FACULTY OF COMPUTING AND INFORMATION MANAGEMENT

HYHRID TRUST MODEL TO PREVENT BLACK HOLE ATTACK IN MOBILE AD-HOC NETWORK

By

PAUL NDETO MUSAU

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF DEGREE OF MASTER OF SCIENCE IN DATA COMMUNICATIONS IN THE FACULTY OF COMPUTING AND INFORMATION MANAGEMENT AT KCA UNIVERSITY.

OCTOBER, 2016

DECLARATION AND RECOMMENDATION

DECLARATION

I declare that this research project is my original work and has not been previously presented elsewhere for the award of degree in any university. I also declare that this research project contains no material written or published by other people except where due reference is made and author duly acknowledged.

Paul Ndeto Musau

REG. NO.: 13/03381

Sign: …… Date: …….

RECOMMENDATION

This research project has been submitted for examination with my approval as the University supervisor.

Faculty of Computing & Information Management

KCA University

Supervisor's Name…**RACHAEL KIBUKU**…. Sign: ……Date: ……

ABSTRACT

Mobile Ad Hoc Network is an emerging technology which allows nodes to communicate together irrespective of where they are located. MANET is composed of mobile devices with self-configuring capability and which exchange information wirelessly without any fixed network infrastructure. Due to the infrastructure-less nature, these mobile devices have to both route and forward traffic for their neighbors.

The neighbor discovery and routing functionality is achieved using the major routing protocols namely AODV, DSDV and DSR. Devices in MANET exhibit high mobility nature, thus the wireless network topology changes rapidly. This change results to new nodes arriving, old ones leaving a certain coverage area, and consequently arise a need for each device to search for updated routing information.

Due to continuous topology instability, MANETs are vulnerable to malicious attacks such as black-hole. The black hole attack involves a malicious node faking a route to unsuspected destination node. This project defines the design and implementation of a model to verify new nodes arriving in MANET so as to avoid chances of them establishing a black-hole attack. The model shall focus on introducing a probe RREQ packet and a trust concept to measure an expectation which a node will have about another's future behavior for a certain activity.

TABLE OF CONTENTS

DEDICATION

I dedicate this research to my loving wife Hilda Mwelu and my parents Philip M. Mueke and Jane N. Musau for the encouragement they gave me all along.

I also dedicate it to my siblings, relatives and friends who assisted me at different levels towards achieving this degree programme.

ACKNOWLEDGEMENT

All the praises go to the Almighty God for his love, good health and blessings that were key to accomplishing this research project.

I greatly express my honor and appreciation to my defense supervisor Rachael Kibuku for her support in fine tuning this work.

Last but not least, I wish to thank my family members and classmates for the support and inspiration they accorded me throughout writing this research project.

LIST OF FIGURES AND TABLES

ABBREVIATIONS AND ACRONYMS

ZRP – Zone Routing Protocol

TORA – Temporally-Ordered Routing Algorithm

RREQ – Route Request

RREP – Route Reply

RERR – Route Error

DSR – Dynamic Source Routing

DSDV – Destination Sequenced Distance Vector

OLSR – Optimized Link State Routing

AODV – Ad-hoc On-demand Distance Vector

AOMDV – Ad hoc On-demand Multipath Distance Vector

UCLA – University of California, Los Angeles

ISO/OSI – International Standardization Organization / Open System Interconnect

OSPF – Open Shortest Path First

FSR – Fisheye State Routing

FSLS – Fuzzy Sighted Link State

TBRPF – Topology-Based Reserve Path Forwarding

CSMA – Carrier Sense with Multiple Access

MAC – Media Access Control

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

IP – Internet Protocol

Ad Hoc – A Latin word meaning, “for this only”

TRREQ – Test Route Request

TRREP – Test Route Reply

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND OF THE STUDY

An ad hoc network is a collection of wireless mobile nodes, which form a temporary and unpredictable network without the help of a centralized administration found in conventional networks (Madhusudhananagakumar & Aghila, 2011). A MANET can be connected to internet, external network or can be a standalone network. The technology focuses on the establishment of networks consisting of devices that are self-configuring, self-healing and collaborate amongst each other to enhance communication. According to (Nigam & Verma, 2014), the ad hoc network does not rely on a pre-established infrastructure like routers, access points and switches found in a wired and wireless network. The devices are organized to help each other in routing and delivering data throughout their neighborhood as some nodes may be several hops between each other (Nigam & Verma, 2014).

The links between the mobile devices in a MANET may change rapidly depending on the devices' mobility speed, power and bandwidth constraints. To ensure efficient communication between the mobile devices, the routing protocols must be designed to effectively adapt to the physical limitations and constraints surrounding the ad hoc environment, and be able to trace routes in spite of the dynamic nature of the topology (Kavitha & Krishnakumari, 2014). Due to the ever changing data routing environment, it becomes challenging for devices to trust each other as they forward and exchange information.

The nodes aiming at harming the MANET, take advantage of this challenge to either intercept or modify the data on transit or consequently drop the messages introducing a Denial of Services attack. Reactive routing protocols such as AODV are efficient in MANET operations since routes are discovered when needed or if a topology change is experienced while data

transmission is going on (Abdelshafy & King, 2016). The topology change may be caused by a new node's arrival, a node leaving the MANET, or a failed link. Since routes are discovered when they are needed for use in AODV, then a malicious node may fake a route to a destination as requested by its victim causing the black hole attack (Singh & Singh, 2014).

Bakshi, Sharma & Mishra (2013) pointed out the following advantages and disadvantages in deployment of a MANET:

1.1.1 Advantages of MANET

i) Running a MANET is affordable as they do not require a backbone infrastructure support as in traditional networks.

ii) The deployment of the MANET is easier as it does not require an already existing infrastructure.

iii) It offers an excellent support to node mobility making it suitable to use in emergency operations.

iv) The routing protocols in MANET are capable of keeping the network fault tolerant.

1.1.2 Disadvantages of MANET

i) The wireless transmission channel in MANET is shared thus reducing the bandwidth capacity among the participating nodes.

ii) Most of the devices' CPUs in MANET are not as powerful as the task they are subjected to.

iii) Devices are battery powered which is drained as more tasks are executed.

iv) Some of the nodes are put in sleeping or idle states if not transmitting any data. This causes a high latency when data is transmitted through them.

v) MANETs are prone to transmission errors due to attenuation and interferences.

vi) Due to high node mobility, decentralized management and unsecure boundaries, the MANET is subjected to several security threats.

The structure of Ad Hoc Network

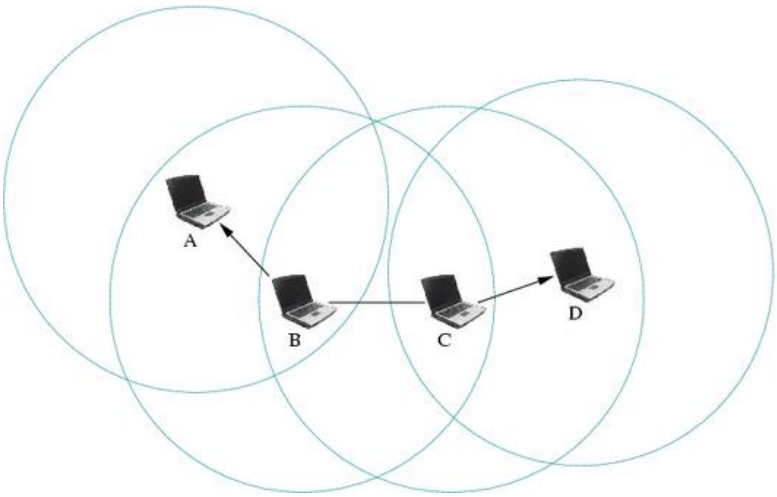

Figure 1.0: The structure of an ad hoc network

1.2 PROBLEM STATEMENT

In MANET, nodes can join or leave the network at any time leading to broken links between nodes or availing new better routes between them. Again, the nodes' operations are powered by batteries; their exhaustion can too lead to broken links. In all these scenarios, the MANET using AODV routing instance is subjected to black hole Attack (Ochola & Eloff, n.d).

The failure by the current security models to verify new nodes arriving in a MANET have triggered the research in this area. The research proposes a hybrid model which identifies and eliminates all suspicious nodes arriving in a MANET.

1.3 RESEARCH OBJECTIVES

1.3.1 Main Objective

The research focuses on getting a proactive trust based mechanism which strengthens the AODV's defense capability against a black hole attack.

1.3.2 Specific Objectives

The specific objectives of the research are:

i. Evaluate the current security approaches that have been employed to mitigate the black hole attack.

ii. Identify and define the controls and measures to be used in building the model.

iii. Design a model to verify new nodes arriving in a MANET and set trust values within specified period of time.

iv. Implement and validate the model in a simulation environment.

1.4 SIGNIFICANCE OF THE STUDY

MANET is a promising networking technology as its areas of application are increasing. The current increase in the use of portable devices and advances in the wireless technologies has raised the interest in doing research on MANETs. MANETs can be used in areas with little or no networking infrastructure or in situations where the established infrastructure is expensive or poses challenges to use (Bang & Ramteke, 2013). Some of MANET applications include, helping coordinate rescue operations in emergent events such as fire outbreaks and earthquakes, facilitate sharing of information among contributors in a conference hall or a classroom, and enhance communication among soldiers in a military battlefield (Bang & Ramteke, 2013). Most of areas of application of MANET require the transmission of the information to be reliable, accurate, timely and secure. For instance, in the case of a military battlefield, the success of the attacking soldiers is depended on the reliability and security capability of the established MANET. MANETs are faced with several security issues that may render the network unreliable or useless at the required time. The black hole attack is one of the major security challenge in MANET as its activities involve dropping packets or reading their contents (Gurja & Dande,

2013). The design and implementation of MANETs should address the initiation of black hole attack as the attack poses a critical threat in data communication.

1.5 SCOPE OF THE STUDY

The scope of this study is limited to implementing a proactive trust model in a MANET, which will verify the trustworthiness of new nodes before and after taking part in MANET operations. The research shall concentrate on identifying malicious nodes using probe packets and trust level values based on the characteristics observed in nodes' behavior. It is assumed that:

a) MANETs are equipped with auto-configuration capabilities.
b) Each node in the network can be distinguished from the others using a unique ID such as the physical network interface address.
c) The nodes have monitoring mechanisms at network or application layer to observe the neighbor's behavior.

The research proposes to use NS-2.35 simulation tool to implement the enhanced AODV routing protocol instance and investigate its efficiency under the attack.

CHAPTER 2: LITERATURE REVIEW

2.1 INTRODUCTION

This chapter focuses on giving out literature review on the routing protocols used in the MANETs, the AODV operation, the Network Layer attacks in a MANET environment and evaluation of various approaches that have been suggested to prevent the black hole attack.

2.2 CURRENT ROUTING PROTOCOLS IN MANET

Routing protocols are rules used by network devices to guide them as they communicate with each other. They facilitate sharing of route information amongst these devices which they use in selecting best paths to forward data traffic. In MANET, routing protocols should be designed with the ability to cope with the ever changing topology, little wireless bandwidth and the transmission ranges which may be affected by the drainage of the devices' power (Hinds, et al., 2013). Suggested here below are classifications of the MANET routing protocols:

2.2.1 Proactive (Table-driven) Routing Protocols

These protocols depend on a maintained routing table consisting of well-known paths to the destination nodes. There is little overhead created as traffic rarely depends on control packets. However, the periodic update packets exchanged amongst neighbors negatively impact the bandwidth and drain the power of the nodes. In a highly dynamic environment, this protocol is not efficient as sending of more topology change packets lead to the degradation of network performance (Hinds, et al., 2013). Protocols in this category include DSDV, OLSR, OSPF, FSR, FSLS and TBRPF.

2.2.2 Reactive (Source-Initiated On-demand Driven) Routing Protocols

These protocols do not maintain specific paths to the destinations in a routing table. A route is only discovered when a need arises. This is achieved by the source flooding the network with route request packets which is followed by route reply packets from various destinations. The routing process presents vulnerabilities to the network. The flooding of the route request packets consumes high bandwidth which significantly leads to network route discovery delays (Hinds, et al., 2013). Reactive routing protocols include AODV and DSR.

2.2.3 Hybrid Routing Protocols

This routing protocol was established on the aspects of both proactive and reactive abilities (Gupta, et al., 2016). It achieves its goal through balancing the less control traffic overhead in proactive protocols and reducing route discovery delays in reactive protocols as it maintains a routing table. Examples are ZRP and TORA.

2.3 AD-HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

AODV is a collaborative protocol based on classic bellman ford routing algorithm. It combines the strengths of DSR and DSDV routing protocols. It uses sequence numbers and periodic beaconing to discover routes. The sequence numbers indicate the freshness of a route and prevent the occurrence of routing loops (Gurja & Dande, 2013).

(Ochola & Eloff, n.d) explain that every node maintains its sequence number in the routing table and increments it whenever a new RREQ or RREP is generated. A higher sequence number refers to the most recent route information. All the nodes within the traffic route, must temporarily maintain the routing information in the routing table until the communication terminates (Nigam & Verma, 2014). The information kept in the routing table include: destination address, next hop address, hop count, destination sequence number, active neighbors

and lifetime. Since AODV is a reactive protocol, routes are made available when a need arises and any route which may not have been used recently is expired. Being a distance vector routing protocol, AODV does not give a complete overview of the network topology but only the next hop node's address and the number of hops to the destination. AODV is capable of handling both unicast and multicast data traffic.

2.3.1 The Operation of AODV Routing Protocol

2.3.1.1 Neighbor Discovery

In MANET, the nodes that can communicate together directly are considered to be neighbors. Each mobile node periodically sends a broadcast Hello message to keep its neighbors within one hop. The hello message's time to live is set to value 1. When a neighbor receives a hello message, it updates its local connectivity information to the node that broadcasted it.

The hello message informs the neighbor node about the activeness of a link. Hello message received from a new neighbor, indicates a change in the local connectivity. If a node fails to receive hello message from its neighbor for several time intervals, it assumes that the neighbor is no longer within the transmission range and the connectivity has been lost.

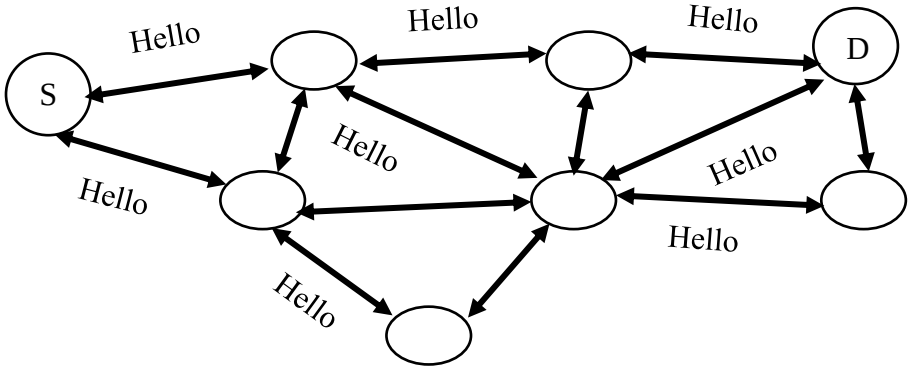

Figure 2.1: Exchange of Hello Message in AODV

Node's IP Address	Sequence Number

Figure 2.2: AODV Hello Message format (Choi, et al., n.d)

2.3.1.2 Route Discovery

According to (Singh & Singh, 2014) the route discovery process utilizes three types of packets: Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages. When a source node wants to communicate with a destination for which it does not have a route, it broadcasts a Route Request (RREQ) packet to all connected nodes. Each node receiving this packet updates its table for the source node and sets up backward pointers. (Gupta, et al., 2016) points out that the RREQ packet contains information about the source's IP address, current sequence number, the broadcast ID and the most recent sequence number for the destination which is known to the source node. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies the RREQ.

Source Address	Request ID	Source Sequence Number	Destination Address	Destination Sequence Number	Hop Count

Figure 2.3: RREQ Packet Format (Vasanthavalli, et al., 2014)

On receiving the RREQ packet, the intermediate node checks its table for a route to the desired destination. If a route is found, it compares the value of the sequence number supplied with the one in the table. If the table's value is higher than the supplied, it generates a Route Reply (RREP) message; else it rebroadcasts the RREQ message.

During the process of forwarding the RREQ, intermediate nodes record in their routing table the address of the neighbor from which the first copy of the broadcast packet was received, therefore establishing a reverse path. If additional copies of the same RREQ are later received, they are discarded.

Source Address	Destination Address	Destination Sequence Number	Hop Count	Life Time

Figure 2.4: RREP Packet Format (Vasanthavalli, et al., 2014)

2.3.1.3 Maintenance of the route

AODV supports low, moderate and high mobility rates. In the event that the source node moves while the data is being transmitted, it can restart the route discovery process to complete the transmission. At other times, an intermediate or destination node may move causing a broken link. This triggers one of the upstream nodes to send a Route Error (RERR) message to the source node, notifying it of the lost connection to the destination node. If the source node had not yet completed the data transmission, it reinitiates the route discovery process again. (Gupta, et al., 2016)

2.3.2 Security Goals in MANET

Securing a mobile ad hoc network is a challenging task since all networking functions like routing and data forwarding are executed by the participating nodes in a self-organizing way. According to (Lalar, 2014) the following parameters can be used to evaluate the security strengths in a MANET.

2.3.2.1 Availability

This implies that the network resources are provided to the authorized nodes at the required time. These resources include both data and the network services and ensures the tolerance of the network in the events of attack.

2.3.2.2 Confidentiality

This feature ensures that the resources are accessible only to the authorized nodes by setting up different privacy levels and classifying the information exchanged among the nodes.

2.3.2.3 Integrity

Integrity ensures that data packets can only be modified by the authorized parties. Modification occurs when the data packet contents are altered either by deleting or inserting extra bits.

2.3.2.4 Authentication

Authentication ensures that the identity of nodes establishing a communication session is correct and they are whom they claim to be. This process is achieved by use of secret keys or a combination of public and a private key.

2.3.2.5 Non repudiation

It ensures that the sender and the receiver cannot ever deny sending or receiving a communication message.

2.4 ATTACKS IN MANET

Routing is a vital mechanism in ad hoc network. As most ad hoc networks are established on untrusted environments, improper and insecure routing procedures render the network into degraded performance as well as exposing it to many types of security attacks. These attacks have been categorized into external and internal attacks.

The internal attacks are executed by a legitimate node within the MANET while the external attacks are performed by unauthorized nodes which are outside the network. The other classification of the attacks is based on the TCP/IP protocol layer they invade. According to (Panicker & Jisha, 2014), attacks at the Network Layer include:

2.4.1.1 Spoofing Attack

In this attack, a node attempts to take IP identity of another node. The malicious node may send fake RREP packets claiming to have a route to a spoofed destination address. If it succeeds, it receives all the packets, modifies or drops the packets (Madhuri, et al., 2014).

2.4.1.2 Wormhole Attack

The attacker receives packets and tunnels them to another colluding malicious node in the network. The tunnel is advertised as having shortest path to the destination thus attracting many data packets. Later, the attacker replays these packets across the network disrupting the routing process. Since the attackers have the overall control over the data across the tunnel, they may drop or intercept the packets (Panicker & Jisha, 2014).

2.4.1.3 Sinkhole Attack

The attacker prevents the cluster head or the base station from getting sufficient and correct information from other nodes. The malicious node attracts data packets to itself from its neighboring nodes and thereafter alters, drops or forwards them selectively (Goyal, et al., 2010).

2.4.1.4 Sybil attack

In this attack, there exist several identical malicious nodes. It happens if a malicious node distributes its secret key to other malicious nodes increasing the chances of an attack (Panicker & Jisha, 2014).

2.4.1.5 Routing Table Poisoning

The attacker alters the route entries in the routing table. This attack may also be executed by injecting a RREQ packet with a high sequence number leading to deletion of RREQ with a low sequence number. Consequently, nodes select wrong routes (Ponsam & Srinivasan, 2014).

2.4.1.6 Rushing Attack

In this attack, the malicious node intercepts the RREQ packets transiting from the source to the destination nodes. The attacker performs duplicate suppression mechanism and replays the duplicate packets to the receiver continuously keeping the destination node's resources busy. It ensures that its duplicate RREQ packets are the first to reach the receiver, before other nodes

receiving the same RREQ packet can react. Later, when other nodes receive the legitimate RREQ packets, they assume these packets are duplicates and discard them. The attacker meets its goal by ensuring its presence in any route discovered by the source node (Panicker & Jisha, 2014).

2.4.1.7 Byzantine Attack

In this attack, a malicious node or a set of malicious nodes collude to create rooting loops, forwarding packets on non-optimal paths and selectively discarding the packets. The routing services are either disrupted or degrade (Madhusudhananagakumar & Aghila, 2011).

2.4.1.8 Gray hole Attack

Gray hole attack is a variant of black hole attack except that it may discard data packets selectively or statistically.

2.4.1.9 Black Hole Attack in AODV Routing Protocol

Black hole problem is a Denial-of-Service attack which occurs when a malicious node exploits AODV and claims to have the shortest path to a destination node (Tseng, et al., 2011). On receiving a RREQ message from a neighboring node, the malicious node sends a fake RREP message with the highest sequence number to the source node. (Ochola & Eloff, n.d), argue that the malicious nodes would not be successful if a RREP message from a normal node reaches the source node first. However, since malicious nodes do not check their routing tables, their RREP messages would consequently be the first to reach the source node.

When the source node receives the RREP message, it assumes that the route discovery process is complete and initiates the data transmission session. On acquiring the route, the malicious node eavesdrops on all the packets or drops them introducing a Denial-of-Service attack.

Black hole attack may be executed by a single malicious node or several nodes working cooperatively. In the figure below, there are 6 nodes where node S generates RREQ to find a fresh route to the destination node D. Nodes 1 and 2 are the intermediate nodes to node D. When node B receives the RREQ packet, it responds to node S with a RREP packet containing a high sequence number, claiming to have the shortest path to node D. Node S, thereafter discards any further RREP it receives as it assumes the discovery is complete. Node B dictates the fate of the packets it receives from node S.

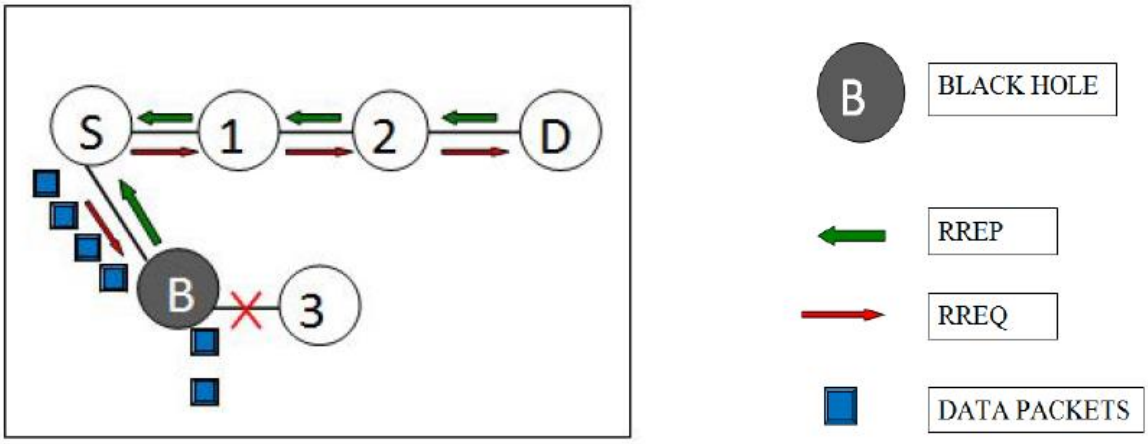

Figure 2.5: Black Hole attack (Vasanthavalli, et al., 2014)

2.5 EVALUATION OF APPROACHES THAT HAVE BEEN USED IN MITIGATING BLACK HOLE ATTACK

Previously, many researchers have proposed several algorithms and procedures to eliminate the black hole attack. Currently, the focus should be driven to establishing efficient proactive mechanisms to avoid the black hole attack.

2.5.1 Trust Based Management Schemes

Trust is an important aspect in mobile ad hoc networks as it ensures nodes handle the uncertainty and uncontrollability in the mobile ad hoc network environment. Working out and managing trust factors in MANET is challenging since it is subjected to complex computational constraints

(Sharma & Jain, 2012). Trust can either be computed directly depending on a node's observation and experience about another's behavior, indirectly through a recommendation or a combination of the two mechanisms.

Through keeping trust history for each node, trust evaluation can be done which assists in isolating good nodes from malicious ones. Trust can be managed using the following parameters: Packet delivery ratio, packet dropping ratio, throughput, network congestion and end to end delay. According to (Singh & Jain, 2014), trust can be classified as follows:

a) **Trust as a risk factor**: Risk is taken when there is no prior information about the node's behavior in the network.
b) **Trust as a belief**: A node believes that another node will act on data traffic normally.
c) **Trust as subjective probability**: Trust expressed as a measure of expected behavior of peers in a specified period of time.
d) **Trust as transitive relationship**: Expresses trust as transitive function, that if node K trusts L and node L trusts M, then node K trusts M.

There has been proposed several trust models which concentrate on strengthening the AODV routing protocol. (Garg & Rewagade, 2013) have proposed a model which quantifies the trust worthiness of all nodes by maintaining history table consisting of sent and received packets. In this model, the trust value T is calculated as follows: $T = R/S$ where S is send packets and R is received packets. The trust value ranges between 0 and 1 with the median of trust values of all nodes being the threshold value. Once a node joins the network, its trust value is set to 0.5. This value changes with respect to the trust value. When the trust value of a node is less than threshold, it is marked as suspicious, else it is a reliable node.

(Sharma & Jain, 2012) established a network model of Trust (AODV) which adds some fields into the routing table. These fields enable a node to keep opinion on trustworthiness of neighbor nodes and record their positive and negative actions. The model is made up of three modules: basic AODV routing protocol, a trust model and trusted AODV routing protocol. It utilizes trust recommendation, trust combination, trust judging, cryptographic and trusted routing behaviors, and trust updating.

Tiwari has proposed an extended AODV namely Trust with Delay Calculation AODV (TWDCAODV). The scheme uses trust values to rank the nodes. The trust values are depended on the node's ability to forward both data and control packets. This ability is derived by counting the number of packets send and those received. The model introduces two weight factors, W1 and W2 which signify the ratio of number of data packets sent to those received and the ratio of number of RREQ received to the number of RREP sent respectively. W1 has a maximum value of 1. The higher the value, the higher the reliability of the node. The product of the two weight factors gives the trust value of the node. This model dictates the transmission of data through a more trusted path rather than the shortest path.

(Gayathri & JanakiRaman, 2015) have suggested a trust framework which promiscuously monitors packets forwarded by a node. Packets which have recently been sent for forwarding are stored in a cyclic buffer. When the packets are forwarded, they are deleted from the buffer and the node's trustworthy increments by one, else it is decremented by one.

(Sharma, et al., 2014) have proposed a model which uses a trust function to build on trust relationships. This approach categorizes nodes as unreliable, reliable and most reliable depending on a set threshold value. In this scheme, each node must retain a trust table which

keeps its neighbors' trust states. A node joining the MANET is marked as unreliable. This status changes with respect to a proposed trust estimation function used to find the trust metric.

2.5.2 Other Approaches used in Mitigating Black Hole Attack

2.5.2.1 PreLude and PostLude (PL2) Method

(Vasanthavalli, et al., 2014) proposes PL2 method which is an enhancement of AODV routing protocol. In this method, the protocol prevents the black hole attack by searching for secure paths. The method checks for existence of malicious activities, detects the suspicious node and then works to remove it. This process is depended on Postlude packets which must be received by the source node within a specified period of time so as to clear the suspicion on the destination node.

2.5.2.2 Distributed Clustering Approach

(Singh & Singh, 2014) have proposed a methodology of arranging nodes into different clusters with each cluster having a cluster head and a check point. In this method, every node within a cluster must acknowledge with cluster head, else it is assumed to be a black hole node. The check points are used to monitor the cluster heads for malicious activities.

2.5.2.3 Multi Stage Authentication

(Madhuri, et al., 2014) have proposed a two stage authentication to prevent black hole attack. The implementation requires each node to affix the one's compliment of its IP address and then signs the destination address with the public key. The destination node tests the authenticity of its source by adding the affixed one's complement and the source address known to it to get all ones. This process isolates new nodes arriving at the MANET's range since it assumes that all nodes participating in MANET are aware of the requirement to appending process and all have

each other's IP addresses in the routing table. AODV is a distance vector routing protocol, thus does not give a complete view of the network topology. If a node fails the authenticity process, it is broadcasted as a malicious node. Thereafter, the method uses a further request procedure to confirm the node. The process is not efficient as the measures used may take long to confirm the threat a node poses in a MANET.

2.5.2.4 New Enhanced Secret Sharing Scheme (NEPSSS)

(Kaur & Singh, 2015) have proposed a two stage approach of detecting black hole attack with secret sharing procedures to keep the authenticity of the data being transmitted across the network. The approach is built on AOMDV which makes the network fault-tolerant as it keeps several loop-free paths.

Nodes sharing information use public and private keys to authenticate each other and check for the message integrity. This approach may lead to drainage of node's energy and high consumption of memory due to the processing and storage of multiple paths. The continual integrity and authentication checks may too result into a significant delay in the network's performance.

2.5.2.5 Using Control Packets to Detect Black Hole Node

(Tiwari & Yadav, 2015) have proposed an approach where a RREQ packet is modified to have two IP addresses of destination node. However, one of the IP address is invalid and aims at identifying a node which may be presenting black hole activities. The new RREQ packet is called DRREQ (Route Request with Detection). Since a black hole node does not check for routes in its routing table, it will end up sending a DRREP (Route Reply with Detection) packet to the source for the both IP addresses. On receiving the DRREP packet for the invalid IP

address, the source node marks the replying node as malicious and notifies all its neighbors to blacklist it.

2.5.2.6 Source and Destination Sequence Number Margin

(Jaiswal & Kumar, 2012) have proposed a method of checking for the difference in the sequence numbers between the source node and the node replying with a RREP packet. They have assumed if the difference is too large, then the reply must have come from a malicious node. The node is then removed from the Route Request Table.

2.5.2.7 BRM – AODV Protocol

(Abdelshafy & King, 2016) have recommended Self-Protocol Trustiness (SPT) a mechanism which clarifies that, "detection of a malicious intruder is accomplished by complying with the normal protocol behavior and lures the malicious node to give an implicit avowal of its malicious behavior." Though the method ignores the use of cryptographic techniques, it modifies the original AODV by keeping the last three per hop times for RREP received for a destination. The per hop time is a value signifying the time taken before a node receives a RREP packet corresponding to an earlier send RREQ packet divided by the hop count included in the RREP.

Each node monitors its neighbor's behavior trying to identify any malicious activities. This is achieved by nodes occasionally sending a fake RREQ packet from a non-existing source IP to unknown destination IP. If the source node receives a RREP packet to any of its fake RREQ packet, then the replying node is marked as a black node by updating its trust level to a threat.

2.5.2.8 Three Way Technique for Preventing Black Hole Attack in MANET using AODV

(Joshi & Kumar, 2016) have suggested a method which identifies three paths to the destination node. The data packets are sent through the first selected path where a destination is expected to

acknowledge with a value matching its sequence number. In the event there is no match, then the replying node is declared as a black hole node and removed from the route list.

2.5.2.9 According to (Jain & Gupta, 2016) the black hole attack can be prevented by introducing these concepts: Broadcast hello packet, suspicious node detection and suspicious node prevention. The proposed mechanism verifies the hello packets which are broadcasted by intermediate or destination nodes. On receiving the broadcast, each node finds the hardware ability of every node and checks it against a set threshold value. Any node identified with unrealistic capabilities is advanced to malicious node status. The prevention mechanism implemented shuts down such nodes to avoid their perceived activities.

2.5.2.10 (Mokbal & Saeed, 2016) have suggested an implementation of a detection method at the source node and intermediate nodes. This procedure involves extracting the destination's sequence number from the routing table and adding to it a predefined value known as gap. The sequence number in the RREP message is extracted too. If it is found that the sequence number in the RREP message is larger than the one in the routing table + gap, then the node which sent the RREP message is entered into the blacklist.

2.6 DETERMINING LINK QUALITY IN MANET

Link quality is a measure which defines the number of packet errors that occur in a network. It can be compromised when all nodes in MANET compete for the bandwidth leading to inter-flow interference (Terdal, et al., 2012). Link quality plays an important role in determining the cause of packet loss in AODV routing protocol.

According to (Gaertner & O'Nuallain, n.d.), link quality prediction algorithms can be categorized according to the input they use in computation. Some of these inputs are, the ratio of transmitted packets to those received in a time interval, signal-power values, and location measurements. A

prediction is deterministic if its output is a subset of a finite set of states. This implies that, packets are expected to be dropped or received successfully within time interval t, in future.

2.7 MANET RESEARCH TECHNIQUES

In order to detect, prevent and analyze the impacts of a black hole node in a MANET under AODV, the following techniques have been applied:

- Analytical Modelling
- Testbeds
- Emulation
- Simulation

2.7.1 Analytical Modelling

The parameters in a MANET exhibit changes which can be expressed as a mathematical analytic function. This method needs these parameters to be simplified so as to obtain the required model with an enhanced performance. However, (Salem & Awwad, 2014) doubt this possibility due to the complex nature of MANETs.

2.7.2 Testbeds

In a testbed, a researcher can use software, actual hardware and networking devices to perform an experiment. Although a testbed may give credible outputs, they are faced with challenges such as the required hardware infrastructure and the effort needed to construct the artifact environment. This implies that the testbed can only work with less number of nodes (Salem & Awwad, 2014).

2.7.3 Emulation

It is a method which combines the hardware and software capabilities in a networking system. Some of the features can be implemented using physical devices while others can be simulated in software (Salem & Awwad, 2014).

2.7.4 Simulation

The method is inexpensive and flexible as it enables the researchers to carry out customizable experiments without the use of physical networking electronics. Many aspects of a network system such as bandwidth, latency and packet loss rate can be collected, tested and analyzed. Most network simulators suffer from the inability to ascertain whether the behavior they exhibit during simulation correspond to a real network environment (Salem & Awwad, 2014).

CHAPTER 3: RESEARCH METHODOLOGY

3.1 INTRODUCTION

Research methodology can be defined as set of tools, methods, techniques and documentation used to investigate a problem in an area of study through collecting and analyzing data, and making a substantive conclusion. This work investigates the two main types of scientific research methodologies namely quantitative and qualitative and selects the most suitable to be used in attaining the objectives of the research.

3.2 QUANTITATIVE APPROACH

In this methodology, a problem is explored through data collection, experiments and simulation with an aim of obtaining results. The results are analyzed and conclusions are drawn. The approach is suitable when the researcher is focused on testing hypothesis, looking at causes and effects, and making extrapolations.

3.3 QUALITATIVE APPROACH

This method focuses on learning and comprehending the experiences, perceptions and opinions of the observer. It consists of activities that discover the observer in the world and turn the domain of focus into a series of illustrations, interviews, note taking, videos and photographs. This approach is most suitable when the investigator is keen on exploring a particular phenomenon.

3.4 THE PROPOSED RESEARCH APPROACH

The researcher proposes to use quantitative approach by building a simulation model. Initially, the various mechanisms which have been suggested to be used in mitigating the black hole attack are evaluated in the literature review. The simulation model is built after identifying the suitable

control parameters and test metrics. The results obtained from the simulation are analyzed with respect to the test metrics and conclusions are made.

3.5 DESIGN SCIENCE RESEARCH METHODOLOGY.

This methodology comprises a set of systematic procedures and perspectives for doing research in computer information systems. It involves designing an artifact and investigating it with an aim of getting a solution to an already established problem (Prat, et al., n.d.). Using this approach, the research work is arranged as follows:

i) Identification, selection and justification of the research problem
ii) Definition of the objectives of the research work
iii) Literature review and evaluation of black hole attack mitigation techniques
iv) Model requirement analysis, designing, building and testing.
v) Analyzing and evaluation the simulation results

3.5.1 Justification of the Design Science Research

This methodology is most suitable for this research as it helps accomplish the following:

i) It gives a systematic approach of executing the research work and adequately investigate and evaluate an issue.
ii) The method is objective oriented and helps in the process of designing an artifact with a focus on the solution.

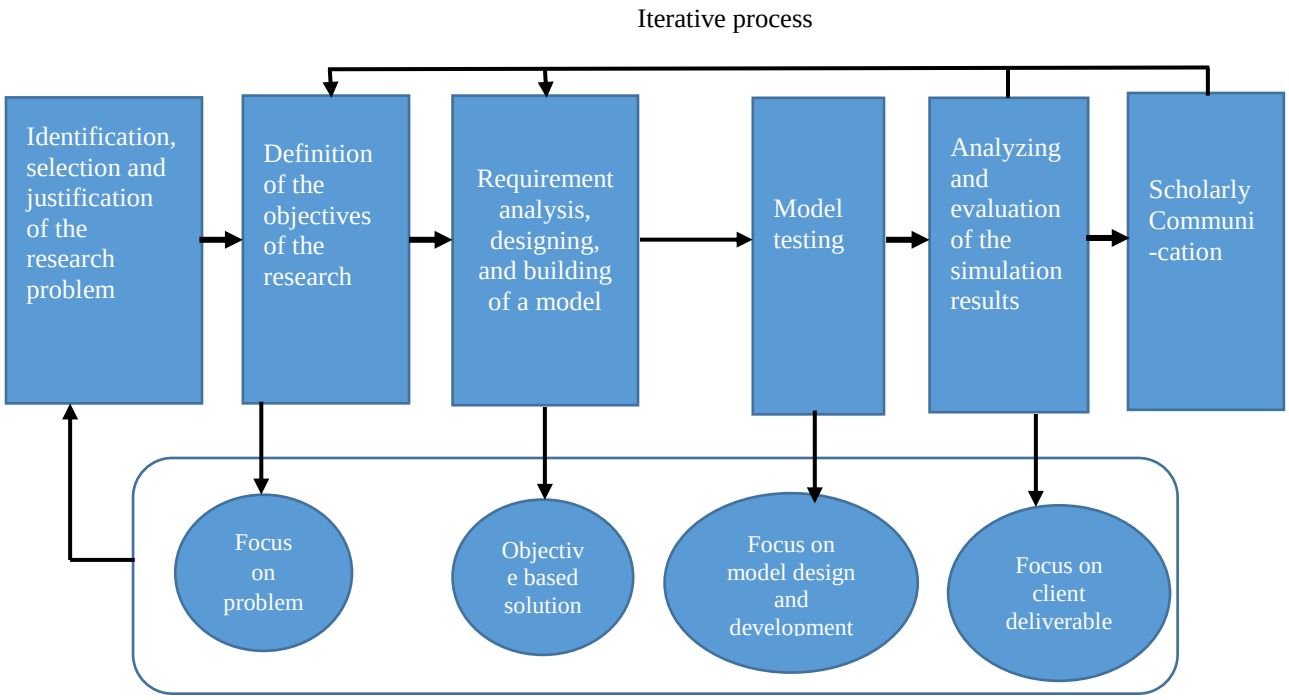

Figure 3.1: Research Methodology (Macario & Ondrejka, 2014)

3.6 EVALUATION OF MANET SIMULATION TOOLS

Simulation is an economical way of carrying out experiments without the use of the real networking hardware. (Salem & Awwad, 2014) have defined a network simulator as a software program that copies the functionalities of a computer network. Since there exist several network simulators, it is hard to select a suitable one for performance testing without carrying out a comparative analysis among them. This section explores the different types of network simulators and chooses the most efficient, accurate, reliable and easiest to use in a MANET environment.

3.6.1 Network Simulator 2 (NS-2)

NS-2 is a popular and open source object-oriented discrete event simulator which offers support for simulation of TCP, routing and multicast protocols over wired and wireless networks. The

simulation combines both C++ and OTcl programming languages (Salem & Awwad, 2014). The simulator runs on both Windows systems installed with Cygwin and Linux systems.

Advantages

- It is an open source software program.
- There is substantive amount of content available to help in developing the scripts.
- It provides a set of randomized mobility models.
- It is easy to use as it allows users to generate traffic and movement patterns.
- Supports many protocols

Disadvantages

- A change in the code requires a recompilation.
- It mixes the compilation and interpretation processes making it complex to analyze and comprehend the code.
- The simulator runs slowly when subjected to many nodes.

3.6.2 Network Simulator 3 (NS-3)

NS-3 is an open source discrete event network simulator designed to work on the ISO/OSI model. It is suitable to simulate both wired and wireless networks and can work well in unicast and multicast data transmissions. It uses C++ and python programming languages; however, it can be developed exclusively using C++. NS-3 is not an extension of NS-2 but a new simulator written from scratch. It is not backward compatible with NS-2 (Chaudhary, et al., 2012).

Advantages

- Its source code is well organized and easy to expand as it consistently uses C++.
- It is freely available for use.
- It is easier to use as compared to NS-2.

- It can handle multiple network interfaces.

Disadvantages

- It has many bugs that have not been fixed.
- Gives support to less protocols.
- It has less user community as compared to NS-2.
- It is challenging to validate data obtained from the simulation.

3.6.3 Global Mobile Information System Simulator (GloMoSim)

It is a scalable wireless network system simulator capable of simulating parallel discrete events. GloMoSim was developed at UCLA Computing Laboratory using Parsec, a C-based language library. It supports protocols such as TCP, CSMA, MAC, UDP, and performs well in mobile IP networks (Jaiswal & Prakash, 2014).

Advantages

- It offers support to a simulation environment with many wireless nodes.
- It supports many wireless protocols.
- It can be used in a parallel environment.
- Its visualization tool is platform independent.

Disadvantages

- It does not support wired network protocols.
- Its low level design assumptions limit the simulator to IP based networks.
- It is not regularly updated.
- It lacks a proper documentation.

3.6.4 Objective Modular Network Testbed in C++ (OMNeT++)

OMNeT++ is a general-purpose discrete event and open component-based simulation framework. It has an extensive graphical user interface (GUI) with an intelligent support (Salem & Awwad, 2014).

Advantages

- Its powerful GUI makes it friendly for use.
- It accurately simulates most hardware.

Disadvantages

- It supports few wireless network protocols
- It lacks completeness in its mobility features.
- It is poorly documented.

3.6.5 Conclusion

The comparative analysis is used to assist in making a choice of the most suitable simulation tool to use in this research. It is observed that the features of each tool have both strengths and limitations. With NS-3, OMNET++ and GloMoSim researchers have the advantage of carrying out simulations with many nodes. NS-3 has much strength when compared with other simulators, for instance; it is the fastest in terms of computational time, the ability to handle multiple interfaces, and more aligned with IP protocols and designs in MANET.

NS-3 may be the best choice for MANET simulation since it is comprised of many features that support the simulation such as a wide range of protocols; however, it is under development and lacks adequate knowledge base as compared to NS-2. The number of working models for NS-3 that can be obtained from research community is not as sufficient as in NS-2, thus attracting fewer researchers to use it.

Despite NS-2 having problems such as interoperability, lack of memory management and complex architectural concepts, this research proposes to use it due to its popularity in the academic researches, rich collection of models, and huge knowledge base.

3.7 NS-2 SIMULATION TOOL

In order to detect and identify a black hole node in AODV routing protocol, this research proposes to simulate mobile ad hoc network scenarios with such malicious nodes using NS-2 network simulator. Network Simulator Version2 (NS-2) was developed by University of California, Berkley. Its latest version, NS-2.35, supports several network objects such as UDP, TCP, applications, traffic source behavior, router queue management mechanisms, routing and multicast protocols over all wireless networks. In addition, it is built on tools which display simulation results, analyze them and convert MANET topologies into NS format.

3.5 BASIC NS-2 ARCHITECTURE

Most procedure process codes are written in C++ programming language. In order to interpret simulation scripts, NS-2 uses OTcl (Object oriented Tool command language) a language which is fully compatible with C++. An OTcl file initiates an event handler, sets up network topology using the network objects and controls the transmission of packets using the event handler.

When the OTcl file is interpreted, NS-2 creates a Network Animator (NAM) file which gives a visual representation of the simulation and a trace file which keeps the behavioral attributes of the simulation objects. The Xgraph or tracegraph is then used to analyze the contents of the trace file.

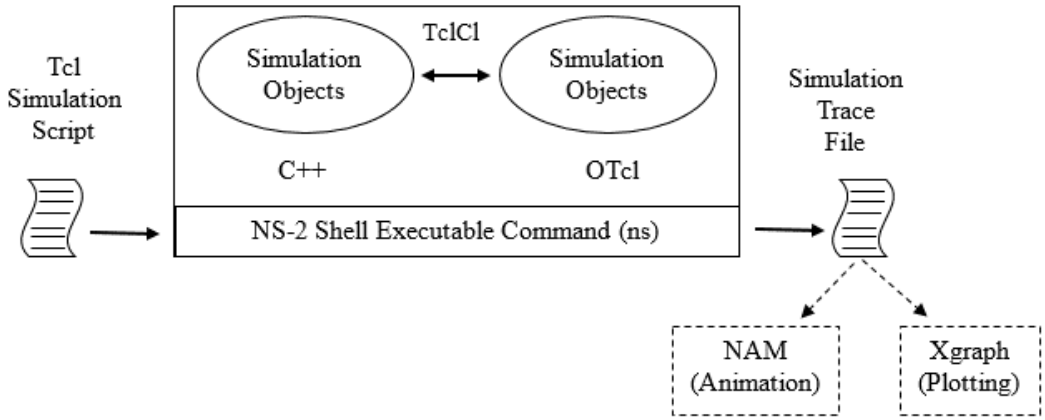

Figure 3.2: The architecture of NS-2

3.6 THE OPERATION OF THE PROPOSED MODEL

The proposed trust model involves modifying the AODV routing protocol operations as follows:

3.6.1 Phase I: Testing the New Node Against Black Hole Attack

A mobile ad hoc network consists of heterogeneous pool of mobile nodes which communicate without a fixed infrastructure. These nodes are tasked with routing information amongst each other despite challenges in security, processing ability, bandwidth and transmission power. The design of the model to verify an arriving node in a MANET, has factored the listed constraints. The model modifies the operation of AODV by introducing a new packet in the routing instance namely TRREQ. When a new node joins the MANET, its neighbors generate and send a TRREQ to it. Though the TRREQ functions like a RREQ packet, it cannot be rebroadcasted.

This packet contains a fake logical identity which is randomly generated and set as the destination's address. If the new node responds with a TRREP claiming to have a route to such a destination address it is marked as untrusted, else it is trusted.

3.6.2 Phase II: Further Trust Value Computation

The existing nodes will promiscuously monitor the forwarding capability of the new node. In this mode, the monitoring nodes will be able to receive all traffic on the network even though not

addressed to them and confirm whether the new node really forwarded the data packets. To confirm a successful packet forwarding, the recently sent packets are kept in a cyclic buffer. A circular buffer will erase old data packets if they are not removed frequently.

Successful forwarding of packets in MANET is subject to the link quality and black-hole attack. The link quality LQ, can be expressed as a ratio of the total hello messages received by a neighbor to those which ought to be received within the same time intervals, $\sum_{t=n}^{t=0} \frac{hmr_t}{ehm_t}$,

where hmr_t is the hello messages received in time interval(s) t, and ehm_t is the expected hello messages to be received in the same time interval(s) t.

The dropping and forwarding rates of data packets in a time interval t, is also considered in determining the trust value T, of a node and is expressed as $\left[1 - \frac{P_f}{P_s}\right] * \left[1 + \frac{P_d}{P_s}\right]$ where

P_f is the number of packets forwarded successfully, P_s is the total packets sent to the new node and P_d is the number of packets dropped by the new node.

For any node already existing in a MANET to be trusted in sending data packets, it should meet the condition, C [0, 1], where 0 is a value representing the expected tolerance on packet loss and 1 represents the link quality.

If the link quality value is equivalent to 1 and a node drops data packets, it is labeled as untrusted and its neighbor broadcasts the untrusted opinion to other nodes. On receiving the opinion, all other nodes immediately blacklist it. On the other hand, if a node drops data packets when the link quality value is less than 1, such node is not blacklisted but the route leading to this node is marked as untrusted until that time this value changes to the expected measure.

3.6.3 Conceptual Design of the Model

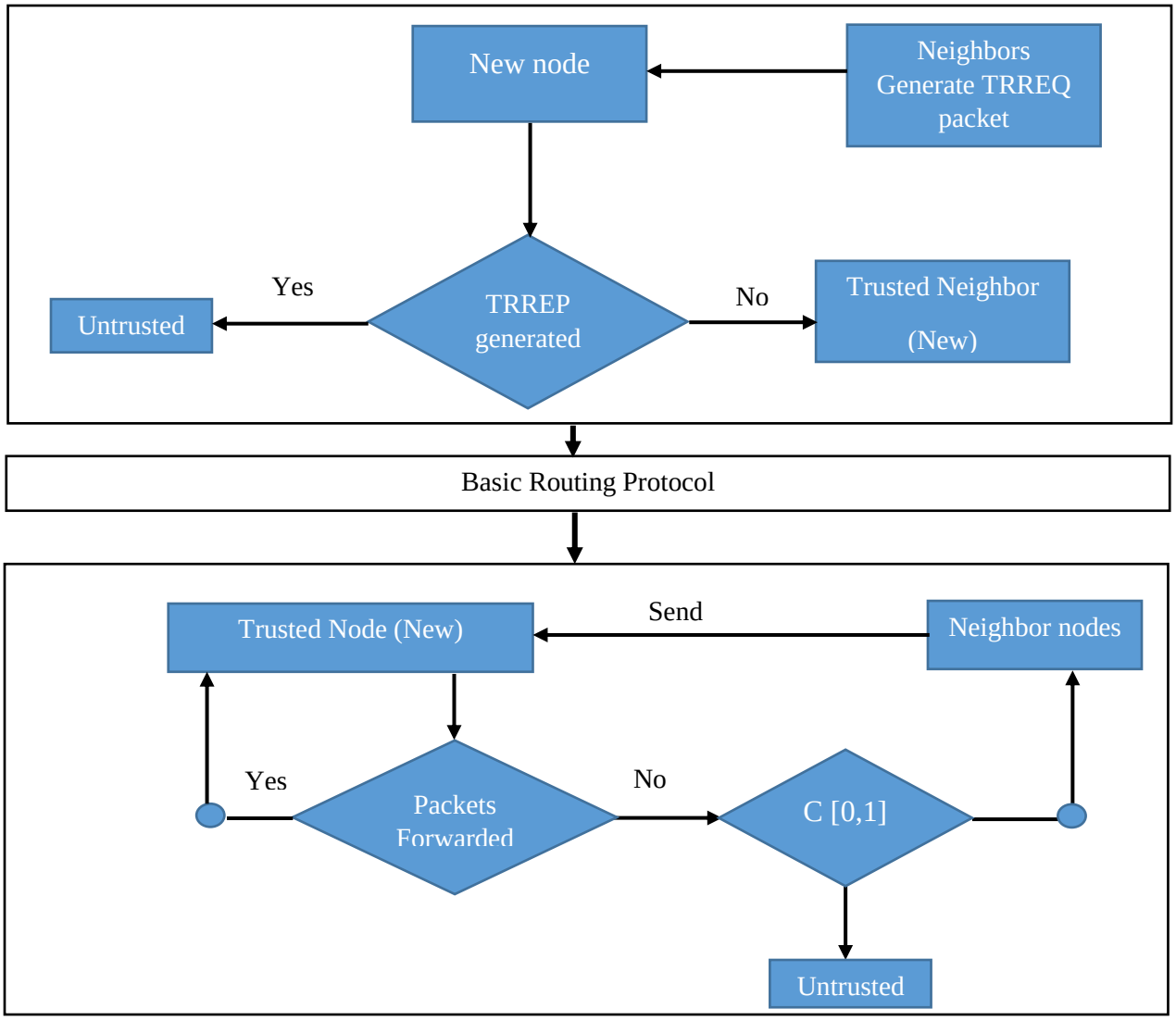

Figure 3.3: Conceptual Design

3.6.4 Proposed Algorithm

Start

i) Deploy a MANET with a set of mobile nodes

ii) Each node keeps a table with neighbor nodes' IDs

iii) Each node, sends a TRREQ packet to any new node in the MANET

iv) If (the new node replies with TRREP)

{

The node is malicious

}

Else

{

It is a trusted node

}

v) If (condition C is met and the node drops a packet)

{

The node is malicious and blacklist process initiated

}

Elseif (condition C is not met and the node drops a packet)

{

The node is trusted but with further monitoring

}

End

3.7 SIMULATION TEST METRICS

This research proposes to use various metrics to evaluate and analyze the performance of AODV in the following simulation scenarios:

i) Normal AODV

ii) Normal AODV under black hole attack

iii) AODV with the hybrid trust model under the black hole attack

3.7.1 End-to-end delay

This parameter defines the time it takes a data packet to reach the destination node successfully. End-to-end delay may be as a result of processing delays, buffer delays, transmission delays or propagation delays.

3.7.2 Throughput

This value defines the number of data bytes transmitted successfully at the destination node.

3.7.3 Jitter

It is a network performance parameter which defines the variation in the delay of received packets. As two nodes communicate, the delay between two packets can vary due to improper queueing, link congestion or erroneous configurations.

3.7.4 Packet Drop

Packet loss is experienced when one or more data packets transmitted across a network fails to get to the desired destination. This may occur due a huge jitter which may be as a result of link congestion, or bit errors caused by channel noise, distortion, signal weakness or attenuation.

3.8 BUILDING THE SIMULATION MODEL

3.8.1 Simulation Controls

The following parameters provided by ns-2 were used to run the experiment:

Parameter	**Value**
Channel type	Channel/Wireless Channel
Radio-propagation model	Propagation/TwoRayDround
Network interface type	Phy/WirelessPhy
MAC type	Mac/802_11
Interface queue type	Queue/DropTail/PriQueue

Link layer type	LL
Antennae model	Antennae/Omni Antennae
Number of nodes	10
Simulation time	38s
Routing protocol	AODV
Maximum speed	2m/s – 20m/s
Transmission range	250 meters
Simulation area	900 * 900 meters
Packet size	1000 bytes
Maximum packets in a Queue	50
Number of channel	2-3
Application traffic	UDP Traffic (CBR)

Table 3.1: Simulation Parameters

3.8.2 Physical Design of the Model

A wireless network environment of 900 * 900m is created on NS-2 containing 10 nodes with varying mobility. Initially, the simulation was setup using the controls in *table 3.1*. This simulation involved the operations of the normal AODV. A second setup was established which contained normal AODV under black hole attack. Finally, the third setup included the hybrid trust model under black hole attack.

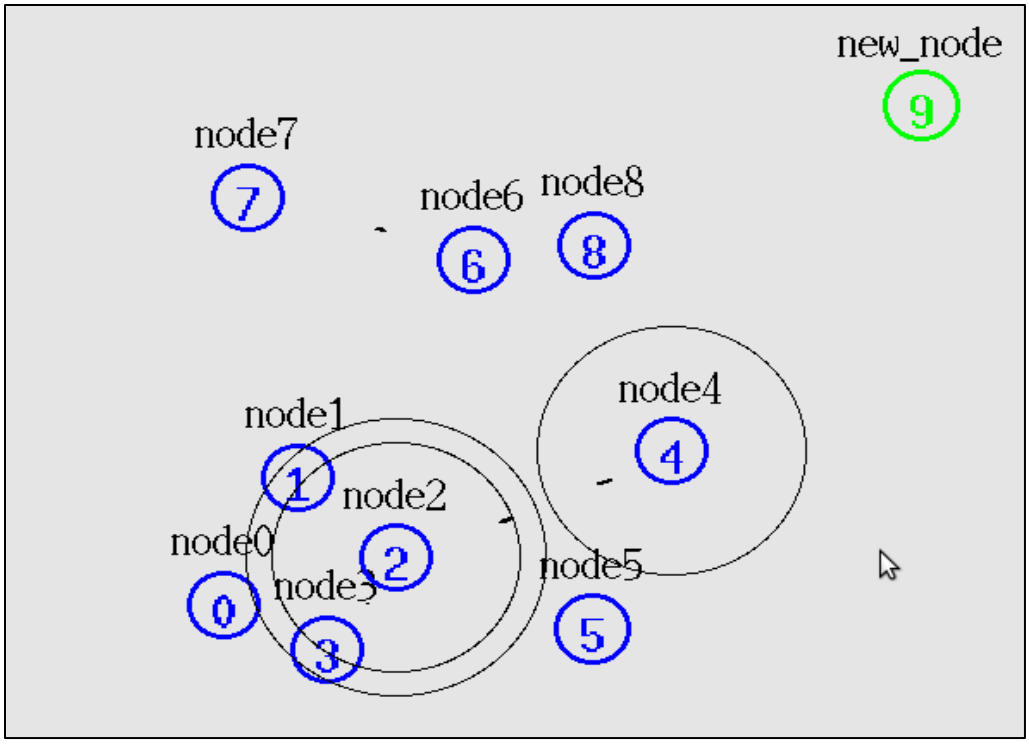

Figure 3.4: Physical Design (New node Model)

Figure 3.4 shows the simulation setup of AODV. A new node is arriving and ready to join the network.

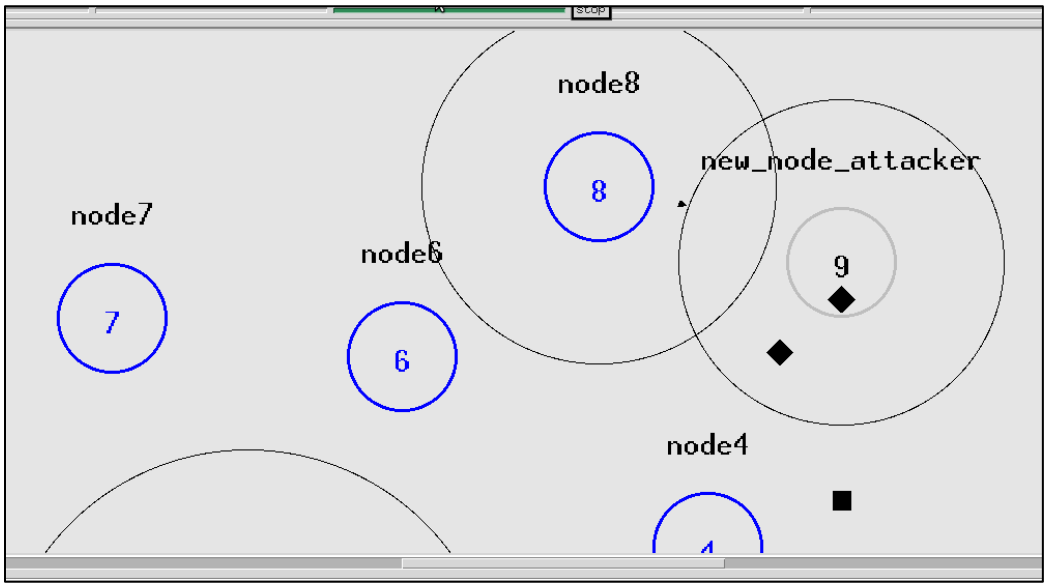

Figure 3.5: Physical Design (The Attack Model)

The figure 3.5 shows a simulation setup running on a normal AODV with inclusion of a black hole attack. The new node 9, which exhibits black hole characteristics, drops all the packets originating from node 8 to node 7.

3.8.3 Hardware and Software Requirements

	Item Description	**Specification**
1	**Hardware**	Laptop, Pentium Duo Core, 2.20GHZ, 64 Bit
2	**Operating System**	Linux Mint
3	**Simulation Tool**	NS-2 Version 2.35
4	**Trace File Analyzer**	Tracegraph202 / Xgraph

Table 3.2: Hardware and Software specifications

CHAPTER 4: SIMULATION RESULTS AND ANALYSIS

4.1 INTRODUCTION

This chapter describes the implementation of the proposed hybrid trust model to meet the set objective. Different simulation scenarios have been discussed and their impact on results is analyzed. NS-2 provides a mechanism to create the following scenarios which have impact on the results of the simulation:

- Mobility scenario
- Traffic handling capability scenario

4.2 COLLECTION OF RESULTS

At first, a network model running AODV was created without a black hole attack implementation. The black hole attack model was then implemented where some nodes dropped packets whenever they were forwarded through them. Finally, the black hole nodes were investigated under the hybrid trust model. Due to their actions, the blacklisting procedures were called and they were eventually isolated from the MANET.

In each scenario, the output from the generated trace files was collected and interpreted graphically using tracegraph.

4.3 ANALYSIS OF THE SIMULATION RESULTS OF AODV AND HYBRID AODV ALL UNDER THE BLACK HOLE ATTACK

AODV protocol was simulated with and without the presence of a black hole node. The results were extracted and graphically presented as shown below. A graphical comparison was done between AODV and Hybrid AODV, all under the black hole attack.

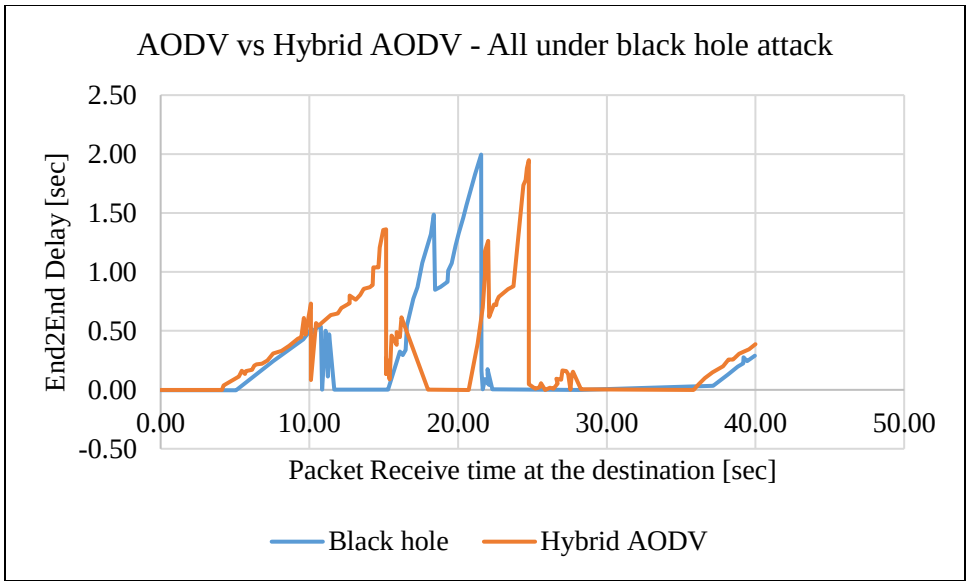

Figure 4.2: End-to-end delay under black hole attack

The figure 4.2 above is a graphical representation of the trace files obtained from the simulation setups of normal AODV (black hole) and hybrid AODV when the black hole attack was implemented. From the graph, it is observable that the end-to-end delay is significantly lower in normal AODV than in the proposed hybrid AODV at most simulation time instances.

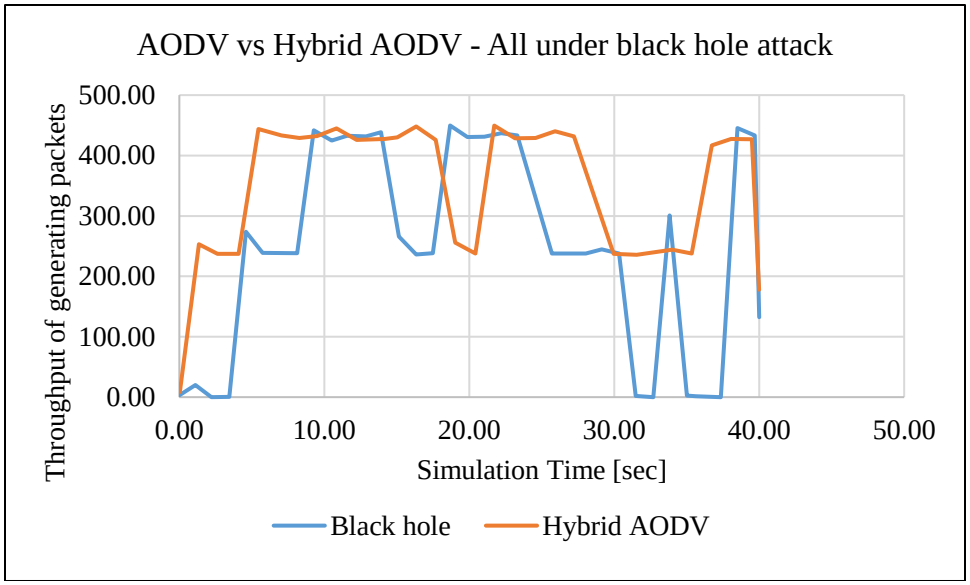

Figure 4.3: Throughput of generating packets under black hole attack

The figure 4.3 above, represents the throughput of generating packets tested on the AODV (black hole) and the hybrid AODV when the black hole activities were activated. It is observed that, at different simulation times the throughput is higher on the hybrid AODV than on normal AODV.

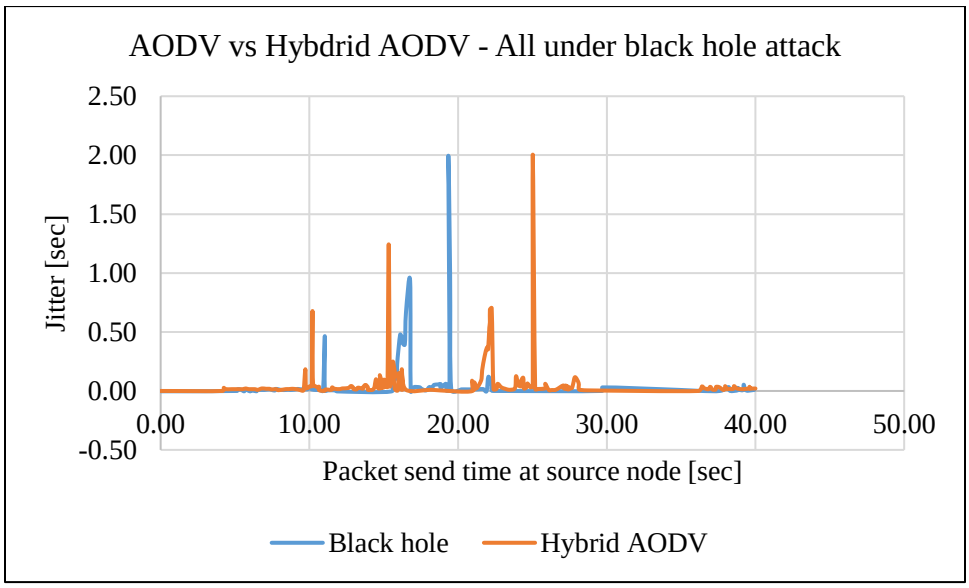

Figure 4.4: Jitter under black hole attack

The figure 4.4 above represents a comparison of jitter as extracted from trace files obtained from normal AODV (black hole) and hybrid AODV simulation scenarios with active black hole activities. As observed in hybrid AODV, the value of jitter is significantly higher in most simulation time instances as compared to the normal AODV.

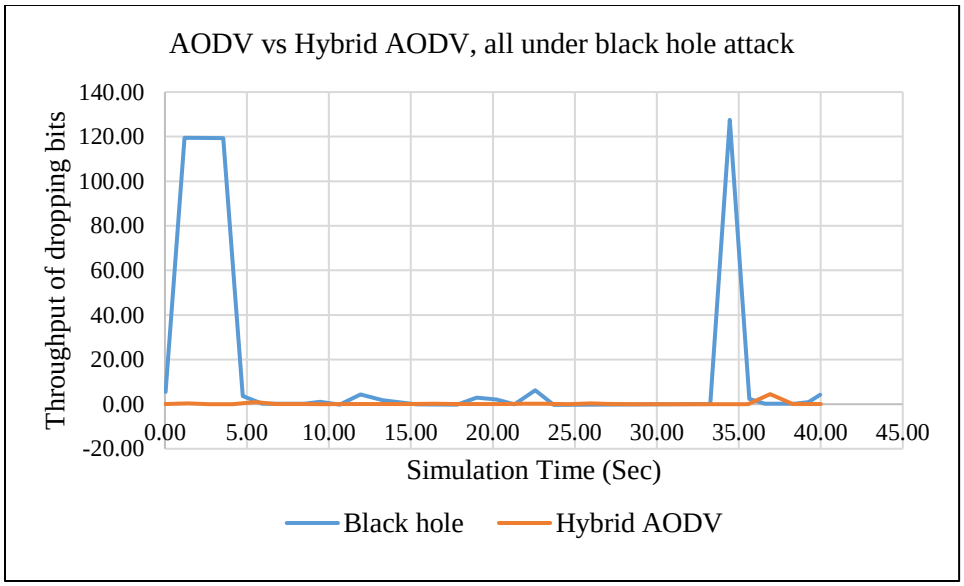

Figure 4.5: Throughput of dropping bits under black hole attack

The figure 4.5 above is a graph showing the throughput of dropping bits. The representation is an analysis of trace files obtained from the normal AODV (black hole) and hybrid AODV simulation scenarios with active black hole events. In this graph, it is evident that the packet dropping rate is higher in the normal AODV routing instance as compared to the hybrid AODV.

4.4 ANALYSIS OF THE SIMULATION RESULTS OF AODV AND BLACK HOLE AODV

AODV protocol was simulated with parameters given in table 3.1. The black hole attack was implemented in the configuration. The results were extracted and a graphical comparison was done between normal AODV and black hole AODV.

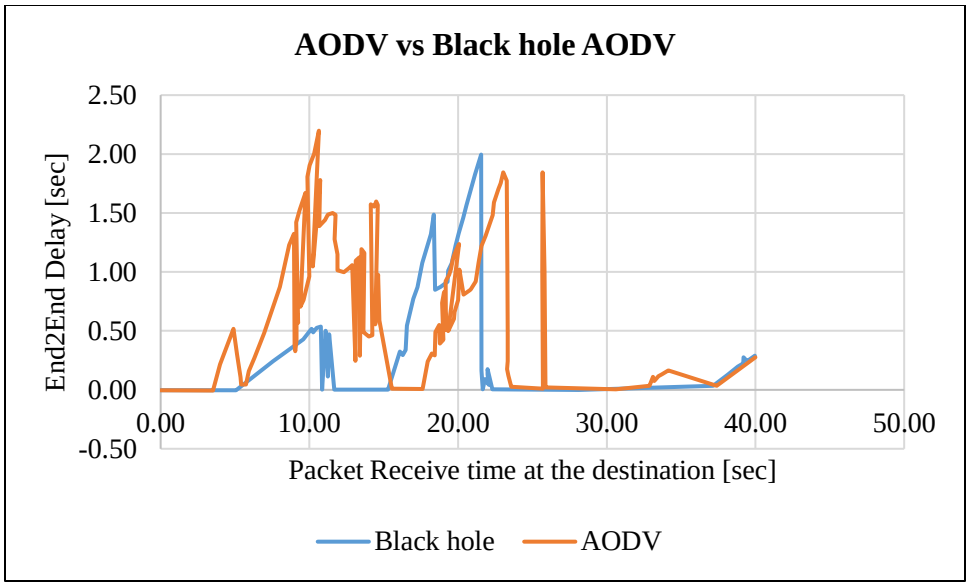

Figure 4.6: End to end delay

The figure 4.6 above represents the comparison of end-to-end delay between AODV (black hole) and AODV with active black hole events. From the graph, it is noticeable that the end-to-end delay is higher in normal AODV simulation scenario than in the black hole AODV scenario, throughout the simulation time.

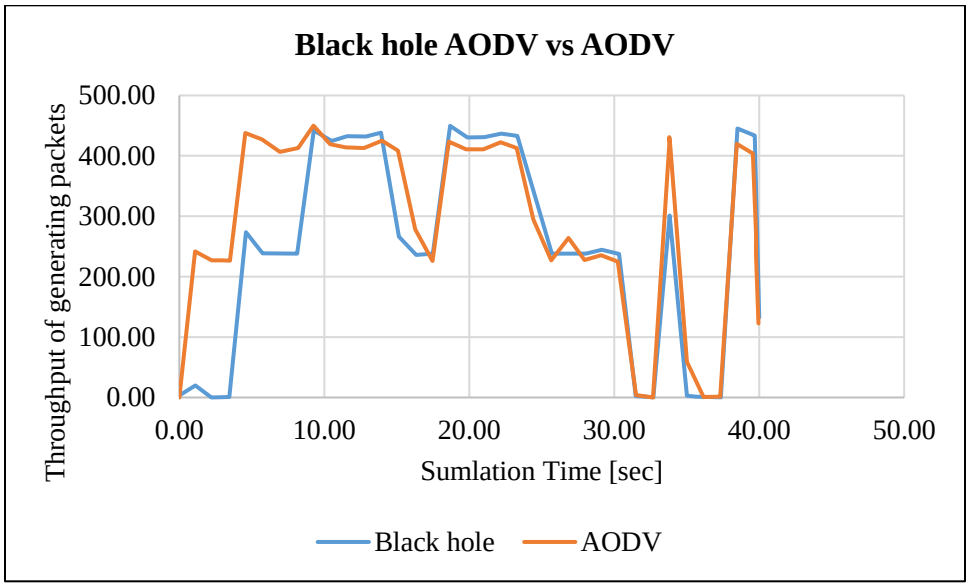

Figure 4.7: Throughput of generating packets

The figure 4.7 above shows that there was a higher throughput in the AODV simulation scenario without active black hole activities than when the protocol was under the attack.

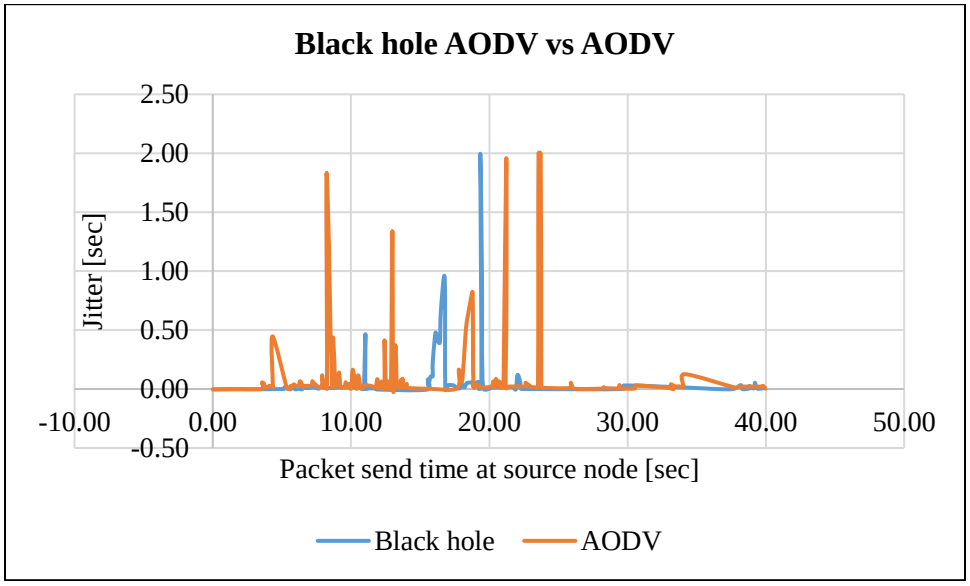

Figure 4.8: Jitter

The figure 4.8 above is a graph showing a comparison in values of jitter in AODV and black hole AODV simulation scenarios. The comparison is established at different instances of simulation time. It is noticeable that the values of jitter are higher in the absence of the black hole activities.

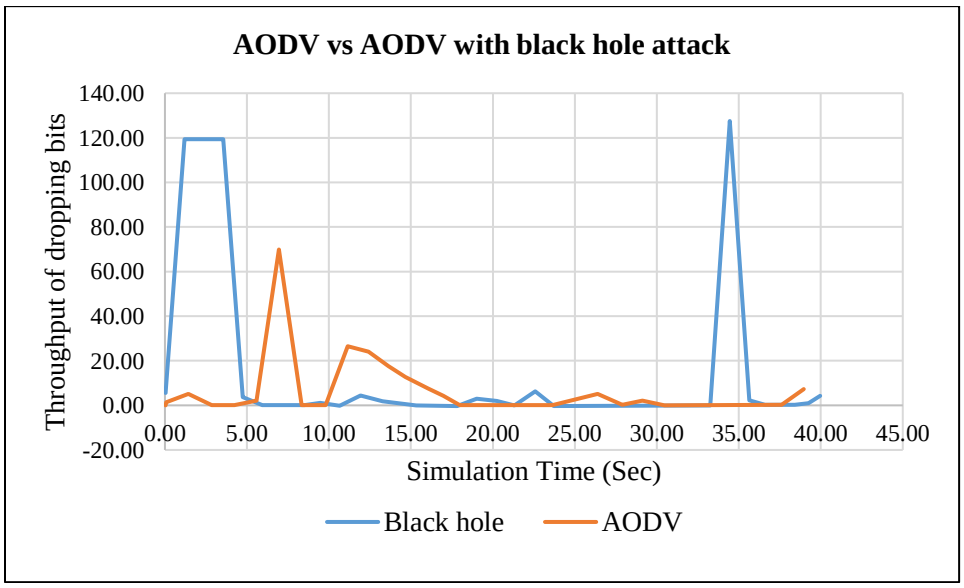

Figure 4.9: Throughput of dropping bits

In the figure 4.9 above, the throughput of dropping bits is analyzed. A comparison is established between normal AODV and black hole AODV simulation scenarios. It is observed that the simulation scenario with black hole activities has many bits being dropped at different instances of simulation time as compared to the simulation scenario with normal AODV.

4.5 CONCLUSION

The implementation and analysis of this work has focused on establishing comparisons between the following scenarios only:

i) AODV and Hybrid AODV with black hole implemented

ii) Black hole AODV and AODV

4.5.1 End-to-end delay

End-to-end delay includes all possible delay occurrences as a result of buffering during queueing at the interface, discovery latency, retransmission delays at the MAC, and propagation and transfer times. It was discovered that, in the presence of the black hole attack, the end-to-end delay was lower as compared to when the attack was controlled. This was because the black hole nodes reply to RREQs immediately without checking the routing table thus decreasing the delays.

4.5.2 Throughput

Throughput was analyzed for 10 nodes within speed times of 2 – 20 milliseconds. The following observations were made:

i) Throughput was higher when the hybrid trust model was implemented in the presence black hole attack.

ii) Throughput was higher when the AODV was not under black hole attack.

iii) The data throughput between source and destination nodes decreased significantly in the presence of black hole nodes.

4.5.3 Jitter

It was observed that the jitter was lower in the presence of black hole attack as black hole nodes provided the path with the fewest number of nodes.

4.5.4 Packet dropping rate

At the time intervals when the black hole nodes were active, the packet drops were higher as these nodes consumed the data packets. The packet dropping rates were lower when AODV was not under attack as well as when the hybrid AODV was implemented.

CHAPTER 5: CONCLUSION AND FURTHER WORK

5.1 INTRODUCTION

With Mobile Ad-Hoc Networks, it is possible to connect many devices where traditional network infrastructure cannot be deployed. However, this type of network has many challenges which need to be overcome in order to make it useful. Security is a major component to consider while deploying a MANET.

The chapter, outlines the accomplishments of this work, challenges, interpretations, future work and conclusions gathered from the simulation results.

5.2 CONCLUSION

In this study, the effects of black hole attack in AODV have been analyzed. AODV routing protocol with black hole nodes was implemented in NS-2.35. Four scenarios were simulated, each with 10 nodes using AODV routing protocol. There were two major scenarios one with an active black hole nodes and in the other scenario, there was implementation of the hybrid trust model which attempted to counter the effects of the black hole nodes. The simulation results were analyzed as follows:

Having investigated black hole attack, it was observed that the network end-to-end delay, throughput and jitter decreased significantly in the presence of the attack. It was also noted that the network packet dropping increased in the presence of the black hole attack activities.

The black hole attack affected the entire MANET connectivity and the high shift in data loss indicated the presence of the attack. It implied that, if black hole activities were increased there would be more data packets lost.

In the presence of the hybrid trust model, it was noted that the network throughput increased as the packet loss decreased. This indicated that the model was able to overcome the malicious effects of the black hole nodes. Through this prevention, this work achieves its main objective as the AODV routing protocol is made stronger against the black hole attack.

5.3 FUTURE WORK

Despite MANETs being easy to deploy, they are exposed to many attacks both internal and external. Currently, there is a lot of research going on in this area. The method used in this work focused on single black hole node.

In the near future, I propose the deployment of the hybrid trust model in this work in a MANET environment with cooperating black hole nodes. It is also important for one to get adequate skills of NS-2 and NS-3 simulators if focused on doing research on MANETs.

REFERENCES

Abdelshafy, A. & King, B., 2016. *Resisting Blackhole Attacks on MANETs.* s.l., s.n., pp. 1055 - 1060.

Bakshi, A., Sharma, A. & Mishra, A., 2013. Significance of Mobile AD-HOC Networks (MANETs). *International Journal of Innovative Technology and Exploring Engineering,* 2(4).

Bang, A. & Ramteke, P., 2013. MANET : History,Challenges And Applications. *International Journal of Application or Innovation in Engineering & Management,* 2(9), pp. 249 - 251.

Brian, K., 1999. *Using Information Technology.* 3rd ed. s.l.:s.n.

Chaudhary, R., Sethi, S., Keshari, R. & Goel, S., 2012. A study of comparison of Network Simulator -3 and Network Simulator -2. *International Journal of Computer Science and Information Technologies,* pp. 3085 - 3092.

Choi, Y., Kang, D. & Bahk, S., n.d. Improvement of AODV Routing Protocol through Dynamic Route Change using Hello Message.

French, C., 1990. *Computer Studies.* 3rd ed. s.l.:s.n.

Gaertner, G. & O'Nuallain, E., n.d. *Link Quality Prediction in Mobile Ad-Hoc Networks,* Ireland: s.n.

Garg, C. & Rewagade, P., 2013. *Trust Evaluation for Detecting Black Hole Attack on AODV Routing Protocol by using Back Propagation Algorithm of Neural Network.* s.l., s.n., pp. 776-780.

Gayathri, D. & JanakiRaman, S., 2015. *Comparative Performance analysis of Trust implemented AODV with Trust implemented OLSR under the Blackhole Attack.* s.l., s.n.

Goyal, P., Batra, S. & Singh, A., 2010. A Literature Review of Security Attack in Mobile Ad-hoc Networks. *International Journal of Computer Applications,* 9(12), pp. 11 - 15.

Gupta, S., Dhaliwal, B. & Malhotra, R., 2016. Simulation Based Comparative Analysis of AODV, TORA and DSR Protocols. *An International Journal of Engineering Sciences,* Volume 17, pp. 70 - 76.

Gurja, A. & Dande, A., 2013. Black Hole Attack in Manet's: A Review Study. *International Journal of IT, Engineering and Applied Sciences Research,* 2(3), pp. 12 - 14.

Hinds, A., Ngulube, M., Zhu, S. & Al-Aqrabi, H., 2013. A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET). *International Journal of Information and Education Technology,* 3(1).

Jain, A. & Gupta, S., 2016. Performance Enhancement of AODV in MANET over Black-Hole Attack. *International Journal of Advanced Research in Computer and Communication Engineering,* 5(2), pp. 467 - 470.

Jaiswal, K. & Prakash, O., 2014. Simulation of MANET using GloMoSim Network Simulator. *International Journal of Computer Science and Information Technologies,* 5(4), pp. 4975-4980.

Jaiswal, P. & Kumar, R., 2012. Prevention of Black Hole Attack in MANET. *International Journal of Computer Networks and Wireless Communications,* 2(5), pp. 599 - 606.

Joshi, K. & Kumar, M., 2016. Three Way Techniques for Preventing Black Hole Attack in MANET Using AODV Protocol. *International Journal of Innovative Research in Computer and Communication Engineering,* 4(2), pp. 1994 - 1997.

Kaur, J. & Singh, T., 2015. A Secured Data Transmission Method using Enhanced Proactive Secret Sharing Scheme to Prevent Blackhole Attack in MANETs - A Review. *International Journal of Computer Applications,* 119(10), pp. 20 - 28.

Kavitha, J. & Krishnakumari, P., 2014. Efficient Neighbor Route Discovery Protocol [ENRDP] for Position Verification in MANET. *Global Journal of Engineering Science and Researches,* 1(7), pp. 7420 - 7430.

Lalar, S., 2014. Security in MANET: Vulnerabilities, Attacks & Solutions. *International Journal of Multidisciplinary and Current Research,* 2(Jan - Feb 2014), pp. 62 - 68.

Macario, G. & Ondrejka, C., 2014. *Virtual Worlds: Theoretical Perspectives and Research Methods,* s.l.: s.n.

Madhuri, N., Krishna, B. & Raju, S., 2014. Secured Routing through Multi Stage Authentication in MANETs. *International Journal of Computer Science and Network Security,* 14(10), pp. 23 - 30.

Madhusudhananagakumar, K. & Aghila, G., 2011. A Survey on Black Hole Attacks on AODV Protocol in MANET. *International Journal of Computer Applications,* 34(7), pp. 86 - 95.

Mokbal, F. & Saeed, K., 2016. Anti-Black Hole Attack Mechanism for Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol in Manets. *International Journal of Computer Applications,* 135(11), pp. 37 - 45.

Nigam, H. & Verma, N., 2014. Improving The Performance of Adhoc Network Using Hybrid Method. *International Journal of Computer Science and Network Security,* 14(10), pp. 66 - 70.

Ochola, E. & Eloff, M., n.d. A Review of Black Hole Attack on AODV Routing in MANET.

O'Leary, J., O'Leary, I. & O'Leary, A., 2015. *Computing Essentials.* McGrwa-Hill International Edition ed. s.l.:s.n.

Panicker, V. & Jisha, G., 2014. Network Layer Attacks and Protection in MANET - A Survey. *International Journal of Computer Science and Information Technologies,* 5(3), pp. 3437 - 3443.

Ponsam, G. & Srinivasan, R., 2014. A Survey on MANET Security Challenges, Attacks and its Countermeasures. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* 3(1), pp. 274-279.

Prat, N., Pontoise, C., Wattiau, C. I. & Akoka, J., n.d. Artifact Evaluation in Information Systems Design - Science Research - A Holostic View.

Rochester, B., 1993. *Computers, Tools for Knowledge Workers.* s.l.:s.n.

Salem, A. & Awwad, H., 2014. Mobile Ad-hoc Network Simulators, A Survey and Comparisons. *International Journal of P2P Network Trends and Technology,* Volume 9, pp. 12 - 17.

Sharma, A., Bhuriya, D., Singh, U. & Singh, S., 2014. Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing. *International Journal of Computer Science and Information Technologies,* 5(4), pp. 5201-5205.

Sharma, P. & Jain, K., 2012. TRUST BASED SECURE AODV IN MANET. *Journal of Global Research in Computer Science,* 3(6), pp. 107-114.

Singh, G. & Singh, G., 2014. Detection and Prevention of Black Hole Using Clustering in MANET Using NS2. *International Journal Of Engineering and Computer Science,* 3(8), pp. 7420 - 7430.

Singh, V. & Jain, M., 2014. Secure AODV Routing Protocols Based on Concept of Trust in MANET's. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* 3(12), pp. 4425 - 4428.

Terdal, P., Mytri, D. & Damodaram, A., 2012. A Link Quality Based Dispersity Routing Algorithm for Mobile Ad Hoc Networks. *I. J. Computer Network and Information Security,* Volume 9, pp. 20-28.

Tiwari, N. & Yadav, R., 2015. Detection of Black Hole Attack using Control Packets in AODV Protocol for MANET. *International Journal of Computer Applications,* 118(24), pp. 23 - 29.

Tiwari, R., n.d. A TRUST MODEL WITH THRESHOLD DELAY TO PREVENT BLACKHOLE ATTACK IN AODV IN MANET.

Tseng, F., Chou, L. & Chao, H., 2011. A survey of black hole attacks in wireless mobile ad hoc networks. *Human-centric Computing and Information Sciences,* 1(4).

Vasanthavalli, S., Gowd, B. & Thenappan, S., 2014. Peruse Of Black Hole Attack and Prevention Using AODV on MANET. *International Journal of Innovative Research in Science Engineering and Technology,* 3(5), pp. 7420-7430.

APPENDICES

Appendix A - TCL Script Code with black hole nodes introduced

```
# Define options
set val(chan)         Channel/WirelessChannel    ;# channel type
set val(prop)         Propagation/TwoRayGround   ;# radio-propagation model
set val(netif)        Phy/WirelessPhy            ;# network interface type
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)           10                         ;# number of mobilenodes
set val(rp)           AODV                       ;# routing protocol
set val(x)            900                ;# X dimension of topography
set val(y)            900                ;# Y dimension of topography
set val(stop)         38                 ;# time of simulation en

#main program - Setting The Simulator Objects
set ns_ [new Simulator]
#create the nam and trace file:
    set tracefd [open thesisaodv.tr w]
    $ns_ trace-all $tracefd
    set namtrace [open thesisaodv.nam w]
    $ns_ namtrace-all-wireless $namtrace $val(x) $val(y)

# set up topography object
set topo       [new Topography]
$topo load_flatgrid $val(x) $val(y)

create-god $val(nn)
#Global node setting

$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 ON \
        -movementTrace ON

#Create the the wireless node
        set n0 [$ns_ node]
        set n1 [$ns_ node]
        set n2 [$ns_ node]
        set n3 [$ns_ node]
        set n4 [$ns_ node]
        set n5 [$ns_ node]
        set n6 [$ns_ node]
        set n7 [$ns_ node]
        set n8 [$ns_ node]
        set n9 [$ns_ node]
#Setting The Initial Positions of Nodes
        $n0 set X_ 125.0
        $n0 set Y_ 182.0
        $n0 set Z_ 0.0

        $n1 set X_ 250.0
        $n1 set Y_ 312.0
        $n1 set Z_ 0.0

        $n2 set X_ 320.0
        $n2 set Y_ 250.0
        $n2 set Z_ 0.0

        $n3 set X_ 186.0
        $n3 set Y_ 438.0
        $n3 set Z_ 0.0

        $n4 set X_ 438.0
        $n4 set Y_ 375.0
        $n4 set Z_ 0.0

        $n5 set X_ 500.0
        $n5 set Y_ 260.0
        $n5 set Z_ 0.0

        $n6 set X_ 375.0
        $n6 set Y_ 562.0
        $n6 set Z_ 0.0

        $n7 set X_ 185.0
        $n7 set Y_ 626.0
        $n7 set Z_ 0.0

        $n8 set X_ 530.0
```

```
$n8 set Y_ 590.0
$n8 set Z_ 0.0

$n9 set X_ 900.0
$n9 set Y_ 900.0
$n9 set Z_ 0.0
$ns_ at 0.0 "[$n9 set ragent_] malicious"
$ns_ at 0.0 "[$n9 set ragent_] malicious"

$ns_ at 0.00 "$n9 setdest 750.0 690.0 30.0"
$ns_ at 2.75 "$n8 setdest 460.0 490.0 20.0"
$ns_ at 10.20 "$n7 setdest 309.0 210.0 20.0"
$ns_ at 11.25 "$n6 setdest 375.0 420.0 20.0"
$ns_ at 9.75 "$n5 setdest 460.0 195.0 20.0"
$ns_ at 0.75 "$n4 setdest 520.0 330.0 20.0"
$ns_ at 1.50 "$n3 setdest 280.0 150.0 20.0"
$ns_ at 5.75 "$n9 setdest 650.0 530.0 20.0"
$ns_ at 19.25 "$n2 setdest 410.0 290.0 20.0"
$ns_ at 21.25 "$n1 setdest 182.0 250.0 25.0"
$ns_ at 12.25 "$n0 setdest 460.0 330.0 25.0"
$ns_ at 23.75 "$n9 setdest 390.0 420.0 20.0"

#Setting The Node Size
$ns_ initial_node_pos $n0 50
$ns_ initial_node_pos $n1 50
$ns_ initial_node_pos $n2 50
$ns_ initial_node_pos $n3 50
$ns_ initial_node_pos $n4 50
$ns_ initial_node_pos $n5 50
$ns_ initial_node_pos $n6 50
$ns_ initial_node_pos $n7 50
$ns_ initial_node_pos $n8 50
$ns_ initial_node_pos $n9 50
# Setting The Labels For Nodes
$ns_ at 0.0 "$n0 label node0"
$ns_ at 0.0 "$n1 label node1"
$ns_ at 0.0 "$n2 label node2"
$ns_ at 0.0 "$n3 label node3"
$ns_ at 0.0 "$n4 label node4"
$ns_ at 0.0 "$n5 label node5"
$ns_ at 0.0 "$n6 label node6"
$ns_ at 0.0 "$n7 label node7"
$ns_ at 0.0 "$n8 label node8"
$ns_ at 0.0 "$n9 label new_node_attacker"

$n0 color blue
$ns_ at 0.0 "$n0 color blue"

$n1 color blue
$ns_ at 0.0 "$n1 color blue"
```

```
    $n2 color blue
    $ns_ at 0.0 "$n2 color blue"

    $n3 color blue
    $ns_ at 0.0 "$n3 color blue"

    $n4 color blue
    $ns_ at 0.0 "$n4 color blue"

    $n5 color blue
    $ns_ at 0.0 "$n5 color blue"

    $n6 color blue
    $ns_ at 0.0 "$n6 color blue"

    $n7 color blue
    $ns_ at 0.0 "$n7 color blue"

    $n8 color blue
    $ns_ at 0.0 "$n8 color blue"

    $n9 color green
    $ns_ at 0.0 "$n9 color black"

set TRREQ0 [$ns_ create-connection UDP $n8 LossMonitor $n9 0]
    $TRREQ0 set fid_ 1
    set cbr0 [$TRREQ0 attach-app Traffic/CBR]
    $cbr0 set packetSize_ 1000
    $cbr0 set interopt_ .07
    $ns_ at 20.0 "$cbr0 start"
    $ns_ at 20.1 "$cbr0 stop"

set TRREP1 [$ns_ create-connection UDP $n9 LossMonitor $n8 0]
    $TRREP1 set fid_ 1
    set cbr1 [$TRREP1 attach-app Traffic/CBR]
    $cbr1 set packetSize_ 1000
    $cbr1 set interopt_ .07
    $ns_ at 20.1 "$cbr1 start"
    $ns_ at 20.2 "$cbr1 stop"

set udp0 [$ns_ create-connection UDP $n4 LossMonitor $n3 0]
    $udp0 set fid_ 1
    set cbr2 [$udp0 attach-app Traffic/CBR]
    $cbr2 set packetSize_ 1000
    $cbr2 set interopt_ .07
    $ns_ at 15.0 "$cbr2 start"
    $ns_ at 18.0 "$cbr2 stop"

set udp1 [$ns_ create-connection UDP $n1 LossMonitor $n0 0]
    $udp1 set fid_ 1
    set cbr3 [$udp1 attach-app Traffic/CBR]
```

```
    $cbr3 set packetSize_ 1000
    $cbr3 set interopt_ .07
    $ns_ at 18.0 "$cbr3 start"
    $ns_ at 24.0 "$cbr3 stop"

set udp2 [$ns_ create-connection UDP $n8 LossMonitor $n7 0]
    $udp2 set fid_ 1
    set cbr4 [$udp2 attach-app Traffic/CBR]
    $cbr4 set packetSize_ 1000
    $cbr4 set interopt_ .07
    $ns_ at 24.0 "$cbr4 start"
    $ns_ at 26.0 "$cbr4 stop"

set udp3 [$ns_ create-connection UDP $n8 LossMonitor $n5 0]
    $udp3 set fid_ 1
    set cbr5 [$udp3 attach-app Traffic/CBR]
    $cbr5 set packetSize_ 1000
    $cbr5 set interopt_ .07
    $ns_ at 28.0 "$cbr5 start"
    $ns_ at 29.0 "$cbr5 stop"

set udp4 [$ns_ create-connection UDP $n0 LossMonitor $n2 0]
    $udp4 set fid_ 1
    set cbr6 [$udp4 attach-app Traffic/CBR]
    $cbr6 set packetSize_ 1000
    $cbr6 set interopt_ .07
    $ns_ at 0.0 "$cbr6 start"
    $ns_ at 3.0 "$cbr6 stop"
set udp5 [$ns_ create-connection UDP $n0 LossMonitor $n8 0]
    $udp5 set fid_ 1
    set cbr7 [$udp5 attach-app Traffic/CBR]
    $cbr7 set packetSize_ 1000
    $cbr7 set interopt_ .07
    $ns_ at 3.0 "$cbr7 start"
    $ns_ at 7.0 "$cbr7 stop"

set udp6 [$ns_ create-connection UDP $n1 LossMonitor $n5 0]
    $udp6 set fid_ 1
    set cbr8 [$udp6 attach-app Traffic/CBR]
    $cbr8 set packetSize_ 1000
    $cbr8 set interopt_ .07
    $ns_ at 7.0 "$cbr8 start"
    $ns_ at 11.0 "$cbr8 stop"
set udp7 [$ns_ create-connection UDP $n7 LossMonitor $n6 0]
    $udp7 set fid_ 1
    set cbr9 [$udp7 attach-app Traffic/CBR]
    $cbr9 set packetSize_ 1000
    $cbr9 set interopt_ .07
    $ns_ at 11.0 "$cbr9 start"
    $ns_ at 16.0 "$cbr9 stop"
set udp8 [$ns_ create-connection UDP $n1 LossMonitor $n4 0]
```

```
    $udp8 set fid_ 1
    set cbr10 [$udp8 attach-app Traffic/CBR]
    $cbr10 set packetSize_ 1000
    $cbr10 set interopt_ .07
    $ns_ at 32.0 "$cbr10 start"
    $ns_ at 34.0 "$cbr10 stop"



### PROCEDURE TO STOP


# ending nam and the simulation
$ns_ at $val(stop) "$ns_ nam-end-wireless $val(stop)"
$ns_ at $val(stop) "stop"
$ns_ at 38.00 "puts \"end simulation\" ; $ns_ halt"
proc stop {} {
   global ns_ tracefd
   $ns_ flush-trace
   close $tracefd

   #Execute nam on the trace file
   exec nam thesisaodv.nam &

   exit 0
}
puts "Starting Simulation....."
    $ns_ at 38.0 "stop"
    $ns_ run
```

Appendix B – An Extract of Trace File

```
D 0.035714286 _0_ RTR LOOP 2 cbr 1020 [0 0 0 0] ------- [0:1 2:0 30 0] [2] 0 0
D 0.035714286 _0_ RTR  TTL 0 tcp 0 [0 0 0 0] ------- [0:0 0:0 0 0] [0 0] 0 0
s 0.053571429 _0_ AGT  --- 3 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [3] 0 0
r 0.053571429 _0_ RTR  --- 3 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [3] 0 0
D 0.053571429 _0_ RTR LOOP 3 cbr 1020 [0 0 0 0] ------- [0:1 2:0 30 0] [3] 0 0
D 0.053571429 _0_ RTR  TTL 0 tcp 0 [0 0 0 0] ------- [0:0 0:0 0 0] [0 0] 0 0
s 0.071428571 _0_ AGT  --- 4 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [4] 0 0
r 0.071428571 _0_ RTR  --- 4 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [4] 0 0
D 0.071428571 _0_ RTR LOOP 4 cbr 1020 [0 0 0 0] ------- [0:1 2:0 30 0] [4] 0 0
```

D 0.071428571 _0_ RTR TTL 0 tcp 0 [0 0 0 0] ------- [0:0 0:0 0 0] [0 0] 0 0

s 0.089285714 _0_ AGT --- 5 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [5] 0 0

r 0.089285714 _0_ RTR --- 5 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [5] 0 0

D 0.089285714 _0_ RTR LOOP 5 cbr 1020 [0 0 0 0] ------- [0:1 2:0 30 0] [5] 0 0

D 0.089285714 _0_ RTR TTL 0 tcp 0 [0 0 0 0] ------- [0:0 0:0 0 0] [0 0] 0 0

s 0.107142857 _0_ AGT --- 6 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [6] 0 0

r 0.107142857 _0_ RTR --- 6 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [6] 0 0

D 0.107142857 _0_ RTR LOOP 6 cbr 1020 [0 0 0 0] ------- [0:1 2:0 30 0] [6] 0 0

D 0.107142857 _0_ RTR TTL 0 tcp 0 [0 0 0 0] ------- [0:0 0:0 0 0] [0 0] 0 0

s 0.125000000 _0_ AGT --- 7 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [7] 0 0

r 0.125000000 _0_ RTR --- 7 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [7] 0 0

D 0.125000000 _0_ RTR LOOP 7 cbr 1020 [0 0 0 0] ------- [0:1 2:0 30 0] [7] 0 0

D 0.125000000 _0_ RTR TTL 0 tcp 0 [0 0 0 0] ------- [0:0 0:0 0 0] [0 0] 0 0

s 0.142857143 _0_ AGT --- 8 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [8] 0 0

r 0.142857143 _0_ RTR --- 8 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [8] 0 0

D 0.142857143 _0_ RTR LOOP 8 cbr 1020 [0 0 0 0] ------- [0:1 2:0 30 0] [8] 0 0

D 0.142857143 _0_ RTR TTL 0 tcp 0 [0 0 0 0] ------- [0:0 0:0 0 0] [0 0] 0 0

s 0.160714286 _0_ AGT --- 9 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [9] 0 0

r 0.160714286 _0_ RTR --- 9 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [9] 0 0

D 0.160714286 _0_ RTR LOOP 9 cbr 1020 [0 0 0 0] ------- [0:1 2:0 30 0] [9] 0 0

D 0.160714286 _0_ RTR TTL 0 tcp 0 [0 0 0 0] ------- [0:0 0:0 0 0] [0 0] 0 0

s 0.178571429 _0_ AGT --- 10 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [10] 0 0

r 0.178571429 _0_ RTR --- 10 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [10] 0 0

D 0.178571429 _0_ RTR LOOP 10 cbr 1020 [0 0 0 0] ------- [0:1 2:0 30 0] [10] 0 0

D 0.178571429 _0_ RTR TTL 0 tcp 0 [0 0 0 0] ------- [0:0 0:0 0 0] [0 0] 0 0

s 0.196428571 _0_ AGT --- 11 cbr 1000 [0 0 0 0] ------- [0:1 2:0 32 0] [11] 0 0