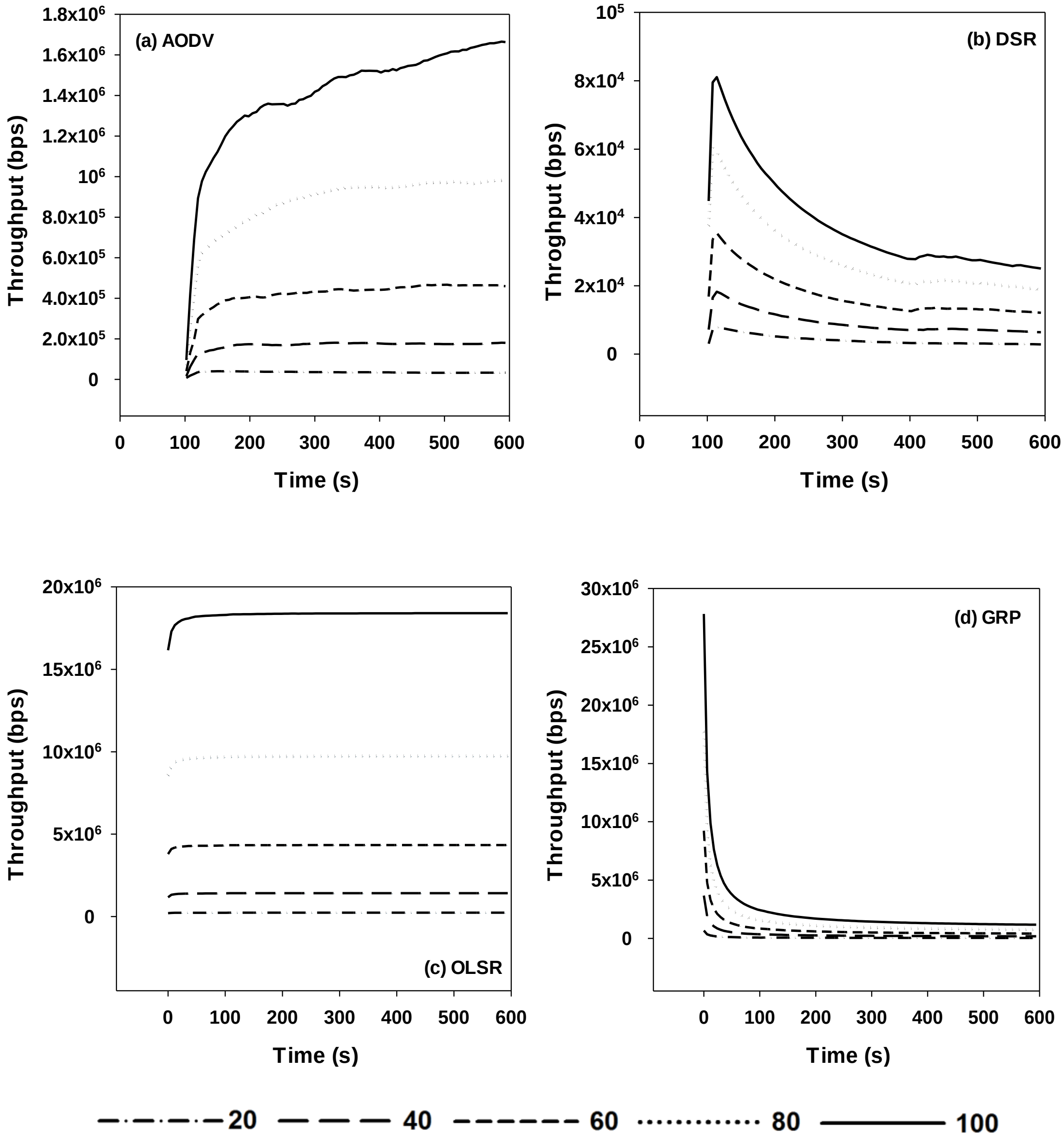


Figure 6.3: Average Throughput with Varying Node Size for (a) AODV, (b) DSR (c) OLSR and (d) GRP

maintains and updates the routing information with the assist of MPR in the network, which leads to the reduction of routing overhead in the network [33]. The larger the network size is, the higher the throughput that can be achieved, as compared to the algorithms of the AODV, DSR and GRP routing protocols. In case of large network size, the amount of the OLSR protocol Hello messages becomes larger, due to a neighbor lists included in the messages. So, if the interval of the Hello message would have been increased in the network, the OLSR protocol could have been improved its performance even than the current one. On the other hand, increasing Hello interval event decreases the periodic broadcast of the Hello messages, thus resulting in less congestion in MANET. Likewise, GRP and AODV protocols are also desirable when the network aims for achieving higher throughputs, despite of the scalability of the network. The GRP source node predefines better routes depending on the gathered data. Therefore it always sends the data packets even if the current routes are disjointed. AODV protocol also follows a routing mechanism known as hop by hop and removes the overhead of the sender/source routing within the network [34]. Related to above, the availability of multiple route information in the AODV assists in producing the higher amount of throughput in the network. For the DSR protocol, it receives a minimum amount of throughput even with the performance tends to be improved in case of denser network. Since the DSR protocol follows a source routing mechanism, the byte overhead in each packet extremely affects the total byte overhead when the network size increases. Therefore, the DSR protocol tends to achieve lower amount of data packets in more stressful network. Figure 6.4 shows the scalability impact on the four routing protocols from another perspective. Since the throughput result of the DSR case is very low as compared to the other protocols it is shown on the same figure by using a different scaling.

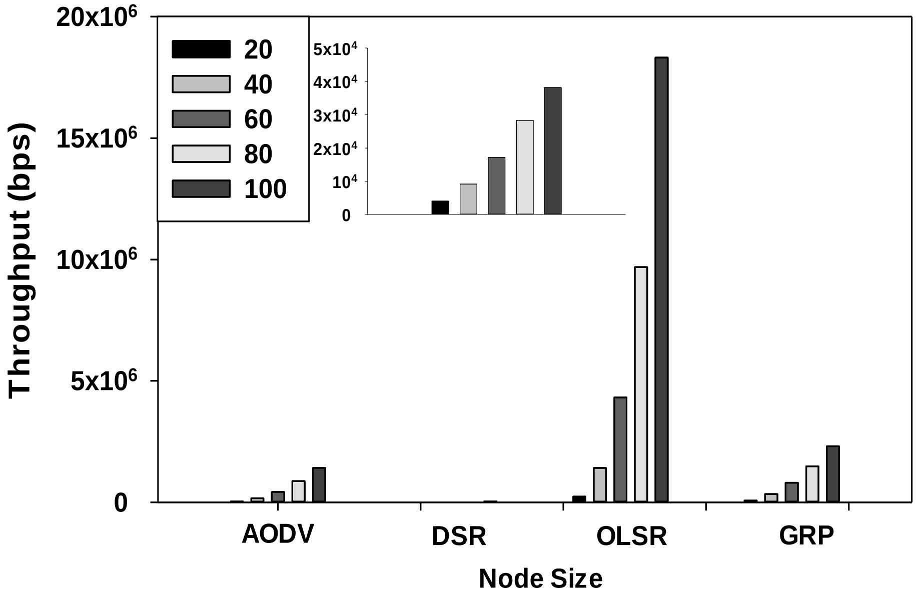


Figure 6.4: Performance of Routing Protocols in term of Throughput with Varying Node Size

6.1.2 Impact of Node Mobility on MANET Routing Protocols

This scenario discusses the effect of node speed on the performance of the routing protocols. The scenario considered in this analysis consists of 60 nodes moving with constant speeds of 10 m/s and 30 m/s and a variable speed changing between 10 m/s and 20 m/s (10-20 m/s). The pause time and start time are set to 50 s and 0 s, respectively.

The Figure 6.5 shows the end-to-end average delay with varying node speeds where the OLSR protocol preserves the lowest delay. It is also noticed that the amount of delay for all protocols increases slightly as the speed of nodes increases.

Due to its reactive approach, the AODV protocol does not maintain the unused routes

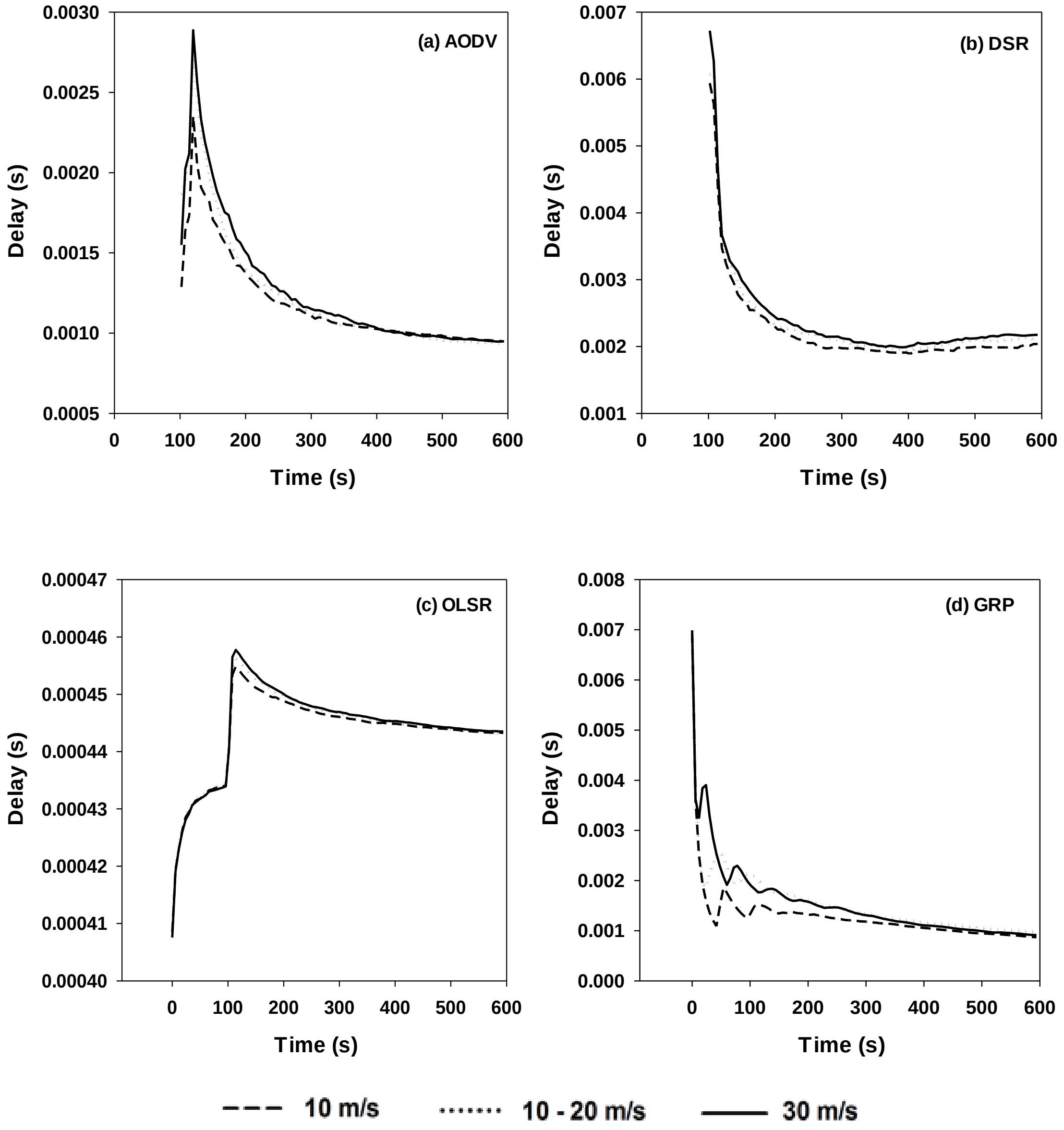


Figure 6.5: Average End-to-End Delay with Varying Node Speeds for (a) AODV, (b) DSR (c) OLSR and (d) GRP

to the destination nodes in the network, by utilizes its on-demand routing strategy. As an alternative, the AODV starts to search for new routes when they become needed. The purpose for this strategy is usually to generate less control traffic. Therefore it raises the networks total end-to-end delay, as the ready to send packets kept in buffers waiting until they are transmitted cross the new chosen routes. The routing protocol

AODV also preserves only one route to the destination in its routing table. Consequently, anytime a route break-down occurs between the nodes in the network (due to high mobility); an additional route discovery mechanism is required each time to establish the new route [34]. This implies that the number of route discovery mechanism is directly related to the number of link failures in the AODV, and when the route discovery mechanism is generated. As a result of node mobility, it takes some time in each occasion, and so more delays are likely to be brought to the network. Similar to the AODV protocol, the DSR protocol does not activate the route discovery mechanism frequently, because of the existence of the abundant route caches in each node. Therefore, a route discovery mechanism is not started unless all cached routes are fragmented. Nevertheless, for these caches it has a high probability to become stale in high mobility network scenario. The interference to the data traffic is also increased in the DSR network as a result to the generation of a high MAC overhead, which happens during the route discovery mechanism [35]. This MAC overhead and the cache staleness cause the network significant performance degradation. Contrast to the AODV and DSR, the OLSR protocol does not obviously show its reaction to link breakage or failure, since it is subset of one of the link state protocols and the associated MPR nodes periodically transmit the information of the topology to different nodes within the network. Therefore, it displays the lowest end-to-end average delay comparing to the other three routing protocols.

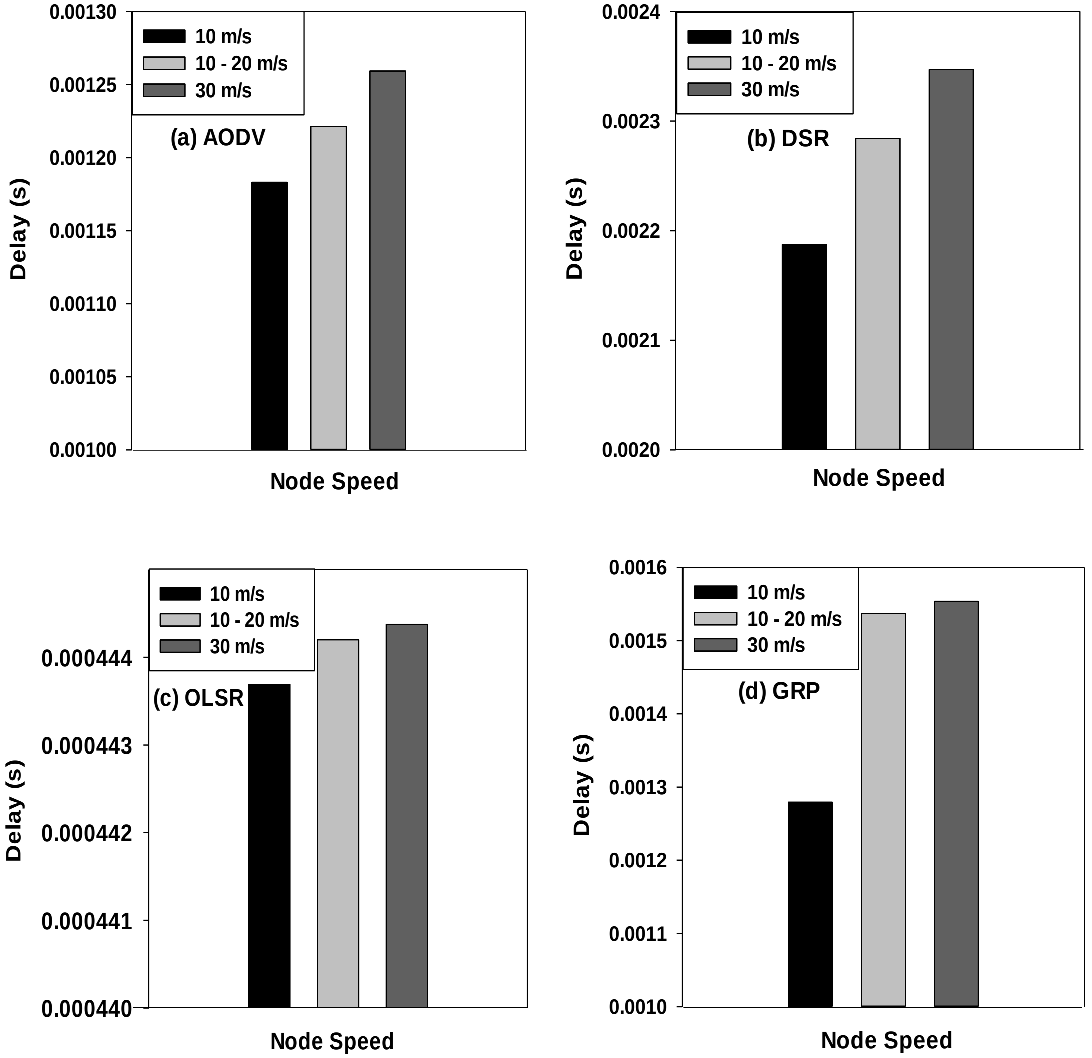


Figure 6.6: Performance of Routing Protocols in terms of End-to-End Average Delay with Varying Node Speed for (a) AODV, (b) DSR (c) OLSR and (d) GRP

Figure 6.6 presents the routing protocols mobility impact as a summary. GRP protocol also shows small reaction to the link breakage or failure, because it depends on the node position information for deciding the best route. When the nodes speed increases in the network, it broadcasts its new location to the source node. Hence, by increasing the nodes speed, the local topology information gets old. Therefore GRP intelligently

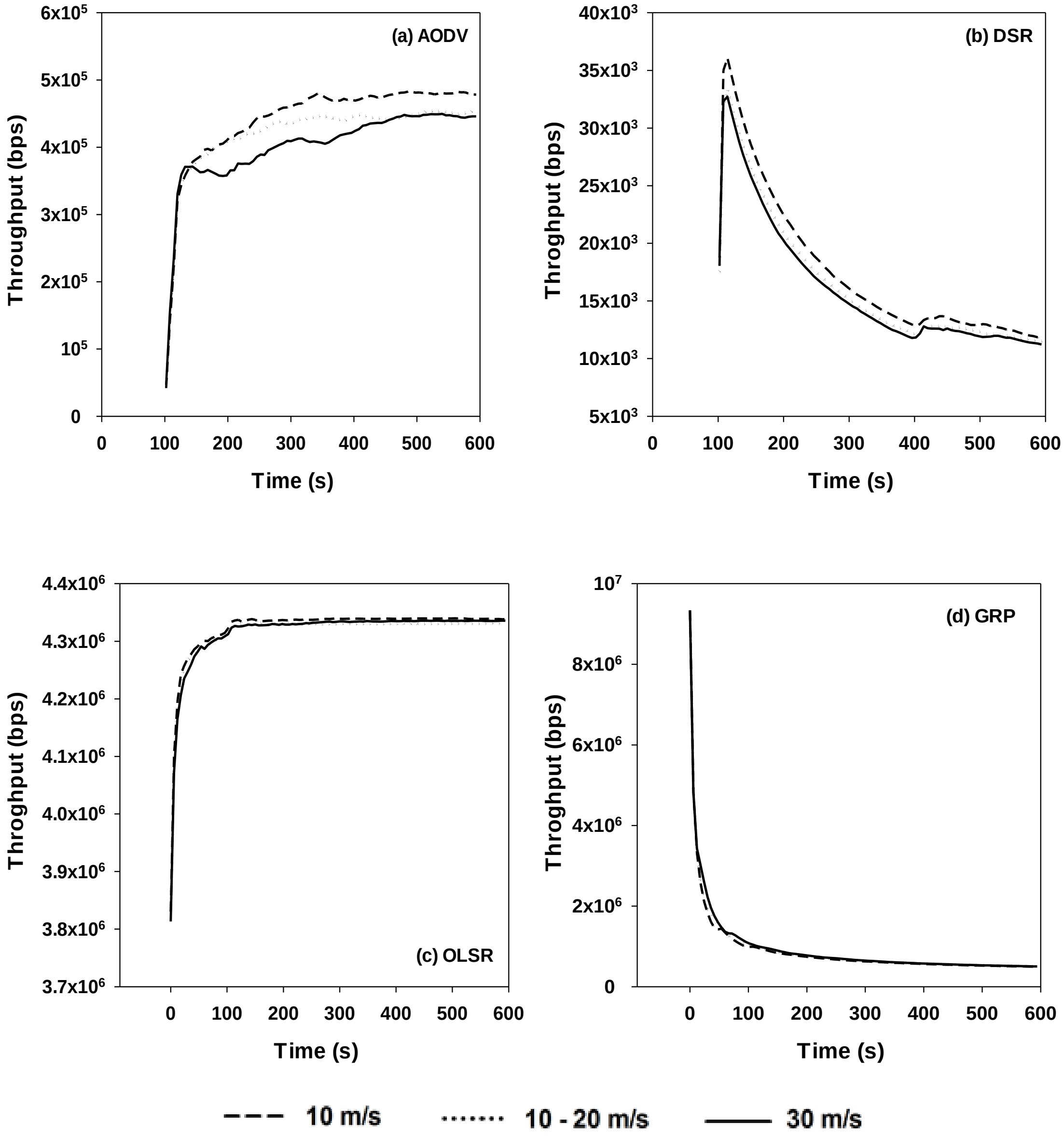


Figure 6.7: Average Throughput with Varying Node Speeds for (a) AODV, (b) DSR (c) OLSR and (d) GRP

generates necessary control messages for tracking the nodes position, causing a higher delay than OLSR protocol.

The Figure 6.7 presents a comparative analysis on the throughput, derived from different mobility scenarios. As noticed from the figure, the throughput decreases slightly for AODV and DSR protocols when the node speed increases to 10-20 m/s and 30 m/s.

When the node speed increases and moves over a specified point, it transmits a flooding packet with its new position. Therefore, when the network topology changes it forces the GRP nodes to send the flooding packets more frequently. Figure 6.7 presents that the throughput of the OLSR protocol is the highest for all mobility speeds compared to other protocols. The OLSR protocol successfully maintains a consistent throughput, even with higher mobility rates in the network, and it keeps its performance at a steady level. In case of increased mobility rates, many frequent changes of the node positions and their neighbor positions occur successively leading frequent changes in the link state, and as well packet losses. With low mobility rate, however, the performance of the AODV protocol is found to be slightly enhanced as the topology of the network remains almost constant for a low speed network. Throughput of AODV protocol is lower than the throughputs of OLSR and GRP protocols at all node speeds since the routing tables are more regularly updated in response to the changes of the topology in the network, causing a fewer packet drops and less performance degradation. Likewise, the DSR protocol stored route cache can effectively be used with a lower node speed in the network. Nevertheless, in a high mobility rate presence, the DSR protocol performs the worse because of its dependency on the cache routes, which are more likely to become stale at higher node speeds. The OLSR protocol outperforms the other three routing protocols due to its ability to preserve the constant information of the network topology. It can be shown that even with a high mobility scenario, the throughput of

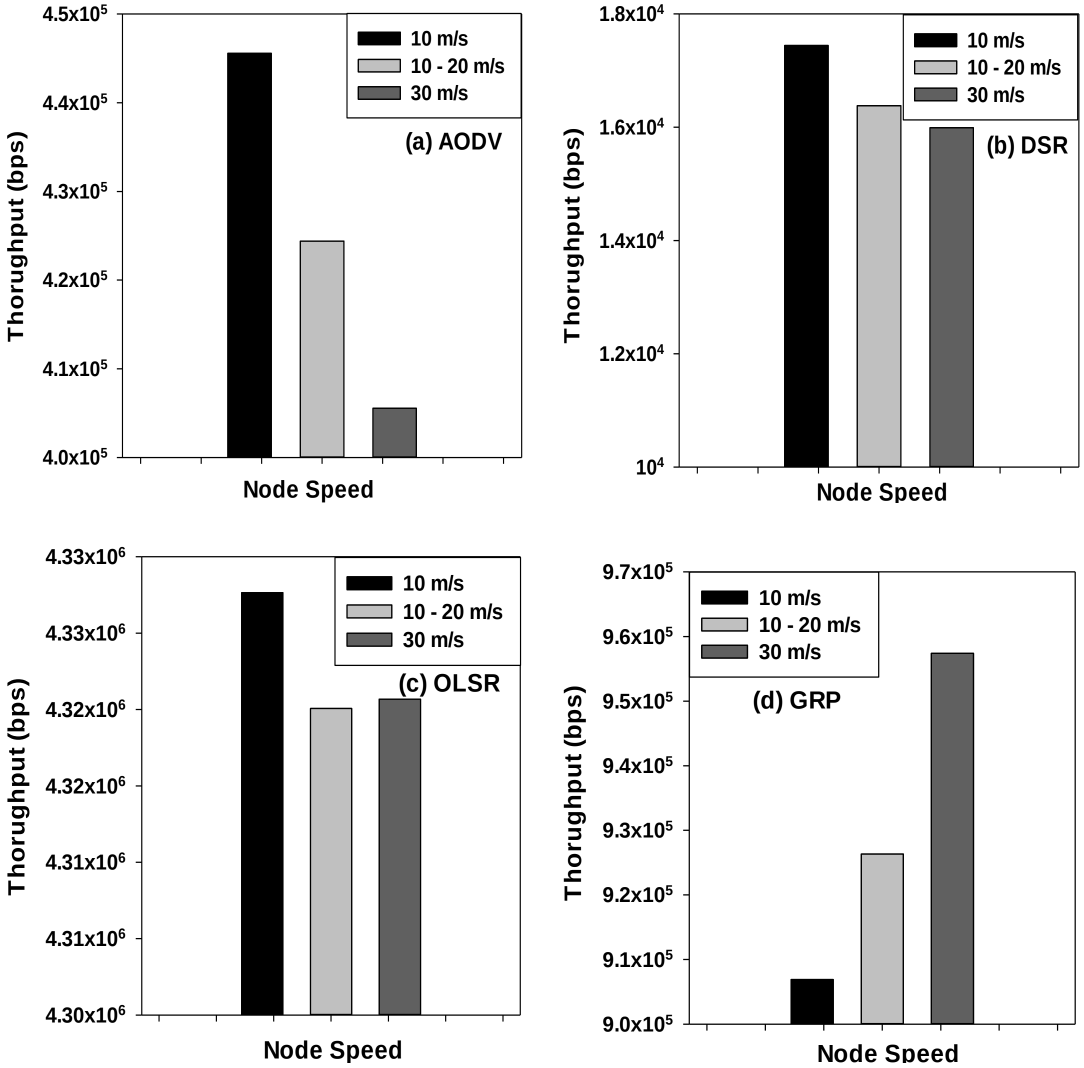


Figure 6.8: Performance of Routing Protocols in terms of Throughput with Varying Node Speed for (a) AODV, (b) DSR (c) OLSR and (d) GRP

OLSR protocol does not decrease significantly. The superiority of the OLSR protocol comes from its ability of instantly detecting the route failure and executing continuous searches for all the routes to all potential destinations. Thus the routing information is updated very quickly. In this case, the number of dropped packets is likely very low, resulting in more data packets are successfully received in the network. Figure 6.8 summaries the mobility impact on the three routing protocols.

6.1.3 Impact of Network Load on MANET Routing Protocols

For this section the results of the simulations discusses the AODV, DSR, OLSR and GRP routing protocols performance with respect to different traffic load in the network. In this part, the model environment contains three separate scenarios including HTTP profile with heavy (object size 1,000 bytes, 5 images with a size of 500 – 2,000 bytes each, and page inter-arrival time 60 s), medium (object size 750 bytes, 3 images with a size of 500 – 2,000 bytes each, and page inter-arrival time 270 s) and low load (object size 500 bytes, 5 images with a size of 10 – 400 bytes each, and page inter-arrival time 360 s) traffic for a network consisting of 60 nodes with mobility rate of 10 m/s. The start time and pause time are set as 0 s and 50 s respectively.

In heavy HTTP traffic load as shown in Figure 6.9 the end-to-end average delay of AODV increases until it reaches its maximum delay limit and stays there till the end of the simulation. Similar to the AODV protocol, the DSR illustrates higher end-to-end average delay when exposed to HTTP heavy traffic. In the beginning of the simulation, the initial DSR delay for heavy, medium and low traffic load is pretty high. The reason for the high delay is because of the needs of the reactive approach to discover the appropriate data packets transmission routes, and in the time that the data packets have been received for transmission. Initially it leads to a high end-to-end average delay and then it starts to gradually reduce reaching to a steady level. The simulation results show that the DSR protocol demonstrates higher end-to-end average delay in heavy, medium and low load traffic compared to other three protocols. On the other hand, the figure shows that when the OLSR exposed to heavy, medium and low traffic, the protocol presents low difference in the end-to-end average delay. The reason for the low delay of

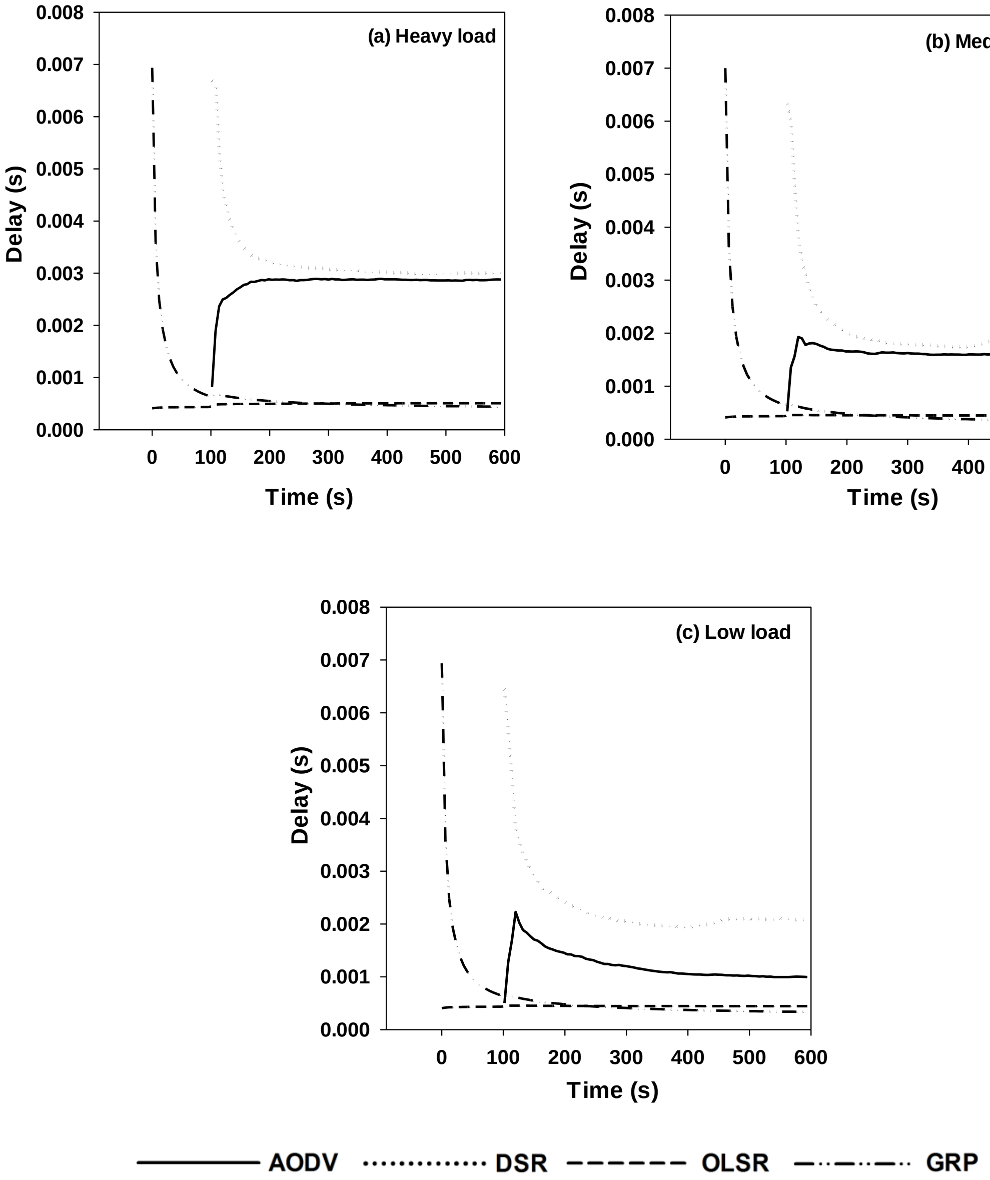


Figure 6.9: Average End-to-End Delay with Varying Node Load for (a) Heavy Load, (b) Medium Load, (c) Low Load

the OLSR protocol is due to is proactive nature. It does not need much time in a route discovery mechanism, as mentioned before, due to the availability of the routes in advance, and also due to the utilizing of the MPR nodes to permit the control messages to be forwarded to other nodes, which also help to minimize the delay.

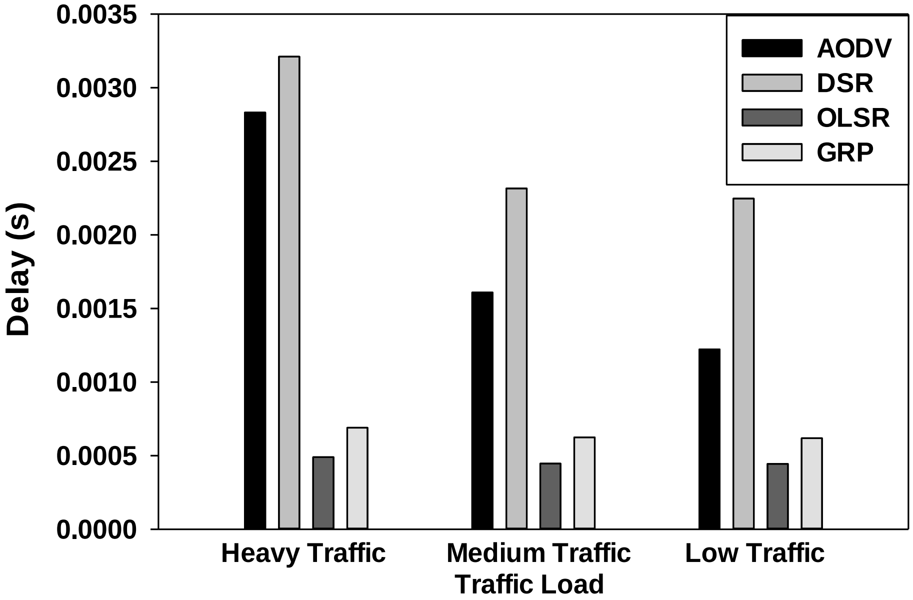


Figure 6.10: Performance of Routing Protocols in terms of End-to-End Average Delay with Varying Traffic Load

Meanwhile, the GRP protocol collects the network information and decides the best routes at the source node. Therefore, it does not expose on delay performance for the three traffic types. Figure 6.10 presents a summary about the network traffic impact on delay for the four routing protocols.

The results in Figure 6.11 discuss the average throughput of the routing protocols under the same three (heavy, medium and low) traffic loads. The simulation results illustrate that the OLSR protocol shows high throughput performance in case of HTTP heavy, medium and low load traffics.

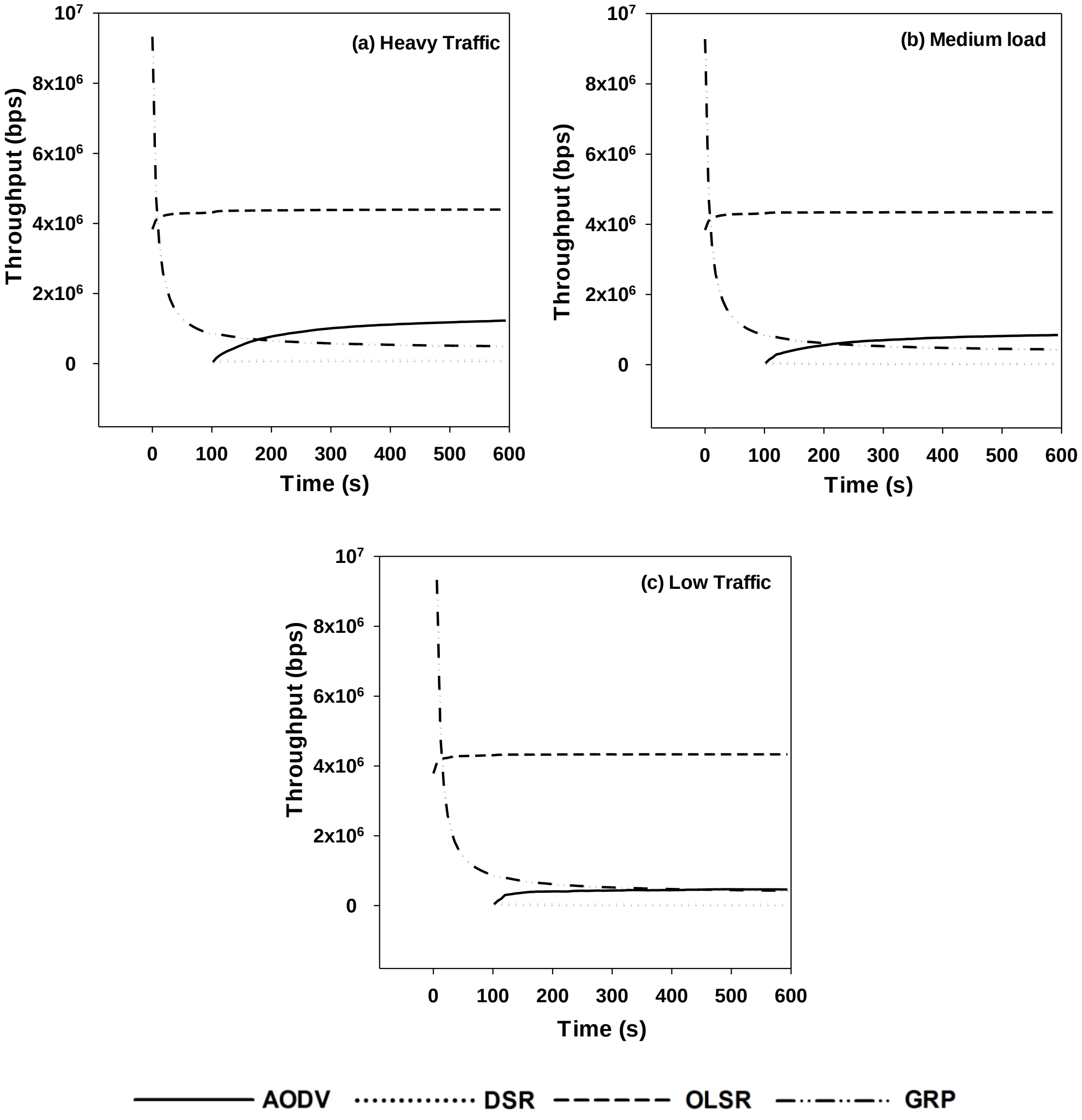


Figure 6.11: Average Throughputs with Varying Node Load for (a) Heavy Load, (b) Medium Load, (c) Low Load

The results also show that the DSR protocol has the lowest throughput, compared to the other three protocols under heavy, medium and low load traffic. It can be noticed from the figure that the throughput of OLSR protocol under HTTP heavy, medium and low load is almost the same which is quite higher than other three MANET routing protocol. The OLSR high performance can be resulted as mentioned to the proactive approached

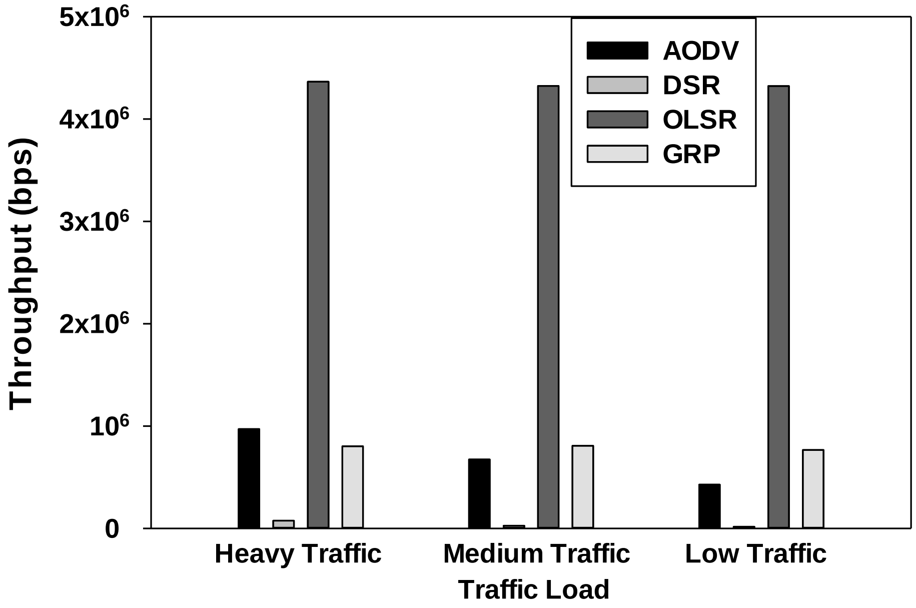


Figure 6.12: Performance of Routing Protocols in terms of Throughput with Varying Traffic Load

which frequently sets up and maintains routing information updates with MPR help, and the mobility factor causes the OLSR to receive more data from other nodes. The results also show that when the number of packets increases for the high traffic, the AODV demonstrates better performance than GRP, because AODV protocol choses lesser number of hops per route, resulting lower dropped data packets. However, GRP maintains its throughput in the three traffic types, due to its proactive approach. Figure 6.12 compares the network traffic impact on throughput of the four routing protocols from another perspective.

6.2 Simulation Results of TCP Variants

This subsection analyzes the results of the three standard TCP variants namely TCP Reno, New Reno and SACK, under different MANET environments. The analysis present the performance of TCP variants measured by two metrics, page response time and retransmission attempts. The effectiveness and efficiency of the time that takes the web page to load is evaluated by a page response time. Hence, in data traffic measurements this parameter plays an important role, where the lower the value is achieved, the faster the task is completed. The quantitative parameter that is known as the retransmission attempt, determines the retransmission attempt rate, and discovers the number of packet drops per second, which is needed to be retransmitted. Hence, the retransmission attempt is lower; the more reliable the TCP variant is. Two type of applications (HTTP, FTP) are used together to increase the load in the network. The routing protocol is selected to be the DSR protocol because of its frequent interacting with TCP than other protocols in MANET environment as presented in [35]. Also for achieving the most accurate result in OPNET, five duplications are run for each scenario in all categories for the TCP scenarios, with different constant seeds of the PRNG [32]. In the simulation results, the x-axis presents the node size and the y-axis presents the page response time or the retransmission attempts.

6.2.1 Impact of Scalability on TCP Variants

This section analyzes three different node sizes (30, 60, and 100 nodes) with node speed of 10 m/s and two type of heavy traffic applications (HTTP and FTP). When the number of nodes is increased in the network, the network experiences an extra high load for the page response time, and therefore the performance of the TCP is expected to be affected.

In Figure 6.13, the page response time is demonstrated for the TCP variants. The page response time increases as extra nodes are added in the network. In a small network (30

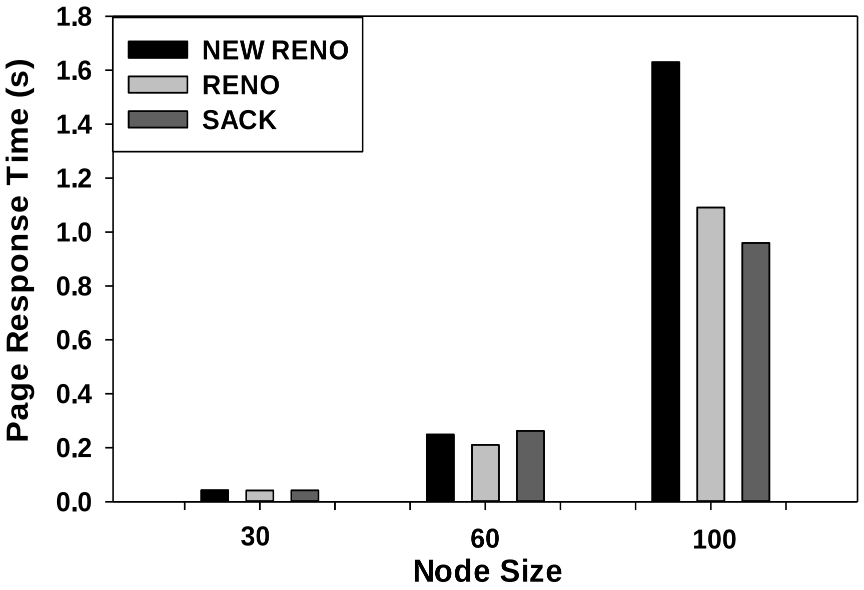


Figure 6.13: Average Page Response Time of TCP Variants with Varying Node Size

nodes), and medium network (60 nodes) all TCP variants has almost the same page response time. On the other hand, SACK and Reno overtakes the New Reno in a large network (100 nodes). In case of large networks, when more links are established, the network becomes more disposed as a result to multipath fading and signal attenuation. This situation forces the TCP to unnecessarily invoke the counterproductive and consume the time of congestion control mechanisms. This leads to performance instabilities and degradations for TCP variants. Thus extra time is needed to finish the data recovery activities, meaning more time is spent to load a web page in the existence of high number of nodes in a network. The results show that both TCP Reno and SACK achieve a shorter page response time compared to TCP New Reno especially at 100 nodes. When congestion and signal attenuation happen in the network due to the heavy load, both TCP Reno and SACK preserve a larger congestion window size and the

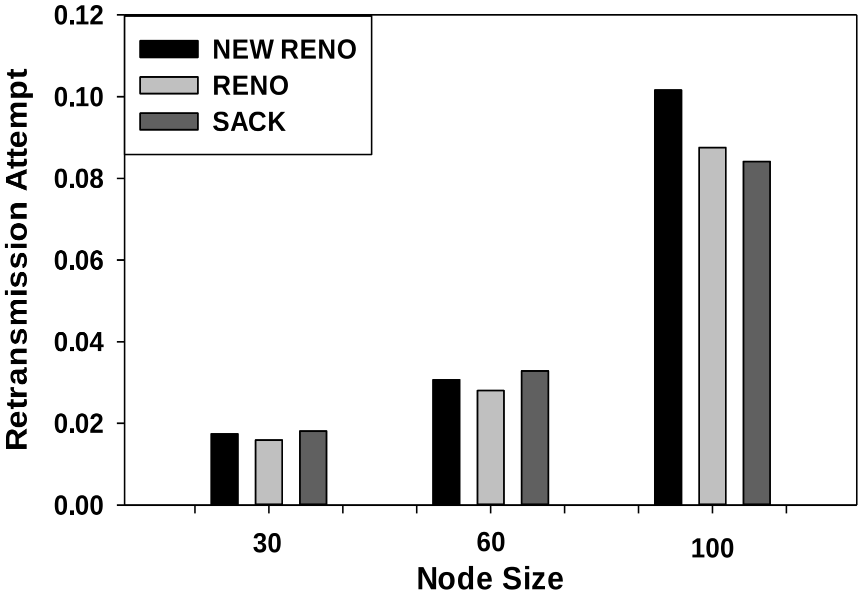


Figure 6.14: Retransmission Attempts of TCP Variants with Varying Node Size

larger the congestion window size is the shorter the web page response time is for a TCP [20].

In the Figure 6.14, the highest packet drops are noticed for the large network size (100 nodes) where TCP New Reno makes the highest retransmission tries, followed by TCP Reno and SACK. When the network size decreases to small size (30 nodes) and medium size (60 nodes), TCP Reno has slightly lower retransmission attempts compared to the other two TCP variants.

In case of wired connection, the TCP retransmissions are triggered frequently because of the network congestions. As compared to the wired medium, the wireless medium provides much extra noisy physical links for the transmissions of the data. Signals spread through wireless links can experience from interference, degradation, and noise

[19]. Hence more data packet is lost that leads to more retransmissions. When the number of nodes is increased, the number of retransmission attempts is also increased for the three windows based congestion control protocols. This is because of disconnection of the physical layer when the receive signals are not connected or linked to a transmitting network signal source, also the increase in the packet error rates in big size network, and the increase of the channel contention as more routing loads are experienced. In larger networks when the network becomes denser, the window mechanisms aggressive employment is counted as one of the primary factors responsible for more retransmission in TCP New Reno. Through the slow start phase, the aggressive and unsuitable window growth of TCP New Reno causes the network to be overloaded, which encourages repeated packet losses on the link layer and extra frequent timeouts in the transport layer. Therefore, repeated link contentions and many link failures happen in the MAC layers and cause an excessive number of retransmission in the network [23].

6.2.2 Impact of Mobility on TCP Variants

This section presents the performance of TCP variants with three different node speeds (10 m/s, 10-20 m/s, and 30 m/s) with a size of 60 nodes and two type of heavy traffic applications (HTTP and FTP).

The Figure 6.15 demonstrates the page response time of the TCP variants, while the mobility speed changes in the network. When the node speed is 10 m/s, the lowest average page response time is observed for TCP Reno and New Reno. For the node speed of 10-20 m/s, TCP Reno remains in accounting for the lowest page response time

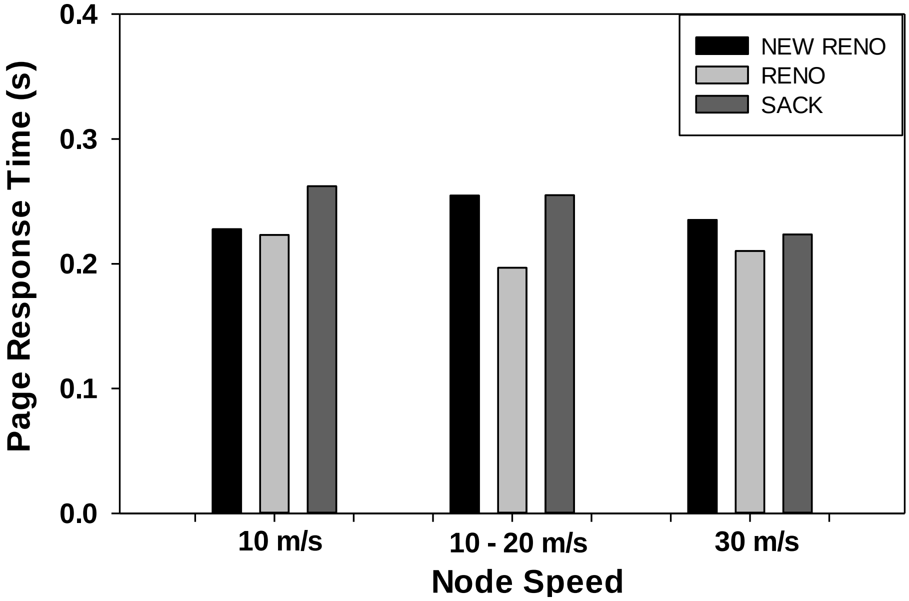


Figure 6.15: Page Response Time of TCP Variants with Varying Node Speed

on average, while TCP New Reno and SACK versions need higher page response time respectively, to load the above mentioned page.

In the higher mobility rate such as 30 m/s, the average page response time of SACK and New Reno is slightly less than that in a 10-20 m/s speed network. It can be also observed that TCP Reno always achieves lowest page response time in all mobility rates compared to others.

From the figure above, it can be concluded that, when the node speed is increased, TCP performance does not always decrease in a wireless environment. When the node speed is set to 30 m/s, it can lead to frequent changes in the topology of the network and frequent link breakages. Nevertheless, it is also possible that it enhances the possibility for the ad-hoc routing protocol to re-establish the breakage link faster [36]. This causes

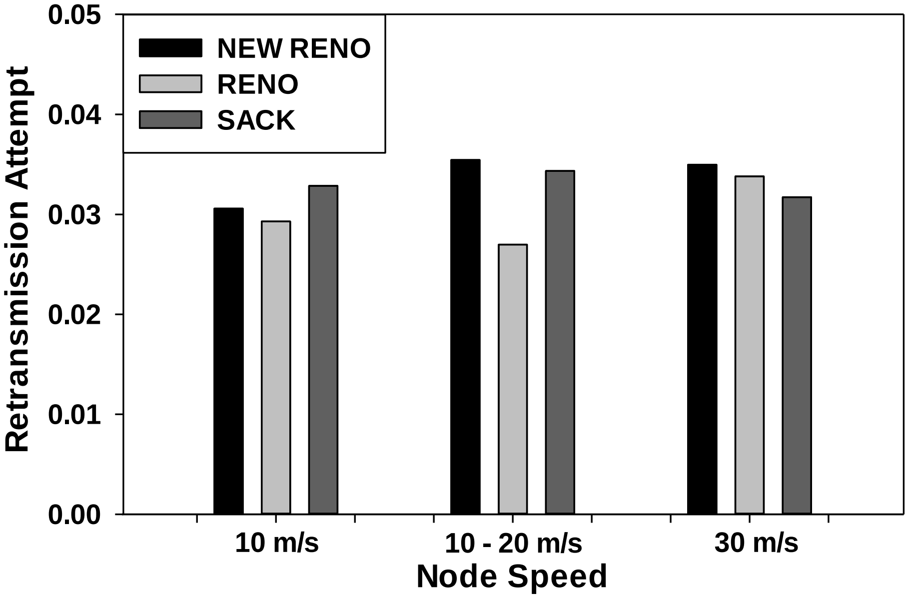


Figure 6.16: Average Retransmission Attempts of TCP Variants with Varying Node Speed

the page response time for high node speed such as 30 m/s to decrease. However, it is not clear that increasing the node speed keeps reducing the response time, as an alternative, it can increase the page response time to a higher extent. Hence, the best right mobility rate choice within MANET can be reflected as an important subject of further research.

The performance of the three TCP variants in terms of retransmission attempt is examined with respect to mobility rate of the network nodes as shown in Figure 6.16. It can be observed from the result of Reno that when the speed of the nodes increases to 10-20 m/s, it can lead to a decrease in retransmission attempts, while when the speed of the nodes is increased to 30 m/s; it leads to an increase in retransmission attempts. It can be conclude from the figure that the TCP Reno variant achieves the lowest average retransmission attempts rate for the low and medium node speeds such as 10 m/s and 10-20 m/s. However, TCP SACK performs the best with high node speed such as 30 m/s.

Different from wired links environment, wireless links environment uses air as a medium for transmission, suffers from wireless link failure and channel error within the wireless network. Since MANET communication is connected with multiple wireless links, the link failures in such a network (either due to mobility of nodes or high bit error rate) can lead to a major amount of packet losses. In reaction to a packet loss in wireless network, TCP retransmits the lost packet again from its own source. Still, in a MANET associated with a high error rate, TCP possibly will have to take multiple retransmissions to deliver a packet to its destination successfully. It can be shown from the figure, when the mobility nodes speed is 10 m/s, the communication route can be considered quite stable, and therefore the dropped packets is few. Oppositely, in a high mobility rate such as 30 m/s, all the three TCP variants retransmit higher amount of data packets, as a response to route breakages in the wireless network. This can be described to the fact that all of the three versions of the TCP variants are not capable of adjusting the size of the congestion window dynamically, consistent with the status of the bottleneck, leading to get more liable to packet losses in a wireless environment.

In case of a link failure takes place, due to the mobility changes, all of three TCP versions mostly distinguish the packet loss through observing the TCP RTO timer. But none of them are designed to handle with such situations (link losses). Therefore they

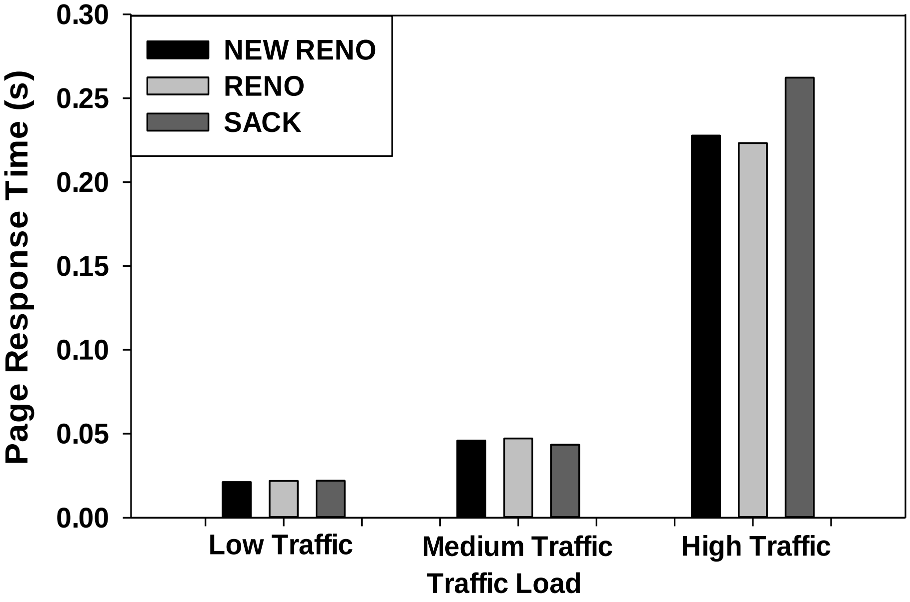


Figure 6.17: Page Response Time of TCP Variants with Varying Traffic Load

all respond similarly. But, the TCP SACK is found to be fairly more robust to the dynamics of the wireless channels. Since SACK version allows a receiver to only indicate the segments that has been received, the sender commonly retransmits only the lost segments, leading to lower number of retransmission attempts as compared to the other two versions.

6.2.3 Impact of Network Load on TCP Variants

This section presents the performance of TCP variants with three different traffic loads (heavy, medium and low) for two applications (HTTP and FTP) with size of 60 and mobility rate of 10 m/s for all network nodes.

The Figure 6.17 illustrates that the page response time for the TCP variants when exposed to low traffic is lower than medium and heavy traffic and all the three variants have almost the same response time at the low and medium traffic. When the network traffic increases due to congestion, the page response time also increases for the medium traffic. In case of heavy traffic, all the three TCP variants show very high response time with TCP SACK as the highest one. When there is large traffic in the network, the TCP Reno, New Reno, and SACK handles many packets dropped due to congestion. Therefore TCP forces to invoke the congestion control mechanisms, leading to performance instabilities and degradations among the three different TCP variants. Thus an extra time is needed to finish the data recovery activities, meaning more time is to be spent to load a web page in the existence of high number of nodes in a network.

In the second part, the performance of the three TCP variants in terms of retransmission attempt is also examined with respect to different load rate of the network nodes. The Figure 6.18 illustrates that all the three variants have similar page response time in the three traffic loads. The similar retransmission attempts of all TCP variants are due to having the same packet size for all nodes, and also queuing the packets at the intermediate nodes, and transmitting to the destination without needing any retransmission by the DSR protocol at the congested networks because of large number of packets (like heavy nodes case). The purpose of that is to decrease the congestion further with the retransmissions. On the other side, when congestion is less as the low load case, the retransmission attempts are carried out to make the delivery of the packets to the destination as demonstrate in [9].

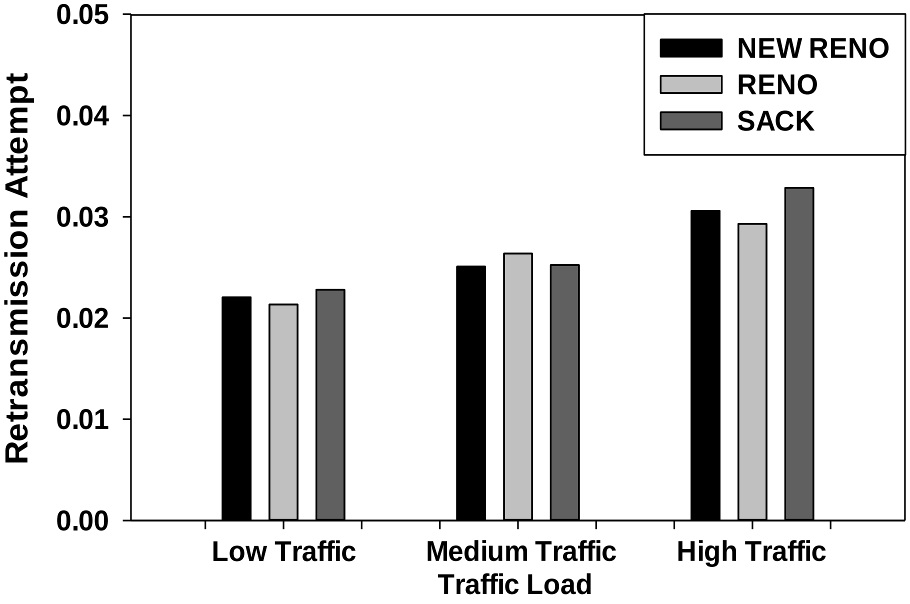


Figure 6.18: Average Retransmission Attempts of TCP Variants with Varying Traffic Load

Chapter 7

CONCLUSIONS AND FUTURE WORK

In this chapter, a conclusion is presented that has been constructed based on the results of the simulations. It makes an attempt to answer research conventional questions. Together with the conclusion, the research limitation is also discussed, and the possibilities of the future research are presented.

This thesis presents and discuss four MANET routing protocols, namely AODV, DSR, OLSR, and GRP, and the basic concepts of three commonly used standard TCP variants, namely, TCP Reno, New Reno and SACK. The simulation results are presented to discuss the performance evaluation of the routing protocols, along with performance evaluation of TCP variants in the same environment regarding how they respond to scalability, mobility, and different traffic load. These results assist in specifying the best appropriate TCP variants and routing protocol which achieve more robust and efficient MANET under different conditions. The significant observations of the study are as follows:

The highest average throughput and the lowest end-to-end average packet delay performances are achieved by the use of OLSR protocol under all the scalability, mobility and traffic load conditions. In other words, the OLSR protocol acts very encouraging in the presence of large number of nods, high mobility under high traffic load. The performance of GRP is acceptable when the nodes size, speed and traffic load is increased. It is observed from the results of the simulations that performance of AODV protocol decreases as the number and speed of nodes and traffic load increase. On the other hand, the DSR protocol shows an extremely low average throughput as a means of dropping more data packets, and high end-to-end average packet delay as the number of nodes, speed and traffic load increase. It can be concluded that the DSR protocol is limited for small networks with low mobility. In summary, the proactive protocols OLSR and GRP are verified to be very efficient and effective routing protocols for MANETs under heavy network size, load, and mobility conditions.

The research also analyzes the performances of the TCP variants with respect to scalability, mobility and traffic load. It is noticed from the simulation results that performances of the TCP variants decrease as the number of nodes, and traffic load increase. On the other hand, it can be observed that when the speed of nodes increases the TCP sometimes shows better performance such as in the page response time for all the TCP variants. It seems that the nodes mobility helps the source node in the network to find more routes and gain an improved connectivity faster. Although, increasing the mobility speed up to 30 m/s can lead to the probability of regular topology fluctuations and frequent link failures, it makes possible for the ad-hoc routing protocol to reestablish the link faster than the RTO duration. If the time required for reestablishing a damaged link is smaller than the RTO, then the TCP examines no data packet loss and thus it does not need to activate the timewasting congestion control mechanisms. This causes the TCP to show higher performance. The TCP SACK outperforms other two TCP variants in terms of page response time and retransmission attempts in a MANET with high number of nodes. The performance of TCP Reno is also remarkable for a medium or small sized network. When the effect of the mobility is observed over the TCP variants, TCP Reno usually presents better performance than others. Simulation results also show that the performance of TCP SACK is also remarkable for high mobility, especially in terms of retransmission attempts. Instead, New Reno TCP is less appropriate for high network and mobility conditions.

When the traffic load effects are analyzed on the routing protocols, it is noted that the performance of the OLSR protocol in terms of throughput is very high in heavy, medium and low traffic. On the other hand, the GRP and AODV has lower throughput than the OLSR, but performs better than DSR. For the end-to-end average delay scenario, the OLSR, GRP and AODV protocols create lower delay than the DSR in low, medium and heavy load traffic scenarios. For the page response time in case of TCP variants, the results illustrate that all three variants has higher response time under medium and heavy load. Also the retransmission attempts for the three variants increases as the traffic increases.

The key goal of this thesis is to create an attempt to perform a complete performance analysis of the four famous routing protocols and three TCP variants in the same framework. Finally, a valuable perception is achieved for this study on the aspects concerning the performance of network routing protocols and TCP variants within MANET. Thereby the major goals of the study have been fulfilled.

Regardless of all these achievements, this research lacked from some privileges. In this research, merely two fixed and one varying node speeds, along with fixed pause time is measured. Therefore, it can be more satisfying if more rates for the speeds and pause times counted in the mobility category. The performance of the network is evaluated with three type of traffic load. Therefore distributing more traffic size may add more assets to the study. Once more, the tuning of the parameters configuration, such as routing protocol and TCP parameters, is set to a realistic value that acts fine. Nevertheless, changing these parameters along with node size, mobility, and load traffic have not been considered. To provide others several future researches information, various subjects are raised during this research. The thesis considered only three network conditions, namely, scalability, mobility, and traffic load. However some other important factors like transmission range and more applications can be considered for the evaluation of the MANET performance. The analysis of the four MANET’s routing protocol performed in this thesis can also be extended for the routing protocols such as ZRP [16], TORA [15], and SSR [37] with more TCP variants such as Tahoe and Vegas [14]. Again for improving the investigation on MANET performance, the cross-layer interactions method [38] can be used. Furthermore, due to the nature of MANET without centralized controls, it is posing exposed to security attacks in the present. Hence, in any future study, such security issues in an ad-hoc network can be followed. Finally, other factors may also pursued, such as pause time impacts, many other mobility rates, nodes with different power capacity, and defective nodes in the network to discuss the performance of MANET.

REFERENCES

[1] D. Tacconi, C. Saraydar and S. Tekinay, “Ad hoc enhanced routing in UMTS for increased packet delivery rates," *IEEE Wireless Communications and Networking Conference*, vol. 2, pp. 1093 - 1098, 2004.

[2] H. Wu, C. Qiao, S. De, and O. Tonguz, “Integrated Cellular and *Ad Hoc* Relaying Systems: iCAR,” *IEEE Journal on Selected Areas in Communications*, VOL. 19, NO. 10, 2001

[3] M. K. Rafsanjani, A. Movaghar, and F. Koroupi, “Investigating Intrusion Detection Systems in MANET and Comparing IDSS for Detecting Misbehaving Nodes,” *World Academy of Science, Engineering and Technology*, vol. 44, pp. 360-368, 2008.

[4] V. Rodoplu, T. H. Meng, “Minimum Energy Mobile Wireless Networks,” *Journal on Selected Areas in Communications*, vol. 17, No. 8, pp. 1333-1344, 1999.

[5] Z.B.A. Hani, and M. D. Bin Baba, “Designing Routing Protocols for Mobile Ad Hoc Network,” *National Conference on Telecommunication Technology Proceedings*, Selangor, Malaysia. vol. 41, pp. 148-150, 2003.

[6] OPNET, Retrieved on October 2012, http://www.opnet.com/.

[7] A. M. Hassan, M. I. Youssef, and M. M. Zahra, "Evaluation of Ad Hoc Routing Protocols In Real Simulation Environments," *The International Conference on Computer Engineering and Systems,* pp. 288-293, 2006.

[8] L. Bajaj, M. Takai, R. Ahuja, K. Tang, R. Bagrodia, and M. Gerla, "Glomosim: A Scalable Network Simulation Environment," *M.S. Thesis*, Computer Science Department, University of California, Los Angeles, 1999.

[9] S. Papanastasiou, L. M. Mackenzie, M. Ould-Khaoua, and V. Charissis "On the Interaction of TCP and Routing Protocols in MANETs," *Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT-ICIW'06),* Guadeloupe, French Caribbean, pp. 62-69, 2006.

[10] T. Camp, J. Boleng and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," *wireless communications and mobile computing*, vol. 2, no. 5, pp. 483-502, 2002.

[11] H. Kaur, D. J. Singh, "Performance comparison of OLSR, GRP and TORA using OPNET," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 2, no. 10, pp. 260 - 267, 2012.

[12] Md. N. I. Khan, R. Ahmed, “Simulation Based Performance Evaluation of Routing Protocols and TCP Variants in Mobile Ad-hoc Networks,” *M.S. Thesis*, Department of Electrical Engineering, Blekinge Institute of Technology, 2010.

[13] M. Bouhorma, H. Bentaouit, and A. Boudhir, “Performance Comparison of Ad-Hoc Routing Protocols AODV and DSR,” *ICMCS International Conference on Multimedia Computing*, pp. 511-514, 2009.

[14] A. Afanasyev, N. Tilley, P. Reiher, and L. Kleinrock, “Host-To-Host Congestion Control for TCP,” *IEEE Communications Surveys & Tutorials*, vol. 12, No. 3 pp. 304 – 342, 2010.

[15] P. Palta, and S. Goyal, “Comparison of OLSR and TORA Routing Protocols using OPNET Modeler,” *International Journal of Engineering Research & Technology (IJERT),* vol. 1, No. 5, pp. 1-6, 2012.

[16] S. Gandhi, N. Chaubey, P. Shah, and M. Sadhwani, “Performance evaluation of DSR, OLSR and ZRP protocols in MANETs,” *International Conference on Computer Communication and Informatics (ICCCI),* Dept. of Computer Sci., Gujarat Univ., Ahmedabad, India, pp. 1 – 5, 2012.

[17] K. Fall, and S. Floyd, “Simulation-Based Comparisons of Tahoe, Reno, and Sack TCP,” *Computer Communication Review*, USA, vol. 26, no. 3, pp. 5-21, 1996.

[18] N. I. Khan, R. Ahmed, and T. Aziz, “A Survey of TCP Reno, New Reno and Sack over Mobile Ad-Hoc Network,” *International Journal of Distributed and Parallel Systems*, vol. 3, no. 1, pp. 49-63, 2012.

[19] X. Kuang, “Modelling and Performance Studies of Integrated Network Scenarios in a Hospital Environment,” *M.S. Thesis*, School of Computing and Mathematical Sciences at Auckland University of Technology, New Zealand, pp. 1-99, 2008.

[20] M. Berger, S. Lima, A. Manoussakisand, J. Pulgarin and B. Sanchez, “A Performance Comparison of TCP Protocols over Mobile Ad Hoc Wireless Networks,” *Electronics, Robotics and Automotive Mechanics Conference*, vol.2, pp.88-94, 2006.

[21] V. Bhanumathi, and R. Dhanasekaran, “TCP Variants - A Comparative Analysis for High Bandwidth – Delay Product in Mobile Ad-hoc Network,” *the International Conference on Computer and Automation Engineering (ICCAE)*, Singapore, Vol. 2, pp. 600-604, 2010.

[22] L. Subedi, M. Najiminaini, and L. Trajkovic, “Performance Evaluation of TCP Tahoe, Reno, Reno with SACK, and NEW Reno using OPNET Modeler,” *M.S. Thesis,* Simon Fraser University Vancouver, British Columbia, Canada, 2009.

[23] S. Bae, K. Xu, S. Lee, and M. Gerla, “Measured Analysis of TCP Behavior across Multihop Wireless and Wired Networks,” *Global Telecommunications Conference GLOBECOM’02*, Vol.1, pp. 153-157, 2002.

[24] A. Ariza-Quintana, E. Casilari, and A. T. Cabrera, “Implementation of MANET Routing Protocols on OMNET++,” *The 1st International Conference on Simulation Tools and Techniques for Communications, Networks And Systems & Workshops*, Marseille, France, No. 80, pp. 660-664, 2008.

[25] S. Ahuja, T. Wu, S. Dixit, “Cache on demand,” *IEEE International Conference on Multimedia and Expo, ICME '02. Vol. 2*, pp. 41-44, 2002.

[26] K. Dhariwal, Mukesh, and S. Sharma, “An Improved Mechanism for Congestion Control in TCP for Ad Hoc Network,” *International Journal of Computer Applications*, vol. 20, no. 2, pp. 21-24, 2011.

[27] M. K. Afzal, A. U. Khan, A. Pescape, Y. B. Zikria, and S. Loreto, “SCTP vs. TCP Delay and Packet Loss,” *IEEE International Multitopic Conference,. INMIC.*, pp. 1- 5, 2007.

[28] M. R. N. Rad and R. Kourdy, “Analysis of TCP Tahoe with slow start and Multiple packet drop in Network on Chip,” *Journal Of Computing*, Vol. 4, No. 5, pp. 231-235, 2012.

[29] U. T. Nguyen, and X. Xiong, “Rate-Adaptive Multicast in Mobile Ad-Hoc Networks,” *International Conference on Wireless and Mobile Computing, Networking and Communications*, (WiMob'2005), vol. 3, pp. 352–360, 2005.

[30] A. Savoia, “Web Page Response Time,” *Software Testing and Engineering Magazine*, pp. 48 – 53, 2001.

[31] High Performance Web Sites: 2012, “The Importance of Front-End Performance,” Retrieved on January 2013, http:// developer.yahii.com/blogs/ydn/posts/2007/03/High-performance.

[32] P. Hellekalek, “Good Random Number Generators are (not so) Easy to Find,” *Elsevier,* Mathematics and Computers in Simulation, Vol. 46, No. 5, pp. 485-505, 1998.

[33] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum and L. Viennit, “Optimized Link State Routing Protocol (OLSR),” *Internet Engineering Task Force* 2003.

[34] C. E. Perkins, E. M. Royer, “Ad-hoc on-demand distance vector routing,” *Second IEEE Workshop on Mobile Computing Systems and Applications. WMCSA '99, Vol. 2, pp. 90 – 100*, 1999.

[35] N. Qasim, F. Said, and H. Aghvami, “Mobile Ad Hoc Networking Protocols' Evaluation Through Simulation for Quality of Service,” *IAENG International Journal of Computer Science,* vol. 36, no. 1, pp. 76-84, 2009.

[36] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva, “A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols,” *ACM/IEEE*

International Fourth Conference on Mobile Networking and Computing, MOBICOM, Dallas, USA, pp. 85-97, 1998.

[37] T. Fuhrmann, "The use of Scalable Source Routing for Networked Sensors," *2nd IEEE Workshop on Embedded Networked Sensors, Sydney*, pp. 163-165, Australia, 2005.

[38] M. Conti, G. Maselli, G. Turi, and S. Giordano, "Cross-Layering in Mobile Ad Hoc Network Design," *Computer*, vol. 37, No. 2, pp. 48-51, 2004.

APPENDIX

Appendix

The appendix shows the network configuration parameters for the simulator, where each table present the parameters used in this study.

Table A.1: General Parameters

General Parameters	Value
Area	1000×1000 m^2
Network size (no. of nodes)	20, 40, 60, and 100
Data rate	5.5 Mbps
Mobility model	Random Way point
File size	Heavy and light load
Traffic type	HTTP
Mobility speed	10, 10 - 20 and 30 m/s
Simulation time	600 seconds
Address mode	IPv4

Table A.2: Wireless LAN Parameters

Wireless LAN Parameters	Value
Physical characteristics	Direct sequence
Data rate	5.5 Mbps
Channel settings	Auto assigned
Packet reception-power threshold (dBm)	-95
RTS threshold (bytes)	None
Fragmentation threshold (bytes)	1024
CTS-to-self option	Enabled
Limit of short retry	7
Limit of long retry	4
Interval AP beacon (s)	0.02
Max. lifetime received (s)	0.5
Size of buffer (bits)	256000
Processing of large packet	Fragment
PCF parameters	Disabled
HCF parameters	Not support

Table A.3: Application HTTP Parameters

Attribute	**Value**
Specification	1.1HTTP
Page inter-arrival time (s)	Exponential (60, 270, 720)
Page properties (bytes)	Constant (500-750-1,000), 5 small and medium image
Server selection	Browse
RSVP parameters	None
Type of service	Best effort (0)

Table A.4: TCP Parameters

TCP Parameters	**Value**
Slow start initial count (MSS)	1
Receive buffer size (bytes)	8,760
Maximum ACK segment	2
Duplicate ACK threshold	3
RTO initial (s)	1.0
RTO minimum (s)	0.5
RTO maximum (s)	64
Gain of RTT	0.125
Gain of deviation	0.25
RTT deviation coefficient	4.0

Table A.5: Profile Configuration for Routing Protocol

Profile Configuration	**Value**
Number of profile	1
Start time (s)	Uniform (100, 110)
Duration (s)	End of simulation
Profile repeatability	Once at start time
Inter-repetition time (s)	Constant (300)
Number of repetitions repetitions	Constant (0)
Repetition pattern	Serial

Table A.6: Profile Configuration for TCP Variants

Profile Configuration	**Value**
Number of profile	2
Start time (s)	Uniform (100, 110)
Duration (s)	End of simulation
Profile repeatability	Once at start time
Inter-repetition time (s)	Constant (300)
Number of repetitions repetitions	Constant (0)
Repetition pattern	Serial

Table A.7: Application Configuration for Routing Protocol

Application Configuration	**Value**
Number of application	1
Start time offset (s)	Constant (5)
Duration (s)	End of profile
Application repeatability	Once at start time
Inter-repetition time (s)	Constant (300)
Number of repetitions	Constant (0)
Repetition pattern	Serial

Table A.8: Application Configuration for TCP Variants

Application Configuration	**Value**
Number of application	2
Start time offset (s)	Constant (5)
Duration (s)	End of profile
Application repeatability	Once at start time
Inter-repetition time (s)	Constant (300)
Number of repetitions	Constant (0)
Repetition pattern	Serial

Table A.9: AODV Parameters

Parameters	**Value**
Route discovery parameters	Default
Active route timeout (s)	3
Hello interval (s)	Uniform (1, 1.1)
Allowed Hello loss	2
Net diameter	35
Node traversal time (s)	0.04
Route error rate limit (pkts/s)	10
Timeout buffer	2
Packet queue size (packets)	Infinity
Local repair	Enabled
Addressing mode	IPv4

Table A.10: DSR Parameters

Parameters	**Value**
Route expiry time (s) in route cache	300
Expiry timer (s)	30
Request table size (nodes) in route discovery	64
Max. request table identifiers in route discovery	16
Max. request retransmissions in route discovery	16
Max. request period (s)	10
Initial request period (s)	0.5
Non propagating request time (s)	0.03
Gratuitous route reply time (s)	1
Max. buffer size (packets)	50
Maintenance handoff time (s)	0.25
Max. maintenance retransmissions	2
Maintenance acknowledgement time(s)	0.5
Route replies using cached route	Enabled
Packet salvaging	Enabled

Table A.11: OLSR Parameters

Parameters	**Value**
Willingness	Willingness default
Hello interval (s)	2.0
TC interval (s)	5.0
Neighbor hold time (s)	6.0
Topology hold time (s)	15.0
Duplicate message hold time (s)	30.0
Address mode	IPv4

Table A.12: GRP Parameters

Parameters Attribute	**Value**
Hello interval (s)	Uniform (4.0, 5.4)
Neighbor expiry time (s)	Constant(10)
Distance moved (m)	1,000
Position request timer (s)	10.0
Backtrack option	Enabled
Routes export	Enabled
Number of initial floods	2

Table A.13: Simulation Seeds

Scenarios	Seeds Number
1	128
2	228
3	328
4	428
5	528
6	628
7	728
8	828
9	928
10	1028

Table A.14: Application FTP Parameters

Profile Configuration	**Value**
Inter request time	360, 720, 3,600
File size	500, 5,000, 50,000
Symbolic server name	FTP