Performance Comparison of MANET Routing Protocols

Ahmad Ibrahim Ahmad

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

Master of Technology
in
Information Technology

Eastern Mediterranean University
August 2021
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Prof. Dr. Ali Hakan Ulusoy
Director

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

Assoc. Prof. Dr. Nazife Dimililer
Director, School of Computing and Technology

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 Technology in Information Technology.

Asst. Prof. Dr. Husnu Bayramoglu
Supervisor

Examining Committee

1. Asst. Prof. Dr. Husnu Bayramoglu

2. Asst. Prof. Dr. Emre Ozen

3. Asst. Prof. Dr. Kamil Yurtkan

ABSTRACT

Mobile ad-hoc networks can be described as a broad topic in a networking field that faces many challenges and issues to secure the network surroundings. There are different types of routing protocols designed to meet different requirements in ad-hoc networks because of their unorganized nature. Network topology can change frequently depending on the availability, velocity, battery life and the number of nodes in these networks. Over the recent years, security issues in ad-hoc networks have seen a great deal of thought. The vast majority of investigation focuses on the exploration of specific explicit security zones, to make sure the routing protocols are well secured. This study mainly discusses reactive and proactive routing protocols designed for mobile ad-hoc networks and compares some of them with simulation results. Packet delivery ratio, end-to-end delay and throughput values for different simulation environments are analyzed in these simulations. In addition to this, security concerns and possible solutions in ad-hoc networks is also considered deeply.

Keywords: ad-hoc networks, routing protocols, reactive, proactive, delay, throughput, comparison, simulation.

ÖZ

Mobil geçici ağlar, ağ çevresini güvence altına almak için birçok zorluk ve sorunla karşı karşıya kalan, bilgisayar ağları alanında geniş bir konu olarak tanımlanabilir. Düzensiz yapıları nedeniyle geçici ağlarda farklı gereksinimleri karşılamak üzere tasarlanmış farklı türde yönlendirme protokolleri vardır. Ağ topolojisi, bu ağlardaki düğümlerin kullanılabilirliği, hızı ve pil ömrüne bağlı olarak sık sık değişebilir. Son yıllarda, geçici ağlardaki güvenlik sorunları üzerinde çokça düşünülmüştür. Araştırmaların büyük çoğunluğu, yönlendirme protokollerinin iyi bir şekilde güvence altına alındığından emin olmak için belirli açık güvenlik bölgelerinin araştırılmasına odaklanır.

Bu çalışma esas olarak mobil geçici ağlar için tasarlanmış reaktif ve proaktif yönlendirme protokollerini tartışmakta ve bazılarını simülasyon sonuçlarıyla karşılaştırmaktadır. Bu simülasyonlarda farklı simülasyon ortamları için paket teslim oranı, uçtan uca gecikme ve verim değerleri analiz edilmektedir.

Anahtar Kelimeler: geçici ağlar, yönlendirme protokolleri, reaktif, proaktif, gecikme, verim, karşılaştırmak, simülasyon.

DEDICATION

To my family.

ACKNOWLEDGEMENT

I'm forever obligated to Almighty Allah for his plentiful effortlessness, arrangement, and motivation all through my program here at EMU.

I'm likewise significantly obliged to my family who upheld and remained with me in my scholarly program. Your affection, good, monetary, and material help were important to the fruitful achievement of my program. I'm ready to come this far because you remained with me.

I would like to use this opportunity to thank Asst. Prof. Dr. Husnu Bayramoglu, that allowed me to have this wonderful research on performance comparison of (MANET) routing protocols, I would like to express my gratitude to him for the guide and help towards my research on this wonderful project, which is an interesting and exhaustive topic at the same time. He has been an inspiration and role model for this topic. His guidance and active support have made it possible to complete this project.

I consider it a privilege to express through the pages of this project, a few words of gratitude and respect to all those who guided and inspired me and the completion of this project work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ADDV	Ad-hoc On-Demand Distance Vector
AODV	Ad-hoc On-Demand Vector
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
DAG	Directed Acyclic Graph
DHCP	Dynamic Host Configuring Protocol
DIPLOMA	Distributed Policy Enforcement Architecture
DNS	Domain Name Service
DSD	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISS	Information Security System
JSM	Join State Messages
LSI	Link State Information
MAC	Media Access Control
MANET	Mobile Ad-hoc Network
OLSR	Optimized Link-State Routing Algorithm
ONA	Open Network Architecture
OPNET	Open Network
OSI	Open Systems Interconnection Model
PDR	Packet Delivery Ratio
PRNET	Packet Radio Network

RRE	Route Reply Error
RREPS	Receive Route Replies
RRP	Route Reply Packet
SURAN	Survival Radio Network
SYN	Synchronize Acknowledge
TCL	Telephone Communication Limited
TCM	Topology Control Message
TCP	Transport Control Protocol
TDP	Table Driven Protocol
TORA	Temporally Ordered Algorithm
TTL	Time To Leave
VANET	Vehicular Ad-hoc Network
VINT	Virtual Inter Network Testbed
VLAN	Virtual Local Area Network
WRP	Wireless Routing Protocol
ZRP	Zone Routing Protocol

Chapter 1

INTRODUCTION

Usually, the characterization of mobile ad-hoc networks MANETs comes up from the freedom to act independently among the nodes. Network topology can change frequently depending on the availability, velocity and battery life of the node. MANETs battle with security issues such as dynamic topology, wireless communication and distributed management. Because of the free movement among the nodes, these constituent segments have changed the comfort zones for MANETs against the issues that are associated with dangers and uncertainty. Security is one of the fundamental distress to protect the correspondence between different nodes in the network climate.

With the broad fast improvement of computers and the wireless correspondence, the mobile computing has effectively developed the field of computer telecommunications. MANET is totally available through the nodes and activities developed in the network, which generally has a unique shape and a restricted transmission capacity and different highlights. Network individuals might be the computers, Personal Digital Assistants (PDAs), cell phones, MP3 players, and computerized cameras, etc. [1].

From today's Internet, mobility is the term used to mean activities has wandering in an alternate area. They can hold their own Internet Protocol (IP) address, without the need to continually changing, which is one of the Mobile IP modernizations. The concepts are for mobile IP nodes, which must manage IP addresses from foreign and domestic agents, as well as packet tunneling, and a fixed network that must remain the same as the first. In any case, early utilization of military on the mobile packet radio network indeed can be viewed as a paradigm of MANETs, with the improvement of Information and Communication Technology (ICT). If the communication hardware, size, and weight constantly reduce, power utilization gets low. From the previous few years, the promotion of mobile phones can be believed to speak with others whenever, anyplace, to get the most recent information, and we have progressively become part of the life. It can be considered as a danger and risk to military in the battlefield to use the network, most of the fundamental communication facilities may not be accessible. For this situation, if among the militaries want to communicate with others, we should depend on these MANETs network infrastructure limitations [1].

The ad-hoc network absolutely, is a wireless which are especially suited to disaster or catastrophic relief operation [2].

While discussing MANETs, the life cycle could be divided into three categoric stage. The first stage happens to be in late 1970s which is called as packet radio network (PRNET). The Defense Advanced Research Project Agency (DARPA) started a research of using packet-switched radio communication that will provide reliability, and trusted communication between computers and urbanized PRNET [4].

The second generation of MANETs happens to emerge in 1980s. By that time, MANETs were enhanced and executed as Survivable Adaptive Radio Networks (SARN). This program brought the new mechanisms of switching a mobile network without using any infrastructure.

In the last generation, which happens to be in 1990s, the concept of ad-hoc networks brought new technology of using microcomputers and other ways of communications [5]. During that time, the new ideology of MANETs was introduced [6, 8].

1.1 Problem Statement

MANETs has a wide range of application areas like disaster rescue, hospital management, data monitoring, wireless sensor networks, etc. The success of communication in these networks has many challenges including switching, routing and network security issues. In order to handle these challenges, several routing protocols and security approaches have been designed [7]. However, there is no and will never be a perfect solution for these challenges due to the nature of computer networks. There is always a room for improvement and therefore it is an open to research area.

Fundamental qualities of MANETs regarding the safety of configuring perspective is not well cleared in line safeguard. In wired networks, routers are utilized to perform the routing functionality for the nodes. Nonetheless, remote channels are open to both users and attackers. There is no overall described principle or spot where to have a traffic from different nodes that will check or access control system which nodes and packets to be authorized before getting access. No protection will be separated inside the network from the external network.

MANETs are the multi-spring network, less infrastructure, and the principle of self-coordinating together. Over the most recent couple of years, securing issues in MANETs have joined a great deal of thought, the vast majority of the investigation focuses on the exploration of specific explicit security zones, to make sure the routing protocols are well secured.

For this purpose, the following objectives have to be examined to ensure the security services which includes [9]:

- Confidentiality
- Integrity
- Authentication

Among all these mentioned security administrations, verification and validation are presumably the greatest significant besides complicated issues in MANETs since it is a strapping of the whole security system. At whatever the authentication and validation are well achieved in MANETs then the arrangement is essentially an issue of getting a count on the gathering by using keys. These safety facilities and administration can be given independently. It simply depends upon change in prerequisites.

1.2 Motivation and Aim of the Study

This study discusses security threats in MANETs, implementations of the solutions are presented, essentials around the security threats, and issues to discuss from the distinctive security perspective, and how the issues must be settled.

With the fast space of mobile devices and their broad use in modern way of life, the worldview of systems networking has move from fixed networks to wireless networks with restricted or without infrastructure support.

MANETs have importance in current unavoidable systems networking because of their positive characters like quick arrangement and without infrastructure. Highly dynamic topology is a static case, because of the network is designed as an undirected connected graph, in which each of the nodes understands its neighbors but at the time does not know any more details about the topology. The dynamic case requires more handling to connect and disconnect network sections.

Stringent resources constraints refer to a device that has limited capabilities in its processes and storage capabilities of the inputs availability to complete the process. Hence, the crucial aim and motivation of this study shows up from understating the need to protect MANETs from different security attacks. Malicious attacks cause different level of harm to the network relying upon the kind of attacks utilized. We still note that a significant study has effectively been made to protect and secure a MANETs from the security issues. We consider that security is a significant help for MANETs, where there is no control to understand and identify attacks that compromise network security comfort zones.

The rest of the proposal is coordinated as follows: Chapter 2 audits the overview on the MANETs, characteristics, features, applications and challenges in MANETs is described. Chapter 3 investigates MANETs routing protocols and focuses on investigating the security outline and attacks in MANETs. The protocols include proactive or Table-Driven Routing protocols, such as Destination-sequenced Distance

Vector (DSDV) [10] and Optimized Link State Routing Protocol (OLSR). Reactive or On-Demand Routing Protocol [11] like Ad-hoc On-Demand Vector [12] (AODV), and Hybrid Routing Protocols like Zone Routing Protocol (ZRP). Chapter 4 examines the related work for the stated problem. Chapter 5 brings up the simulation results and discussion about MANET routing protocols: AODV, DSDV and OLSR. The last chapter provides the conclusion of this study and provides some future works.

Chapter 2

LITERATURE REVIEW

MANETs is a dynamic network established by an autonomous system of mobile nodes connected via wireless links. The movable nodes are allowed to move randomly, and without any existing fixed infrastructure [13]. Subsequently, MANETs can be organized in a catastrophe event and so on. For this purpose, a successive connection breakage occurs mainly due to the node.

In 2011, authors explored a MANETs routing protocol. The motivation here is the network that can contain thousands of nodes. Source, destination, and the address of the next node, which is govern under the guidance of IP [14]. Every node in the process continues to maintain the data information about the destination nodes.

The authors in [14] asserted the features of an ad-hoc on-demand routing protocol as both an on-demand and table-driven protocol. The packet size in the routing protocol is uniform contrasted with dynamic source routing, while unicasting and multicasting are upheld by ad-hoc on-demand distance vector. The protocol can only keep one route between source and destination. Before that, the route can maintain the information only when its active, by the time it gets expired the maintenance will be terminated.

Dynamic source routing is one of reactive protocols. The route is discovered only when it is needed and required. The intermediate node does not keep any information to

route the packet. Less network overhead is achieved as the quantity of message trade between the node.

Conducting about the evaluation of MANETs, characteristics and the applications of MANETs is done by [Vijayalakshmi: 2016]. The author explains the benefits of using MANETs in our today's world. He explains that, its advantageous to use MANETs which helps in reducing the cost of infrastructure that we are using before, simplifying in establishment as the routing is performed exclusively by the nodes utilizing to forwards packets [15][16].

The communication in MANETs is occurred by utilizing multi-path ways. Nodes in MANETs share the wireless medium and the geography of the network changes powerfully. In MANETs, breaking of connection is exceptionally continuous, as nodes are allowed to move to anyplace. The range and quantity of nodes relies upon the applications wherein the clients utilizing MANETs [17]. Routing is a difficult undertaking in MANETs. Nodes ought to coordinate to move the packet to destination node since every node of the network can discuss just with those nodes situated inside its transmission span, while the source and destination nodes can be situated a good way off a lot higher than [18]. Every one of the nodes in a multi-bounce or multi-path wireless network, help out one another to frame a network without the presence of any infrastructure.

The accessibility of the network, classification and uprightness of the information can be accomplished by guaranteeing that security issues have been met [Kirti Gupta: 2017]. MANETs regularly experience numerous attacks because of the behavior of the network like open medium which leads to change in the topology dynamically. These

components have changed the situation of the MANETs against the security issues. Majority of the dialogue concerns the static and network based on wired systems. However, MANETs is at yet in needing further conversation and improvement as far as security [19]. With the development of progressing and new methodologies of networking, new issues are emerging for the rudiments of routing protocols. The routing that is planned significantly for the internet is different with MANETs. The traditional routing was by using connected wired to a non-dynamic backbone which cannot support the ad-hoc because of its movement [20]. Because of different elements which include absence of physical infrastructure and dynamic topology, the routing protocols are more vulnerable to the security attacks. The significant weaknesses which have been so far investigated are generally these sorts which involves dynamic nature, and open remote network. The features of MANETs makes it to be exploited to the attackers either from inside or outside of the network.

Moreover, a recent study discusses the issues that are associated with MANETs. These problems include battery limitations of the nodes, throughput, distributed operation in ad-hoc networks, hidden and exposed terminals and others. Wireless ad-hoc networks do not have a central coordinator to distribute bandwidth among the nodes. For this purpose, nodes have to be scheduled to allocate a way to have access to the channel which requires control of information among the nodes [21].

Hidden nodes are the types of nodes that are not accessible from the initial person that sends the data session, but can be accessible to the receiver. In many cases, the hidden terminals are bringing out a collision from the receiver nodes. The occurrence of the hidden terminals can expressively reduce the throughput of media access protocol that are used in ad-hoc wireless networks [21]. While for the exposed terminals, the nodes

that are currently in the processing range from the sender are banned from making a transmission. So, to work on the proficiency of the protocol, the exposed nodes must be allowed to communicate but under the guidance of fashion without causing any collision to the data transmission.

Another study shows that, by applying the standards of MANETs, a Vehicular ad-hoc network (VANET) can be set up in a wireless mode by vehicles utilizing MANETs [22]. Vehicles can straightforwardly interact among each other without support of framework and infrastructure. Additionally, VANETs are used for monitoring vehicles and transportation system paradigm.

Conclusively, it can be seen that many of different scholars and researchers hold their views about the concepts of MANETs. Mostly, they emphasize about the security issues that are disturbing the comfort zone of MANETs. They presented some of the attacks and weaknesses of MANETs. Additionally, they present the principle of the attacks, types that compromise the MANETs and several security procedures that can protect MANETs.

The investigation on MANETs is as yet in a beginning phase, more of the research can be conducted on incorporated ways to deal with securing the routing and information security on various layers.

Chapter 3

OVERVIEW OF MANETS

MANETs is a self-arranging network, each node in an association is independent. The nodes are allowed to move aimlessly and put together themselves self-assertively. Communication in MANETs is occurred by utilizing multi-bounce ways. Geography of the network changes sporadically and powerfully. In MANET, breaking of correspondence is exceptionally regular, as nodes can move anyplace.

Over the most recent few years, the utilization of wireless networks has gotten increasingly mainstream. An infrastructure network [35] comprises of wireless network nodes and at least one bridge, which associate the wireless network to the wired network [36]. These extensions are called base stations. A mobile node inside the network looks for the closest base station, connects and speaks with it.

The significant reality is that all communication occurs between the wireless nodes and the base station but not between different wireless nodes. While the mobile node is traveling around and suddenly when the mobile node is out of range of the current base station, a handover to a new base station will allow the mobile node to communicate with the new base station without interruption. Ad-hoc networks, unlike infrastructure Networks, do not have any infrastructure. there are no fixed routers, no base stations, administration at the center. All nodes are dynamically connected to one another and can move at random. As a result, all nodes serve as routers, requiring them

to find and maintain routes to all other nodes in the network, as well as propagate packets. MANETs can be used in situations where there is little or no communication infrastructure, such as in emergency searches and rescue operations, or in situations when individuals need to transmit information quickly such as gathering.

The author in [35] explained that “MANETs is made up of a number of MANETs routers,” says the author (MRs). These MRs organize and maintain a routing system among themselves via dynamic wireless interfaces. A MR, like any other internet protocol (IP) router, can be connected to a set of nodes. These nodes link to the MR, which allows them to access the MANET. The topology of a MANET's network and communication links may shift more frequently than in fixed wired or fixed wireless networks due to relative motions of MR, to environmental impacts (particularly wireless characteristics), and to relative motions of MR. These and other considerations influence the design of the Internet Protocol (IP) for MANETs. MANETs can be used to extend the wireless mobile range of more traditional fixed infrastructure network designs, or they can be used as stand-alone networks in certain circumstances.

3.1 Characteristics and Features of MANETs

For MANETs, there are some available features in routing protocols that are adventures of wireless nodes connected without using dynamically centralized control nodes. Therefore, all of the nodes are open to moving subjectively. In consequence of that, the available topology in the network may change its stage at a dubious time. This implies to a node that is inside the reach to communicate effectively, while another wireless network will only just depend on their closet nodes to advance and move the packets as a switch. The routing protocol is liable for taking and developing

information starting with one node then onto the next. A few different factors such as capacity requirement and security makes the routing protocols face many challenges.

The characteristics of MANETs can be categorized into five categories which includes [36]:

- Network scalability: Popular network management methods are now mostly designed to function on fixed or small wireless networks. Large networks with tens of thousands of nodes are used in MANETs applications, such as sensor networks and tactical networks [37]. The ability to scale these networks is crucial to their success. The path to a big network made up of nodes with limited resources is not easy, and there are many hurdles to overcome in areas like addressing, routing, location management, configuration management, interoperability, security, and high-capacity wireless technologies. etc.
- Dynamic topologies: Because nodes in MANETs can travel independently, the network topography, which is typically multi-bounced, can vary on a regular and erratic basis, resulting in course alterations, unceasing association, and possibly pack difficulties.
- Multi-hop routing: There is no default router available. Every node act as a router, forwarding packets across mobile hosts to enable information sharing.
- Autonomous and infrastructure-less: MANETs don’t depend on any settled framework or unified network. Every node works in dispersed shared mode, goes about as an autonomous switch and produces free information.
- Variation in link and node capabilities: Every node may be equipped with at least one radio interface with varying transmission limits and the ability to work across several repeat gatherings. This heterogeneous radio capability

might potentially enable upside-down joins. Additionally, every node may have a different programming/gear configuration, allowing for a greater degree of adaptability in terms of getting ready limits. The network configuration for this heterogeneous association might be complex, necessitating dynamic changes in response to changing situations. (Power and channel conditions, traffic load/ dissemination assortments, blockage, and so on). This becomes a more pressing issue in flexible uniquely specified relationships since each node is likely to act as both an end system and a switch at the same time, requiring more energy to transport packages between nodes.

3.2 Applications of MANETs

The planning of employments for MANETs is varying, going from huge extension, flexible, extraordinarily association, too little, static associations They are limited by the availability of power Aside from older applications that migrate from a standard infrastructure coordinated environment to a highly customized environment, a slew of new networks can and will be built for the new climate [37].

In the event where there is a collective struggle required, MANETs assume a significant part in wireless communication and gives viable correspondence. Some of the most common uses are as follows:

- Military Battlefield: Military hardware presently regularly contains a type of PC gear. The military could exploit the improvised frameworks network to abuse common association development to maintain an information network between fighters, vehicles, and military information headquarters. This field gave birth to the core methodologies for unusually selected association.

- Local Level: Using scratch pas PCs or palmtop PCs, a mobile ad-hoc network can independently interface a second and brief sight and sound association to spread and split information amongst individuals at events such as assembling or homeroom. Another possible near-level application could be in home associations, where devices can communicate directly to exchange data. Basically, in other ordinary resident conditions like taxi, sports field, boat and little plane, convenient exchanges will have various applications.
- Business sector: In emergency/rescue situations, such as fires, floods, or earthquakes, a mobile ad-hoc network can be employed for failed aid projects. When there is a need for a non-existing or damaged communication network to be established and sent quickly, emergency rescue drills should be conducted. Over a small portable, information is passed from one rescuer to the next. Other commercial situations include transportation to-convey unrehearsed flexible correspondence, low authorization, and so forth.
- Personal Area Network (PAN): Short-range MANETs can handle intercommunication between different PDAs (like a PDA, a PC, and a cell). Repetitive wired connections are being phased out in favor of long-distance affiliations. The PAN is potentially a promising MANETs application field that will be inescapable registering setting in the future [37].

3.3 Challenges in MANETs

Problems that are associated with MANETs are well cleared. These problems include battery limitations of the nodes, throughput, distributed operation in ad-hoc networks, hidden and exposed terminals and others [38]. Wireless ad-hoc does not have a central coordinator to distribute bandwidth among the nodes. For this purpose, nodes have to

be scheduled to allocate a way to have access to the channel which required control of information among the nodes.

Hidden nodes are the types of nodes that are not accessible from the initial person that sends the data session but can be accessible to the receiver. In many cases, the hidden terminals are bringing out a collision from the receiver nodes. The occurrence of the hidden terminals can expressively reduce the throughput of media access protocol that are used in ad-hoc wireless networks. While for the exposed terminals, the nodes that are currently in the processing range from the sender are banned from making a transmission. So, to work on the proficiency of the protocol, the exposed nodes must be allowed to communicate but under the guidance of fashion without causing any collision to the data transmission.

MANETs is a self-facilitated network that is based on a distance association of beneficial center locations. Every device has the ability to communicate with other devices. It's also a network with several bounces. Despite MANETs extensive history, they still have a few flaws and architectural issues to overcome [38].

- Limited bandwidth: Connections in wireless networks may have a low capacity when compared to infrastructure networks. Ad-hoc networks are affected from multiple access and fading in radio transmission rate.
- Dynamic in topology: Because of dynamic geography or topologies, nodes may have less sincere between them.
- Packet loss and transmission error: Route’s break more frequently due to node mobility, resulting in a greater packet loss ratio.

- Security threats: Because of its mobility and wireless nature, ad-hoc networks pose unique security issues. The trust management between nodes in ad-hoc or wireless networks leads to several security vulnerabilities.
- Mobility: Ad-hoc networks experience frequent route breakage as a result of their dynamic behavior and changes in network structure.

Few more challenges of MANETs can also be listed as follows:

- The channel is unprotected from outside signal.
- The wireless media is difficult when compared to the wired media.
- Collisions may occur due to hidden nodes.
- The channel has time differing and asymmetric properties [39].

Furthermore, besides these problems, we still have some more difficulties and complexity in the comfort zone of MANETs. Since MANETs is utilized in military exercises, it requires flexibility. Each mobile node must be capable of managing network reinforcement and fulfilling the task since the network has been structured to satisfy the needs. MANETs is a network that has no central organization or association. Whereas every device can connect with every other device, identifying and controlling problems becomes more complex [24]. Due to each network node is self-contained, it includes all of the essential equipment for a radio interface with varied transmission and receiving restrictions, resulting in an unbalanced association.

In MANETs, every node goes probably as a switch and can propel packets of the data to various node to give information dividing between the flexible center points [40].

There is a need for routing protocols to handle the communication and manage these challenges in MANETs. There are different types of MANETs routing protocols which is discussed in the next chapter.

Chapter 4

MANET ROUTING PROTOCOLS

MANETs is a self-designing network where nodes move autonomously inside the network. Each node may change its link state from one device to another which leads to highly dynamic topology [25]. The devices play the role of a router in the network.

4.1 Types of MANETS

The most appreciated technique to categorize the nodes in a MANETs is how the nodes keep maintaining their state and get the data [26]. Generally, MANETs routing protocols can be classified as follows [27]:

- Reactive routing protocols
- Proactive routing protocols
- Hybrid routing protocols

4.1.1 Reactive or On-Demand Routing Protocols

Reactive routing protocol [28] is a type of protocol that does not have any predetermined routing table; therefore, it can likewise be called an On-Demand routing protocol [29]. More of a survey stated that the reactive or on-demand routing protocol is used to reduce or decline the control traffic while sending the information or messages which can be used to promote discovering a new route. In this process, there is no need to distribute the information, the bandwidth will be consumed at the time of transferring the data from one node to another. In the same case, when data source wants to deliver a packet of information or data to a destination, it will activate the discovery process, which will take the shortest route possible. The nodes can only stop

responding only if the node is no longer in need of any data information from the source.

The determination of the route will continuously occur until there is no need for that. It means that the discovery will only be terminated if the node is fully occupied or not needed. The following is a list of some examples of reactive routing protocols. [30][31][32]:

- Ad-Hoc On Demand Distance Vector (AODV)
- Dynamic Source Routing (DSR)
- Temporally Ordered Routing Algorithm (TORA)

4.1.1.1 AODV

AODV is a reactive or on-demand routing protocol for ad-hoc networks that provides loop-free routing. It is designed to behave organically in a network of portable nodes, despite a variety of network activities such as nodes. The routing table is maintained by AODV at each node [33].

Aside from that, AODV is a message coordinating technique for computers. It allows these adaptive computers, also known as centers, to send signals to other centers with which they are unable to communicate directly. AODV accomplishes this by identifying the communication pathways that can be used. AODV checks for loops in these routes and attempts to identify the quickest route to the destination. AODV is also ready to go to deal with route modifications and can create new routes if existing ones are broken.

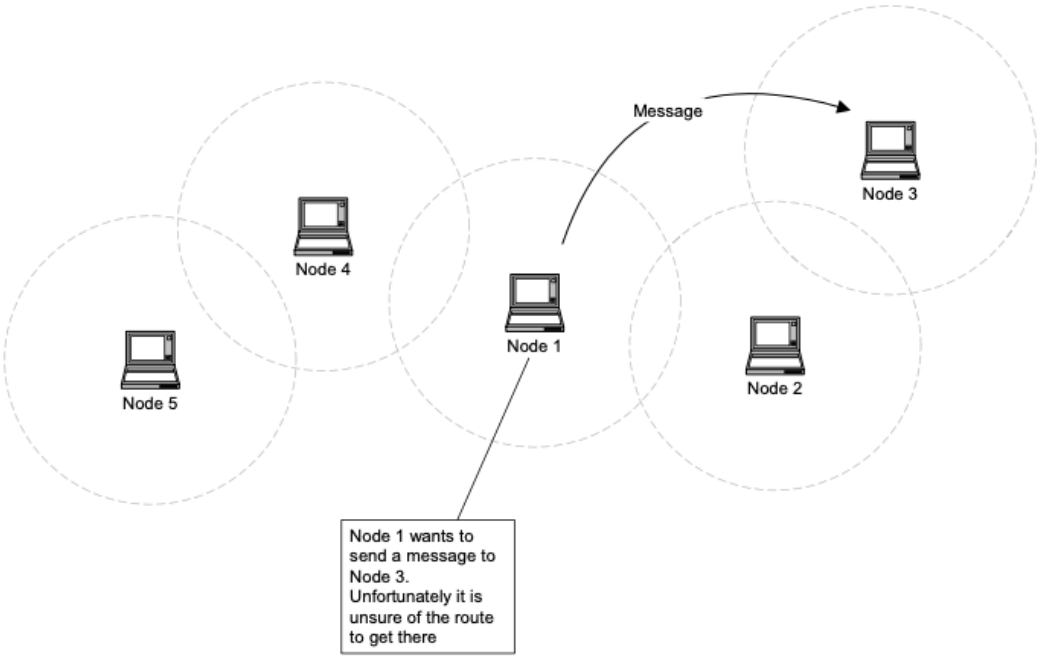

Figure 1: Communication of AODV with other Nodes

It can be seen from the above Figure 1 that we have five nodes in a wireless network that want to communicate. The circles show the scope of correspondence for every node. Due to the restricted reach, every node can just speak with the nodes close to it. Nodes that can speak with straightforwardly are viewed as neighbors a node monitors are broadcasting a “HELLO” message [34]. A Route Request (RREQ) message is sent when a node needs to make an impression on another node that isn't its neighbor. The RREQ message contains a few crucial bits of information, including the source, destination, message life expectancy, and a sequence number that fills in an unusual ID.

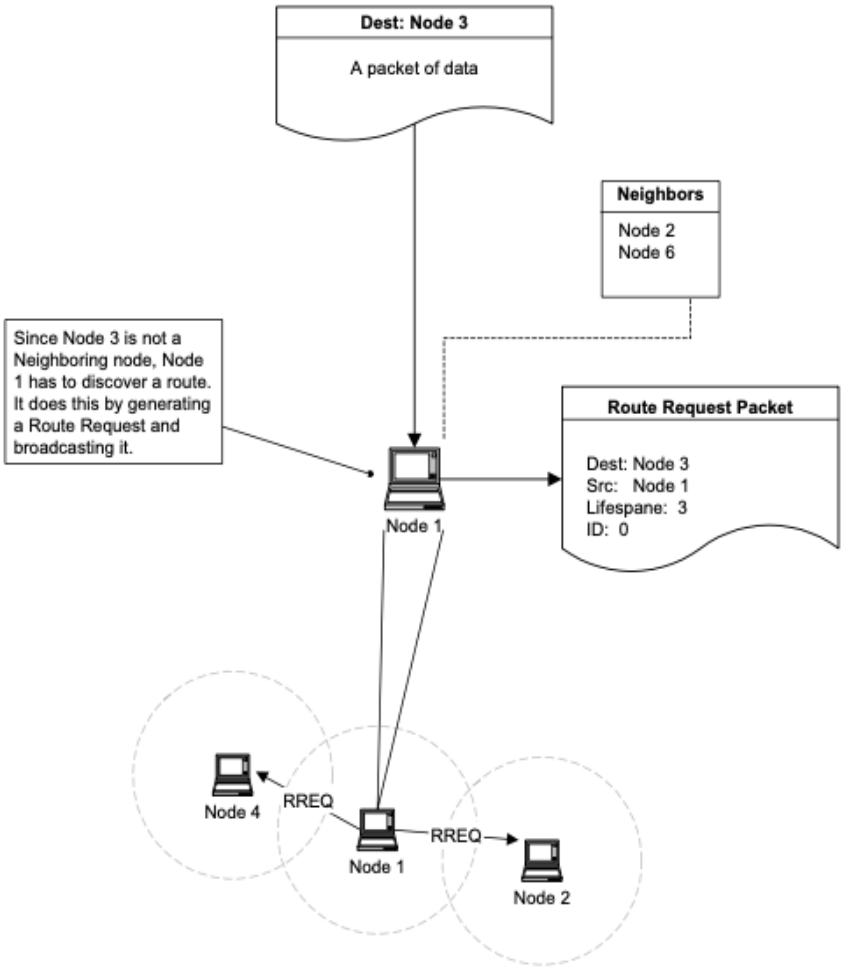

Figure 2: RREQ in AODV

Node 1 wants to send a message to Node 3 as seen in the diagram above. Node 2 and Node 4 are Node 1's neighbours. Node 1 sends an RREQ since it can't interact directly with Node 3. Node 4 and Node 2 both hear the RREQ.

When Node 1's neighbours receive the RREQ message, they have two options: If they are the destination, they can send a Route Reply (RREP) message to Node 1 indicating that the request has been received, or they can replay the (RREQ) until it has reached the end of its life expectancy. Node 1 will rebroadcast the request if it does not receive a response within a given amount of time. The RREQ message will have a longer life

expectancy and a new ID number this time. The nodes that are used in the RREQ use the sequence number and do not rebroadcast an RREQ.

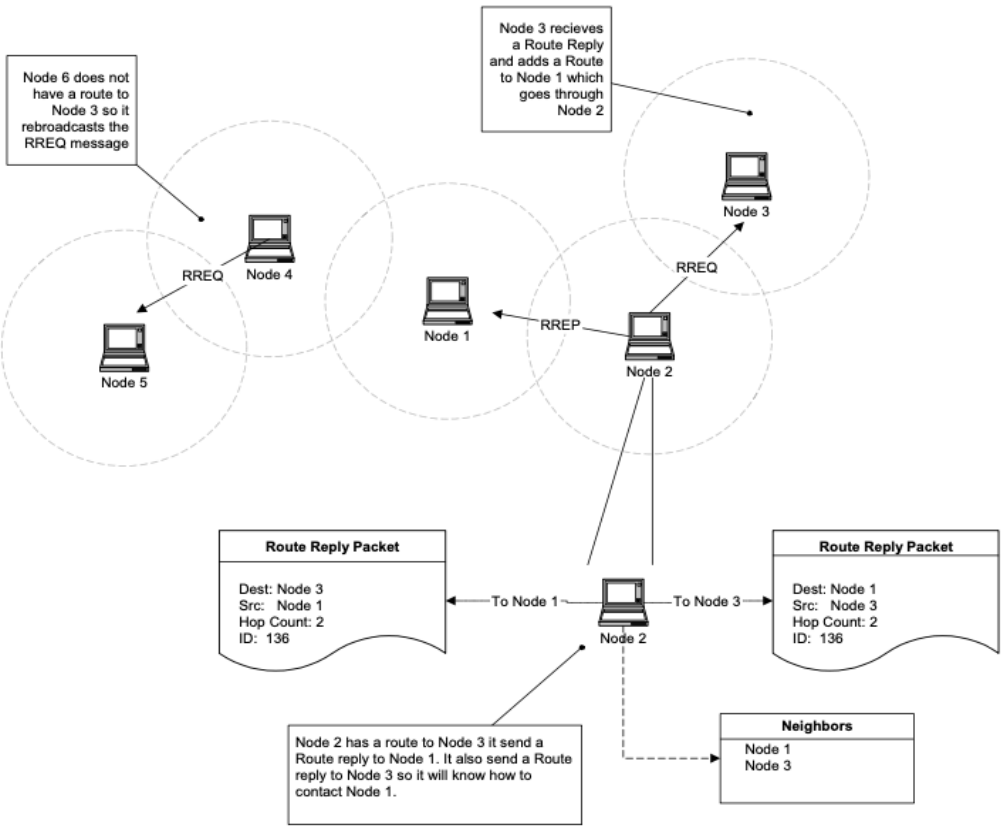

Figure 3: RREP in AODV

Figure 3 depicts how the RREP packet behaves during the procedure. Node 2 has a route to Node 3 and responds to RREQ by sending out an RREP, as shown in the diagram. Because Node 4 does not have a route to Node 3, it must rebroadcast the RREQ. Time stamps are provided by sequence numbers. They let nodes to determine how "fresh" their data is on each node. Every time a node sends a message, it increases its own sequence number. Every node keeps track of the sequence number of the vast number of different nodes connecting with one another. A newer packet has a higher sequence number. It is possible for distinct nodes to figure out which is which using this concept.

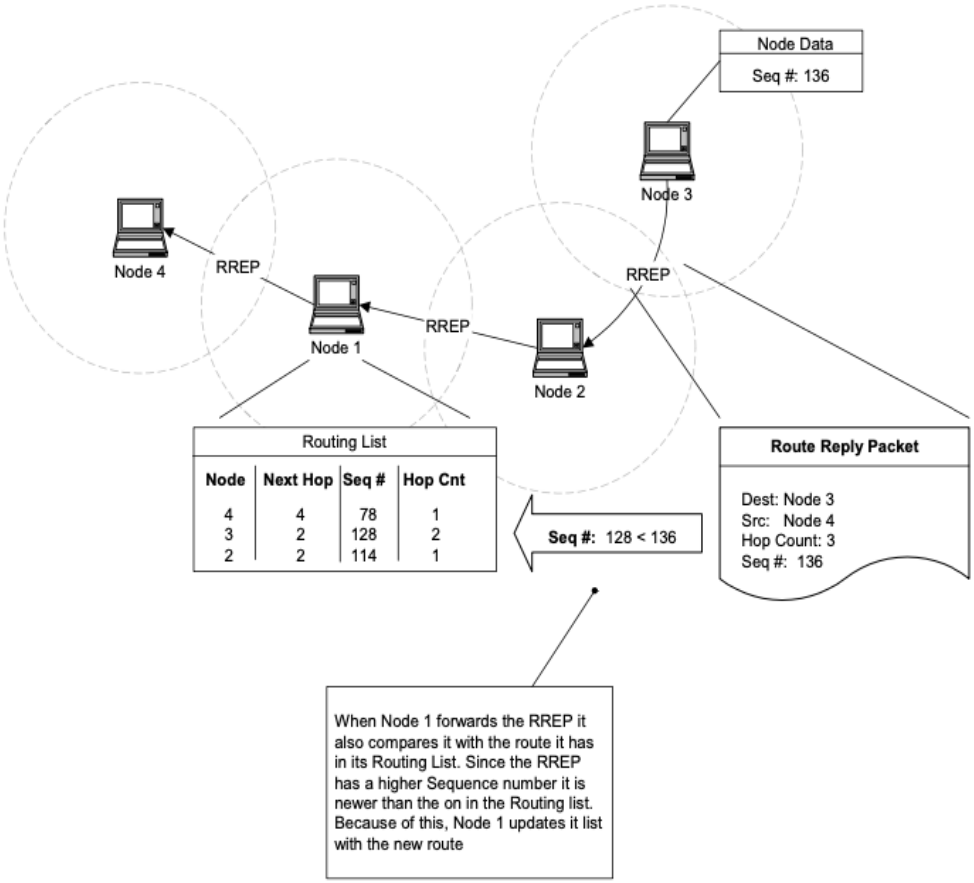

Figure 4: Sequence Numbers in AODV

Node 1 forwards an RREP to Node 4 as seen in Figure 4. It recognizes that the RREP route has a higher sequence number than the routing list route. The route in the Route Reply is then replaced by Node 1's current route.

4.1.2 Proactive or Table-Driven Routing Protocols

Proactive routing protocols [34] can likewise be said as table-driven routing protocols, which are utilized to keep up with the routing table protocol. The location of the nodes is intermittently refreshed in the routing tables of all through nodes in the network. The nodes send a “Hello” message intermittently to refresh the network table. The best benefit of utilizing proactive convention is that it has quick packet routing and great dependability in packet conveyance.

Moreover, sending control messages periodically will help the nodes to maintain all the updated information about the routing table. Every node in proactive routing protocol keeps the data routing tables, and if any progression happens in the network, the table should be refreshed. The table should be refreshed regularly to mirror the network geography or topology changes. These types of protocols cause more overhead particularly in the network as they share the routing information with the neighbors. Nonetheless, movement of the route will be constantly accessible when required.

Some of the sample of proactive routing protocols can be listed as:

- Destination-Sequenced Distance Vector (DSDV)
- Wireless Routing Protocol (WRP)
- Optimal Link-State Routing (OLSR)

4.1.2.1 DSDV

DSDV is a type of table-driven routing protocol requiring every node to intermittently communicate directing updates. Table-driven calculations are based on Bellman-Ford algorithm. Every node in the network keeps a routing table that has entries for every one of the destinations, and the number hops needed to arrive at every one of them. Every section has a grouping number related with it. This instrument permits the protocol stay away from the development of loops. Every node occasionally sends refreshes labeled all through the network with a monotonically expanding even succession number to promote its area. This information contains the location of the objective, the quantity of bounces to arrive at the objective and the succession number of the data got with respect to the objective. At this point when the neighbors of the communicating node get this update, they perceive that they are one jump away from

the source node and remember this data for their distance vectors. Each node stores the “following directing jump” for each reachable objective in their routing table. At the point when a neighbor B of A discovers that A is not reachable, it promotes the sequence to A with a package’s measurement, and a sequence number one more prominent than the most recent for compelling any nodes with B on the way to A.

4.1.2.2 OLSR

OLSR is like Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) which picks an allotted switch on each associate and perform flooding of topology information. Using “Hello” messages, nodes discover 2-bounce neighbor information and plays out a scattered arrangement of a lot of multipoint moves (MPRs) [32]. Nodes select MPRs with the ultimate objectives that there exists a way to all of its 2-bounce neighbor through a center picked as an MPR. These MPR centers then stores and forward messages that contain the MPR selectors. This working of MPRs makes OLSR epic from other association state coordinating shows several different ways. The sending way for messages isn’t split between all center points yet contrasts depending upon the source.

4.1.3 Hybrid Routing Protocol

Hybrid routing protocol combines both dominance of reactive and proactive routing algorithm. They establish connection using proactive route and then serves sequentially for the demand of some active nodes. Correspondence between nodes in various territories will just depend on the started source that was set up at the beginning. The protocol provides good features of reactive and proactive protocols. Zone routing protocol (ZRP), Hazy-Sighted link state routing protocol (HSLS) can be given as an example.

4.1.3.1 ZRP

ZRP can be said as the type of hybrid routing protocol that uses both proactive and reactive routing protocols when sending the data in the network. The ZRP structure is intended to join between the differentiating proactive and reactive methodologies. ZRP utilizes a proactive system for node revelation inside direct neighborhood nodes, while zone correspondence is performed utilizing reactive [33]. The size of a zone (region) is described by the number K which represent the number to arrive the zone edge. The directing zone of every node is a part of network, where all nodes inside a distance not exactly or equivalent to K bounces are reachable.

Each routing protocol has its own advantages and disadvantages. Besides, they all have some security issues and some solutions for these security concerns. The related work about these issues and solutions is discussed in the next chapter of the thesis.

4.2 Security Overview

An important contribution on security overview MANETs stated that, security is the principal pressure for the major accessibility of the network. Availability of the network, and uprightness of the information can be promoted by ensuring that security issues have been met. Network often encounter the evil impacts of a couple of safety attacks because of it features like changes in their topology.

It is the new emerging development that engages customers to speak without wired network to their geological territory, that is the explanation it is currently alluded to as less framework network. The fundamental issues that worried the atmosphere of MANETs are said to be as follows:

- Peer to peer architecture
- No centralized control facilities

- Adversary inside network
- No predefined boundary
- Changing scale

Peer-to-peer architecture is said to be one of the fundamental vulnerabilities in MANETs [32]. Wired networks are devoted to switches, however, for the MANETs, every one of the nodes will accept the obligation of going about as the switch to advance the packet starting with one node then onto the next. For wireless networks, there are no limitations of wireless channel association. It's both accessible network to the clients and outsider specialists. Due to the availability to every network, user, and malicious attackers, it made the atmosphere of MANETs face many challenges in networks concerning information security system (ISS). In view of this explanation, there is no way from guard in MANETs concerning security plan point of view. The limit becomes obscured that is utilized to isolate inside the network from the external organization. So, there is not very much characterized foundation to convey a single security arrangement over MANETs.

Furthermore, no centralized control facilities are also one of the most important issues and challenges when discussing the problems that are related to MANETs. MANETs do not have any unified control facility which may prompt numerous security issues. It ends up with difficulty to recognize and distinguish any attack. Traffic can’t be seen from an essential issue rather the control is moving at each node. The recognizable pieces of proof may become more inconvenient because a node failure may be identified from the adversary or network issues. Because of the absence of a secure network, we can’t understand which node to be trusted and untrusted.

Additionally, adversary inside the network shows that nodes can openly join and disconnect with the network at every period. This will make the nodes behave maliciously and it will be hard and difficult to distinguish the conduct of the nodes which is influenced by destructive attacks. This kind of attack is one of the most dangerous compared to the external attacks. Because, an external attack refers to the risk outside of the network node in which it will attempt to exploit the framework weaknesses using malignant programming infections, interruptions, hacking, social designing, and harm.

Likewise, there is no predefined boundary in MANETs. Therefore, we can't indisputably characterize the actual cutoff of the network. The nodes work in a wandering environment where they are allowed to join and leave the wireless network. At the point when the attacker comes in the wireless extent of a node, it will have the choice to talk with that node. The attacks incorporate the accompanying:

- Eavesdropping impersonation
- Tempering reply
- Denial of service (DOS) attack

Along the lines of changing scale, the adaptability of MANETs keeps evolving continually. It's difficult to expect the number of nodes in MANETs at some future time. This requires the routing protocol in MANETs to be made practical to this developing scalability.

In light of the security information system, MANETs are more compromised and vulnerable especially at the end devices, because of the weak protection. An attacker can enter into the network and create a very weak link to make effects in the security

network administrations. However, there are some solutions the security concerns in MANETs. The characteristics of security solutions in MANETs can be categorized as follows:

- The solution to the security in MANETs should be implemented in individual components, to give aggregate insurance and security to the whole network.
- By using all of the security components like prevention, detection, and reaction.
- By making the security moderate just as in commonsense asset imperatives and dynamic situation network.
- By applying the application, transport, network, link, and physical layer stack protocols. By applying them to the security, they will help to understand the attacks and which layer has to take the responsibility to rectify the problem efficiently.
- Be careful with insider and outsider threats. The security solution should take the responsibility of avoiding the attacks by insiders and outsiders. The particular reasons for circumstances are that according to the insider attacks it ought to stay away from any assaults from the remote and organization geography while the instance of insider assaults is just for the intruder which works as the third-party when the two nodes are communicating to each other. So, it will get access and compromised to gain many pieces of knowledge from a different network.

To show the various methods of keeping MANETs away from any attacks and intrusions, we need to arrange the protocols of MANETs first. In reactive approach, the route must be analyzed on-demand and choose among different routes detected.

This has similar overheads of route processes compared to the proacting routing protocol. Just a modest quantity of power and bandwidths are consumed in this process. Much delay will happen to wait to receive RREPs to analyze the process. Discussing about the disadvantages of using this process include respective of data for maintenance and slow reaction on restructuring and failures.

In proactive approach, protocols are responsible for the update of the routing information periodically to other different nodes that are available in the network. Sending packet is quicker in proactive routing protocols. One of the most disadvantages of using such protocols is the high overhead. There are various benefits and weaknesses in proactive approaches:

- Multipoint Relaying: When a device sends “Hello” messages, every node in the process will send “Hello” packets to each other. After all, it will generate order to overcome the retransmission multipoint mechanisms. This process of multipoint relaying will also help to restrict other nodes that have regular time intervals, by sending the new broadcast bundles to check for the association among its neighbors.
- Link or neighbor sensing: It is a mechanism that is linked together and have a relationship among each other, which use in sending a "Hello" packet. This will create a network among each of the nodes. In MANETs, this is the same way of sending "Hello" packets to create a relationship among the nodes.
- Link state messaging and route calculation: There are three different categories which includes multiple relay selection, forwarding of traffic and link state functionality. For multiple relay selection, all of the nodes have to maintain multiple relay procedures to run for the process. Originally, multiple relaying

selectors are used to forward a route, so that is the reason it's smarter to be utilized to forward link-state information (LSI). This is the reason why multiple relaying selectors have been used to send link-state messages due to this way, size will likewise be decline which is valuable in connecting state messages.

Furthermore, we understand that there is a guarantee for different transferring ways before sending sequences, so those nodes who select the most handing-offs are liable for finishing join state messages (JSM). The selected nodes in the interface state technique must transmit a connection state message to the network, which is referred to as a topology control message (TC). Because it sends messages to the nodes and then establishes connections between the center points, TC plays a significant role in the development of a network.

We have many types of attacks in MANET which broadly classified depend on the protocol used: active/passive and internal/external attacks. The classification is very useful because the attacker can exploit in the network either as active attacks, passive attacks, internal attacks, or external attacks.

In active attacks, the content of the data packet is changed actively by an attacker node. An attacker node may likewise stream some false data to the network [34]. There are various active attacks which could be done at different layers.

Attacks at application layer include:

- Repudiation attack: This occurs due to deny of contribution.

- Attacks by virus and worm: Viruses and worms infect the application system, operating system, or application software installed on mobile devices to carry out attacks.

Attacks at the transport layer include:

- TCP SYN attack: It is a Denial of Service (DOS) in nature which legitimate users not to get the service of the network when an attack occurs.
- TCP session hijacking: After the attacker steals sensitive information that is being transferred, the attacker spoofs the IP address of the victim node to hijack the TCP connection.
- Jellyfish attack: The attacker must first gain access to the forwarding group, after which it must delay the data packets unduly before transmitting them.

Attacks at network layer include:

- Flooding attack: An attacker depletes network resources, such as bandwidth and battery power, in order to disrupt routing and decrease network performance.
- Route tracking: This type of attack is used to retrieve sensitive data that has been sent through multiple intermediate nodes.
- Message Fabricate Modification (MFM): In this type of attack, a bogus stream of messages is added to the information being communicated, and the information is altered in some way.
- Blackhole attack: The attacker node broadcasts bogus routing information into the network, claiming to have found the best path, causing other good nodes to transfer data packets to the malicious one [30].

- Wormhole attack: Among other things, this is one of the most hazardous attacks. A pair of collaborating attackers' records packets at one site and replays them at a different location over a secret high-speed network in this attack [29]. For example, let's say we have two nodes A1 and A2 which are linked through connection. Every node of the packets which is received from A1 will forward to another node in which another malicious does not exist. So, these two nodes will trade the data and afterward create traffic among one another. The traffic between the two nodes will go through the wormhole among another network. Because of this cycle, it will violet the progression of the directing parcels. These sorts of assaults are exceptionally difficult to identify in a network and it very well may be the reason that harms the entirety of the organizations [40]. The best way to keep away from this sort of assault is by utilizing packet which is used to confirm and approve the circumstance data measure.
- Link spoofing attack: To disrupt routing processes, a rogue node will promote bogus linkages with non-neighbors. With a target's two-hop neighbors, an attacker can broadcast a bogus link.

Attacks at link layer include:

- Media Access Control (MAC) DOS attack: At the link layer, Typically, there is only one channel that is frequently used. Keeping the channel busy around a particular node causes a denial of service at the node, which drains the node's battery life and results in a DOS assault.

- Traffic monitoring and analysis: This is a passive type of attack in nature; however, an attacker performs this type of analysis to determine what type of communication is taking place.
- Bandwidth stealth: Due to network congestion, the attacker node illegally steals a significant portion of the bandwidth.
- MAC targeted attack: Every piece of data that is shared between numerous nodes relies on the MAC layer to ensure that the data is collected efficiently and effectively and delivered to its intended destination.

Attacks at physical layer include:

- Jamming attack: A DOS attack on the physical layer is also possible. A jammer attack is an example. Radio transmission messages can be lost or damaged as a result of jamming and interference.
- Compromised attack: These are caused by compromised entities or stolen devices, such as the physical capture of a MANET node.
- Malicious Message injection: The attacker injects fake streams into the legitimate message streams that are being routed through intermediate nodes. The attacker disrupts the network's functionality due to a malicious message.
- Eavesdropping attack: This type of attack occurs when unwanted receivers view messages and chats. MANET nodes share wireless media and wireless communication, and they broadcast nature using RF spectrum, which can be easily intercepted with receivers tuned to the right frequency.

On the other hand, internal attacks refer to the attacker that needs to have a typical admittance to the network so that to take part in an ordinary movement of the network.

The invader will try to acquire access to the network as a new node by either compromising a current node in the network or threatening mime, and then it will begin its poisonous direct. External attacks are less authentic and dangerous than inside attacks [31].

However, external attacks are mostly outside the network that needs to gain admittance to the network what's more. When they acquire induction to the network, they start sending counterfeit bundles. This reduces the execution of the whole network environment. These sorts of attacks can be halted by executing security endeavors like firewall, where the passage of unapproved individuals to the network association can be lightened.

As it is mentioned above, there are several types of attacks and security concerns in MANETs. However, there are also some solutions to these security issues. The following list defines the main security solution in MANETs:

- By securing the routing: MANETs have several attacks that are easily damaging the network completely. Because of this, we must discuss some solutions that will work on the mobile nodes that is negotiated in the network [39]. One of the crucial difficulties is to get the switch, to give credibility, and reliability in the network. The responsibility of securing the router include:
    - Encrypting your network with a strong passphrase
    - Changing all the default passwords
    - Use your mobile to find your router's gateway (IP address)
    - Access advanced network settings in the preferences of a network you are connected to
    - Find security settings in your router’s firmware

- By securing the multicasting: In MANETs, all of the nodes may become neighbors in multicasting groups and send/receive traffic. Due to this, it might end in a DOS attack. The design that is utilized to get the multicast traffic is distributed policy enforcement architecture (DIPLOMA).
- Privacy awareness: It represents the security mindfulness which is not entrenched in the writing. Thus, as a beginning point, we present the understandings of protection, which are contemplated for this work. After the idea of mindfulness is presented, we give a meaning of privacy mindfulness.
- Intrusion detection system: It is a network security instrument that can be an equipment gadget or programming that ceaselessly screens an organization network for pernicious movement and makes a move to forestall it, including announcing, hindering, or dropping it when it happens.
- Multi-layer intrusion detection technique: In multi-layer intrusion detection, there are two general approaches to the process which are anomaly detection and misuse detection.

After considering the security issues and solutions in MANETS, simulations were performed to compare some of the proactive and reactive MANET routing protocols, in terms of packet delivery ratio, average end-to-end delay and throughput. The results of these simulations and discussion can be found in the next chapter.

Chapter 5

SIMULATION RESULTS AND DISCUSSION

In order to compare some of the proactive and reactive routing protocols in terms of packet delivery ratio (PDR), average end-to-end delay (EED) and throughput, simulations were performed in this study. AODV, DSDV and OLSR MANETs routing protocols were used in these simulations. Simulation parameters are as shown in Table 1.

Table 1: Simulation parameters

Simulation time	200 seconds
Area	300m×1500m
Node placement	Random
Mobility pattern	Random way point
Speed	72km/h
Pause time	5, 10, 15, 20, 25, 30, 35, 40, 45, 50
Application	CBR
Packet size	uniform distribution 64 bytes
Number of nodes	25, 50, 100
Simulator	NS-3.33
MAC layer protocol	IEEE 802.11

The following is an explanation of the above parameters:

- Simulation Time: The NS-3 simulator's default simulation time is 200 seconds.
- Simulation Area: 300m*1500m was also used because it was the default simulation area.
- Node placement: The nodes are put at random because, prior to network startup, most people choose node positions based on metrics that are independent of the network state or presume a set network operation pattern that remains constant during the network's lifetime.
- Mobility pattern: Because numerous data models have been suggested in the database field to offer unique querying facilities over collections of moving objects, the mobility pattern: random way point is used. The emphasis on the geometric features of trajectories is a common aspect of most of these models.
- Speed: Because the velocity of the node within the simulation area is 72k/h, we selected that as our default speed.
- Pause Time: 5, 10, 15, 20, 25, 30, 35, 40, 45, 50 are utilized, so that to see the effective in the results. Normally, it will stop at every pause time and then continue moving.
- Application: Constant bit rate (CBR) is used, which is an encoding method that maintains the bitrate constant. This is done since variable bit rate (VBR) can vary, so CBR is used.
- Packet Size: The data flow is modeled as a CBR through User Diagram Protocol (UDP), where each packet size is 64 bytes.
- Number of Nodes: 25, 50 and 100 are used, so that to see the effective difference in the result.

- Simulator: The Ns-3 network simulator is used, and it was created to provide an open, extensible network simulation platform for networking research and education. In a nutshell, ns-3 provides models of how packet data networks work and perform, as well as a simulation engine that allows users to run simulations.
- MAC Layer Protocol: The Media Access Control (MAC) data communication networks protocol sub-layer, also known as the Medium Access Control, is a sub-layer of the seven-layer OSI model's data link layer.

5.1 Evaluation Criteria

5.1.1 PDR

The ratio of the packets that are effectively conveyed to a destination contrasted with the total number of packets that have been conveyed by the sender.

5.1.2 EED

This is the time taken for a packet to cross from a transmitter to a receiver. It plays an important role about influencing the user's fulfillment with the application. It incorporates catching, digitizing, encoding/compacting media information, transporting them from the source to the destination, and showing them to the client.

5.1.3 Average Throughput

It is the all-out payload over the whole meeting partitioned by the total time. Total time is determined by taking the distinction in timestamps between the first and last packet. The duration of the throughput normally starts with the transmission of first packet to the last packet.

5.2 Simulation Results and Analysis

As it is represented in Table 1, in the simulations conducted with AODV, DSDV and OLSR routing protocols, 25, 50 and 100 nodes; 5, 10, 15, 20, 25, 30, 35, 40, 45 and 50

seconds pause time were used. The change in PDR, EED and average throughput is displayed with respect to the changing pause times in the simulation results. The simulation results for PDR with AODV routing protocol is as shown in Figure 5. As it can be seen from the figure, as the number of nodes increases, PDR also increases. The simulation area will be more crowded as the number of nodes increases and whenever a link breakage occurs, it will be easier to establish the route again through other nodes. On the other hand, PDR seems stable as the pause time increases, for all number of nodes.

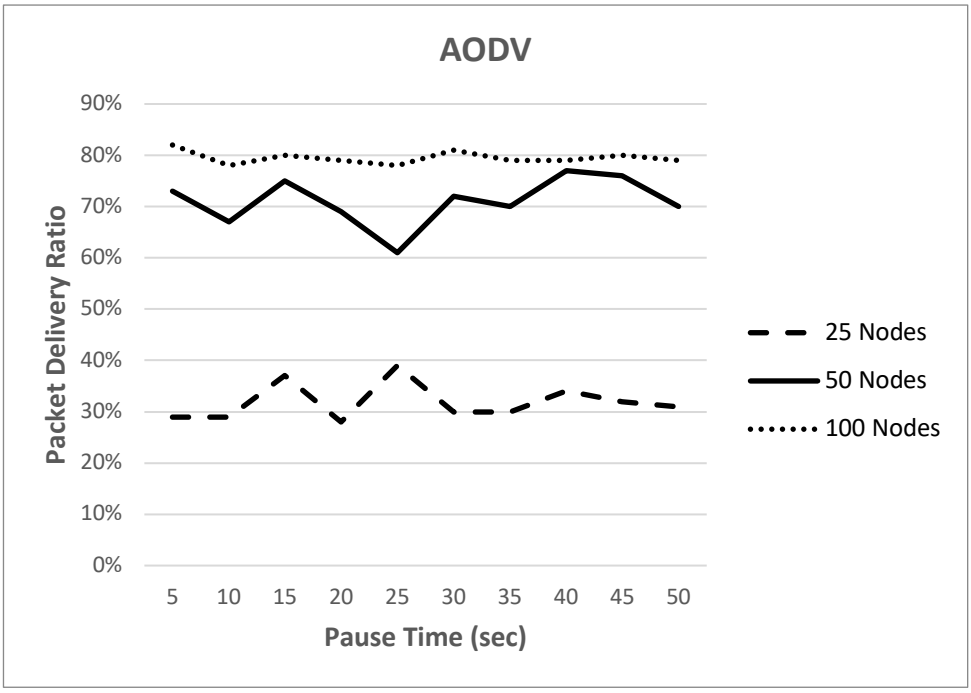

Figure 5: PDR with AODV

On the other hand, as the number of nodes increases, since there will be a greater number of nodes on the route with more packet processing time, it is expected for EED to increase. But this phenomenon is not observed from Figure 6. Average EED is minimum for 100 nodes. It is more for 25 nodes and the highest for 50 nodes. As it is mentioned above, PDR is the highest for 100 nodes. This means, maximum number of

packets are delivered with 100 nodes from source to destination. Once we consider the success rate also, it seems it is acceptable for 100 nodes to have the smallest EED. In addition to this, delay may change dramatically according to the number of nodes on the route. The source and destination nodes are selected completely randomly in the simulations and therefore delay may vary from the expectations.

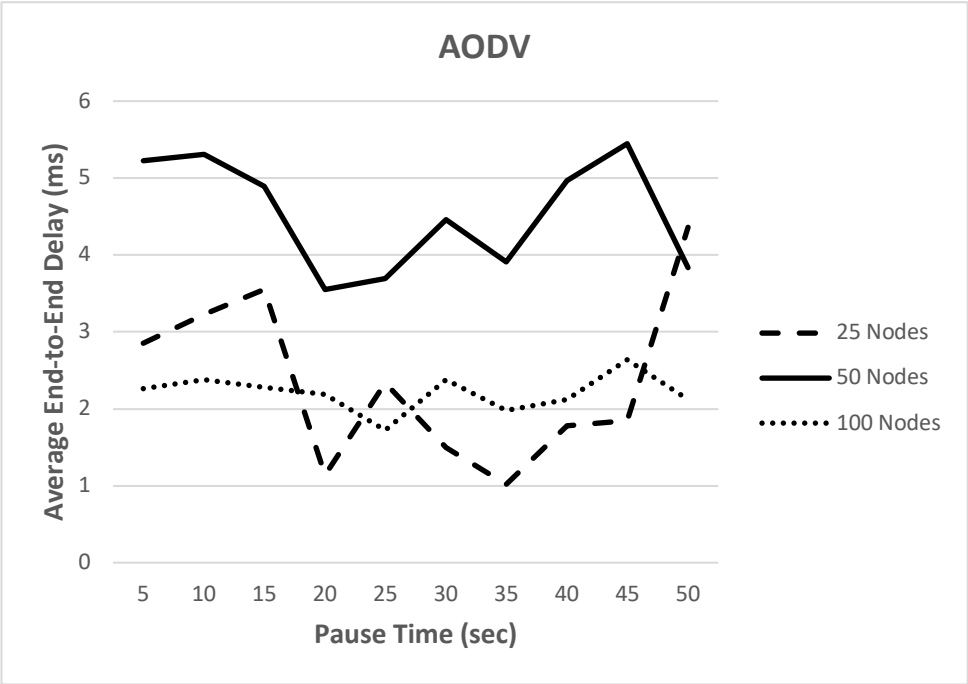

Figure 6: EED with AODV

The average throughput obtained with AODV for 25, 50 and 100 nodes is as shown in Figure 7. As it can be seen from the figure, throughput increases as the number of nodes decreases. Throughput of a network is also related to the amount of resources used in a network. Although PDR is minimum for 25 nodes, since there is the smaller number of nodes which means less number of resources in the network, the utilization of these limited resources will be higher. Therefore, maximum throughput is obtained for 25 nodes. On the other hand, although PDR is the highest with 100 nodes, since

the amount of utilized resources in the network is low, throughput is the lowest among the others.

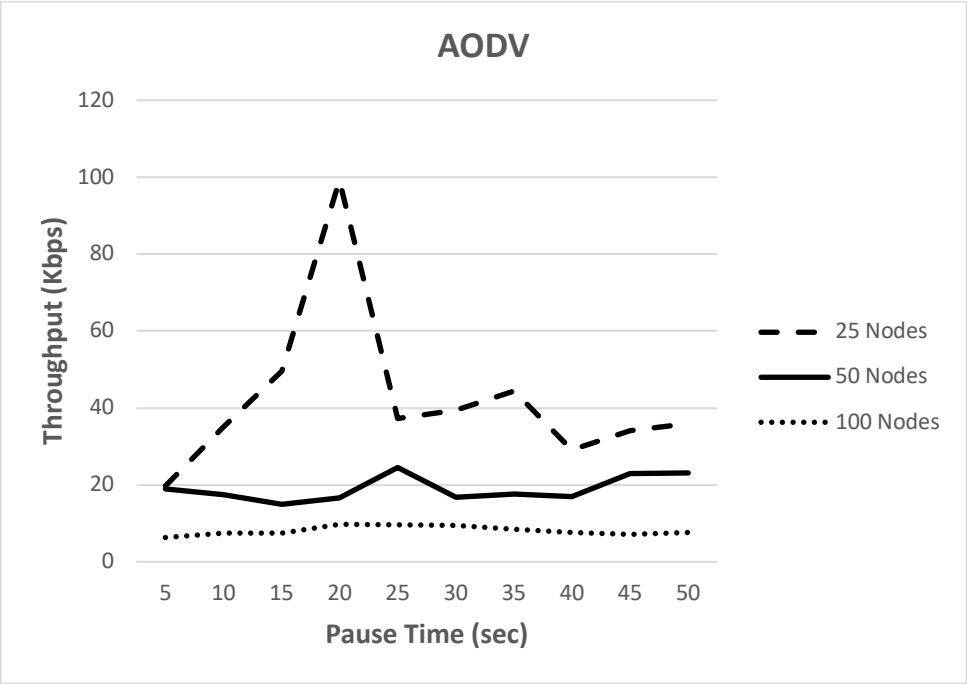

Figure 7: Average Throughput with AODV

The simulation results for PDR with DSDV routing protocol is as shown in Figure 8. As it can be seen from the figure, as the number of nodes increases, PDR also increases. The simulation area will be more crowded as the number of nodes increases and whenever a link breakage occurs, it will be easier to establish the route again through other nodes. On the other hand, PDR seems stable as the pause time increases, for all number of nodes.

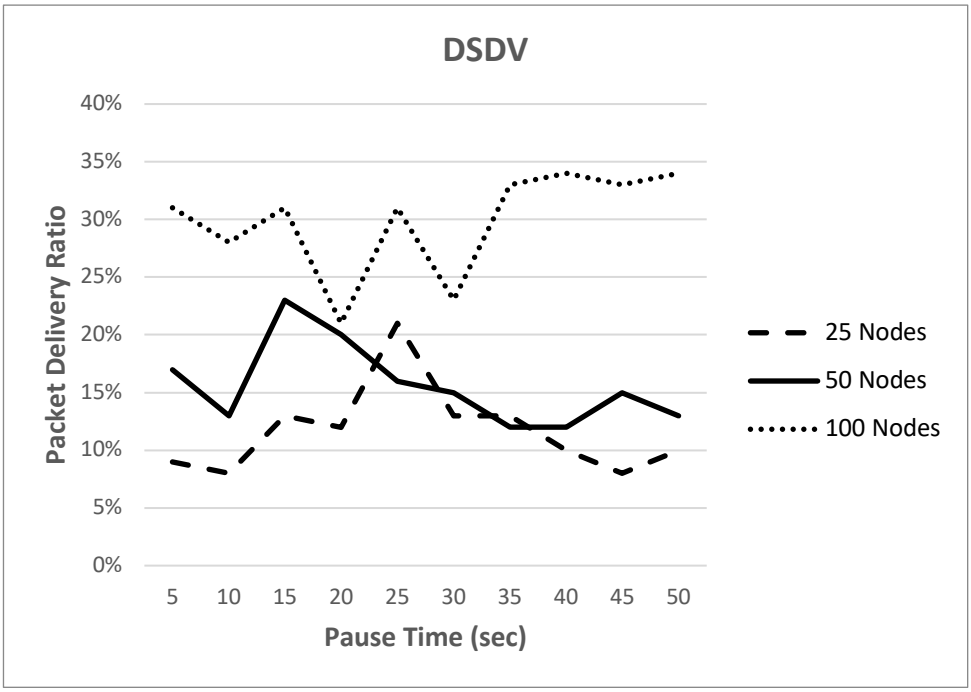

Figure 8: PDR with DSDV

Average EED with DSDV can be seen in Figure 9. Although it may not be very clear to see it, once the average of all values is taken for 25, 50 and 100 nodes, the highest EED will be obtained for 100 nodes and lowest for 25 nodes with DSDV. This could be the result of utilizing proactive approach. The next node is already known by a node and there is no need to trigger an on-demand route request. So, as the number of nodes increases, EED increases as it could be expected.

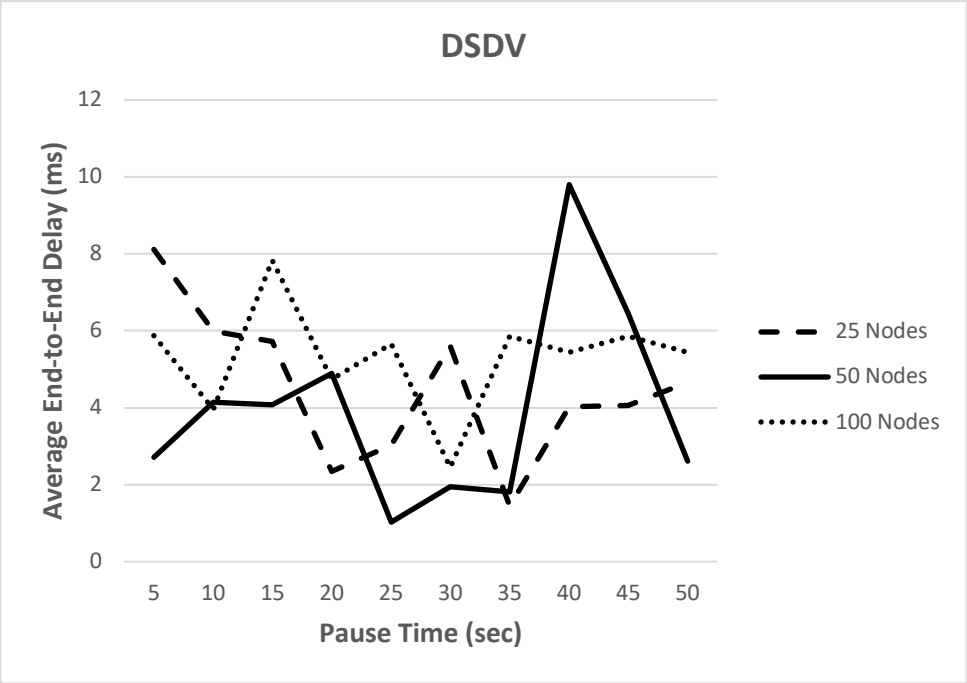

Figure 9: Average EED with DSDV

Average throughput, which is the total payload of the entire session over the total pause time, is also considered for DSDV in the simulations. As it can be seen from Figure 10, throughput is the highest for 100 nodes. PDR is also the highest for 100 nodes with DSDV. Since proactive routing protocol is utilized, highest PDR generated the highest throughput in the network.

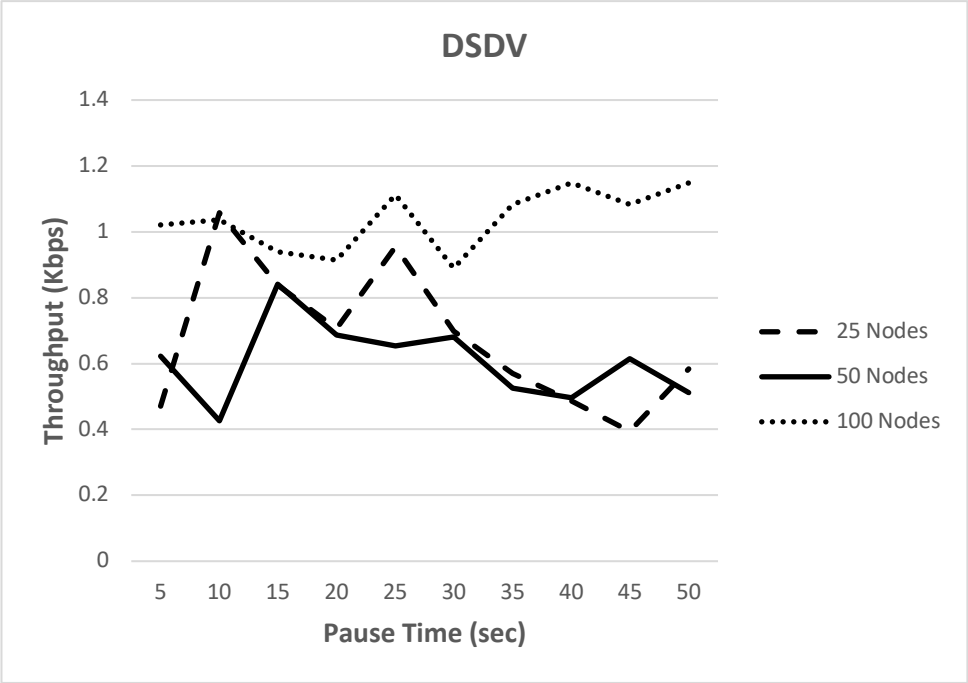

Figure 10: Average Throughput with DSDV

In the classical OLSR hop-by-hop routing is used, which means when a packet reaches an intermediate node, the protocol will check the routing table of the local node and then forward the packet to the next hop which exactly can be seen from figure 11. The higher the number of the nodes, the lower the PDR obtained.

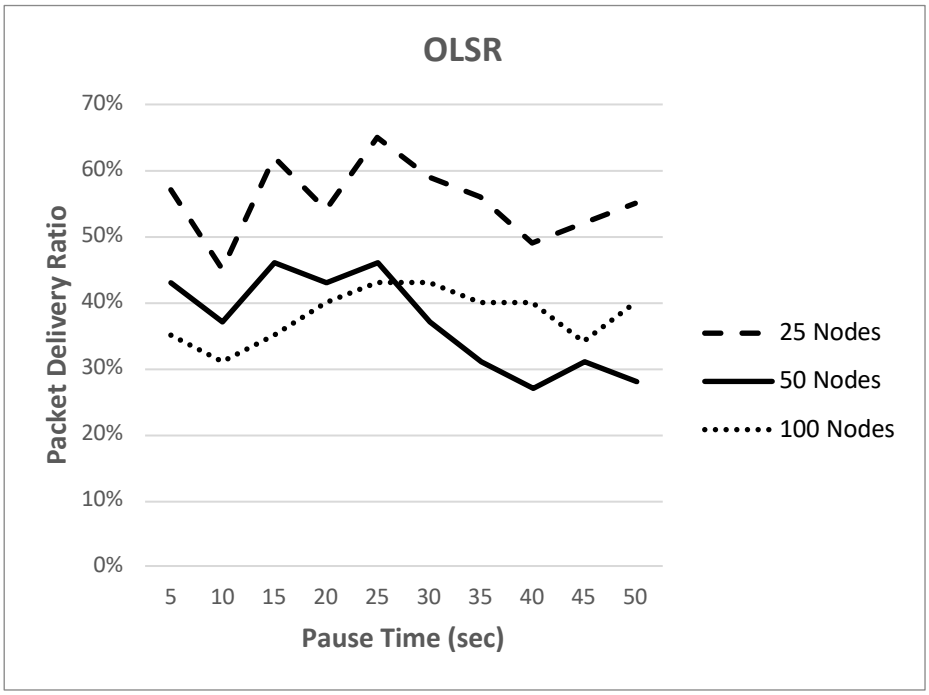

Figure 11: PDR with OLSR

Average EED with OLSR can be seen in Figure 12. As it can be seen from the figure, minimum EED is obtained for 100 nodes. Although PDR is not high for 100 nodes, this means for those packets that are delivered from source to destination, it took less time than the other scenarios with 25 and 50 nodes.

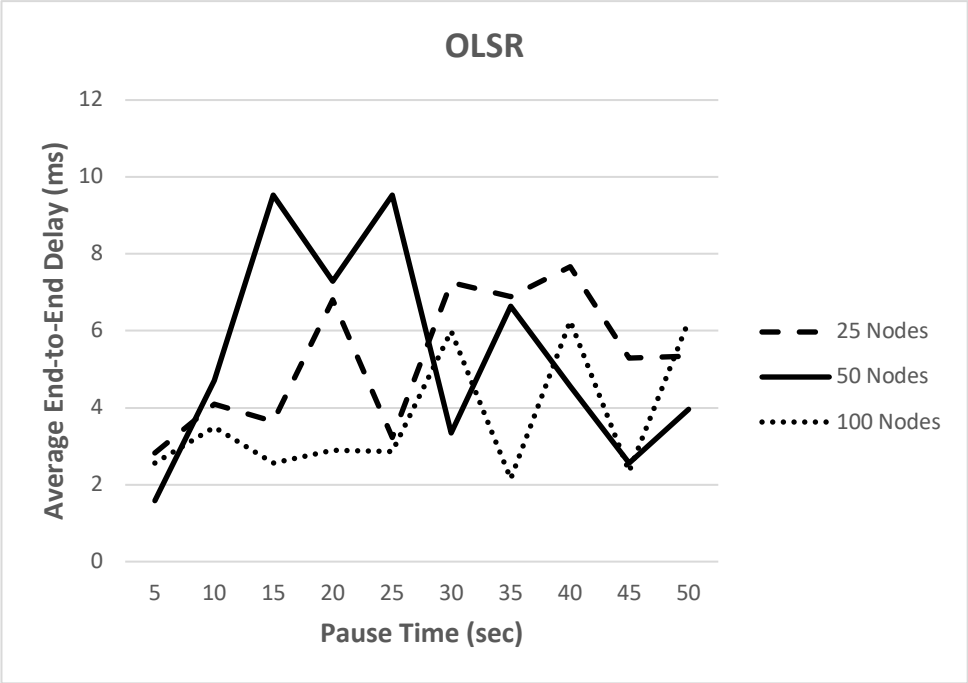

Figure 12: EED with OLSR

Throughput is also observed with OLSR as shown in Figure 13. As the figure suggests, the results represents exactly the same characteristics with PDR in Figure 12. If PDR is high, throughput is also high. This means, the network resources are utilized well while delivering the packets to the destination nodes.

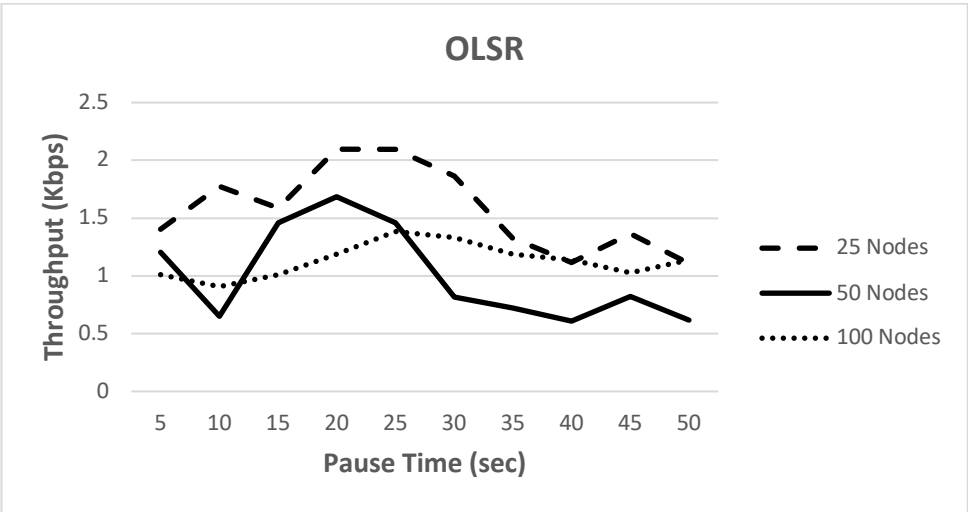

Figure 13: Average Throughput with OLSR

PDR and throughput for 100 nodes obtained by different MANET routing protocols is shown in Figure 14 and Figure 15. As it can be seen from these figures, AODV performs much better than DSDV and OLSR in terms of PDR and throughput. AODV is a reactive protocol which means the route will be established once the source node needs to send a packet to a destination node. Consequently, the route will be established according to the current status of the nodes and network topology. Therefore, the success rate is higher. On the other hand, for proactive protocols, the routing tables are populated and kept ready for data transmission. When there is a need to send a packet, an entry in the table could be used immediately. But the selected next node, although it could be used to forward the packet, might not be the most feasible node on the route to destination. So, as the results suggests, PDR and throughput are worse for proactive protocols when compared with AODV.

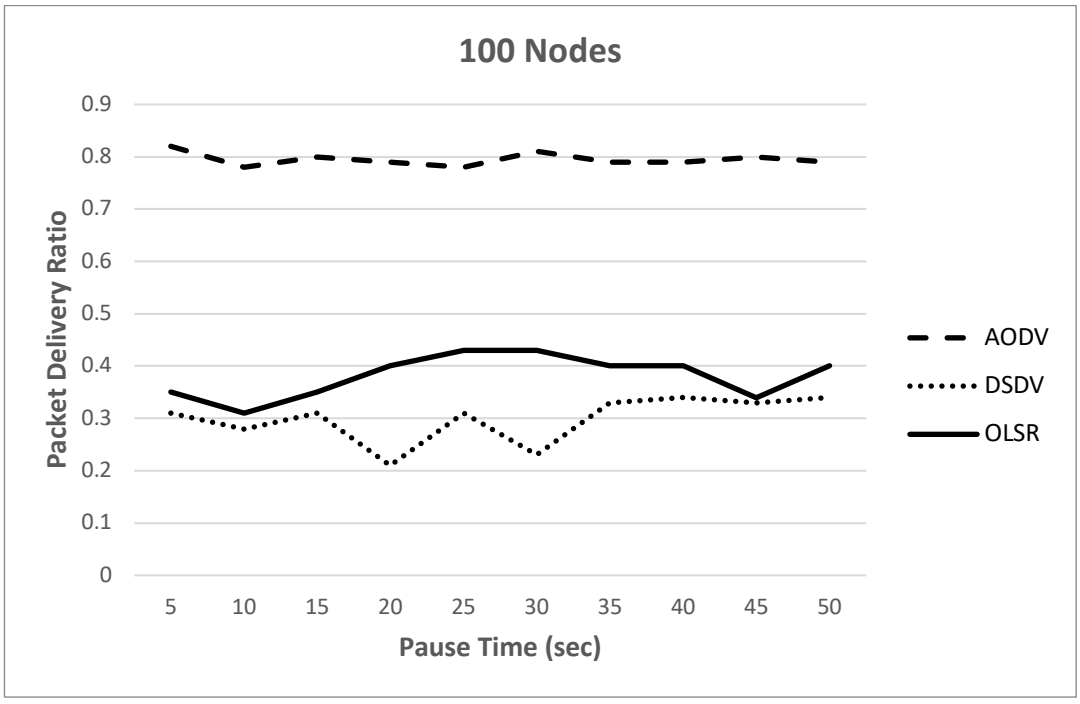

Figure 14: PDR for 100 Nodes

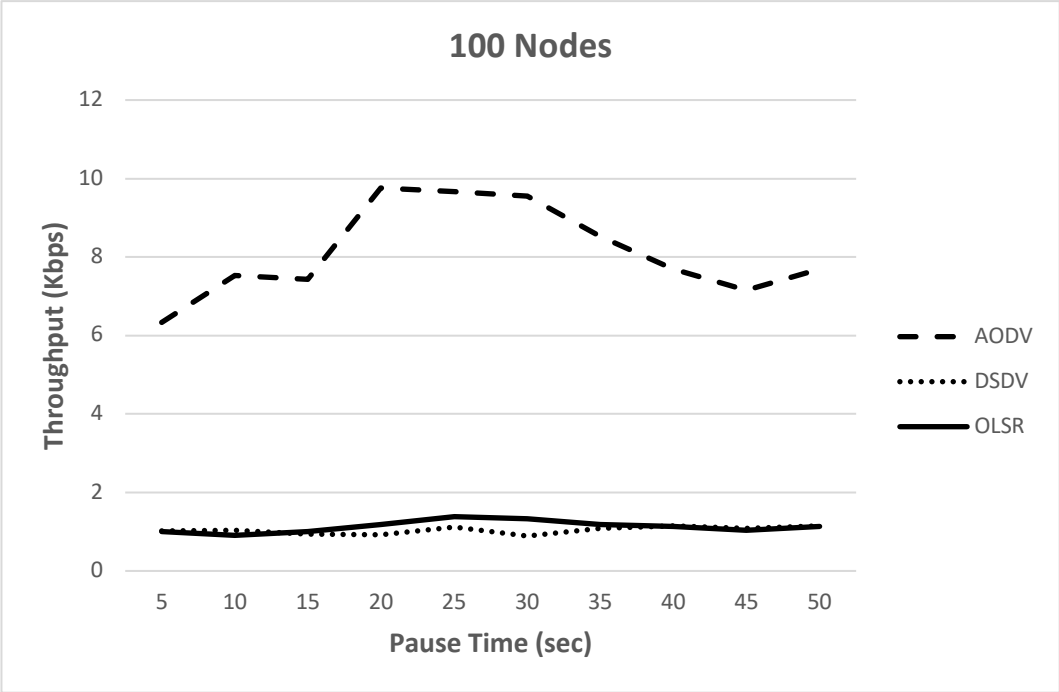

Figure 15: Throughput for 100 Nodes

Chapter 6

CONCLUSION

Academics holds somehow related opinion regarding the security, problems and issues in MANETs. During this study, the concept of MANETs and types of attacks were investigated. MANETs have the capacity to continuously configure infrastructure mobile networks. Security is mainly the warrior for the essential usefulness of the network. By ensuring that security issues have been addressed, network services can be made available, as well as the integrity and confidentiality of data. Because of properties such as open medium, dynamic topology change, and a lack of monitoring and management, MANETs are routinely subjected to a variety of security assaults.

MANETs is the new arising innovation which empowers clients to communicate with no actual wired network to their topographical area that is the reason it is now referred to as infrastructure network.

Analysis among AODV, DSDV and OLSR routing protocols were done with some simulation results. It has been seen that AODV which is a reactive MANETs routing protocol, outperforms the proactive DSDV and OLSR routing protocols in terms of PDR and throughput.

6.1 Future Work

Simulations could be performed in order to identify the security issues in MANETs as a future work of this study.

REFERENCES

[1] Al-Omari, S. A. K., & Sumari, P. (2010). An overview of mobile ad hoc networks for the existing protocols and applications. *arXiv preprint arXiv:1003.3565*.

[2] Bhatt, D., & AGRAwAL, B. I. J. E. N. D. R. A. (2017). Major challenges of mobile adhoc networks. *Orient. J. Comput. Sci. Technol.: Int. Open Access Peer Rev. Res. J*, *10*(2), 417-421.

[3] Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In Mobile computing (pp. 153-181). *Springer, Boston, MA*.

[4] Zaslavsky, A., & Tari, Z. (1998). Mobile computing: Overview and current status. *Journal of Research and Practice in Information Technology*, 30(2), 42-52.

[5] Senthilkumar, P., Baskar, M., & Saravanan, K. (2011). A study on mobile ad-hock networks (manets). *JMS, (1), 28.*

[6] Frodigh, M., Johansson, P., & Larsson, P. (2000). Wireless ad hoc networking: the art of networking without a network. *Ericsson review, 4(4), 249.*

[7] Hoebeke, J., Moerman, I., Dhoedt, B., & Demeester, P. (2004). An overview of mobile ad hoc networks: applications and challenges. *Journal-Communications Network*, 3(3), 60-66.

[8] Bang, A. O., & Ramteke, P. L. (2013). MANET: history, challenges and applications. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 2(9), 249-251.

[9] Thomson, C., Wadhaj, I., Tan, Z., & Al-Dubai, A. (2019). Mobility aware duty cycling algorithm (MADCAL) a dynamic communication threshold for mobile sink in wireless sensor network. *Sensors*, 19(22), 4930.

[10] IEEE Computer Society LAN MAN Standards Committee. (1999). Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *ANSI/IEEE* Std. 802.11-1999.

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

[12] Sarkar, S. K., Basavaraju, T. G., & Puttamadappa, C. (2007). Ad hoc mobile wireless networks: principles, protocols and applications. *Auerbach publications*.

[13] Haas, Z. J., Deng, J., Liang, B., Papadimitratos, P., & Sajama, S. (2003). Wireless ad hoc networks. *Wiley Encyclopedia of Telecommunications*.

[14] Hoebeke, J., Moerman, I., Dhoedt, B., & Demeester, P. (2004). An overview of mobile ad hoc networks: applications and challenges. *Journal-Communications Network,* 3(3), 60-66.

[15] Kumar, M., & Mishra, R. (2012). An overview of MANET: History, challenges and applications. *Indian Journal of Computer Science and Engineering (IJCSE)*, 3(1), 121-125.

[16] Roy, B., Banik, S., Dey, P., Sanyal, S., & Chaki, N. (2012). Ant colony based routing for mobile ad-hoc networks towards improved quality of services. *Journal of Emerging Trends in Computing and Information Sciences,* 3(1), 10-14.

[17] Freebersyser, J. A., & Leiner, B. (2001). A DoD perspective on mobile ad hoc networks. *In Ad hoc networking* (pp. 29-51).

[18] Biswas, K., & Ali, M. (2007). Security threats in mobile ad hoc network.

[19] Pequeño, G. A., & Rivera, J. R. (2007). Extension to MAC 802.11 for performance Improvement in MANET.

[20] Lu, S., Li, L., Lam, K. Y., & Jia, L. (2009, December). SAODV: a MANET routing protocol that can withstand black hole attack. In 2009 *international conference on computational intelligence and security* (Vol. 2, pp. 421-425). *IEEE*.

[21] Bhatt, D., & AGRAwAL, B. I. J. E. N. D. R. A. (2017). Major challenges of mobile adhoc networks. *Orient. J. Comput. Sci. Technol.: Int. Open Access Peer Rev. Res. J,* 10(2), 417-421.

[22] Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., & Weil, T. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE communications surveys & tutorials, 13(4), 584-616.*

[23] Song, J. H., Hong, F., & Zhang, Y. (2006, December). Notice of Violation of IEEE Publication Principles: Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks. In 2006 *Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06) (pp. 497-502). IEEE.*

[24] Thomson, C., Wadhaj, I., Tan, Z., & Al-Dubai, A. (2019). Mobility aware duty cycling algorithm (MADCAL) a dynamic communication threshold for mobile sink in wireless sensor network. *Sensors*, 19(22), 4930.

[25] Gorantala, K. (2006). Routing protocols in mobile ad-hoc networks. *A Master'thesis in computer science*, pp-1-36.

[26] Mittal, S., & Kaur, P. (2009, December). Performance Comparison of AODV, DSR and ZRP Routing Protocols in MANET's. In 2009 *international conference on advances in computing, control, and telecommunication technologies (pp. 165-168). IEEE.*

[27] Bitam, S., Mellouk, A., & Zeadally, S. (2013). HyBR: A hybrid bio-inspired bee swarm routing protocol for safety applications in vehicular ad hoc networks (VANETs). *Journal of Systems Architecture*, 59(10), 953-967.

[28] Mittal, S., & Kaur, P. (2009, December). Performance Comparison of AODV, DSR and ZRP Routing Protocols in MANET's. In 2009 *international conference on advances in computing, control, and telecommunication technologies* (pp. 165-168). *IEEE*.

[29] Song, J. H., Hong, F., & Zhang, Y. (2006, December). Notice of Violation of IEEE Publication Principles: Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks. In 2006 *Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06) (pp. 497-502). IEEE.*

[30] Zapata, M. G., & Asokan, N. (2002, September). Securing ad hoc routing protocols. *In Proceedings of the 1st ACM workshop on Wireless security* (pp. 1-10).

[31] Ramanathan, R., & Redi, J. (2002). A brief overview of ad hoc networks: challenges and directions. *IEEE communications Magazine*, 40(5), 20-22.

[32] Chlamtac, I., Conti, M., & Liu, J. J. N. (2003). Mobile ad hoc networking: imperatives and challenges. *Ad hoc networks*, 1(1), 13-64.

[33] Hoebeke, J., Moerman, I., Dhoedt, B., & Demeester, P. (2004). An overview of mobile ad hoc networks: applications and challenges. *Journal-Communications Network*, 3(3), 60-66.

[34] Gagandeep, A., & Kumar, P. (2012). Analysis of different security attacks in MANETs on protocol stack A-review. *International Journal of Engineering and Advanced Technology (IJEAT)*, 1(5), 269-75.

[35] Bhatt, D., & AGRAwAL, B. I. J. E. N. D. R. A. (2017). Major challenges of mobile adhoc networks. Orient. J. Comput. Sci. Technol.: *Int. Open Access Peer Rev. Res. J,* 10(2), 417-421.

[36] Al-Maashri, A., & Ould-Khaoua, M. (2006, November). Performance analysis of MANET routing protocols in the presence of self-similar traffic. In Proceedings. 2006 31st *IEEE Conference on Local Computer Networks* (pp. 801-807). IEEE.

[37] Freebersyser, J. A., & Leiner, B. (2001). A DoD perspective on mobile ad hoc networks. *In Ad hoc networking* (pp. 29-51).

[38] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer networks*, 38(4), 393-422.

[39] Schollmeier, R., Gruber, I., & Finkenzeller, M. (2002, May). Routing in mobile ad-hoc and peer-to-peer networks a comparison. *In International Conference on Research in Networking* (pp. 172-187). *Springer, Berlin, Heidelberg*.

[40] Mittal, S., & Kaur, P. (2009, December). Performance Comparison of AODV, DSR and ZRP Routing Protocols in MANET's. In 2009 *international conference on advances in computing, control, and telecommunication technologies* (pp. 165-168). *IEEE*.

[41] Zhang, Z., Pazzi, R. W., & Boukerche, A. (2010). A mobility management scheme for wireless mesh networks based on a hybrid routing protocol. *Computer Networks,* 54(4), 558-572.