Comparison based Performance Analysis of CBR and TCP Traffic under AODV Routing Protocol in MANET

A thesis report submitted to the Department of Electrical and Electronic Engineering, Khulna University of Engineering & Technology in partial fulfillment of the requirements for the degree of

BACHELOR OF SCIENCE IN ELECTRICAL & ELECTRONIC ENGINEERING

by

Miraz Uz Zaman
0903010

Supervised by

Dr. Mohammad Shaifur Rahman
Professor, Dept. of EEE

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
KHULNA UNIVERSITY OF ENGINEERING & TECHNOLOGY

September 2014

Declaration of Authorship

I, Miraz Uz Zaman, declare that this thesis titled, '**Comparison based Performance Analysis of CBR and TCP Traffic under AODV Routing Protocol in MANET**' and the work presented in it at my own. I confirm that this work was done wholly or mainly at this University. Any part of this thesis has previously not been submitted for a degree or any other qualification at this University or any other institution. I have clearly quoted the published work of others which have been consulted in this thesis. I also have acknowledged all main sources of help.

Signed: _____

Date: _____

Abstract

Ad-hoc networking is a concept in computer communication which means that user want to communicate with each other form a temporary network, without any form of centralized administration. For this purpose, a routing protocol is needed. For mobile ad-hoc network (MANET) and other wireless ad-hoc network AODV is the most popular routing protocol. Because AODV is capable of both unicast and multicast routing. It is an on demand algorithm, loop-free, self-starting, and scales to large numbers of mobile nodes. The transmission of information in a MANET relies on the performance of the traffic scenario (application traffic agent and data traffic) used in a network. The traffic scenario determines the reliability and capability of information transmission, which necessitates its performance analysis. The objective of this thesis is to compare the performance of TCP/FTP and UDP/CBR traffic in AODV routing protocol generally implemented in a mobile ad hoc environment. An empirical study has been done using NS-2. Exhaustive simulations have been done to analyze results, which are evaluated for performance metrics, such as throughput, packet delivery ratio, average end to end delay and average routing load. The effect of variations in simulation time, number of nodes, and speed of mobile nodes on the network performance is analyzed over a wide range of their values. It is observed that the TCP/FTP offers a far better performance for throughput than UDP/CBR; in case of PDR, former offers an almost constant trend, whereas the latter shows highly varying (rising and falling) trends in all the three aforementioned scenarios. The average end to end delay of latter is lesser than former. The results follow these trends over a wide range of simulation parameters..

MANETs are highly vulnerable to attacks due to their inherent characteristics like lack of infrastructure and complexity of wireless communication. Security is an essential requirement in mobile ad-hoc networks. The black hole attack is one of the well-known security threats in wireless mobile ad-hoc networks. In this thesis paper a simple detection and prevention technique for black hole attack have been proposed.

Acknowledgements

At first I would like to express my deep gratitude to Almighty Allah. It is a pleasure to express amenity to all those people who provided me help and support throughout this thesis course.

I would like to express my very great appreciation to Dr. Mohammad Shaifur Rahman, Professor, Department of Electrical and Electronic Engineering, Khulna University of Engineering & Technology (KUET), Khulna, Bangladesh for his valuable and constructive suggestions during the planning and development of this thesis work. His willingness to give his time so generously has been very much appreciated.

Contents

List of Figures

List of Tables

Abbreviations

ALOHA	**A**bramson's **L**ogic of **H**iring **A**ccess
AODV	**A**d-hoc **O**n demand **D**istance **V**ector
CBQ	**C**lass **B**ased for **Q**ueueing
CBR	**C**onstant **B**it for **R**ate
DARPA	**D**efense **A**dvanced **R**esearch **P**rojects **A**gency
DSR	**D**ynamic **S**ource **R**outing
DSDV	**D**estination **S**equence **D**istance **V**ector
FTP	**F**ile **T**ransfer **P**rotocol
IP	**I**nternet **P**rotocol
MANET	**M**obile **A**d hoc **Net**work
NAM	**N**etwork **A**ni**m**ator
OLSR	**O**ptimized **L**ink **S**tate **R**outing protocol
OTCL	**O**bjective **T**ool **C**ommand **L**anguage
RREP	**R**oute **Rep**ly
RREQ	**R**oute **Req**uest
SEAD	**S**ecure **E**fficient **A**d hoc **D**istance vector routing protocol
TCL	**T**ool **C**ommand **L**anguage
TORA	**T**emporarily **O**rdered **R**outing **P**rotocol
TCP	**T**ransmission **C**ontrol **P**rotocol
UDP	**U**ser **D**atagram **P**rotocol
VINT	**V**irtual **I**nter **N**etwork **T**estbed
WLAN	**W**ireless **L**ocal **A**rea **N**etwork
WRP	**W**ireless **R**outing **P**rotocol
WSN	**W**ireless **S**ensor **N**etwork

Dedicated to my beloved Parents...

Chapter 1

Introduction

1.1 Inauguration

In todays fast and rapidly growing world of technologies, more and more businesses understand the advantages of usage of computer networking. Today, many people carry numerous portable devices, such as laptops, mobile phones, PDAs and mp3 players, for use in their professional and private lives. For the most part, these devices are used separately that is, their applications do not interact. Imagine, however, if they could interact directly: participants at a meeting could share documents or presentations; business cards would automatically find their way into the address register on a laptop and the number register on a mobile phone; as commuters exit a train, their laptops could remain online; likewise, incoming email could now be diverted to their PDAs; finally, as they enter the office, all communication could automatically be routed through the wireless corporate campus network. These examples of spontaneous, ad-hoc wireless communication between devices might be loosely defined as a scheme, often referred to as ad hoc networking, which allows devices to establish communication, anytime and anywhere without the aid of a central infrastructure. Actually, ad-hoc networking as such is not new, but the setting, usage and players are. In the past, the notion of ad-hoc networks was often associated with communication on combat fields and at the site of a disaster area; now, as novel technologies such as Bluetooth materialize, the scenario of ad-hoc networking is likely to change, as is its importance.

So,a wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data [1].

1.2 Motivation

The objective of this thesis is to compare the performance of TCP/FTP and UDP/CBR traffic in AODV routing protocol generally implemented in a mobile ad hoc environment. An empirical study has been done using NS-2. Exhaustive simulations have been done to analyze results, which are evaluated for performance metrics, such as throughput, packet delivery ratio and average end to end delay. The effect of variations in simulation time, number of nodes, number of connection and speed of mobile nodes on the network performance is analyzed over a wide range of their values. To see how this two connection will work out in malicious environment, malicious node have added in AODV routing protocol. Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Another important motivation of this thesis is to give a solution about Black-hole attack in MANET. Black-hole is one of the most threaten attack in MANET. In this thesis paper a simple solution will be presented.

1.3 Thesis Framework

Chapter 2 narrates literature review on comparison base performance analysis of CBR and TCP connection on AODV and different mitigation technique of black-hole attack. This chapter also narrates Ad-hoc network, classification of ad-hoc network and brief description on mobile ad-hoc network. By the end of this chapter importance of this thesis will figure out.

Chapter 3. In this chapter describes classification of routing protocol, general description on different types of routing protocol and a brief discussion on Data traffic types.

Chapter 4 the simulation tool called NS2 is introduced and adding of malicious node is also described.

Chapter 5 outlines different types of attack in mobile ad-hoc network. A new routing protocol is proposed which detects and mitigates black hole attack.

Chapter 6 holds the brief discussion about the simulation results and analysis.

Chapter 7 describes conclusion and future work.

Chapter 2

Literature Review

2.1 Background

A Mobile Ad Hoc Network (MANET) is a wireless network comprising wireless mobile nodes communicating with one another for some ad hoc purpose. In such networks, there is no fixed infrastructure available; therefore, they are well suited for the infrastructure less environments. In such scenarios, MANETs features like mobile nodes, abruptly changing topology, no physical network boundary, communication with the nodes within wireless range, support the need of communication. In a mobile ad hoc network, nodes move arbitrarily, therefore the network may experience rapid and unpredictable topology changes. Routing paths in MANETs potentially contain multiple hops, and every node in MANET has the responsibility to act as a router. The MANET imposes several challenges for communication, out of which one of the important challenges is to provide secure and efficient routing of data in the network which can ensure efficient and secure routes for communication. The transmission of information in a MANET relies on the performance of the traffic scenario (application traffic agent and data traffic) used in a network. The traffic scenario determines the reliability and capability of information transmission, which necessitates its performance analysis. So its need to analyze and compare the performance between constant bit rate (CBR) and transmission control protocol (TCP) in AODV.

As AODV routing protocol is anticipated to offer a range of flexible services to mobile and nomadic users by means of integrated homogeneous architecture. So there are some limitations in MANET they are energy constrained node, low channel bandwidth, node mobility, high channel error rates, channel variability and packet loss. The security of the AODV protocol will be threatened by malicious node which is due to those limitations. So its important to analyze the behavior of AODV protocol under malicious environment. The security of the AODV protocol is compromised by a particular type of attack called Black Hole attack. Black hole attack is one of the security threat in which the traffic is redirected to such a node that

actually does not exist in the network. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. In this thesis, an effective solution to the black hole attack on AODV protocol have proposed.

2.2 Related Works

2.2.1 Performance Comparison Over TCP and CBR in AODV

There are different trends of research towards MANET. One of the specific areas of research belongs to the traffic scenario analysis. Here different traffic scenarios that are available for a MANET are analyzed under various conditions. The traffic model is subject to various changing environments to which a MANET is generally prone, and then their effects are studied on various performance metrics to analyze network performance when implemented using AODV routing protocol. In [2] the paper carries out the performance evaluation of an Ad hoc On demand Distance Vector (AODV) routing protocol for Transmission Control Protocol/File Transmission Protocol (TCP/FTP) and User Datagram Protocol/Constant Bit Rate (UDP/CBR) traffic types, subjected to two varying parameters; number of node and mobility. The conclusions are drawn based on performance metrics, such as, throughput, routing overhead, packet delivery ratio, and average end to end delay, to evaluate the performance.

A similar comparison is provided for variable node density and pause time [3, 4, 5]. Researchers have also stressed on comparison between TCP and CBR for different routing protocols [6, 7, 8]. Although various authors in their research have provided a performance based comparative analysis between the two traffic scenarios namely, TCP/FTP and UDP/CBR, a great deal of concatenation is still required to be made in such work too, to provide some more specific results. In this thesis, efforts have been made to compare the performance of TCP/FTP and UDP/CBR under AODV routing protocol, together for most frequent and vulnerable varying parameters to a MANET, like simulation or run time of a network, number or density of mobile nodes, no of connections and speed of mobile nodes. These variations are made on a wide range of their values; exhaustive simulations are done to provide clear trends for performance metrics like, throughput, packet delivery ratio, average routing load and average end-to-end delay. All these parameters forming a simulation environment provides basis to verify various characteristics offered by two aforementioned traffic scenarios. Again in those paper inclusion of malicious node was avoided which one of the important factor for performance degradation in AODV routing protocol.

2.2.2 Prevention Technique of Black-hole attack

Secure ad hoc routing protocol has been proposed as a technique to enhance the security in MANET. In [9], Hu et al. proposed a common key encryption system for Dynamic Source Routing (DSR) [10]. In Secure AODV (SAOV) [11] and Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [12], secure routing protocol using hash functions have been proposed. In [13], Authenticated Routing for Ad hoc Networks (ARAN), anode-based secure routing protocol using public key encryption system is proposed. Hu and Perrig [14] survey the weakness and strength of various secure routing protocols. The above mentioned secure protocols can only guard against external attacks. However, for the internal attacks coming from compromised hosts could still have severe impacts on network performance and its connectivity. Therefore, detecting the internal attack launching from these compromised hosts is indispensable.

Huang et al. [15] propose a method in which the packet flow is observed at each node. In this method, they define a total of 141 features with traffic related and topology related, and suggest anomaly detection means with interrelation between features.

In [16], Huang et al. construct an Extended Finite State Automaton (EFSA) according to the specification of AODV routing protocol; modelize normal state; and detect attacks with both specification based detection and anomaly detection. In specification based detection, they simply detect attacks as deviant packet from condition defined by EFSA. Also, in anomaly detection, they define normal state and compare it with condition of EFSA and amount of statistic of transition, and then detect attacks as a deviation from those states. From the characteristics of the black-hole attack, it needs to take a destination sequence number into account.

In [15], feature related to the destination sequence number has not been taken into account as the feature to define the normal state. In [16], the threshold is used and the feature is defined as the number of time that the destination sequence number is greater than the threshold. However, since a destination sequence number changed depending on the network environment, up to a threshold it may be difficult to successfully discriminate between the normal state and the state where black-hole attack took place. And hence cause degradation in detection accuracy.

2.3 Opportunities of Thesis

In this recent trends of research in MANET for both Performance comparison over TCP and CBR in AODV And mitigation technique of AODV there are some great scope of research. Efforts have given in this thesis to meet above requirement. List of the opportunities of thesis

a. To compare the performance of TCP/FTP and UDP/CBR under AODV routing protocol, together for most usual and vulnerable varying parameters to a MANET.

b. To compare the performance of TCP/FTP and UDP/CBR under AODV routing protocol by creating malicious node with different scenario.

c. To propose a simple mitigation technique by taking account destination sequence number.

2.4 Wireless Ad-hoc Network

A wireless ad-hoc network is a collection of mobile/semi-mobile nodes with no pre-established infrastructure, forming a temporary network. Each of the nodes has a wireless interface [18] and communicate with each other over either radio or infrared. Laptop computers and personal digital assistants that communicate directly with each other are some examples of nodes in an ad-hoc network. Nodes in the ad-hoc network are often mobile, but can also consist of stationary nodes, such as access points to the Internet. Semi mobile nodes can be used to deploy relay points in areas where relay points might be needed temporarily. Wireless networking is an emerging technology that allows users to access information and services electronically, regardless of their geographic position [19].

2.4.1 History of Wireless Ad-hoc Network

The roots of ad-hoc networking can be traced back as far as 1968, when work on the ALOHA network was initiated (the objective of this network was to connect educational facilities in Hawaii). [20] Although fixed stations were employed, the ALOHA protocol lent itself to distributed channel access management and hence provided a basis for the subsequent development of distributed channel-access schemes that were suitable for ad-hoc networking. The ALOHA protocol itself was a single-hop protocol that is, it did not inherently support routing. Instead every node had to be within reach of all other participating nodes. Inspired by the ALOHA network and the early development of fixed network packet switching, DARPA began work, in 1973, on the PR net (packet radio network) a multi-hop network. [21] In this context, multi-hopping means that nodes cooperated to relay traffic on behalf of one another to reach distant stations that would otherwise have been out of range. PR net provided mechanisms for managing operation centrally as well as on a distributed basis. As an additional benefit, it was realized that multi-hopping techniques increased network capacity, since the spatial domain could be reused for concurrent but physically separate multi-hop sessions. Although many experimental packet radio networks were later developed, these wireless systems did not ever really take off in the consumer segment. When developing IEEE 802.11-a standard for wireless local area networks (WLAN) the Institute of Electrical and Electronic Engineering (IEEE) replaced the term packet-radio network with ad-hoc network. Packet-radio networks had come to be associated with the multi-hop networks of large-scale military or rescue operations, and by adopting a new name, the IEEE hoped to indicate an entirely new deployment scenario.

Today, vision of ad-hoc networking includes scenarios where people carry devices that can network on an ad hoc basis. A users devices can both interconnect with one another and connect to local information points for example, in airport user can retrieve update on flight departures, gate changes, and so on. The ad hoc devices can also relay traffic between devices that are out of range.

2.4.2 Classification of Wireless Ad-hoc Network

Wireless networks can be classified in three types:

2.4.2.1 Infrastructure Network

Infrastructure network consists of a network with fixed and wired gateways. A mobile host communicates with a bridge in the network (called base station) within its communication radius. The mobile unit can move geographically while it is communicating. When it goes out of range of one base station, it connects with new base station and starts communicating through it. This is called handoff. In this approach the base stations are fixed [22].

2.4.2.2 Infrastructure less (Ad-hoc) Network

In ad hoc networks all nodes are mobile and can be connected dynamically in an arbitrary manner. All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. Ad hoc networks are very useful in emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrain [23].

2.4.2.3 Mesh Network

It serves as access networks that employ multi-hop wireless forwarding by non-mobile nodes to relay traffic to and from the wired Internet. In such an environment, hybrid technologies and/or hierarchical network organization can be used for ad hoc and infrastructure wireless links.

These three types of network can be depicted in following figure

a. Infrastructure: Cellular wireless networks

b. Ad hoc: Wireless sensor networks

c. Hybrid: Mesh networks

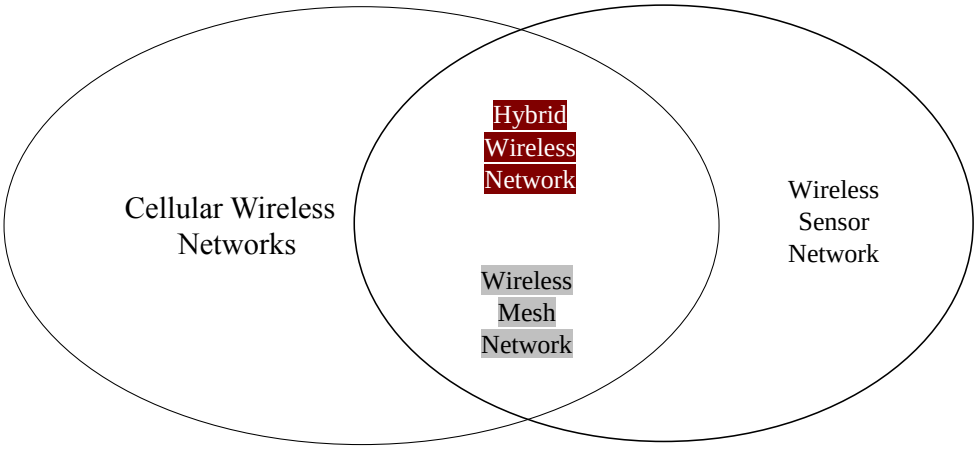


FIGURE 2.1: Types of Wireless Ad-hoc Network

2.4.3 Issues in Wireless Ad-hoc network

There are different issues in wireless ad-hoc network for mechanism. These issues have been depicted here.

a. Medium access scheme

b. Routing

c. Self-Organization

d. Security

e. Link state

f. Distance Vector

g. Source routing

h. Flooding

2.4.4 Pertinence of Wireless Ad-hoc Network

So far, ad hoc networks have only been considered for military applications, where a decentralized network configuration is an operative advantage or even a necessity. In the commercial sector, equipment for wireless, mobile computing has not been available at a price attractive to large markets. However, as the capacity of mobile computers increases steadily, the need for unlimited networking is also expected to rise. Commercial ad-hoc networks could be used in situations where no infrastructure (fixed or cellular) is available. Examples include rescue

operations in remote areas, or when local coverage must be deployed quickly at a remote construction site. Ad hoc networking could also serve as wireless public access in urban areas, providing quick deployment and extended coverage. The access points in networks of this kind could serve as stationary radio relay stations that perform ad-hoc routing among themselves and between user nodes. Some of the access points would also provide gateways via which users might connect to a fixed backbone network [24] At the local level, ad-hoc networks that link notebook or palmtop computers could be used to spread and share information among participants at a conference. They might also be appropriate for application in home networks where devices can communicate directly to exchange information, such as audio/video, alarms, and configuration updates. Perhaps the most far-reaching applications in this context are more or less autonomous networks of interconnected home robots that clean, do dishes, mow the lawn, perform security surveillance, and so on. Some people have even proposed ad hoc multi-hop networks (denoted sensor networks) for example, for environmental monitoring, where the networks could be used to forecast water pollution or to provide early warning of an approaching tsunami. [25] Short-range ad-hoc networks can simplify intercommunication between various mobile devices (such as a cellular phone and a PDA) by forming a PAN, and thereby eliminate the tedious need for cables. This could also extend the mobility provided by the fixed network (that is, mobile IP) to nodes further out in an ad-hoc network domain. The Bluetooth system is perhaps the most promising technology in the context of personal area networking.

2.4.5 Ad-hoc Network vs Mobile Ad-hoc Network

Ad-hoc networks form spontaneously without a need of an infrastructure or centralized controller. This type of peer-to-peer system infers that each node, or user, in the network can act as a data endpoint or intermediate repeater. Thus, all users work together to improve the reliability of network communications. These types of networks are also popularly known to as mesh network because the topology of network communications resembles a mesh. The redundant communication paths provided by ad hoc mesh networks drastically improve fault tolerance for the network. Additionally, the ability for data packets to hop from one user to another effectively extends the network coverage area and provides a solution to overcome non-line of sight (LOS) issues.

Networks because the topology of network communications resembles a mesh. The redundant communication paths provided by ad hoc mesh networks drastically improve fault tolerance for the network. Additionally, the ability for data packets to hop from one user to another effectively extends the network coverage area and provides a solution to overcome non-line of sight (LOS) issues. Mobile applications present additional challenges for mesh networks as changes to the network topology are swift and widespread. Such scenarios require the use of Mobile Ad hoc Networking (MANET) technology to ensure communication routes are updated quickly and accurately. MANETs are self-forming, self-maintained, and self-healing, allowing

for extreme network flexibility. While MANETs can be completely self-contained, they can also be tied to an IP-based global or local network (e.g. Internet or private networks). These are referred to as Hybrid MANETs.

A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links the union of which form a random topology. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human induced disasters, military conflicts, emergency medical situations etc.

Chapter 3

Ad-hoc Routing Protocol & Data Traffic Type

3.1 Ad-hoc Routing Protocol

Mobile ad hoc networks (MANET) are networks which routing is based on multi-hop routing from a source to a destination node or nodes. These networks have quite a many constrains because of uncertainty of radio interface and its limitations e.g. in available bandwidth. Also some terminals have limitations concerning battery energy in use. There are numerous applicable protocols for ad hoc networks, but one confusing problem is the vast number of separate protocols. Each of these protocols is designed to perform its task as well as it is possible according to its design criteria. The protocol to be chosen must cover all states of a specified network and never is allowed to consume too much network resources by protocol overhead traffic. A key issue is the necessity that the Routing Protocol must be able to respond rapidly to the topological changes in the network. In these networks, each node must be capable of acting as a router. As a result of limited bandwidth of nodes, the source and destination may have to communicate via intermediate nodes [26]. Major problems in routing are Asymmetric links, Routing Overhead, Interference, and Dynamic Topology.

3.1.1 Classification of Routing Protocols

The Routing Protocols for ad hoc wireless networks can be divided into three categories based on the routing information update mechanism. They could be Reactive (On-demand), Proactive (Table-driven) or Hybrid. Figure 2 shows the three categories of Ad hoc routing protocols and various proposed Protocols under each category [27, 28, 29].

The table-driven ad hoc routing approach is similar to the connectionless approach of forwarding packets, with no regard to when and how frequently such routes are desired. This is not the

case, however, for on-demand routing protocols. When a node using an on-demand protocol desires a route to a new destination, it will have to wait until such a route can be discovered. On the other hand, because routing information is constantly propagated and maintained in table-driven routing protocols, a route to every other node in the ad hoc network is always available, regardless of whether or not it is needed.

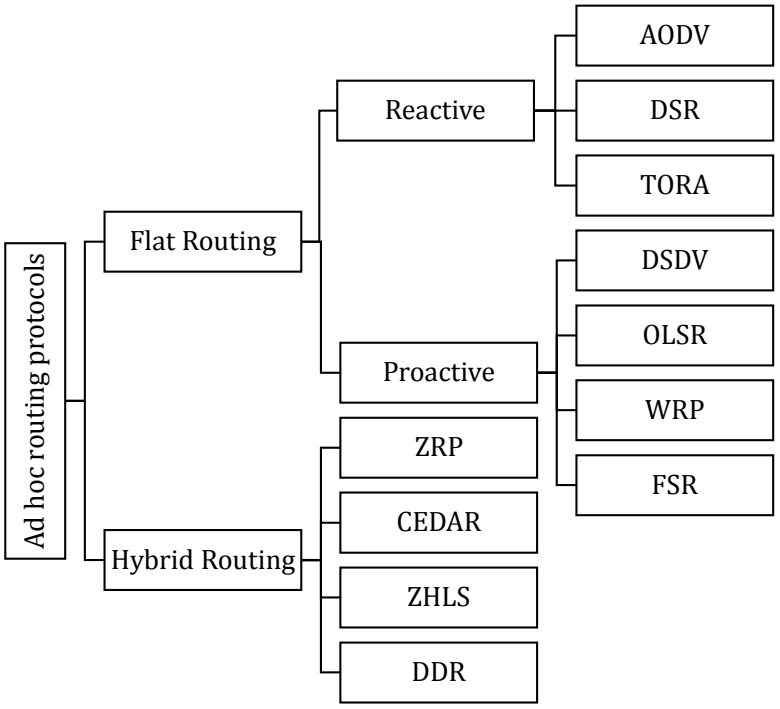


FIGURE 3.1: Classification of Routing Protocol

3.1.2 Proactive Routing Protocols

These protocols always maintain up-to-date information of routes from each node to every other node in the network. These protocols continuously learn the topology of the network by exchanging topological information among the network nodes. Thus, when there is a need for a route to a destination, such route information is available immediately. Different protocols keep track of different routing state information [30]. These protocols require each node to maintain one or more tables to store up to date routing information and to propagate updates throughout the network. As such, these protocols are often also referred to as table-driven. These protocols try and maintain valid routes to all communication mobile nodes all the time, which means before a route is actually needed. Periodic route updates are exchanged in order to synchronize the tables. Some examples of table driven ad hoc routing protocols include Dynamic Destination Sequenced Distance-Vector Routing Protocol (DSDV) [31], Optimized Link State Routing Protocol (OLSR) [32] and Wireless Routing Protocol (WRP) [33]. These protocols differ in the number of routing related tables and how changes are broadcasted in the network structure.

3.1.2.1 Destination Sequenced Distance-Vector Routing Protocol (DSDV)

DSDV is proposed by Perkins and Bhagwat. The Destination-Sequenced Distance-Vector (DSDV) [31] Routing protocol is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements such as making it loop-free. The distance vector routing is less robust than link state routing due to problems such as count to infinity and bouncing effect. In this, each device maintains a routing table containing entries for all the devices in the network. In order to keep the routing table completely updated at all the time each device periodically broadcasts routing message to its neighbor devices. When a neighbor device receives the broadcasted routing message and knows the current link cost to the device, it compares this value and the corresponding value stored in its routing table. If changes were found, it updates the value and re-computes the distance of the route which includes this link in the routing table.

3.1.2.2 Optimized Link State Routing Protocol (OLSR)

Clausen and Jacquet proposed the Optimized Link State Protocol, a point-to-point proactive protocol that employs an efficient link state packet forwarding mechanism called multipoint relaying [28, 29]. It optimizes the pure link state routing protocol. Optimizations are done in two ways: by reducing the size of the control packets and by reducing the number of links used for forwarding the link state packets. Here each node maintains the topology information about the network by periodically exchanging link-state messages among the other nodes. OLSR is based on the following three mechanisms: neighbor sensing, efficient flooding and computation of an optimal route using the shortest-path algorithm. Neighbor sensing is the detection of changes in the neighborhood of node. Each node determines an optimal route to every known destination using this topology information and stores this information in a routing table. The shortest path algorithm is then applied for computing the optimal path. Routes to every destination are immediately available when data transmission begins and remain valid for a specific period of time till the information is expired.

3.1.2.3 Wireless Routing Protocol (WRP)

The Wireless Routing Protocol, as proposed by Murthy and Garcia-Luna-Aceves [33], is a table-based protocol similar to DSDV that inherits the properties of Bellman Ford Algorithm. The main goal is maintaining routing information among all nodes in the network regarding the shortest distance to every destination. Wireless routing protocols (WRP) is a loop free routing protocol. WRP is a path-finding algorithm with the exception of avoiding the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbors. Each node in the network uses a set of four tables to maintain more accurate information: Distance table (DT), Routing table (RT), Link-cost table (LCT),

Message retransmission list (MRL) table. In case of link failure between two nodes, the nodes send update messages to their neighbors. WRP belongs to the class of path-finding algorithms with an important exception. It counters the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbors. This eliminates looping situations and enables faster route convergence when a link failure occurs.

3.1.3 Reactive Routing Protocol

The reactive or on-demand routing protocols are based on Query-Reply topology in which they do not attempt to continuously maintain the up-to-date topology of the network. When a route is desired, a procedure is invoked to find a route to the destination node. The major goal of on demand or reactive routing protocols is to minimize the network traffic overhead. These routing protocols are based on some type of "query-reply" dialog. They do not attempt to continuously maintain the up-to-date topology of the network. Rather, when the need arises, a reactive protocol invokes a procedure to find a route to the destination; such a procedure involves some sort of flooding the network with the route query. As such, such protocols are often also referred to as on demand. The common element in reactive protocols is the mechanism used for discovering routes. The source node emits a request message, requesting a route to the destination node. This message is flooded, i.e. relayed by all nodes in the network, until it reaches the destination. The path followed by the request message is recorded in the message, and returned to the sender by the destination, or by intermediate nodes with sufficient topological information, in a reply message. Thus multiple reply messages may result, yielding multiple paths - of which the shortest is to be used. Some examples of source initiated ad hoc routing protocols include the Dynamic Source Routing Protocol (DSR), Ad Hoc On-Demand Distance Vector Routing Protocol (AODV), and Temporally-Ordered Routing Algorithm (TORA).

3.1.3.1 Ad Hoc On-Demand Distance Vector Routing Protocol (AODV)

The Ad Hoc On-Demand Distance Vector [25] (AODV) routing protocol enables multi-hop routing between participating mobile nodes wishing to establish and maintain an ad-hoc network. AODV is based upon the distance vector algorithm. The difference is that AODV is reactive, as opposed to proactive protocols like DV, i.e. AODV only requests a route when needed and does not require nodes to maintain routes to destinations that are not actively used in communications. As long as the endpoints of a communication connection have valid routes to each other, AODV does not play any role.

Features of this protocol include loop freedom and that link breakages cause immediate notifications to be sent to the affected set of nodes, but only that set. Additionally, AODV has support for multicast routing and avoids the Bellman Ford counting to infinity problem. The

use of destination sequence numbers guarantees that a route isfresh. The algorithm uses different messages to discover and maintain links. Whenever a node wants to try and find a route to another node, it broadcasts a Route Request (RREQ) to all its neighbors. The RREQ propagates through the network until it reaches the destination or a node with a fresh enough route to the destination. Then the route is made available by unicasting a RREP back to the source.

The algorithm uses hello messages (a special RREP) that are broadcasted periodically to the immediate neighbors. These hello messages are local advertisements for the continued presence of the node and neighbors using routes through the broadcasting node will continue to mark the routes as valid. If hello messages stop coming from a particular node, the neighbor can assume that the node has moved away and mark that link to the node as broken and notify the affected set of nodes by sending a link failure notification (a special RREP) to that set of nodes. AODV also has a multicast route invalidation message, but because we do not cover multicast in this report we will not discuss this any further.

Route Table Management

AODV needs to keep track of the following information for each route table entry

a. Destination IP Address: IP address for the destination node.

b. Destination Sequence Number: Sequence number for this destination.

c. Hop Count: Number of hops to the destination.

d. Next Hop: The neighbor, which has been designated to forward packets to the destination for this route entry.

e. Lifetime: The time for which the route is considered valid.

Route Discovery

AODV uses a route discovery process to dynamically build new routes on an as need basis. AODV is a distributed algorithm using distance vector algorithms, such as the Bellman Ford

algorithm. When a route to a destination is unknown, AODV creates a route request packet and broadcasts it to its neighbors. Route request messages contain the source ID, destination ID, source sequence numbers, destination sequence numbers, hop count and broadcast ID. The source sequence number and broadcast ID increment each time a new route request is generated. The destination sequence number is the source sequence number of the destination node as last recorded by the source node.

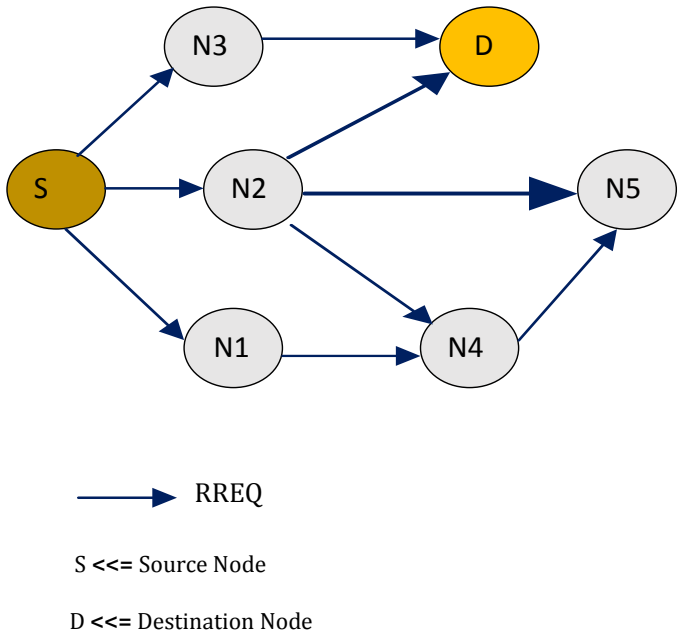


FIGURE 3.2: Route request (RREQ) flooding

Forwarding of RREQs is done when the node receiving a RREQ does not have a route to the destination. It then rebroadcast the RREQ. The node also creates a temporary reverse route to the Source IP Address in its routing table with next hop equal to the IP address field of the neighboring node that sent the broadcast RREQ. This is done to keep track of a route back to the original node making the request, and might be used for an eventual RREP to find its way back to the requesting node. The route is temporary in the sense that it is valid for a much shorter time, than an actual route entry. When the RREQ reaches a node that either is the destination node or a node with a valid route to the destination, a RREP is generated and unicasted back to the requesting node. While this RREP is forwarded, a route is created to the destination and when the RREP reaches the source node, there exists a route from the source to the destination.

Route Maintenance

When a node detects that a route to a neighbor no longer is valid, it will remove the routing entry and send a link failure message, a triggered route reply message to the neighbors that are actively using the route, informing them that this route no longer is valid. For this purpose AODV uses an active neighbor list to keep track of the neighbors that are using a particular route. The nodes that receive this message will repeat this procedure. The message will eventually be received by the affected sources that can chose to either stop sending data or requesting a new route by sending out a new RREQ.

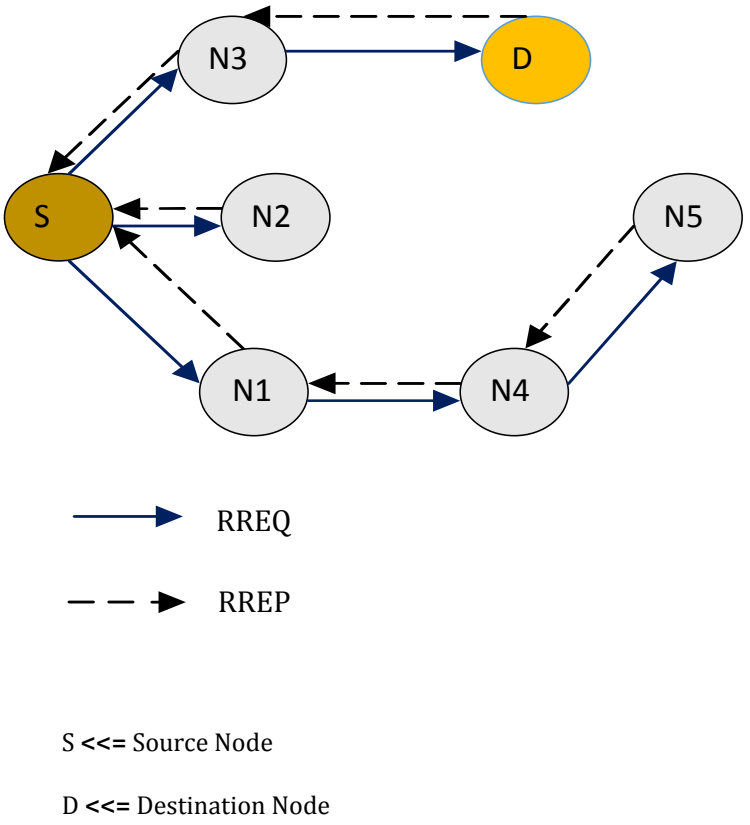


FIGURE 3.3: Route Reply Propagation

Properties

The advantage with AODV compared to classical routing protocols like distance vector and link-state is that AODV has greatly reduced the number of routing messages in the network. AODV achieves this by using are active approach. This is probably necessary in an ad-hoc network to get reasonably performance when the topology is changing often.

AODV is also routing in the more traditional sense compared to for instance source routing based proposals like DSR. The advantage with a more traditional routing protocol in an ad-hoc network is that connections from the ad-hoc network to a wired network like the Internet is most likely easier.

The sequence numbers that AODV uses represents the freshness of a route and is increased when something happens in the surrounding area. The sequence prevents loops from being formed, but can however also be the cause for new problems. What happens for instance when the sequence numbers no longer are synchronized in the network? This can happen when the network becomes partitioned, or the sequence numbers wrap around.

AODV only support one route for each destination. It should however be fairly easy to modify AODV, so that it supports several routes per destination. Instead of requesting a new route

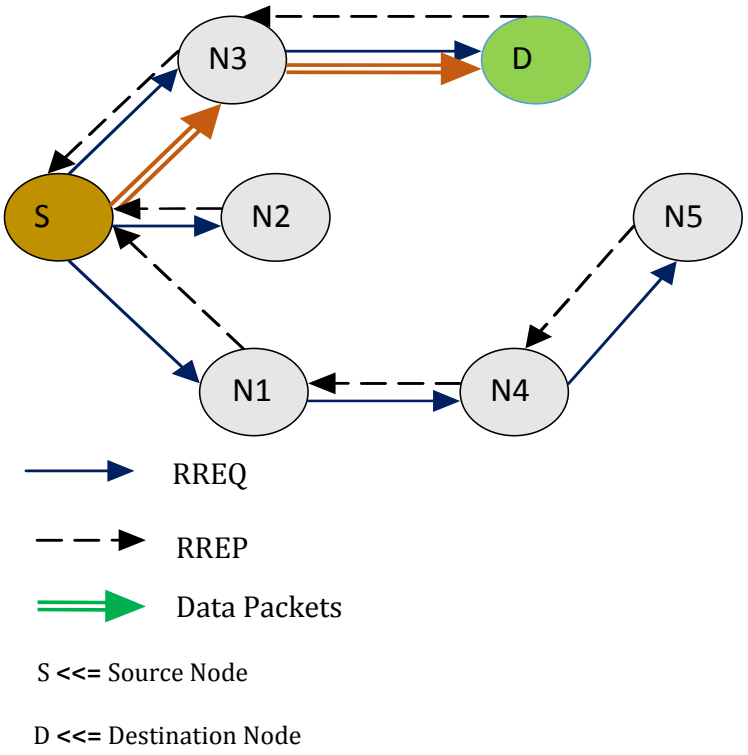


FIGURE 3.4: Data Packet Propagation

when an old route becomes invalid, the next stored route to that destination could be tried. The probability for that route to still be valid should be rather high.

Although the Triggered Route Replies are reduced in number by only sending the Triggered Route Replies to affected senders, they need to traverse the whole way from the failure to the senders. This distance can be quite high in numbers of hops. AODV sends one Triggered RREP for every active neighbor in the active neighbor list for all entries that have been affected of a link failure. This can mean that each active neighbor can receive several triggered RREPs informing about the same link failure, but for different destinations, if a large fraction of the network traffic is routed through the same node and this node goes down. An aggregated solution would be more appropriate here.

AODV uses hello messages at the IP-level. This means that AODV does not need support from the link layer to work properly. It is however questionable if this kind of protocol can operate with good performance without support from the link layer. The hello messages add a significant overhead to the protocol.

AODV does not support unidirectional links. When a node receives a RREQ, it will setup a reverse route to the source by using the node that forwarded the RREQ as next hop. This means that the route reply, in most cases is unicasted back the same way as the route request used. Unidirectional link support would make it possible to utilize all links and not only the bi-directional links. It is however questionable if unidirectional links are desirable in a real

environment. The acknowledgements in the MAC protocol IEEE802.11 would for instance not work with unidirectional links.

3.1.4 Dynamic Source Routing (DSR)

DSR is an on-demand protocol designed by D. B. Johnson, Maltz and Broch to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table update messages required in the proactive routing protocols. The distinguishing feature of Dynamic Source Routing (DSR) [34] is the use of source routing. DSR is a reactive protocol i.e. it doesnt use periodic updates. It computes the routes when necessary and then maintains them. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass, the sender explicitly lists this route in the packets header, identifying each forwarding hop by the address of the next node to which to transmit the packet on its way to the destination host. There are two basic parts of DSR protocol: route discovery and route maintenance. Every node maintains a cache to store recently discovered paths. When a node wants to send a packet, it first checks the cache whether there is an entry for that. If yes then it uses that path to transmit the packet. Also it attaches its source address on the packet. If there is no entry in the cache or the entry is expired, the sender broadcasts a route request packet to all its neighbors asking for a path to the destination. Until the route is discovered, the sender host waits. When the route request packet arrives to any other nodes, they check whether they know the destination asked. If they have route information, they send back a route reply packet to the destination. Otherwise they broadcast the same route request packet. Once the route is discovered, the sender will send its required packets using the discovered route as well as insert an entry in the cache for future use. Also the node keeps the age information of the entry to recognize whether the cache is fresh or not. When any intermediate node receives a data packet, it first sees whether the packet is sent to itself or not. If it is the destination, it receives that else it forwards the packet using the path attached on the packet.

3.1.5 Temporally Ordered Routing Algorithm (TORA)

The Temporally-Ordered Routing Algorithm (TORA) was developed by Park and Corson. Temporarily ordered routing algorithm (TORA) is highly adaptive, loop-free, distributed routing algorithm based on the concept of link reversal. It uses directed acyclic graphs (DAG) to define the routes either as upstream or downstream. This graph enables TORA to provide better route aid for networks with dense, large population of nodes [35]. However to provide this feature TORA needs synchronization of the nodes which limits the application of the protocol. TORA is a fairly complicated protocol but what makes it unique and prominent is its main feature of propagation of control messages only around the point of failure when a link failure occurs. In

comparison, all the other protocols need to re-initiate a route discovery when a link fails but TORA would be able to patch itself up around the point of failure. This feature allows TORA to scale up to larger networks but has higher overhead for smaller networks. TORA involves four major functions: creating, maintaining, erasing and optimizing routes. Since every node must have a height, any node which does not have a height is considered as an erased node and its height is considered as null. Sometimes the nodes are given new heights to improve the linking structure. This function is called optimization of routes.

3.2 Data Traffic

Data and traffic agent that takes the responsibility to transport the data in the network are of different types and offer different characteristics in the network [36]. It is necessary to understand the characteristics and therefore the performance to find the suitability of each type in a network. The two types of data/traffic agent types used in the network are as follows

3.2.1 Control Bit Rate (CBR)

It is also known as user datagram protocol. This type of traffic implies data of UDP type and application traffic agent is CBR. Here, the former is a transport layer protocol and latter is application layer protocol. It offers transmission of data at constant bit rate and does not communicate in phases, and traffic moves in one direction from source to destination without any feedback from destination. It offers three basic characteristics mentioned below:

3.2.1.1 Unreliable:

The network is quiet unreliable as it does not set up communication in phases and does not rely on acknowledgements to recover the lost messages. The sender node does not take the responsibility of the successful delivery of data.

3.2.1.2 Unidirectional:

As no acknowledgements are transmitted from receiver, only one way communication is done i.e. on the forward link. The destination does not send any data packet to the receiver, therefore it offers unidirectional traffic.

3.2.1.3 Predictable:

The UDP/CBR has predictable nature of transmission, as it offers constant bit rate, fixed and known packet size, fixed and known packet interval, and fixed and known packet stream duration.

3.2.2 Transmission Control Protocol(TCP)

It is also known as file transfer protocol (FTP). In such a traffic scenario, TCP represents the data type and FTP represents the application traffic agent of any application which transports TCP data. Here TCP is a transport layer protocol and FTP is an application layer protocol. This scenario offers connection oriented transmission environment, where communication occurs in phases, namely, connection establishment, data transmission, connection termination. The three basic characteristics offered are:

3.2.2.1 Reliable

TCP/FTP offers reliable communication, as it offers guaranteed delivery of data by employing the acknowledgements which guarantees the delivery of data at a destination. In case acknowledgements are not received till the timeout period, retransmissions are made to ensure the delivery of data at the receiver. We can say that positive acknowledgements, timeouts, and retransmissions are required to guarantee the delivery of data in a network.

3.2.2.2 Bi-directional:

Here in TCP/FTP, in one direction i.e. the forward direction, the sender transmits the data and in the other direction i.e. the reverse direction, the receiver acknowledges the sender by transmitting acknowledgements. So, in this way bi-directional communication occurs.

3.2.2.3 Conforming:

The network while working with TCP/FTP, offers conforming nature. The network is conforming in the context of transmissions as it offers both flow and congestion control. Flow control by preventing overflow of recipient buffer, and congestion control by keeping the track of acknowledgements, time outs, and retransmissions.

Chapter 4

Simulation Study

4.1 Network Simulator

In communication and computer network research, network simulation is a technique where a program models the behavior of a network either by calculating the interaction between the different network entities (hosts/packets, etc.) using mathematical formulas, or actually capturing and playing back observations from a production network. The behavior of the network and the various applications and services it supports can then be observed in a test lab; various attributes of the environment can also be modified in a controlled manner to assess how the network would behave under different conditions. A network simulator is software that predicts the behavior of a computer network. In simulators, the computer network is typically modeled with devices, links, applications etc. and the performance is analyzed. Typically, users can then customize the simulator to fulfill their specific analysis needs. Simulators typically come with support for the most popular protocols and networks in use today, such as WLAN, Wi-Max, TCP, WSN, cognitive radio. There are many both free/open-source and proprietary network simulators. Examples of notable network simulation software are, ordered after how often they are mentioned in research papers:

- NS (open source)
- OPNET (proprietary software)
- NetSim (proprietary software)

4.2 Network Simulator (NS2)

NS is an event driven network simulator developed at UC Berkeley that simulates variety of IP networks. It implements network protocols such as TCP and UPD, traffic source behavior such

as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and more.

4.2.1 History of Network Simulator

NS started as a variant of the original network simulator made in 1989 and many modifications are made during the past years. In 1995, the development of NS became supported by The Defense Advanced Research Projects Agency (DARPA) through the Virtual Inter Network Testbed (VINT) project at Xerox Palo Alto research Center (PARC), and at the Information Sciences Institute (USC/ISI) of the University of Southern California, etc. Currently, NS development is supported through DARPA with Simulation Augmented by Measurement and Analysis for Networks (SAMAN) and National Science Foundation (NSF) with Collaborative Simulation for Education and Research (CONSER), in collaboration with other researchers including The ICSI (International Computer Science Institute) Center for Internet Research (ICIR) [37].

4.2.2 Operation system and Installation of NS

NS can run under both UNIX and Windows operating systems. There are many components needed to be installed before running NS. The user can choose to install it partly or completely. For beginners it is suggested to make a complete installation which automatically installs all necessary components at once and it requires 320 MB disk space. Installing it partly could save some disk space. When operated under Windows, a piece of software called Cygwin is required before the installation of NS2. Cygwin could provide a Linux-like environment under Windows. During installation of Cygwin, components XFree86-base, XFree86-bin, XFree86-prog, XFree86-lib, XFree86-etc, make, patch, perl, gcc, gcc-g++, gawk, gnuplot, tar and gzip must be chosen because they are required by NS2 installation. A good reference for installation of NS2 under Windows is Reference [38].

4.2.3 Use of NS-2

NS2 is an object oriented, discrete event driven network simulator. It is written in C++ and OTcl Tcl (Tool command language) script language with Object-oriented extensions developed at MIT (Massachusetts Institute of Technology). In order to reduce the processing time, the basic network component objects are written using C++. Each object has a matching OTcl object through an OTcl linkage.

Figure 4-1 [37] shows the simplified user view of NS. The procedure of using NS2 to simulate the network and analyze the simulation result is as follows. Firstly, the user has to program with OTcl script language to initiate an event scheduler, set up the network topology using the

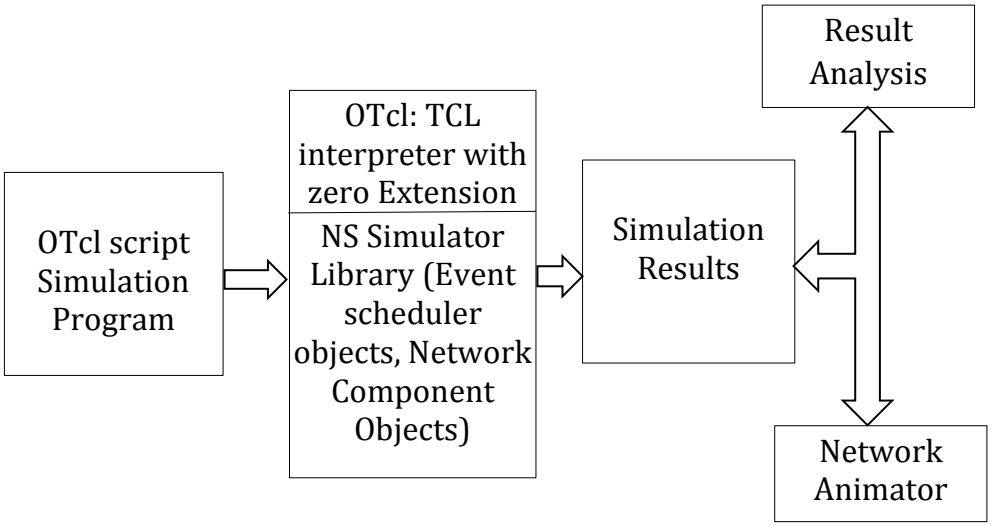


FIGURE 4.1: Simplified User View of NS

network objects and tell traffic sources when to start and stop transmitting packets through the event scheduler. OTcl script is executed by NS2. The simulation results from running this script in NS2 include one or more text based output files and an input to a graphical simulation display tool called Network Animator (NAM). Text based files record the activities taking place in the network. It can be analyzed by other tools such as Gwak and Guplot to calculate and draw the results such as delay and jitter in form of figures. NAM is an animation tool for viewing network simulation traces and real world packet traces. It has a graphical interface which can present information such as number of packets drops at each link.

4.3 Mobil Networking in NS-2

4.3.1 Basic Wireless Model in NS-2

The wireless model essentially consists of the Mobile Node at the core, with additional supporting features that allows simulations of multi-hop ad-hoc networks, wireless LANs etc [39]

4.3.2 Creating Mobile Nodes

To create mobile nodes, the user will firstly set the value of parameters which will be used when configuring mobile nodes. The OTcl code for setup of the mobile nodes part is shown in Table 4.1, Table 4.2 and Table 4.3

To sum up, the above scripts create mobile nodes objects; create the ad hoc routing protocol, link layer, interface queue, MAC layer, and the network interface with an antenna, propagation

Table 4.1: Part of the Tcl script for setting of parameters

Part of the Tcl script for setting of parameters	Explanations
set val(chan) Channel/WirelessChannel	Channel type
set val(prop) Propagation/TwoRayGround	Radio-propagation model
set val(mac) Mac/802_11	MAC type
set val(ifq) Queue/DropTail/PriQueue	Interface Queue type
set val(ll) LL	Link Layer type
set val(ant) Antenna/OmniAntenna	Antenna model
set val(ifqlen) 50	Max Packet in ifq
set val(nn) 6	Number of mobile nodes
set val(rp) AODV	Routing protocol

Table 4.2: Part of the Tcl script for configuration of nodes

```
$ns_ node   -config -adhocRouting $val(rp) \
            -llType $val(ll) \
            -macType $val(mac) \
            -ifqType $val(ifq) \
            -ifqLen $val(ifqlen) \
            -antType $val(ant) \
            -propType $val(prop)\
            -phyType $val(netif) \
            -channelType $val(chan) \
            -topoInstance $topo \
            -agentTrace ON \
            -routerTrace ON \
            -macTrace OFF \
            -arpTrace OFF \
            -movementTrace OFF
```

model. More explanations about the function of these components achieved in NS2 can be found in Table 5.3.

In NS-2, routing protocols supported for ad hoc networks includes DSDV, DSR, TORA (Temporally Ordered Routing Algorithm), and AODV protocols.Presently, ns-2 consists of over 300,000 lines of source code, and there is probably a comparable amount of contributed code that is not integrated directly into the main distribution (many forks of ns-2 exist, both maintained and unmaintained). It runs on GNU/Linux, FreeBSD, Solaris, Mac OS X and Windows versions that support Cygwin. It is licensed for use under version 2 of the GNU General Public License.

4.3.3 Trace file formats in wireless networks

Trace file is one of the text based results that the user gets from a simulation. It records the actions and relevant information of every discrete event in the simulation. There are a variety of forms for trace files. Simulations using different simulation networks or using different routing

TABLE 4.3: Mobile node components and their functions

Components	Functions
Link layer	Simulation of data link layer protocol including packet
fragmentation and	assembling, and reliable link protocol.
ARP	Connect to LL, resolves all IP to MAC address.
Interface Queue	The class PriQueue is implemented. It provides priority to
routing protocol	packets by inserting them at the head of queue.
MAC layer	Can choose IEEE 802.11 protocol or TDMA as the MAC layer.
Network Interface	It is used by mobile node to access the channel.
Radio propagation model	It used Friss-space attenuation at near distance and
	two ray ground at far distance.
Antenna	An omni-directional antenna is used.

protocols could get trace files having different trace file formats. For example, a wired network and a wireless network have absolutely different format for recording each event. In the same network, for example in wireless networks, each routing protocol has its own format of the routing record.

In the trace file, actions of different layers in the network can be traced. It includes agent trace, router trace, MAC trace and movement trace. All of these traced events can be written to a file in a predefined format. When the user simulates large events, the trace file can be very large. It will not only require time to generate the trace file during simulation but also need space to store it. As a result, user should always choose part of the choices to trace. For example, in simulation of Section 5, the author would always take the agent trace and the router trace on, and MAC trace and movement trace off, since what the author interested in is the actions of nodes in the routing layer.

An example of one record in the wireless trace file is listed as follows:

r 5.000000000 _3_ RTR — 2 cbr 512 [0 0 0 0] ——- [3:1 4:0 32 0] [0] 0 0

The word field which will be used to explain the above record means a component which is separated by spaces.

The first field can be r, s, f and D for received, send, forward and drop. The second field gives occurring times for the event. The third field is the node number. The fourth field is the trace name that can be AGT, RTR, MAC, and IFQ. AGT, RTR and MAC represent transport, routing and MAC layer separately. IFQ indicate events related to the interface priority queue.

The number after the dashes is a globally unique sequence number of a packet. The letters after the number give the traffic type. Traffic types can be CBR (Constant Bit Rate), TCP (Transport Control Protocol) and ACK. The number right after the packet type is the packet size in bytes. The following two square brackets separated by the dashes are MAC and routing layer information such as source and destination addresses.

With the information recorded in each event, performance metrics such as packet delivery ratio, throughput, packet loss, and end-to-end delay can be calculated with the help of some additional programs, e.g. Gawk, Perl, Gnuplot and Tracegraph.

4.3.4 Tools used in NS-2

4.3.4.1 Generation of node movement

A tool called setdest is developed by CMU (Carnegie Mellon University) for generating random movements of nodes in the wireless network. It defines node movements with specific moving speed toward a random or specified location within a fixed area. When the node arrives to the movement location, it could be set to stop for a period of time. After that, the node keeps on moving towards the next location. The location setdest is at the directory of ns/indep-utils/cmu-scen-gen/setdest/. Users need to run make before they use setdest. The format of the command of setdest is as follows and explanations of each option are shown in Table 5.4.

./setdest [-n _of_nodes] [-p pausetime] [-s maxspeed] [-t simtime] [-x maxx] [-y maxy] ¿ [outdir/movement-file]

Table 4.4: Setdest sub-command explanation

Setdest sub-command	Explanations
-n num_of_nodes	Total number of node in the scenario.
-p pausetime	Duration when a node stays still after it arrive a location. If this value is set to 0, it means that the node wont stop when it arrive a location and keep on moving.
-s maxspeed	Maximum moving speed of nodes. Nodes will move at a random speed chosing from the range [0, maxspeed].
-t simtime	Simulation time duration this scenario keeps.
-x maxx and -y maxy	Maximum length and width of the area.

In output files, besides the movement scripts there are also some other statistics. They include link changes and route changes.

4.3.4.2 Traffic Generation

To generate random flows of traffic, a Tcl script called cbrgen can be used. This script helps to generate the traffic load. The load can be either TCP or CBR. This script locates in the directory of ns/indep-utils/cmu-scen-gen. The file name is cbrgen.tcl. This tool is used according to the following command line and explanations for each option are shown in Table 4-6.

ns cbrgen.tcl [-type cbr—tcp] [-nn nodes] [-seed seed] [-mc connections] [-rate rate]

Table 4.5: cbrgen sub-command explanation

cbrgen sub-command	Explanations
-type cbr—tcp	Type of the generated traffic, TCP or CBR.
-nn nodes	Total number of nodes.
-seed seed	Random seed.
-mc connections	Number of connections.
-rate rate	Number of packets per second. In CBR, packet length is fix as 512 byte.

4.3.5 Adding Malicious Node to AODV

To add malicious node two files in AODV have to be modified they are:

- aodv.cc
- aodv.h

For to set a malicious node in TCL following change

$ns at 0.0 "[$mnode_(5) set ragent_] hacker"

4.3.5.1 Relevant tools used for data analysis-GAWK

AWK is a computer program that is designed to process text-based data. The name AWK comes from its designers Alfred Aho, Peter Weinberger, and Brian Kernighan. GAWK is AWK developed by GNU (GNU is a recursive acronym for GNUs Not UNIX).

Using AWK, a command file and an input file should be given. A command file can be a file or a command line input. The command file would tell AWK how to deal with the input file. It is composed of patterns and actions. For an input file, every line of the input file will be examined to judge whether this line matches the pattern. If this is the case, this line will be processed by the corresponding action.

During the processing of the input file, GAWK will first separate the input file into pieces of records. The record separator is \n by default. That is why AWK normally parses the file line by line. Each record is composed of several fields; different fields are separated by white space by default. In the command file, $1 represents the first field of a record. In actions, GAWK uses printf to print out the processing result.

BEGIN and END are two special patterns in GAWK. Their corresponding actions are executed only at the beginning and the ending of the execution of a command file.

4.4 Simulation Parameter

The simulation experiments can be classified broadly as CBR (UDP) based simulations and TCP based simulations. The routing protocols were tested with both CBR and TCP traffic to get a more complete picture of their performances. Both the CBR and TCP Each simulation set consisted of 50 independent simulation runs under similar (not identical) conditions.

Following Network Parameter have been considered during simulation

Table 4.6: Network Parameter During Simulation

Network Parameter	Maximum Speed of Node m/s	Pause Time ms	No of node	Connection
Maximum speed of Node	10-60	10	55	30
Pause Time	20	100-500	25	24
No of node	20	10	5-55	Node +/-1
Connection	20	10	55	5-55

The network designed consists of basic network entities with the simulation parameters presented in table.

Table 4.7: Simulation Parameter

Examined Protocol	AODV
Channel Type	Wireless channel
Wireless Standard	802.11a
Simulation Area	800*800
Simulation Time	100 sec
Number Of Nodes	5,10,15,25,35,45, 55,65
Mobility	All node
Node Movement Mode	Random Waypoint
Transmitting Power	5j
Traffic Type	CBR, TCP
Maximum Speed	10-40 m/s
Pause Time	100-500 s
No of connection	5-55
Packet Size (bytes)	512
Performance Parameter	Throughput, E2E delay, PDF, Average Routing Load

Chapter 5

Black-hole Attack - Detection Technique

5.1 MANET Attack

Ad-hoc networks form when stations with similar architecture come into close proximity and start to communicate spontaneously. Therefore, ad-hoc networks must create their own infrastructure in a dynamic and distributed way, without any centralized coordination. Ad-hoc networks are often used for military systems, disaster area networks and conference networks. Thus it is obvious that with lack of infrastructural support and susceptible wireless link attacks, security in ad hoc network becomes inherent weakness.

Nodes within nomadic environment with access to common radio link can easily participate to set up ad hoc infrastructure. But the secure communication among nodes requires the secure communication link to communicate. Before establishing secure communication, link the node should be capable enough to identify another node. As a result node needs to provide his/her identity as well as associated credentials to another node. However delivered identity and credentials need to be authenticated and protected so that authenticity and integrity of delivered identity and credentials cannot be questioned by receiver node. Every node wants to be sure that delivered identity and credentials to recipient nodes are not compromised. Therefore it is essential to provide security architecture to secure ad hoc networking. Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information[40].Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber-attacks than wired network there are a number of attacks that affect MANET.

5.2 Classification of Attack in MANET

It was found that many of the presently existing attacks have some common features and have been categorized into different attacks based on their minor differences. So they can be categorize into two broad categories: DATA traffic attacks and CONTROL traffic attacks. This will help in future designing of security measures which will be able in mitigating those broad categories in one go. As previously discussed, attacks are categorized into two broad categories: DATA traffic attacks and CONTROL traffic attacks.

This classification is based on their common characteristics and attack goals. For example: Black-Hole attack drops packets every time, while Gray-Hole attack also drops packets but its action is based on two conditions: time or sender node. But from network point of view, both attacks drop packets and Gray-Hole attack can be considered as a Black-Hole attack when it starts dropping packets. So they can be categorized under a single category. There are few attacks that have implications on both DATA & CONTROL traffic, so they cannot be classified into these categories easily [41]

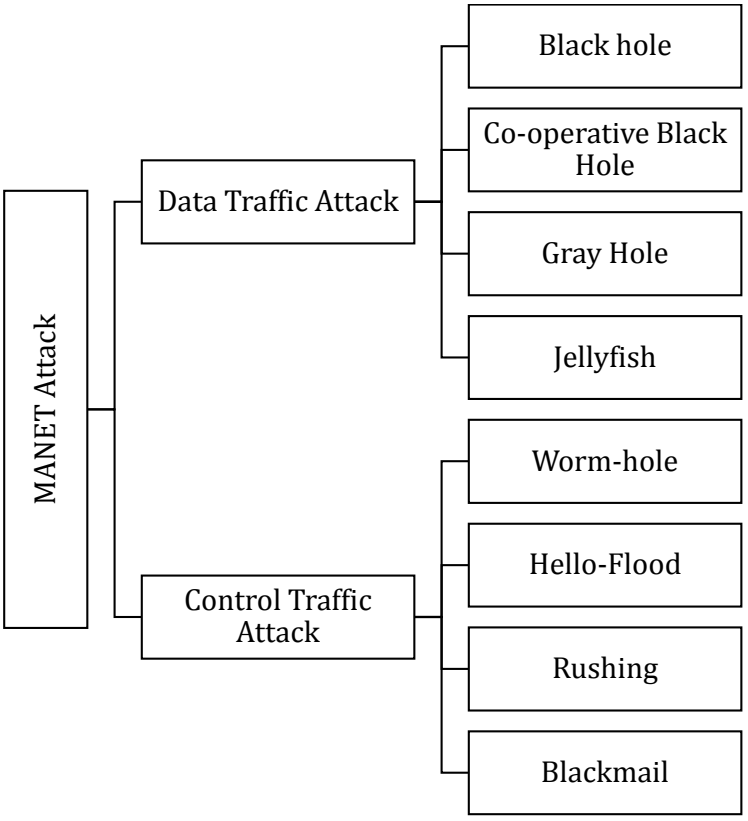


FIGURE 5.1: Classification of attack in MANET

5.3 Black hole Attack

A black hole is a node that always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node. Since

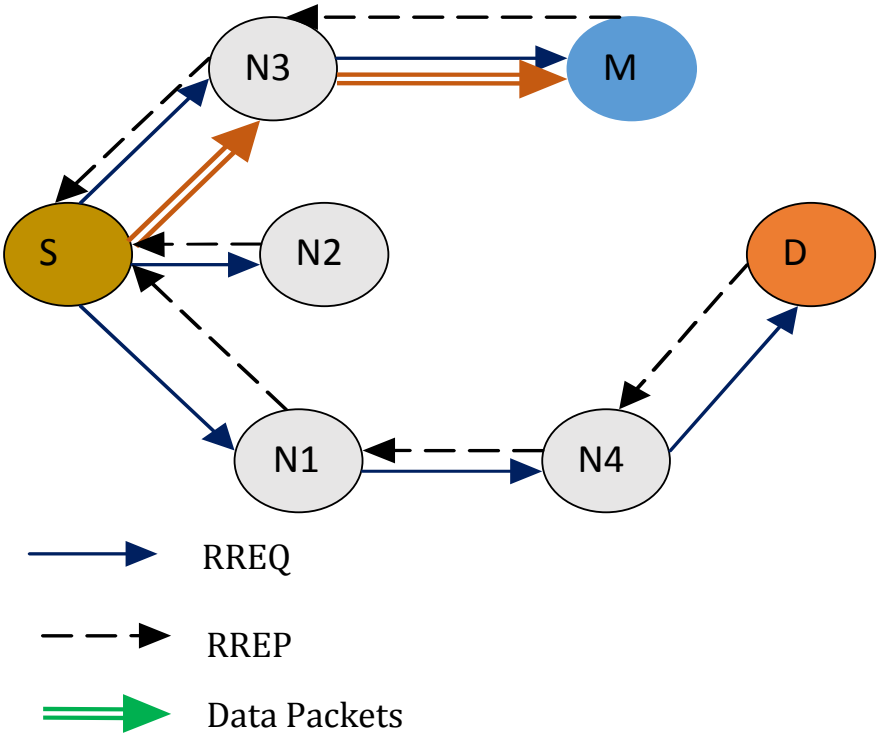


FIGURE 5.2: Black hole attack in MANET

a black hole node does not have to check its routing table, it is the first to respond to the RREQ in most cases. Then the source routes data through the black hole node, which will drop all the data packets it received rather than forwarding them to the destination. In this way the malicious node can easily misroute lot of network traffic to itself and could cause an attack to the network with very little effort on it. These black hole nodes may work as a group.

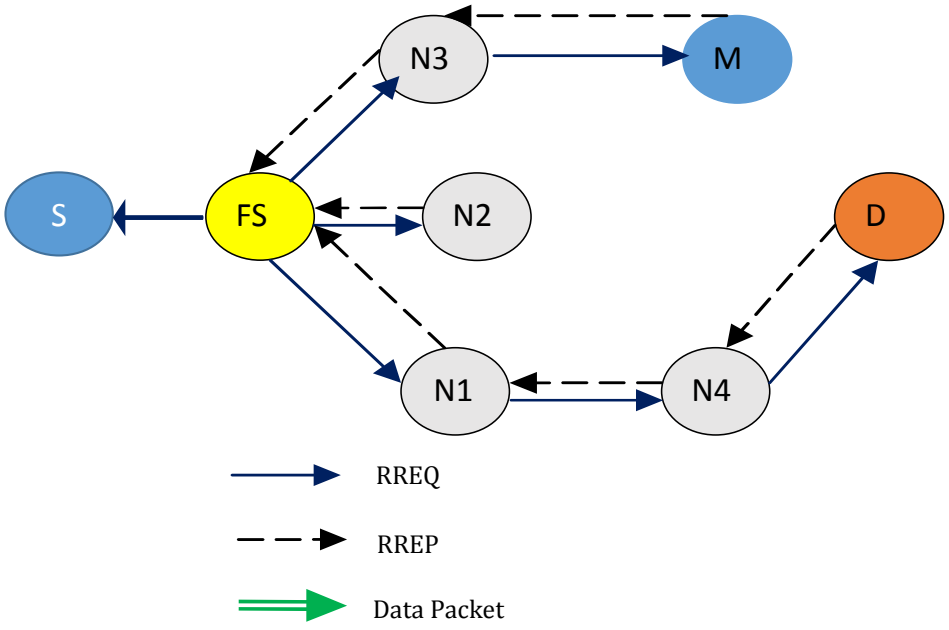
In Figure 5.2 Destination Sequence Number is a 32-bit integer associated with every route and is used to decide the freshness of a particular route. Node N3 will now send it to node. Since node N1 and node N2 do not have a route to node D, they would again broadcast the RREQ control message. RREQ control message broadcasted by node N3 is also expected to be received by

node M (assumed to be a malicious node). Thus, node M would generate a false RREP control message and send it to node N3 with a very high destination sequence number subsequently sent to the node S. However, in simple AODV, as the destination sequence number is high, the route from node N3 will be considered to be fresher and hence node S would start sending data packets to node N3.

5.4 Proposed Detection technique of Black hole attack - Sequence number Comparison scheme with false source node

There are a number of detection technique. But in every technique there are some lackings. In this technique it is tried to keep lackings as lower as possible. This approach find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is large difference between the sequence number of a false source node or intermediate node who has sent back first RREP or not. This false source node is always will be ahead of source node. If proper routing path found then false source node will be automatically connected to source node and normal AODV process will start. Generally, the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-table. Then compare the first destination sequence number with the false source node sequence number, if there exists much more differences between them, surely it is from the malicious node, immediately remove that entry from the RR-Table. Destination Sequence Number is a 32-bit integer associated with every route and is used to decide the freshness of a particular route. The larger the sequence number, the fresher is the route.

In Figure 5.3, Node N3 will now send it to node. Since node N1 and node N2 do not have a route to node D, they would again broadcast the RREQ control message. RREQ control message broadcasted by node N3 is also expected to be received by node M (assumed to be a malicious node). Thus, node M being malicious node, would generate a false RREP control message and send it to node N3 with a very high destination sequence number, that subsequently would be sent to the false source node FS. However, in simple AODV, as the destination sequence number is high, the route from node N3 will be considered to be fresher and hence node S would start sending data packets to node N3. In this method before sending data packets firstly false source node will check the difference between sequence numbers. If it is too large, obviously the node will be a malicious one, and it will be isolated from the network. Otherwise it simply transfers the data packets to the destination node by establishing routing with source node.



S <<= Source Node

D <<= Destination Node

M <<= Malicious Node

FIGURE 5.3: Proposed Detection Technique of Black hole attack

5.5 Advantages of Sequence number Comparison scheme with false source node

- This solution may be used to maintain the identity of the malicious node as MN-Id, so that in future, it can discard any control messages coming from that node.
- This method can find multiple black hole nodes.
- Main benefit of this method is simplicity.
- In this method all nodes do not monitor each other so a lot of energy is not consumed for monitoring.

Chapter 6

Result Analysis and Discussion

The results of simulations are analyzed and discussed in this chapter. The results are analyzed and discussed in different perspective of node. The perspectives are varying no of nodes, no of connections, maximum speed. Then different performance matrices are analyzed for two different connections CBR and TCP. Later adding malicious node in AODV performance variation in different performance matrices is also analyzed.

6.1 Performance Metrics

Four important performance metrics are evaluated for analyzing simulation performance:

6.1.1 Average Throughput

Throughput is the ratio of the total amount of data that a receiver receives from a sender to a time it takes for receiver to get the last packet. A low delay in the network translates into higher throughput. Delay is one of the factors effecting throughput, other factors are routing overhead, area and bandwidth. Throughput gives the fraction of the channel capacity used for useful transmission and is one of the dimensional parameters of the network.

6.1.2 Average End-to-End delay of Data Packets

The term end to end delay refers to time taken by a packet to be transmitted across a network from source to destination node that includes all possible delays caused during route discovery latency, retransmission delays at the MAC, propagation and transfer times. The protocol which shows higher end to end delay it means the performance of the protocol is not good due to network congestion.

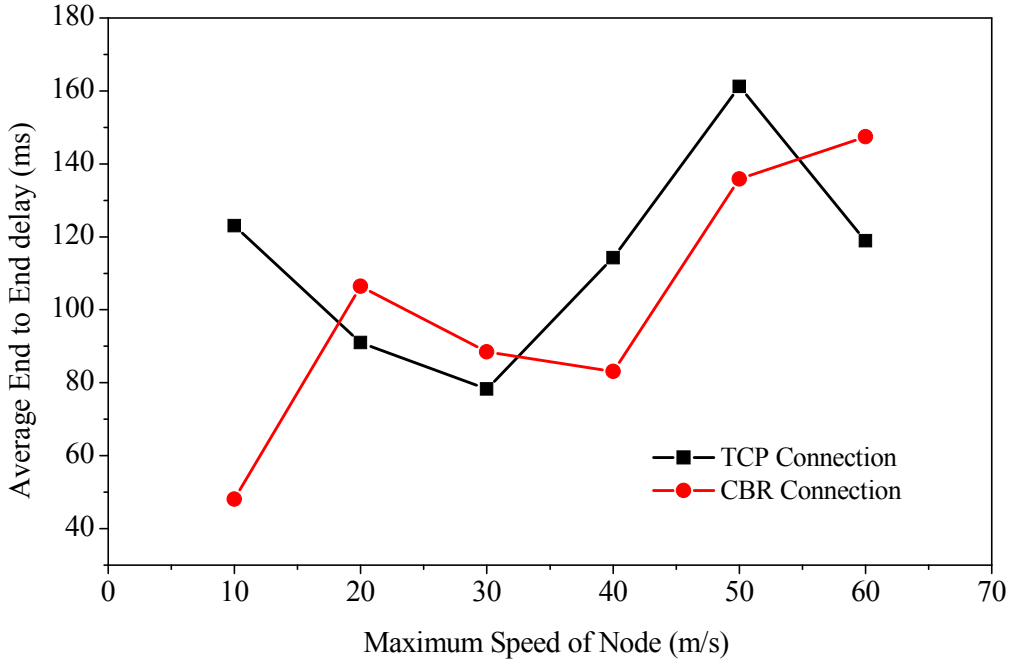


FIGURE 6.1: Average End to End delay vs Maximum Speed of Node

6.1.3 Packet delivery fraction

The ratio of the data packets delivered to the destinations to those generated by the sources. All these metrics are not completely independent. For example, lower packet delivery fraction means that the delay metric is evaluated with fewer samples. In the conventional wisdom, the longer the path lengths, the higher the probability of a packet drops. Thus, with a lower delivery fraction, samples are usually biased in favor of smaller path lengths and thus have less delay.

6.1.4 Average Routing Load

The average number of routing packets that are transmitted per data packet delivered. The routing packets are computed in terms of different control packets that are used by the routing protocol algorithm. It gives a measure of the protocol overhead.

6.2 Simulation Result

6.2.1 Average End to End Delay (e2e)

Average end to end delay for different perspective of node have been depicted in figure 6.1, figure 6.2, figure 6.3, figure 6.4 and figure 6.5

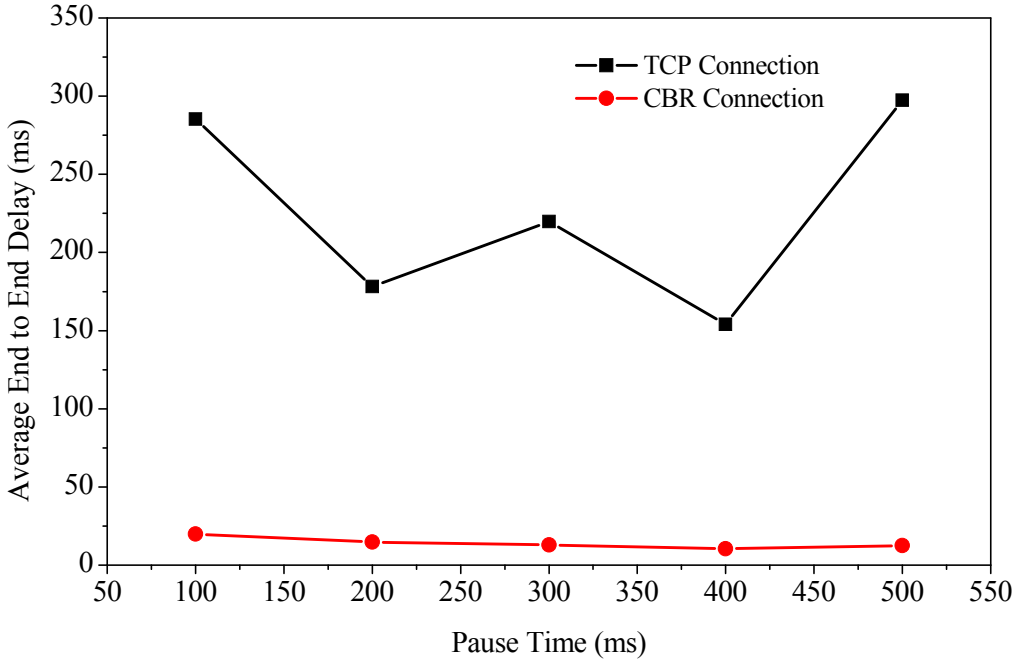


FIGURE 6.2: Average End to End delay vs Pause Time

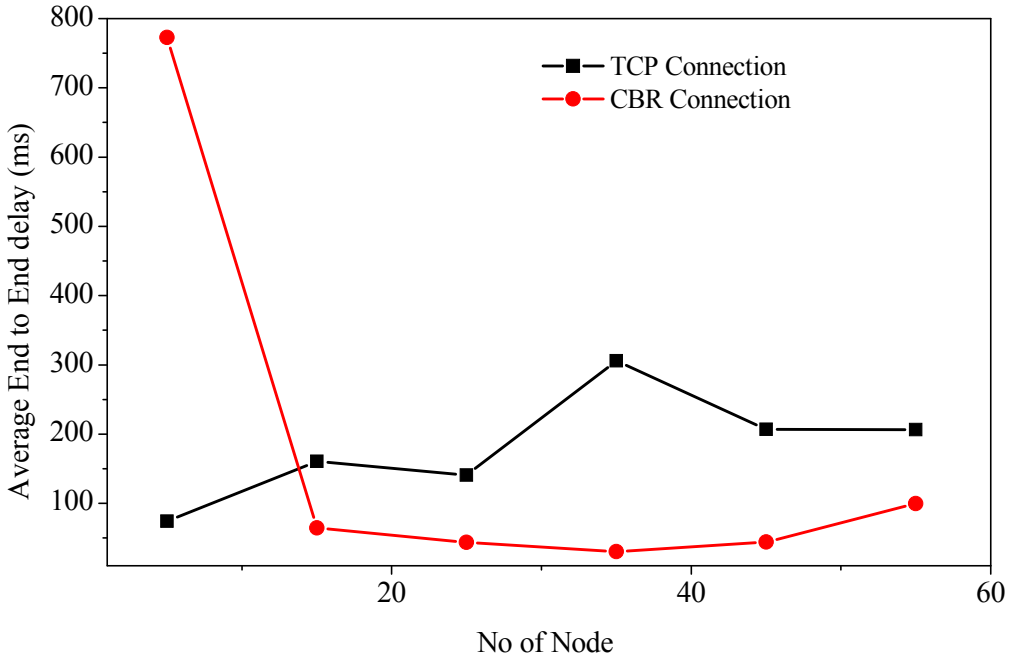


FIGURE 6.3: Average End to End delay vs No of Node

In figure 6.1 when maximum speed of node is low then node cannot come close to generate routing packets, which leads to lower e2e value. When maximum speed is increasing then e2e value is also increasing as generation of routing packet is increasing. CBR, on the other hand, does have control bit rate so with increasing maximum speed e2e is also increasing.

In figure 6.2 when pause time is increasing then e2e value is decreasing till 200s this indicates

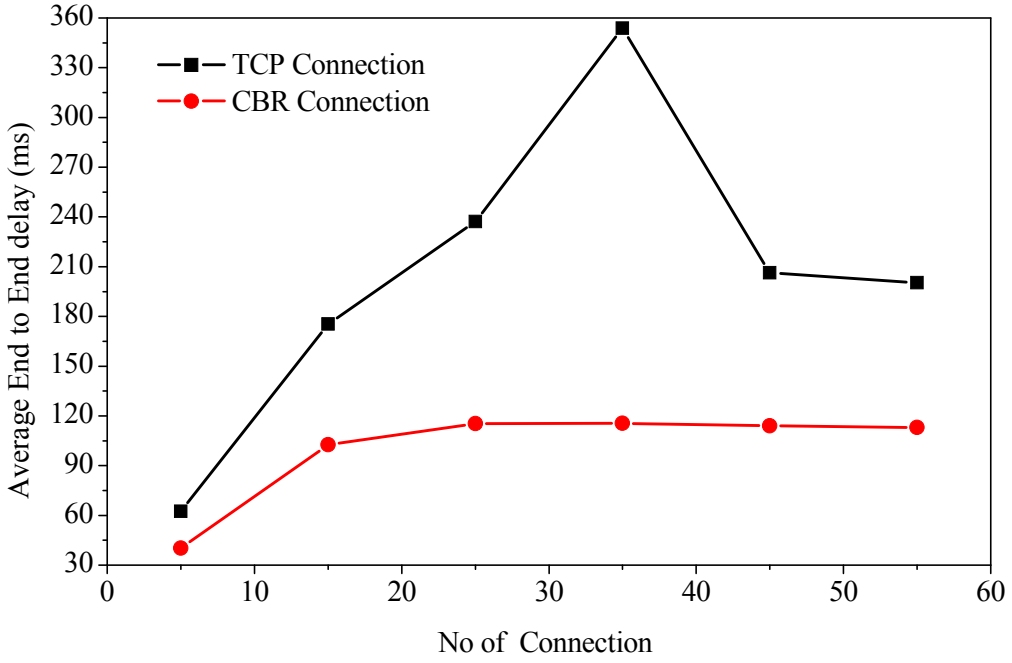


FIGURE 6.4: Average End to End delay vs Connection

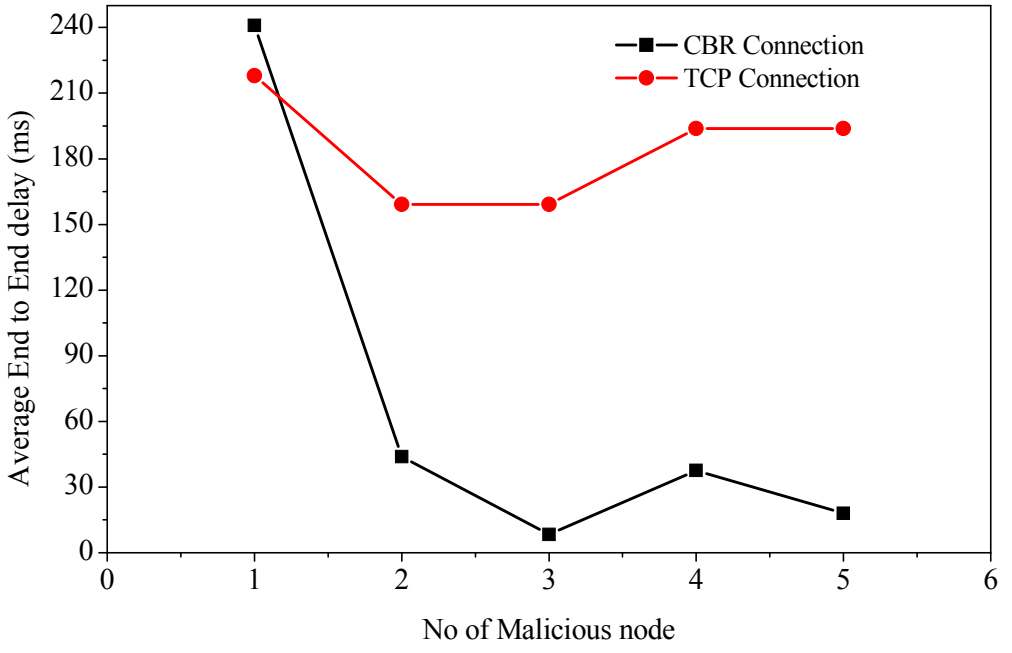


FIGURE 6.5: Average End to End delay vs No of malicious node

node reaches its destination in this time. Again e2e is increasing with increasing pause time. CBR, on the other hand, does have control bit rate so with increasing pause time e2e is constant.

In figure 6.3 when no of node is increasing then node can easily come close to generate routing packets, which leads to lower e2e value. CBR, on the other hand, does have control bit rate so with increasing maximum speed e2e is constant.

In figure 6.4 when no of connection is increasing and again the network have constant no of nodes then e2e is approximate to constant for both CBR and TCP connections.

In figure 6.5 when no of malicious node is increasing then both for TCP and CBR average end to end delay is decreasing. This is because when no of malicious node is increasing then generating data packet will decrease so less e2e is required. But average end to end delay is higher in TCP connection.

6.2.2 Packet Delivery Ratio (PDR)

Packet delivery ratio for different perspective of node have been depicted in figure 6.6, figure 6.7, figure 6.8, figure 6.9 and figure 6.10

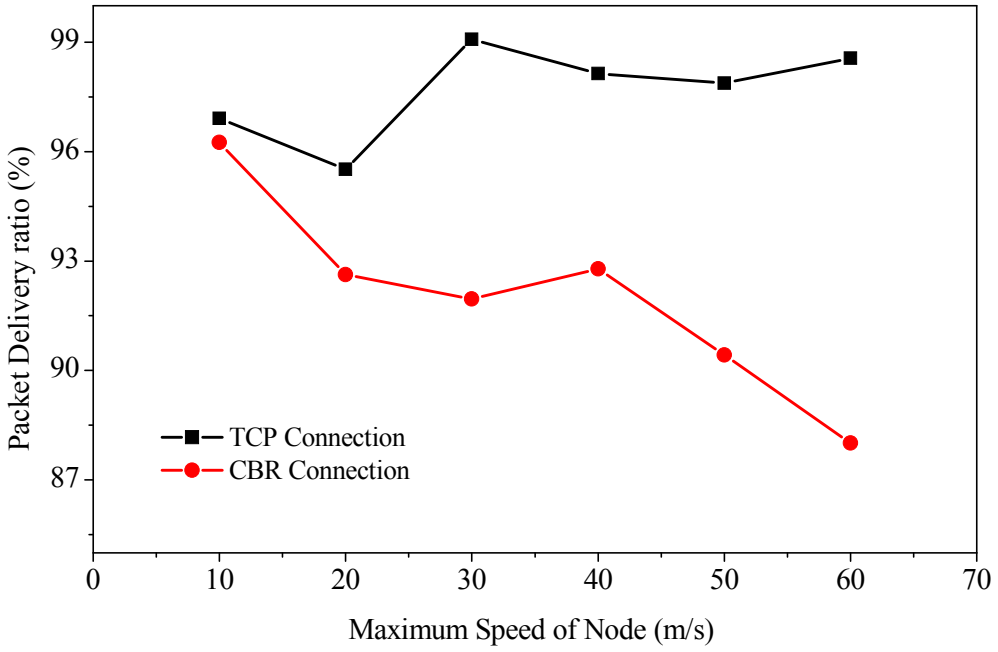


FIGURE 6.6: Packet Delivery Ratio vs Maximum Speed of Node

In figure 6.6 for TCP when maximum speed is increasing then PDR is also increasing as routing packet can quickly reach to the destination. CBR, on the other hand, PDR is decreasing.

In figure 6.7 when pause time is increasing then PDR is almost constant for both CBR and TCP connection. But CBR connection has high PDR then TCP. Because for CBR connection total dropped packet is zero so PDR will be more if every other parameter in network is constant.

In figure 6.8 when no of node is increasing then probability of dropping packet is also increasing so PDR is decreasing for TCP connection. CBR, on the other contrary, does not have drop packet so with no of node PDR is constant.

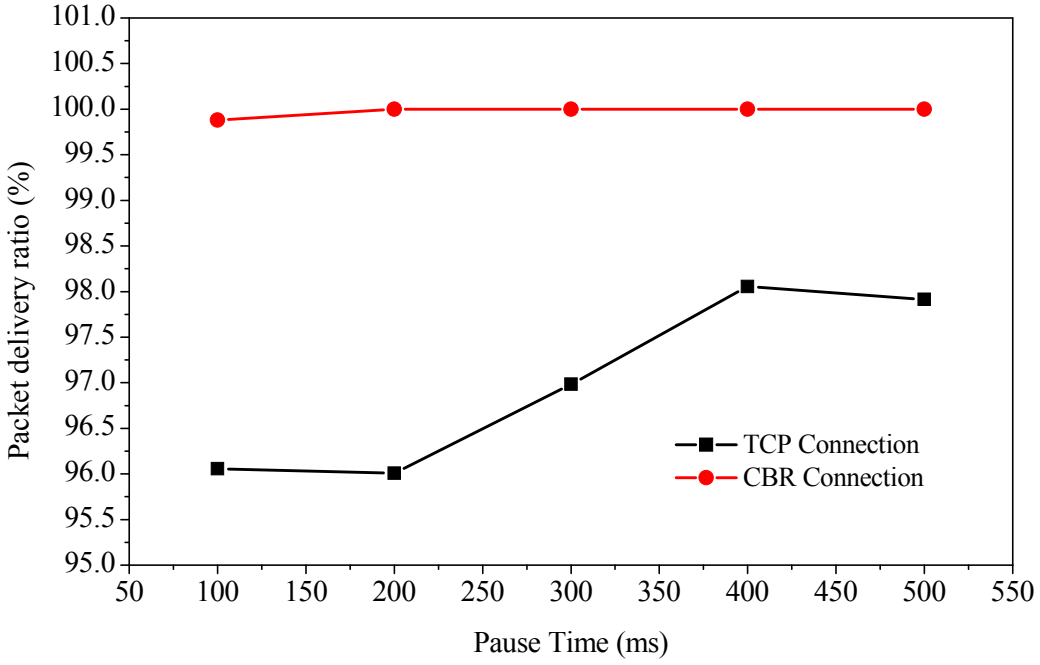


FIGURE 6.7: Packet Delivery Ratio vs Pause Time

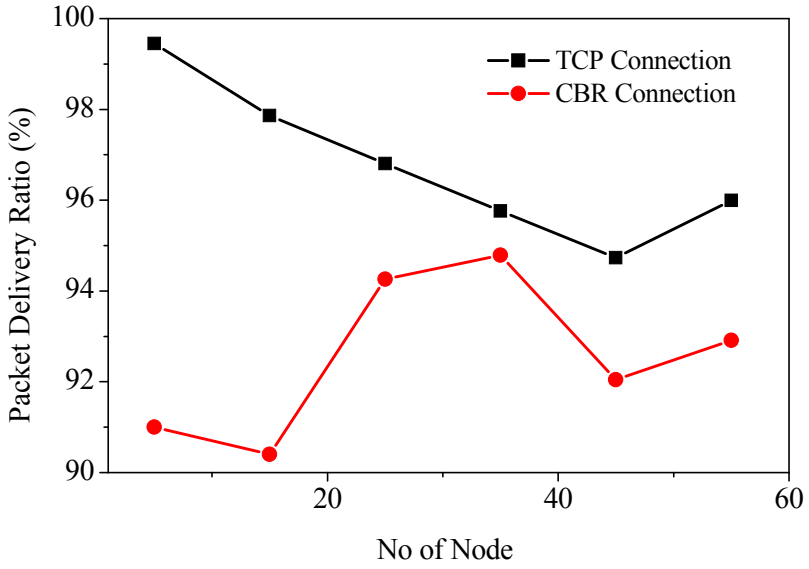


FIGURE 6.8: Packet Delivery Ratio vs No of Node

In figure 6.9 when no of connection is increasing and again the network have constant no of nodes then PDR is decreasing for both CBR and TCP connection. But CBR connection has high PDR value then CBR connection.

In figure 6.10 when no of malicious node is increasing then both for TCP and CBR pdr is decreasing. This is because when no of malicious node is increasing then generating data packet

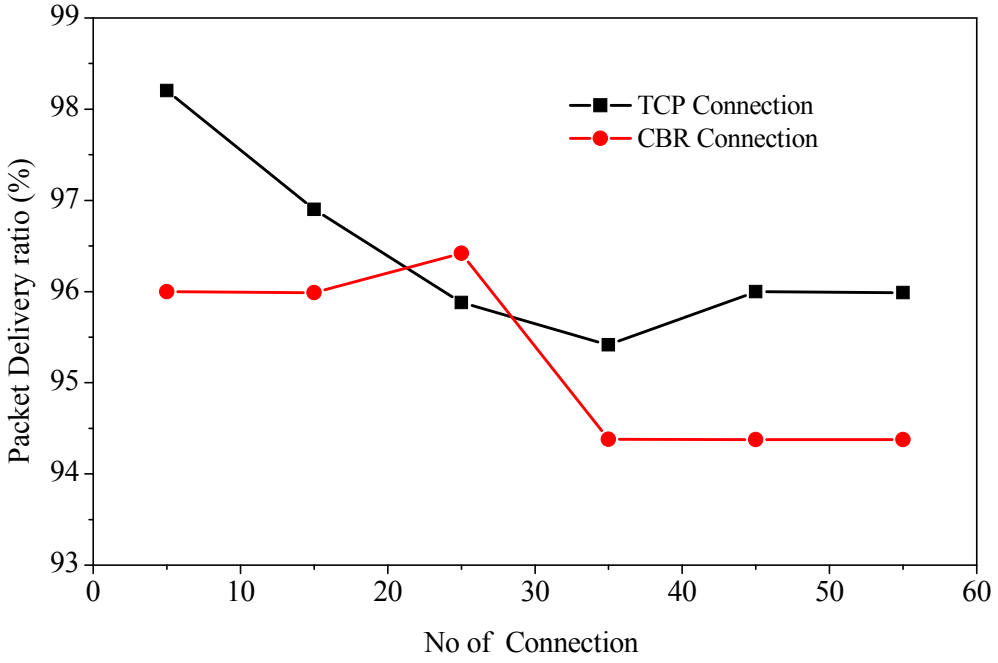


FIGURE 6.9: Packet Delivery Ratio vs No of Connection

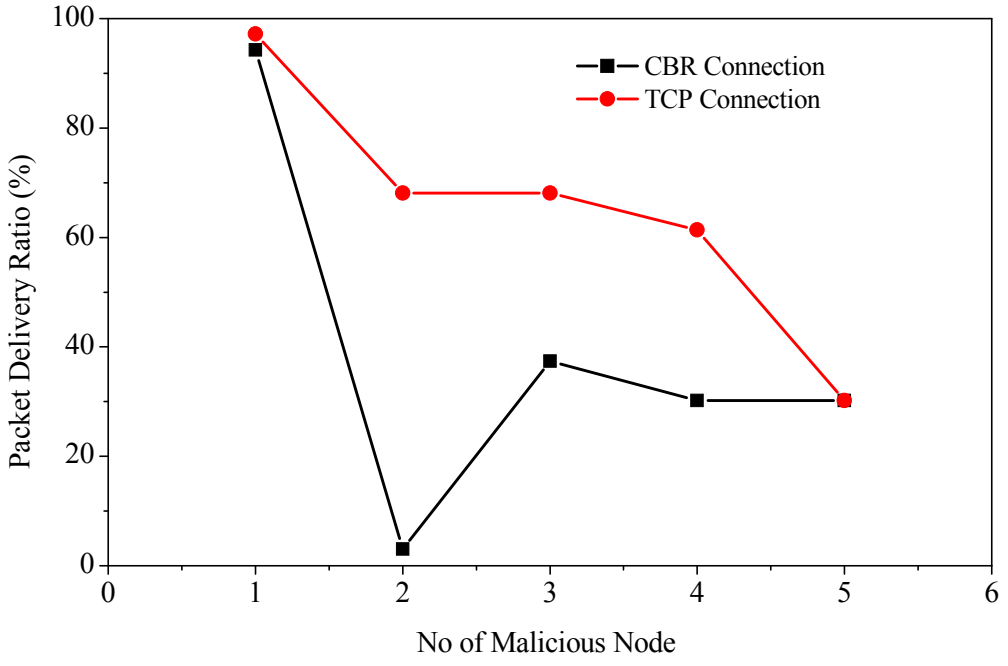


FIGURE 6.10: Packet Delivery Ratio vs No of Malicious Node

will decrease so less pdr is required. But pdr is higher in CBR connection.

6.2.3 Average routing load (overhead)

Average routing load for different perspective of node have been depicted in figure 6.11, figure 6.12, figure 6.13, figure 6.14 and figure 6.15.

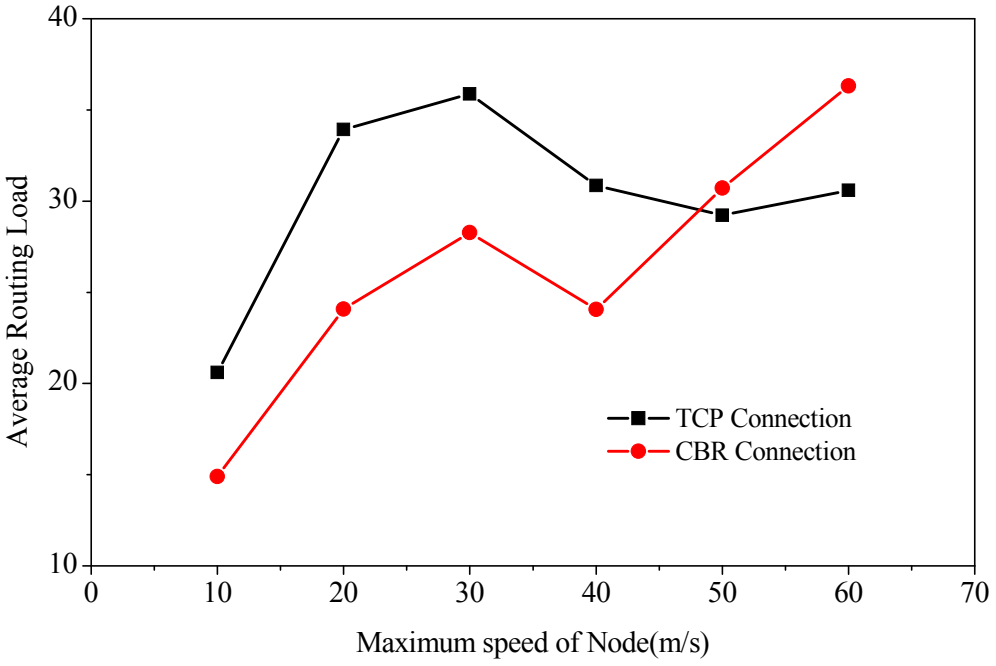


FIGURE 6.11: Average Routing Load vs Maximum Speed of Node

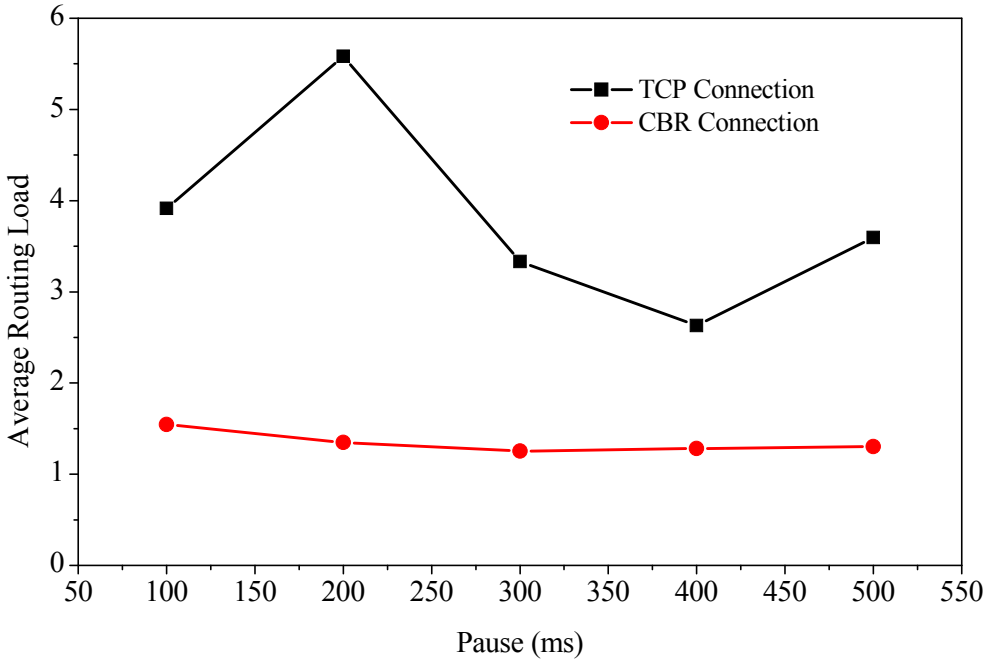


FIGURE 6.12: Average Routing Load vs Pause Time

In figure 6.11 for TCP when mobility of node is increasing then average routing load is increasing till 30 m/s again it is decreasing for both CBR and TCP connection. It is because when node

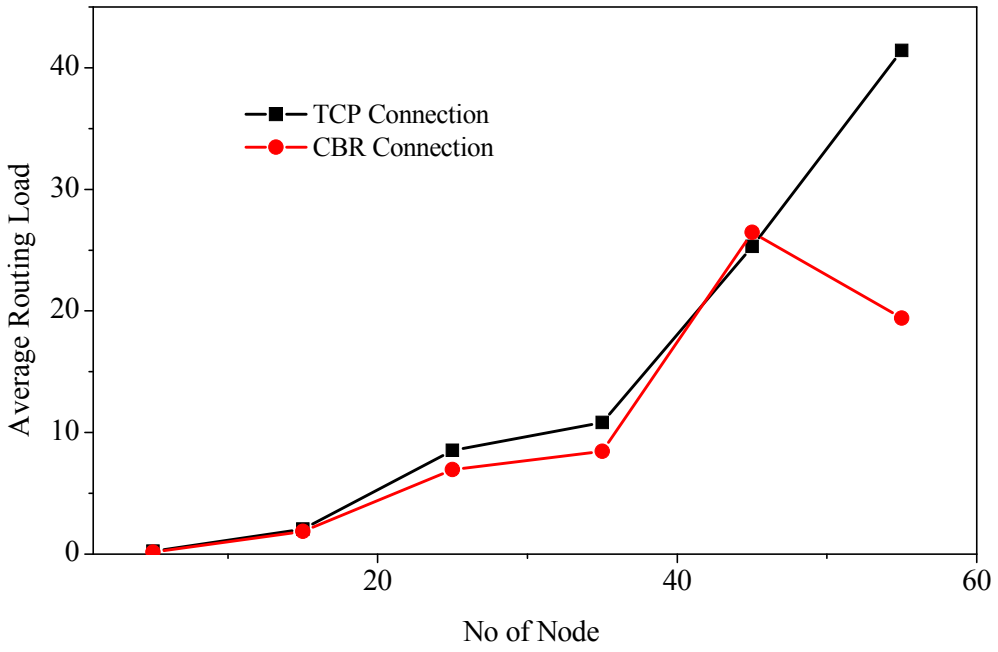


FIGURE 6.13: Average Routing Load vs No of Node

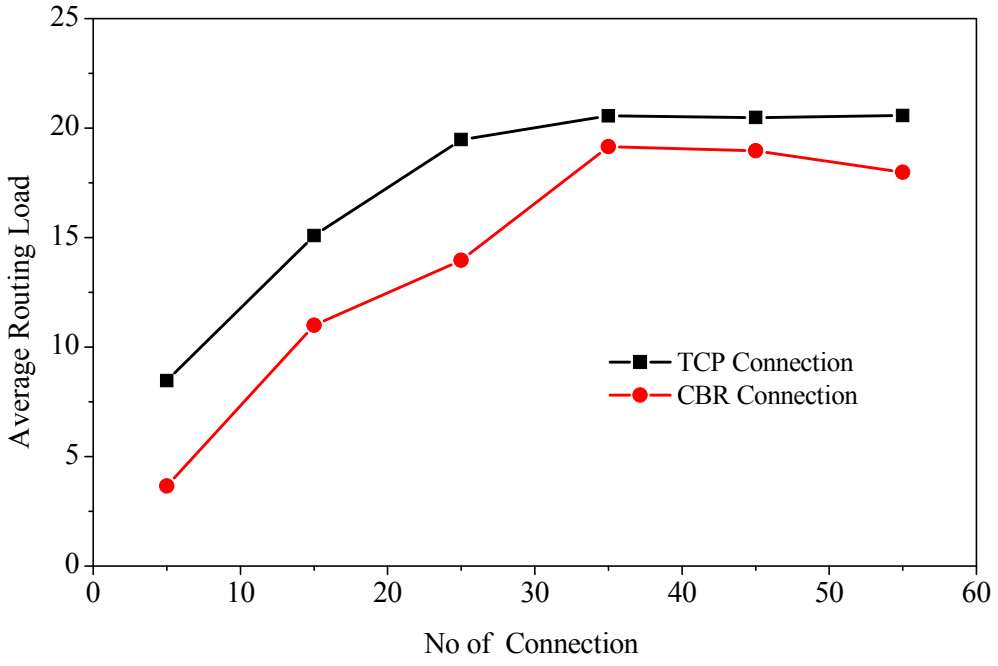


FIGURE 6.14: Average Routing Load vs No of Connection

speed increased to 30 m/s then they are coming closer to generate much data packet with respect to routing packet.

In figure 6.12 average routing load for TCP connection is greater than CBR connection. IT is almost for CBR connection. Due to constant bit rate of CBR connection.

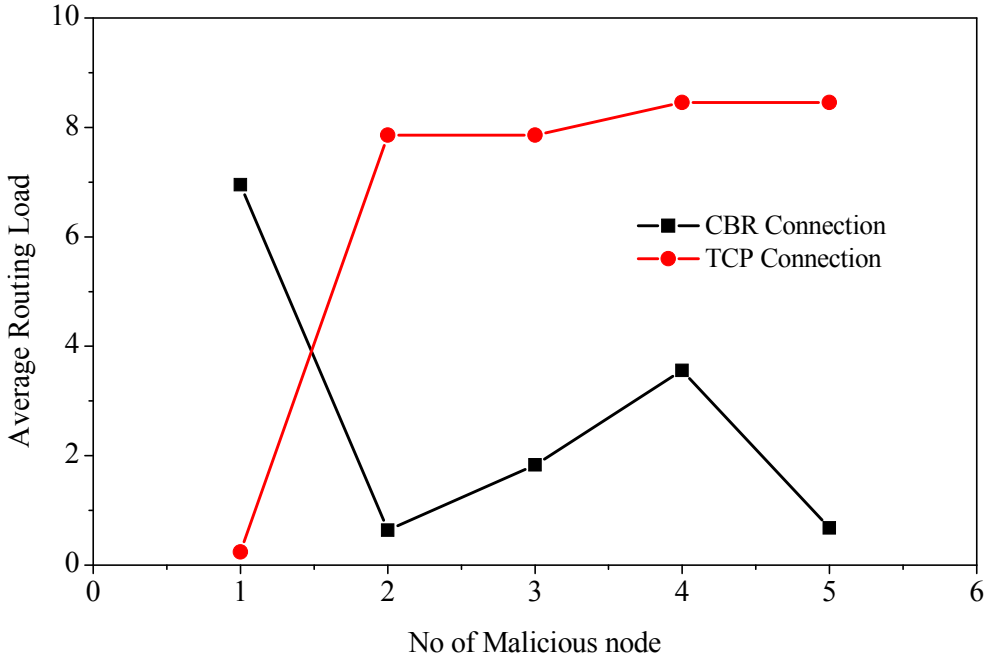


FIGURE 6.15: Average Routing Load vs No of Malicious Node

In figure 6.13 when no of node is increasing then no of generating data packets with respect to outing packets is increasing so average routing load is increasing for both CBR and TCP connection.

In figure 6.14 when no of connection is increasing then no of generating data packets with respect to outing packets is increasing so average routing load is increasing for both CBR and TCP connection. But CBR connection has lower overhead than TCP connection.

In figure 6.15 for TCP when no of malicious node is increasing then average routing load is increasing. For CBR when no of malicious node is increasing then average routing load is decreasing. It depends on the nature of node if malicious node fall in the era of generating data packet then average routing load will decrease.

6.2.4 Average Throughput

Average throughput for different perspective of node have been depicted in figure 6.16, figure 6.17, figure 6.18 and figure 6.19.

In figure 6.16 since throughput is calculated over the number of packets delivered, TCP has lesser throughput than CBR.

In figure 6.17 average throughput for CBR connection is greater than TCP connection for increasing number of node due to absence of congestion. TCP generates maximum traffic over stable link so throughput decrease.

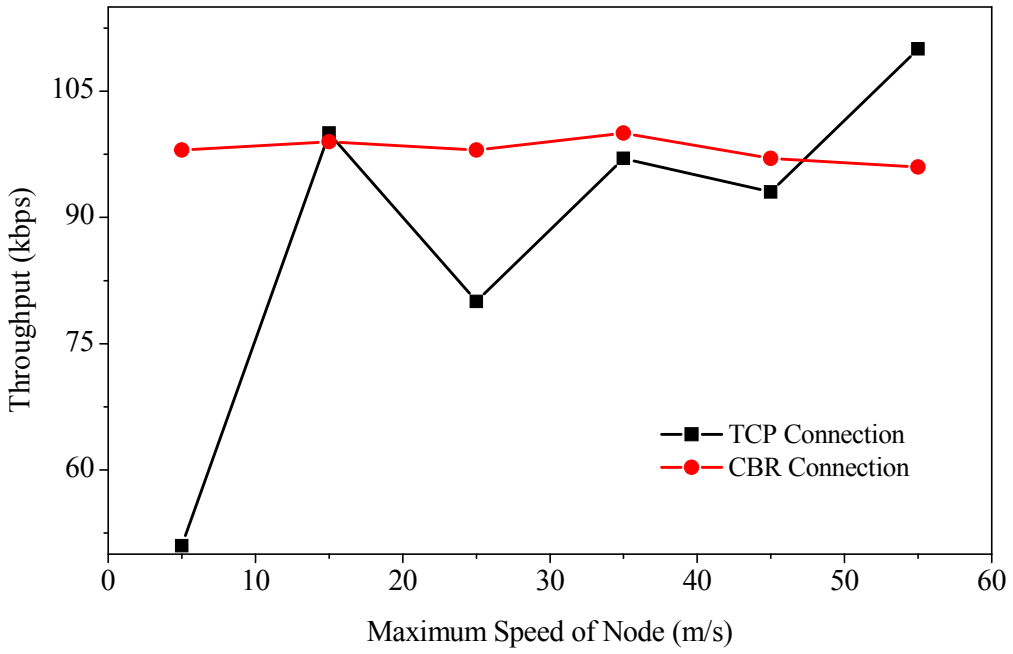


FIGURE 6.16: Average Throughput vs Maximum Speed of Node

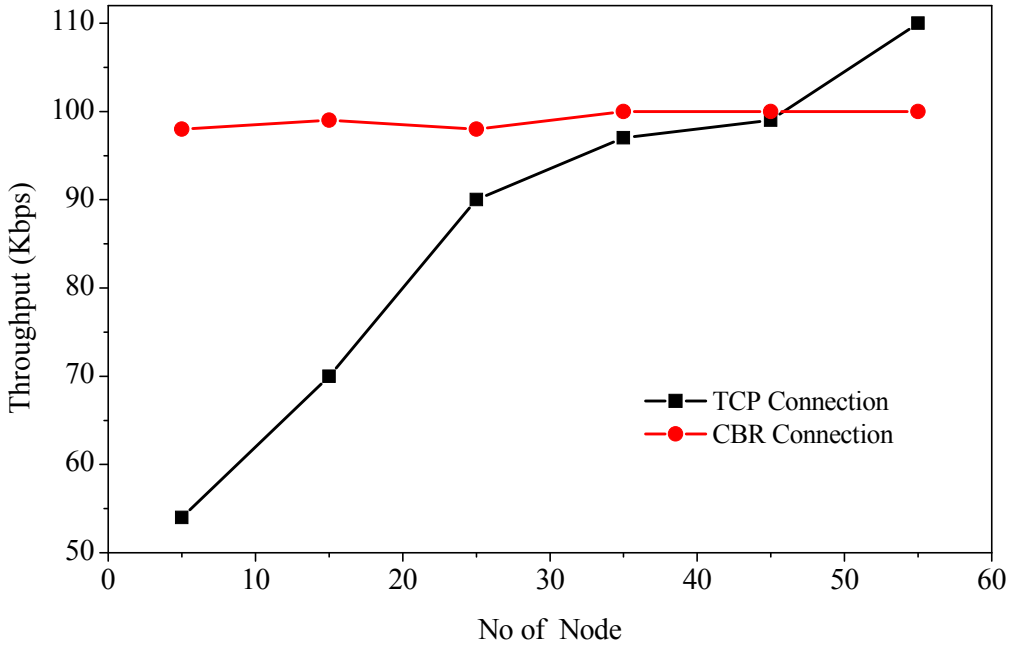


FIGURE 6.17: Average Throughput vs No of Node

In figure 6.18 when no of connection is increasing then throughput is constant for both CBR and TCP connection. CBR connection has greater throughput than TCP connection.

In figure 6.19 when no of malicious node is increasing then no of dropped data packets is increasing if malicious node will fall in the era of generating data packet so throughput will vary

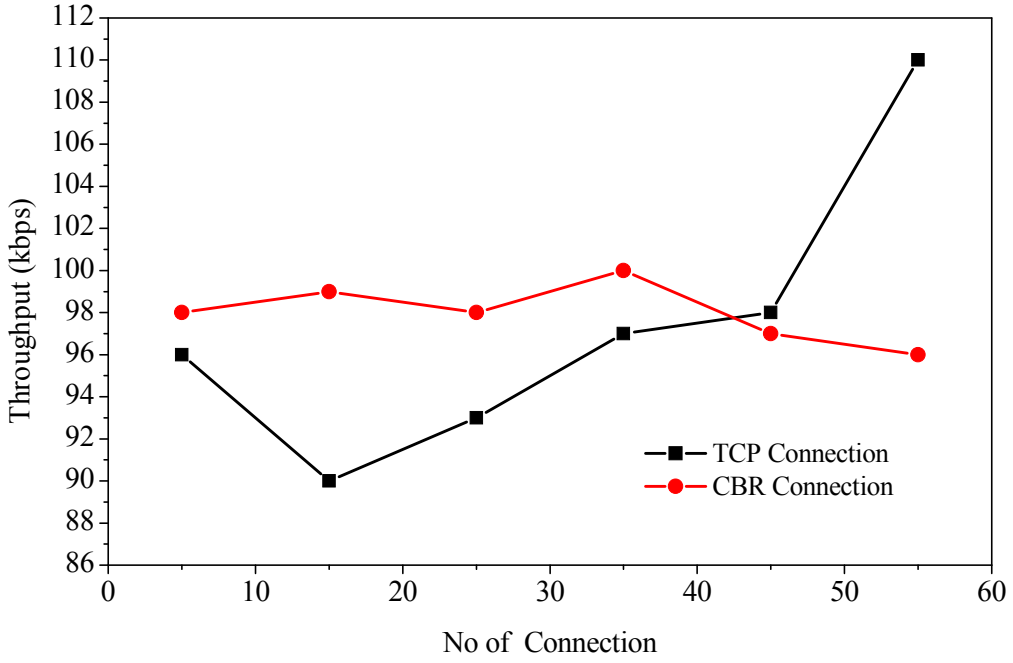


FIGURE 6.18: Average Throughput vs No of Connection

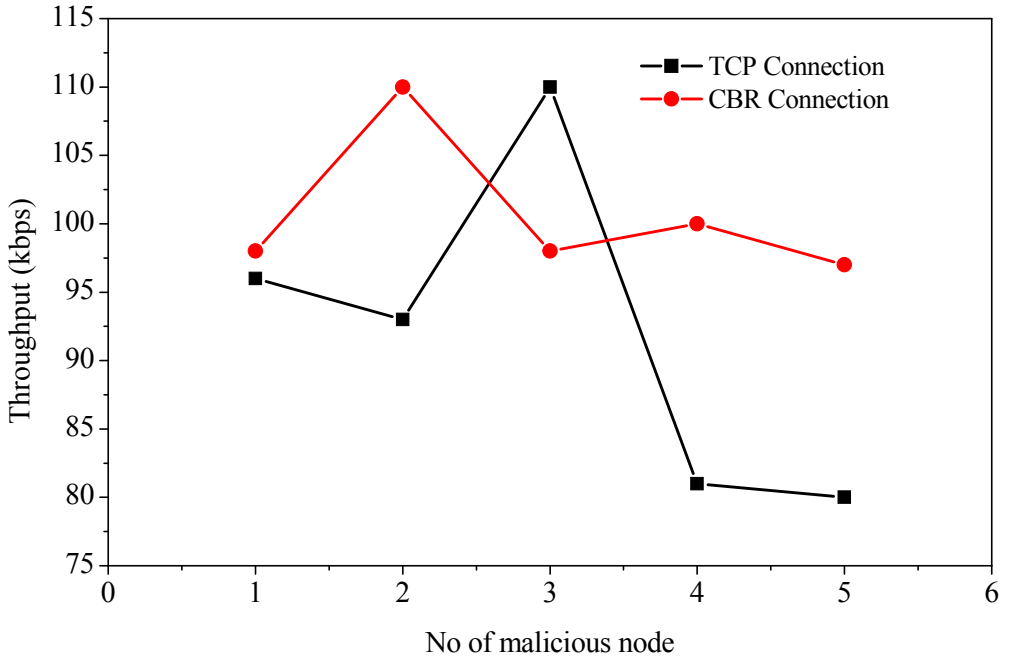


FIGURE 6.19: Average Throughput vs No of Malicious Node

for both CBR and TCP connection. Generally it is found that CBR connection has greater throughput than TCP connection.

6.3 Summary of Simulation Result

Summary of Simulation result from fig 6.1-6.19 have been depicted in following table Where, E2E – Average End to End Delay, PDR - Packet Delivery Ratio, Overhead - Average Routing Load, Throughput - Average Throughput

Table 6.1: Comparison Result Between CBR and TCP Connection

Matrics/ Parameter	Maximum Speed of Node	Pause Time	No of node	No of Connection	No of Malicious node
	CBR / TCP	CBR / TCP	CBR / TCP	CBR / TCP	CBR / TCP
E2E	Low / High	Low / High	Low / High	Low / High	Low / High
PDR	Low / High	High / Low	Low / High	Low / High	Low / High
Overhead	Low / High	Low / High	Low / High	Low / High	Low / High
Throughput	High / Low	High / Low	Low / High	Low / High	Low / High

6.4 Discussion

In this thesis two traffic scenarios that are TCP/FTP and UDP/CBR have been implemented in the network under test. To find the suitability from these two available traffics in a network various environments, like average throughput, packet delivery ratio (PDR) , average end to end delay and average Routing Load have been used. Then the results are compared. The various conclusions drawn from various experiments, observations, and analysis done in this thesis are as follows:

Average Throughput: Out of the two traffic types i.e. TCP/FTP and UDP/CBR, the former one provides far better performance than the latter. This proves that the network working with AODV provides better efficiency with TCP/FTP than UDP/CBR.

Packet Delivery Ratio (PDR): Although the PDR of UDP/CBR has greater maximum and minimum values than TCP/FTP, the latter offers almost a constant trend, whereas, the former offers highly varying (rising and falling trends), in all the four scenarios. Therefore, TCP/FTP is more reliable than UDP/CBR.

Average End to End Delay: The UDP/CBR offers lesser, average end to end delay, than TCP/FTP, therefore better speed of transmission, but as an exception in the scenario of number of nodes, as the density of nodes increases, the average end to - end delay also increases and the speed of transmission decreases.

Average Routing Load: The UDP/CBR exhibits lesser, average routing, than TCP/FTP, therefore better efficiency of transmission.

Chapter 7

Conclusion & Future Work

7.1 Conclusion

This study provided a detailed investigation of the operation and performance of AODV routing protocol and two traffic scenarios that are TCP/FTP and UDP/CBR. Using simulation, the performance of AODV routing protocol under these traffic scenarios was compared and concludes the better one for AODV.

This research shows that the better performance of AODV routing protocol of two traffic scenarios with TCP/FTP. TCP/FTP have better throughput, packet delivery ratio, average routing load than UDP/CBR. So TCP/FTP traffic scenarios is the best choice for AODV.

This thesis also present a simple mitigation technique of black hole attack. Which holds several advantage over other technique like simplicity, detection of multiple black hole etc.

7.2 Future Work

Ad-hoc networking is a rather hot cake in recent research of computer communications. This means that there is much research going on and many issues that remains to be solved.

- The behavior of TCP over ad-hoc network routing protocols should be an area of interesting research. From the simulation results, it can be seen that TCP exhibits several intriguing properties over ad-hoc network. Further research is required to understand fully TCPs behavior over ad-hoc network.
- Apply propose mitigation technique of black hole attack. Because black Hole Attack is a main security threat that affects the performance of the AODV routing protocol.

- Hand-over of real-time traffic between nodes. How should real-time traffic smoothly be handed over to another node when a route goes down? Should flooding be used before a route is found?
- Connecting ad-hoc networks to the internet through access point.
- Mobile IP: Integration of mobile IP into the ad-hoc networks.

Bibliography

[1] en.wikipedia.org/wiki/Wirelessadhocnetwork

[2] Sandeep Sandhu, Anirudh Menon, Parikshit Sinha, Nirav Afinwale, Payal T. Mahida ,"Comparative Analysis of TCP Traffic and UDP Traffic under AODV using Mobile Ad Hoc Network, ijarcsse Volume 4, Issue 5, May 2014.

[3] Vikas Singla, Ajay Kumar, Rakesh Singla, CBR andTCP Based Performance Comparison of Various Protocols of MANET: A Review, National Journal on Advances in Computing and Management, Vol. 1, No. 2, October 2010.

[4] Deepti Verma, Deepika Chandrawanshi, Comparative Performance Evaluation of AODV over CBR and TCP Traffic, IJCST, Vol. 2, Issue 2 June 2011.

[5] V.R. Sarna Dhulipala, R.M. Chandrasekran, R. Prabakaran, Timing Analysis and Repeatability Issues of Mobile Ad Hoc Networking Applications Traffic, International Journal of Recent Trends in Engineering, Vol.1, No.1 May 2009.

[6] Ajay Kumar, Ashwani Kumar Singla, Performance Evaluation of MANET routing protocols on the basis of TCP Traffic pattern, International Journal of Information Technology Convergence and Services (IJITCS), Vol. 1, No. 5, October 2011.

[7] Thomas Clausen, Philip Jacquet, Laurent Viennot, Comparative Study of CBR and TCP Performance of MANET Routing Protocols, Mindpass Center for Distributed Systems.

[8] Vikas Singla, Parveen Kakkar, Traffic Pattern based performance Comparison of Reactive and Proactive Protocols of Mobile Ad Hoc Networks, International Journal of Computer Applications, Vol. 5, No. 10, August2010.

[9] Y. C. Hu, A. Perrig, and D. B. Johnson, Ariadne:A secure on-demand routing protocol for ad hoc networks, in Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pp. 12-23, Sept. 2002.

[10] D. B. Johnson, D. A. Maltz, and Y. C. Hu, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), IETF Internet Draft, draft-ietfmanet-dsr-10, July 2004.

[11] M. G. Zapata, Secure Ad Hoc on-demand Distance Vector (SAODV) Routing, IETF Internet Draft,draft-guerrero-manet-saodv-03, Mar. 2005.

[12] Y. C. Hu, D. B. Johnson, and A. Perrig, SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, in The 4th IEEE Workshop on Mobile Computing Systems and Applications, pp.3-13, June 2002

[13] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer, Authenticated routing for ad hoc networks, IEEE Journal on Selected Areas in Communications," vol. 23, no. 3, pp. 598-610, Mar. 2005.

[14] Y. C. Hu and A. Perrig, A survey of secure wireless ad hoc routing, IEEE Security and Privacy Magazine,vol. 2, no. 3, pp. 28-39, May/June 2004.

[15] Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, Crossfeature analysis for detecting adhoc routing anomalies, in The 23rd International Conference on Distributed Computing Systems (ICDCS03), pp. 478-487, May 2003.

[16] Y. A. Huang and W. Lee, Attack analysis and detection for ad hoc routing protocols, in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID04), pp. 125-145, French Riviera, Sept. 2004.

[17] Dimitri Bertsekas and Robert Gallager, Data Networks - 2nd ed. Prentice Hall, New Jersey, ISBN 0-13-200916-1

[18] Charles E.Perkins. Ad hoc Networking, Addison-Wesley, 2001

[19] Theodore S. Rappaport, Wireless Communications: Principles and Practice. New Jersey, Prentice Hall. ISBN 0-13-375536-3.

[20] N. Abramsson-The ALOHA system another alternative for computer communications in AFIPS Conf. Proc., vol 37, FJCC,1970, pp. 695-702

[21] J.Jubin and J.D.Tornow, The DARPA packet radio network protocol, Proc. Of the IEEE, vol 75, No.1, Jan 1987, pp.21-32.

[22] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu and Jorjeta Jetcheva, A performance Comparison of Multi-hop Wireless Ad Hoc Network Routing Protocols. Mobicom98, Dallas Texas, 25-30October, 1998

[23] Larry L. Peterson and Bruce S. Davie, Computer Networks -A Systems Approach. San Francisco, Morgan Kaufmann Publishers Inc. ISBN 1-55860-368-9.

[24] Whats Behind Ricochet: A Network Overview http://www.ricochet.net/rico chetadvantage/techoverview.

[25] D.C.Steere et. al., Research challenges in environmental observation and forecasting systems MOBICOM 2000, pp. 292-299.

[26] C. E. Perkins, Ad hoc Networking, Pearson Publication.

[27] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks, SCS Communication Networks and Distributed Systems

[28] Modeling and Simulation Conference (CNDS 2002), Jan 2002. M. Zapata, N. Asokan, Securing ad hoc routing protocols, WiSe02, ACM 1-5813-585-8, September 28, 2002, pp.1-10.

[29] E. M. Royer and Chai-Keong Toh, A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks.

[30] A. Boukerche, B. Turgut, N. Aydin, M. Z. Ahmad, L. Blni, and D.Turgut, Routing protocols in ad hoc networks: A survey, Elsevier Computer Networks, 55 (2011) 30323080.

[31] C. E. Perkins and P. Bhagwat, Highly Dynamic Destination Sequenced Distance-Vector (DSDV) for Mobile Computers, Proc. ACM Conf. Communications Architectures and Protocols, London, UK, August 1994, pp. 234-244.

[32] T. H. Clausen et al., The Optimized Link-State Routing Protocol. Evaluation through Experiments and Simulation, Proc. IEEE Symp. Wireless Personal Mobile Communications 2001, Sept. 2001.

[33] S.Murthy, C. Siva Ram and B.S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall, Chapter 7, 2004.

[34] D. B. Johnson, D.A Maltz, and J. Broch, DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks, Ad Hoc Networking, C.E. Perkins, Ed., Addison-Wesley, 2001, 139-172.

[35] A. K. Gupta, H. Sadawarti, and A. K. Verma, Performance analysis of AODV, DSR and TORA Routing Protocols, IACSIT International Journal of Engineering and Technology, vol.2, vo.2, April 2010.

[36] Bijan Paul, Md. Ibrahim, Md. Abu Naser Bikas, Experimental Analysis of AODV and DSR over TCP and CBR Connections with Varying Speed and Node Density in VANET, International Journal of Computer Applications, Vol. 24, No. 4, June 2011.

[37] A tutorial named NS by example: http://nile.wpi.edu/NS

[38] NS2 installation instruction under windows operating system: http://140.116.72.80/ smallko/ns2

[39] NS manu Trace file record format http://wcc.iiita.ac.in/ns/ns2-trace-formats.htmlal http://www.isi.edu/nsnam/ns/ns-documentation.html

[40] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard : Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks.pdf www.sersc.org/journals/IJSEIA/vol2_no3_2008/4. pdf

[41] Hoang Lan Nguyen: A Study of Security Attacks on Multicast in Mobile Ad Hoc Networks www.cse.yorku.ca/ lan/defense.pdf