MITIGATING THE EFFECT OF BLACK HOLE AND GREY HOLE ATTACKS ON MANET AODV ROUTING PROTOCOL USING A MODIFIED TRUST BASED SCHEME

BY

ZAHRADDEEN NAKARGO IBRAHIM, B. ENG (ABU), 2015
(P16EGCM8013)

A DISSERTATION SUBMITTED TO THE DEPARTMENT OF ELECTRONICS AND TELECOMMUNICATIONS ENGINEERING, AHMADU BELLO UNIVERSITY, ZARIA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF A MASTER OF SCIENCE (M.Sc.) DEGREE IN TELECOMMUNICATIONS ENGINEERING

DECEMBER, 2019

DECLARATION

I declare that the work in this dissertation entitled “Mitigating the Effect of Black hole and Grey-hole Attacks in MANET AODV Routing Protocol using A Modified Trust-based Scheme’’ has been carried out by me in the Department of Electronics and Telecommunications engineering. The information derived from literature has been duly acknowledged in the text and a list of references provided. No part of this dissertation has been previously presented for another degree or diploma at this or any other institution.

ZAHRADDEEN NAKARGO IBRAHIM _____ _____

(Student) Signature Date

CERTIFICATION

This dissertation entitled "MITIGATING THE EFFECT OF BLACK HOLE AND GREY-HOLE ATTACKS ON MANET AODV ROUTING PROTOCOL USING A MODIFIED TRUST-BASED SCHEME" by Zahraddeen Nakargo IBRAHIM meets the regulations governing the award of degree of Master of Science (MSc) in Telecommunications Engineering of the Ahmadu Bello University, and is approved for its contribution to knowledge and literary presentation.

Dr. A. D. Usman	_____	_____
(Chairman, Supervisory Committee)	(Signature)	Date
Dr. A. M. S Tekanyi	_____	_____
(Member, Supervisory Committee)	(Signature)	Date
Dr. A. D. Usman	_____	_____
(Head of Department)	(Signature)	Date
Prof. Sani A. Abdullahi	_____	_____
(Dean, School of Postgraduate Studies)	(Signature)	Date

DEDICATION

This dissertation is dedicated to Almighty Allah alone, my sustainer and my helper, the Lord of the worlds, master of the day of Judgment, the most Beneficent and the most Merciful.

ACKNOWLEDGEMENT

All praise is due to Almighty Allah, the most exalted in power, the first not by beginning and the last not by ending, the master of the day of judgment. I would like to express my deepest gratitude and sincere appreciation to my supervisory team, Dr A. D. Usman and Dr. A. M. S. Tekanyi for their endless and tireless support, encouragement, fatherly advice, constant motivation, and understanding. They taught me how to be creative, innovative, follow due process, abide by instruction, and last but not the least, inculcate discipline in me. Their suggestions have been invaluable towards the successful completion of this research work. Their positive impact on my life will never elapsed till the end of my life. I pray to Almighty God to reward them abundantly, guide and protect them and their family against any calamity Amen. I acknowledge and appreciate the contributions by members of staffs of Communications Engineering, Ahmadu Bello University, Zaria. especially, Dr. S. M. Sani, Dr. K. A. Abubilal, Dr. M. J. Musa, Dr. U.F. Abdul-Aguye, Dr. H.A. Abdulkarim, and Dr. S. Yaro for their helpful suggestions and critical comments which always helped in improving the quality of this research work. Thanks to Ahmadu Bello University, Zaria, Nigeria for providing enabling platform for the ETEP. My appreciation also extends to Engr. Saidu Waziri, Engr. Ajayi, Engr. Habu, Engr. Eziekel, Engr. Frank, Engr. Ya'u, Engr. Aminu Abba, and so many to mentioned. Special thanks go to my esteem friends within the faculty, such as Engr. Yusuf Zakari, Engr Ziaulhaq Muhammad, Engr Abduljalil Kassim, Engr Mubarak Mustapha, Engr Usman Musa, Engr Zakka Augustine, Engr Abbas Sada, Engr Abubakar Sokoto, Engr Muzakkar Saleh. To my colleagues who made my stay in the university a valuable and memorable experience, thank you very much. Finally, I would like to express my deepest appreciation to my family. Thanks to my parents, brothers, and sisters whose love and sincere prayers have always been with me. Thank you very much. Special thanks to my

uncle Alhaji Bashir, you have been a source of encouragement and inspiration to me. Thank you for being such a wonderful family.

Zahraddeen Nakargo IBRAHIM

December, 2019

ABSTRACT

A Mobile-Ad-hoc-Network (MANETs) is a set of wireless networks that has the ability of operating without an existing infrastructure (that is base station). Lack of central control makes this type of network vulnerable to different security attacks, which degrades the entire network performance. Mitigating techniques such as mobile agents, fuzzy logic, trustiness and neighbors, genetic algorithm, cross layer cooperation, clustering algorithm, route redundancy, and message parameters, etc. have been used in different literature, but there are still a great number of malicious activities (such as black hole, grey-hole, worm-hole, spoofing, eavesdropping etc.) that affect the performance of MANET. Among the most common attacks is denial of service, which prevents source nodes from communicating with the destination node by dropping either the entire packets or some of the packets. Therefore, in this research work, a Modified Trust based Scheme (MTS) was adopted using fuzzy logic to isolate and avoid destructive nodes from sharing or having access to the network resources. The Ad hoc on Demand Distance Vector (AODV) routing protocol was used. Network Simulator 2.35 (NS-2.35) was used to run the MTS simulation of this research to obtain its results for evaluation with the existing Intrusion Detection System (IDS) of the work of Shaikh and Rajan, (2018). Results showed that MTS performed better than IDS by 12.6% when packet delivery ratio was tested against mobility speed (0-40m/s), 45.5% reduction in network overhead when it was tested against mobility speed and 13.7% improvement in throughput when it was tested against mobility speed. As a result, network overhead was reduced and both packet delivery ratio and throughput were improved due to mobility support of the modified technique. AODV routing protocol was adopted because it performs optimally with mobile networks.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

MANETs	Mobile Ad hoc Networks
RERR	Route Error
RREQ	Route Request
RREP	Route Reply
NS-2	Network Simulator Version 2
BH	Black hole
GH	Grey-hole
DOS	Denial of Service
CI	Computational Intelligence
NNs	Neutral Networks
SI	Swarm Intelligence
FIS	Fuzzy Inference System
PDR	Packet Delivery Ratio
AODV	Ad-hoc on Demand Distance Vector routing protocol
DSR	Dynamic Source Routing
DSDV	Destination Sequenced Distance Vector
OLSR	Optimized Link State Routing
NAM	Network Animator
IDS	Intrusion Detection System
MTS	Modified Trust-based Scheme
OTCL	Object Oriented Tool Command
TTL	Time to Live

CHAPTER ONE

INTRODUCTION

1.1 Background of the Research

Several problems are yet to be solved in order for Mobile Ad hoc Networks (MANETs) to be successfully arranged. Quite a number of these problems are attached to MANETs routing (Ali *et al*., 2008). MANETs is an autonomous network that does not require an infrastructure to be able to communicate with each other. Nodes in MANETs are basically deployed in an unrestricted environment, hence, the tendency of nodes to carry out malicious acts is very high (Jain *et al*., 2018). Ad hoc on demand Distance Vector (AODV) routing protocol provides an alternative for an infrastructure-less network to be able to convey packets from source to destination despite the absence of central control in the network. In this routing protocol, each node serves as a router as well as a host for communication to be able to take place between two nodes that are out of radio range *(*Hiremath, 2016*)*. Natural ability of MANET makes it attractive and applicable to areas such as environmental monitoring, military battle field, area affected by natural disaster (such as flooding, hurricane, etc.), in a situation where there is no existing infrastructure for communication *(*Gurung & Chauhan, 2018*)*. Despite the growth in MANETs, demand for certain characteristics peculiar to it are faced with key number of challenges (Eldein *et al*., 2017) such as

i. Limited bandwidth

ii. Routing protocol

iii. Routing overhead

iv. Dynamic topology

v. Battery constraint

vi. Power management

This research therefore, mitigate the effect of black hole and grey hole attacks during routing of information and subsequently reduced routing overhead.

1.2 Significance of the Research

The significance of this research work is to develop a modified trust based scheme to mitigate the effect of Black Hole (BH) and Grey- Hole (GH) attacks in MANETs using Ad-hoc on Demand Distance Vector (AODV) routing protocol by incorporating each node with a trust evaluator to monitor the adjacent node.

1.3 statement of Research Problem

One of the major challenges in MANET is reliable and secured transmission of information from one point to another point. Lack of central control render this network vulnerable to different attacks that deteriorate MANET performance. Despite the tremendous work done to mitigate the effect, the network still suffers from reduction in packet delivery ratio, throughput, and increased in network overhead because of inadequate routing protocol (Chandure, 2011). Hence, this necessitate the need to further modify trust-based scheme in an attempt to improve packet delivery ratio, throughput, and reduction in network overhead. Thus, this research present mitigating the effect of black hole and grey- hole attacks on MANET AODV routing protocol using a modified trust-based scheme (MTS).

1.4 Aim and Objectives

The aim of this research is to develop a modified trust scheme to reduce the effect of black hole and grey-hole attacks in Ad hoc on Demand Distance Vector based MANET routing protocol.

The objectives of this research are as follows:

i. To replicate the work of Shaikh and Rajan (2018).

ii. To develop a modified trust-based scheme using a fuzzy logic

iii. To implement the modified trust-based scheme using Network Simulator-2 (NS-2)

iv. To compare the results obtained from modified trust scheme with those of (Shaikh & Rajan, 2018) using network overhead, packet delivery ratio, and throughput as performance metrics.

1.5 Scope of Research

This research work is limited to reduction of single black hole and sequence number-based grey- hole attacks to improve the network performance. Network simulator-2 was used to obtain the results by varying the nodes speed from 0 to 40m/s.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This section is divided into two parts. The first part discusses the fundamental concepts and theoretical background relevant to this research. The second part presents critical review of the relevant literatures in this specific field of research. The two mentioned components will assist in the understanding of the approach to take in the determination of the problem in question and also pave a way for improvement to achieve better results.

2.2 Review of Fundamental Concepts

The fundamental concepts of this research work are presented in this sub-subsection. The review outlines the important principles and relevant theoretical model equations, methods and tools related to this research field and the challenges in particular.

2.2.1 Mobile Ad-hoc Network (MANETs)

MANETs is a structure-less network that operate without a central control. Contrary to the conventional wireless communication, MANETs is recognized to effectively function in a constant changing topology due to mobility nature of nodes in MANETs (Nath *et al*., 2017). MANETs is more susceptible to security threats than connection-oriented network due to peculiar behavior of MANETs such as dynamic topology, battery constrained, multi hop communication, etc. Since MANET has no clear boundary that makes it available for legitimate users and destructive attackers within the network which eventually affect the performance of the network. Routing protocols in MANETs is among the serious challenges faced by this network which is very difficult to detect as the malevolent node advertises itself

with the shortest path to the intended destination (Chandure, 2011). Working principle of MANETs is shown in Figure 2.1.

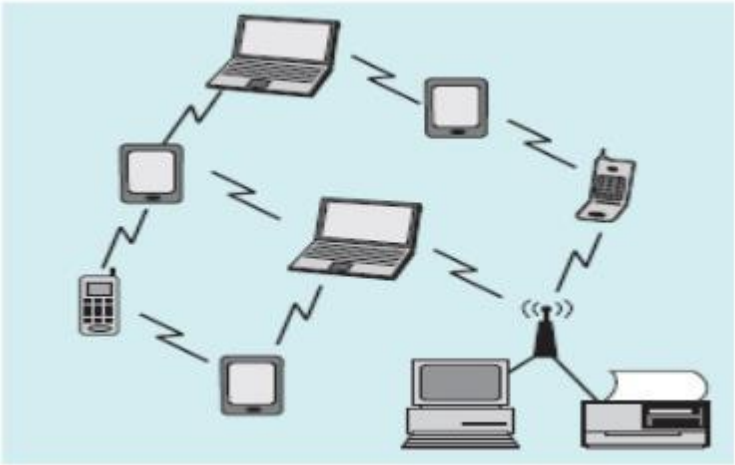

Figure 2.1: Mobile Ad-hoc Network (Eldein *et al*., 2017).

Over the years, MANETs has gain attention by institutions, research groups, and industries due to its peculiar characteristics that make it cheap in terms of implementation and can easily be deployable as no existing infrastructure is required. The network comprises of self-configured devices such as cell phones, laptops, PDAs, printers, etc. *(*Eldein *et al.*, 2017*).*

2.2.1.1 Characteristics of MANET

In recent years, the study of MANETs has been developed and constructed as it is becoming very popular. The network is easily deployed since it requires no infrastructure. Any wireless device incorporated with radio transceiver can also form the network. These devices are wireless in nature and may be using battery power which makes them autonomous with a freedom of movement while still communicating with each other. Some of the characteristics of MANETs (Eldein et al., 2017) include the following four:

i. **Infrastructure-less Network:** Devices that form this type of network are able to communicate with each other even when the two devices are out of radio range using multi-hop communication to convey packet from source to destination node. Lack of central control makes it necessary for nodes in the network to act as a router in order to forward a packet to a host. Hence, the network is self-configured in nature.

ii. **Dynamic Topology:** Freedom for nodes to move around the network and also to join or leave the network any time leads to constant change in the topology.

iii. **Bandwidth Constraints:** Unlike wired links, nodes in MANETs communicate through a wireless medium which is limited as a result of multiple access, multiple fading, noise, congestion, fluctuation, and signal interference which greatly affect the performance of the link ability.

iv. **Multi-Hop Communications:** For two nodes in the network that are out of range of each other to successfully exchange information between each other have to use neighboring node to be able to convey the information.

2.2.2 Routing Protocols in MANETs

Protocols are agreed rules that administer reliable communication among the wireless nodes in the network. Quite a number of routing techniques are announced which are applicable to MANETs. Although, routing in MANETs is also faced with quite a number of challenges such as frequent change in topology, limited range, and scalability. Routing in MANETs is broadly divided into three categories (Ochola *et al.*, 2017) which are as follows:

i. **Proactive routing protocols:** This type of routing protocol is also referred to as table driven routing protocols all the nodes keep the routing information of each node even when not required.

To maintain this routing information in their routing tables, each node updates its routing table periodically to ensure potential route whenever there is change in topology. This protocol makes it easy to establish connection between source node and the destination node without any un-necessary route discovery. Frequent update leads to degradation of network performance because of overhead. Proactive protocols achieve more with static network than with dynamic network due to scalability problem. Proactive consists of routing protocols such as Destination Sequenced Distance-Vector Routing Protocols (DSDV) and Optimized Link State Routing (OLSR) protocol (Ochola *et al*., 2017).

ii. **Reactive Routing Protocols:** Reactive routing protocol is also called on demand routing protocol as routes are only established when needed. Periodic update in reactive protocol is not needed as routes are only created on demand from source node to communicate with the destination node. The source node starts route discovery procedure when the path is successfully realized and a data is sent to the destination that require constant maintenance for route reliability. Since routes are created only on demand, this protocol offers more advantage than proactive one. Reactive protocol reserves more energy and bandwidth, because no periodic updates are required as devices in the network are resource constrained and hence improves performance of the network. Reactive protocol also has different routing protocols such as Ad-hoc on-demand Distance Vector (AODV) routing protocol and Dynamic Source Routing (DSR) protocol (Ochola *et al*., 2017).

iii. **Hybrid Routing Protocols:** Hybrid protocol is a combination of proactive and reactive routing protocols.

This protocol uses proactive routing protocol for route discovery, while in case there is a change in topology, it uses reactive routing protocols to determine an alternative route. It also consists of Zone Routing Protocol (ZRP), Hazy Sighted Link State (HSLS) protocol and secure routing protocol. Figure 2.2 shows the different types of routing protocols in MANET (*Ochola et al*., 2017).

In this research work, reactive routing protocol is adopted because it performs optimally for mobile network with less tendency of network overhead.

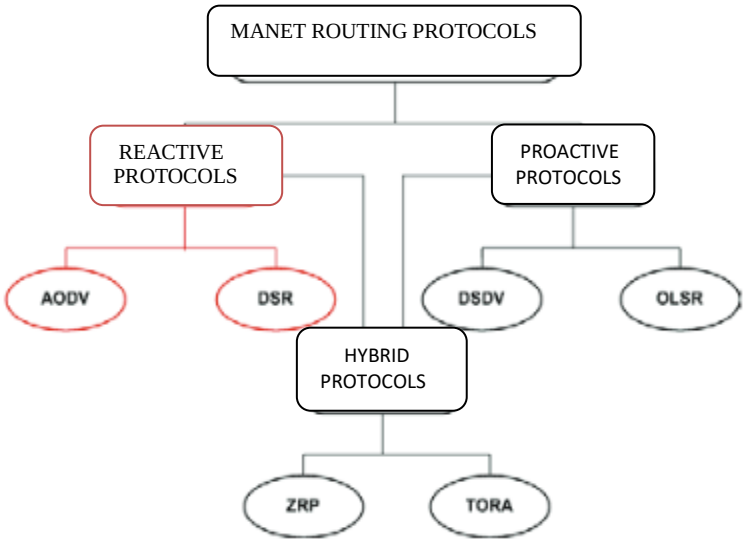

Figure 2.2: Hierarchy of MANET Routing Protocols (Ochola *et al.*, 2017)

In this research work, reactive routing protocol was used due to its mobility support, fast convergence, and utilization of bandwidth. Some of the properties of routing protocols (Seyed *et al.*, 2012) include the following five:

i. **Loop free:** To prevent wastage of CPU resources, routing protocol should provide routes that are loop-free in order to attain better performance of the network.

ii. **Distributed Operation:** Provision of distribution by the protocols makes the network robust to failure and growth as it is independent of centralized control.

iii. **Low Overhead Control Traffic:** Avoidance of unwanted messages is necessary by the protocols in order to efficiently utilize the limited bandwidth in the network.

iv. **Optimal Route:** This is a very important factor in MANETs that must be addressed by the protocol when considering the path with shortest number of host. It will also address bandwidth and CPU wastage.

v. **Fast Convergence:** As the network topology is dynamic due to the mobility nature of the network, protocols should be flexible to this frequent change in topology by determining new optimal routes.

2.2.3 Ad Hoc on Demand Distance Vector (AODV) Routing Protocol

To ensure loop free path, AODV routing protocol joins the advantage of both Dynamic Source Routing (DSR) protocol and Destination Sequence Distance Vector (DSDV) routing protocol. The protocol uses DSR for route maintenance whenever a change in topology is encountered, while DSDV is used for route detection and addition of sequence number. In AODV, the nodes only obtain the address of the destination node while in DSR, each node contain the complete routing information about the network (Devi, 2017). Due to the lack of central control in MANETs, routing is done through multi-hop communication, that is, communication takes place between nodes that are in radio range of each other. Hence the most commonly used routing protocol in MANETs is AODV (Singh, 2017). Route discovery and route maintenance are the two basic tasks of this protocol. Each node in AODV sends "hello" message to an intermediate node which is updated periodically to ensure connectivity when path is required for source node to communicate with target node (Chandure, 2011).

To determine the latest and freshest path to destination, intended node sequence number is used with integer standards. AODV works on three messages for a source node to sends data to a target node. For a successful routing, source node sends a broadcast Route Request (RREQ) packet throughout the network until it reaches the target node or any intermediates node which has the destination address in its routing table. If the packet is received by the target node, Route Reply (RREP) packet is generated by the destination or intermediate node which is unicast to the source node. As different RREP messages may be received by the source node, the most recent route with highest sequence number is chosen as the optimal path to the destination. Since nodes in MANETs are mobile in nature with a dynamic topology, this can easily lead to a broken link as node in the route may change position to another route. However, Route Error (RERR) packet is used by the adjacent node to alert the source node about the broken link. Hence, path chosen by the source is utilized until the end of transmission and unused routes are removed from the memory buffer after a given time (Singh, 2017). These types of AODV messages are shown in Figure 2.3.

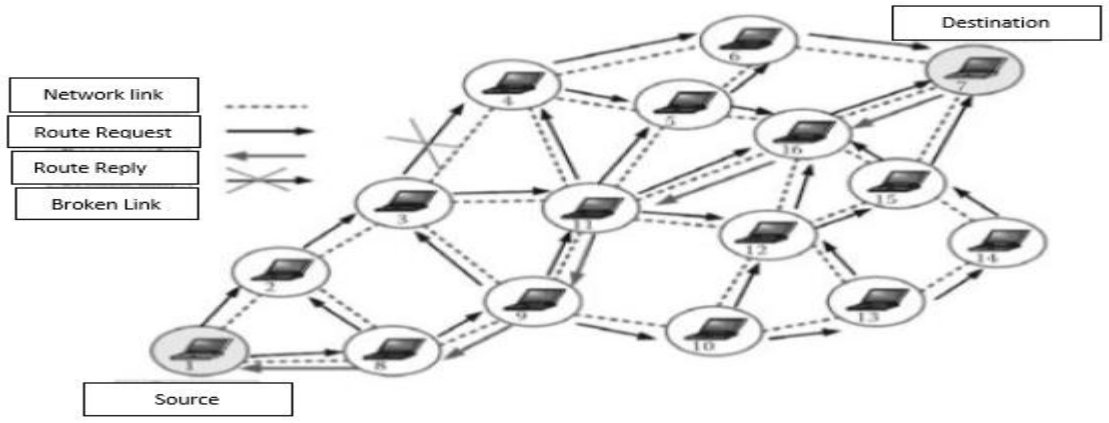

Figure 2.3: AODV Schematic Diagram (Loo *et al*., 2016)

AODV is developed to ensure source to destination communication due to absence of reliable active path among nodes. Routing in MANETs is actualized by transmitting the packets

within themselves whenever the need arises. Each node maintains a routing table which consists of the route information about the neighboring nodes with their internet protocol address. For effective performance of the network, AODV protocol is designed in such a way that each node has to trust each other. To ensure active temporary network with self-configuration among the mobile nodes, AODV is used to facilitate the process. None of the cellular node is required to store route information while inactive (Hiremath, 2016). There are two ways in which a node updates its sequence number in AODV which are as follows (Chandure,2011):

I. **Control messages in AODV**: If the RREQ packet is received by the destination node, it quickly updates its sequence number by increasing it to maximum before sending back the RREP packet. The sequence number received by the source node is usually higher than the sequence number in the routing table. Every RREQ packet in the network contains Time to Live (TTL) value which presents the number of hops in each RREQ packet.

II. **Route discovery in AODV**: As the network is flooded with RREQ packets, when the packet is received by the destination node or neighboring node with enough fresh routes to destination, it sends the RREP packet to the source node from which communication is established between the source and the destination node. Route discovery in AODV is depicted in Figure 2.4

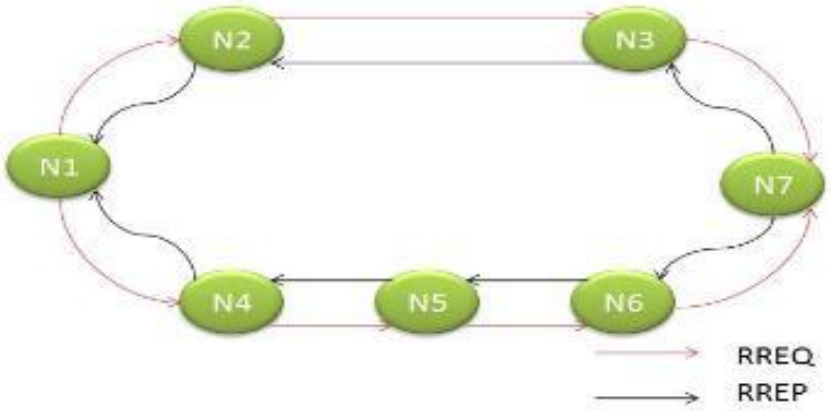

Figure 2.4: Route Discovery in AODV (Chandure, 2011).

2.2.4 Attacks on Ad hoc Network

Any clever threat on network security by a malevolent node that affects the system performance is known as an attack. Largely, in MANET two types of attacks exist which include external attack and internal attack. External attack, as the name implies, launches it attack from outside the network which may not necessarily affect the network performance. Unlike the external attack, internal attack is more destructive and more difficult to detect as destructive node from inside the network launches the attack which distorts the normal activity of the system. Internal attack is additionally divided into two groups which are active attack and passive attack (Sivagurunathan & Prathapchandran, 2016). Passive attack, such as eavesdropping, launches an attack by over-hearing the activities of the network to acquired important information about the data being transferred in the network without affecting the network performance. While active attack directly affects the network performance by either altering the transmitted data or deceitfully advertising false route that has direct effect on the network *(*Sivagurunathan & Prathapchandran, 2016*)*. An active attack is also a type of attack in which an un-authorized user attempt to modify, changes, or alter the message information during transmission (Choudhury *et al*., 2015).

2.2.5 Types of Active Attacks

An active attack can be either internal attack in which the attack is launched from a malicious internal node or an external attack which come from an adversary outside node (Liu *et al*., 2005). Three of these attacks are as follows (Vu & Soneye, 2009):

I. **Masquerade Attack:** The invader falsely attempts to access information greater than they are permit to. The attacker may also try to illegally access login identification or passwords by avoiding the authentic code tools through security breach finding.

II. **Session Reply Attack:** In this type of attack, the hacker obtains the user identification login without the permission of the original user. Therefore, the attacker has full access to the network resources as much as the legitimate user in the network.

III. **Denial of Service (DOS) Attack:** Practically, DOS is poor services as a result of un-necessary over flooding of the network beyond which the router can handle that lead to packet drop.

In ad-hoc network, four major security objectives need to be addressed (Vu & Soneye, 2009):

I. **Confidentiality:** This simply means providing shield against any passive attack in order to ensure privacy of the data information that is been transmitted.

II. **Integrity:** It is basically an effort to avoid any change or modification of the transmitted packet, the main aim is to be able to obtain the original packet that was transmitted.

III. **Authentication:** For data to be reliable, there is a need for verification process so as to ensure that the transmitted data truly comes from the sender that claims to be one.

IV. **Availability:** Key aspect of security goals is to ensure availability of network resources any place, any time for the genuine user to access and share the network

resources. The proposed work deals with internal attack such as black hole and grey-hole attacks.

2.2.5.1 Black Hole Attack

Black hole attack is a type of attack, which takes part during route discovery by falsely advertising itself as the node with shortest path to the destination. If the packet reaches such a node meant for the destination, it either consumes or drops the entire packet. There are two types of black hole attacks namely; single black hole attack and cooperative black hole attack (Sharma & Johari, 2017).

I. **Single Black hole Attack**: Single black hole attack is a type of attack in which a malevolent node after receiving RREQ packet from the source or intermediate node, it quickly generates false RREP message with highest sequence number and fresh enough route with least number of hops to destination node without even checking its routing table. When the source node receives RREP packet from the malicious node, the node wrongly start sending data packets through that route without considering reply from normal nodes in the network. During the transmission, when the packet reaches the destructive node, the node drops the entire packet that is meant for the destination node (Chandure, 2011). Single black hole attack is shown in Figure 2.5

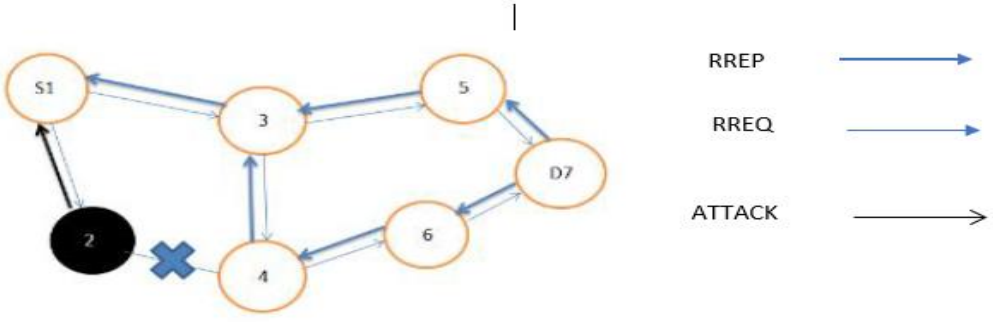

Figure 2.5**:** Single Black Hole Attack (Sharma & Johari, 2017).

II. **Cooperative Black Hole Attack**: When two or more nodes coordinate themselves in a network to carry out malicious activities, it is called cooperative or collaborative black hole attack. These suspicious nodes work together in order to drop or consumes the entire packet transmitted by the source node which is meant to be forwarded to the destination node. They also take part during route discovery, immediately when they received RREQ packet. They falsely advertise themselves as the nodes with shortest route to the destination by producing a highest sequence number with a minimum number of hops to the destination without even checking their routing tables for the destination's node address. As soon as transmitted data is received by the destructive nodes, the entire packet is dropped by the malevolent path formed by them. Figure 2.6 shows cooperative black hole attack (Sharma & Johari, 2017).

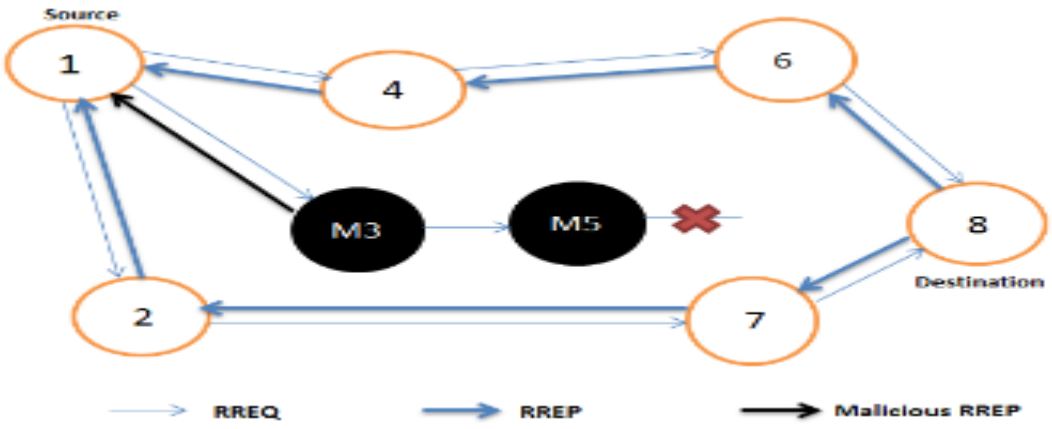

Figure 2.6: Cooperative Black Hole Attack (Sharma & Johari, 2017)

2.2.5.2 Grey- Hole Attack

Grey- hole attack is another security attack which is an extension of black hole attack. This type of attack drops packet based on selectivity. It is very difficult to detect as it behaves maliciously and it also switches to a normal node within the network. Figure 2.7 shows how grey-hole attack is carried out.

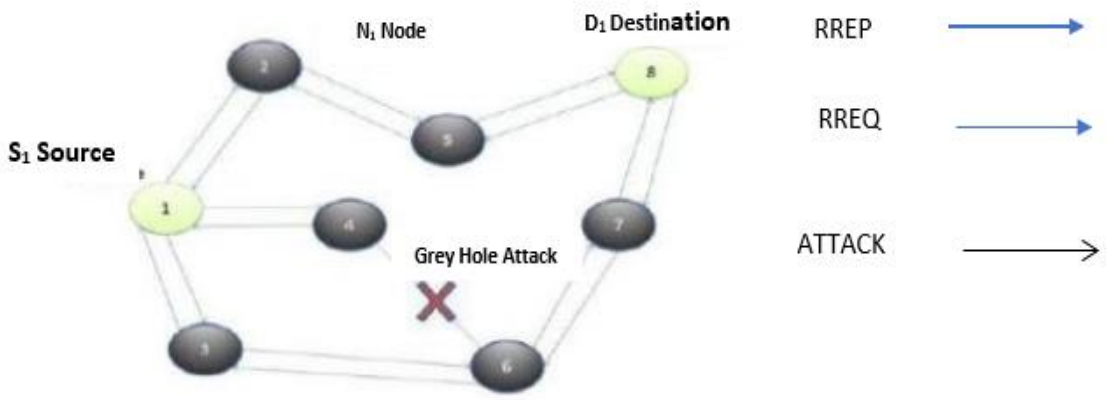

Figure 2.7: Grey- Hole Attack (Jeevamaheswari *et al.,* 2018)

There are two types of grey- hole attacks: which are smart base grey- hole attack and sequence number base grey- hole attack (Gurung & Chauhan, 2018).

i. **Smart Base Grey- Hole Attack**: This type of attack is very difficult to detect as the node behaves normally during path discovery, but start dropping the packet received from the source node based on random selection. Hence, this type of attack is more difficult to detect as compared to black hole attack.

ii. **Sequence Number Base Grey- Hole Attack**: This is a type of attack that take part during path discovery where by the malicious node advertises itself as the node with the shortest path to the destination by generating false sequence number with minimum number of hops.

2.2.6 Computational Intelligence (CI)

CI, first coined by John McCarthy in 1956, not only shows the ability to adapt to the changing situations, but also possesses the attributes for generalizing, discovering, reasoning and association (Abbas., *et al* 2015). CI consist of different techniques such as fuzzy logic,

artificial neural network, evolutionary computing, swarm intelligence and artificial immune systems (Abbas et al., 2015). Figure 2.9 shows the different classification of CI techniques.

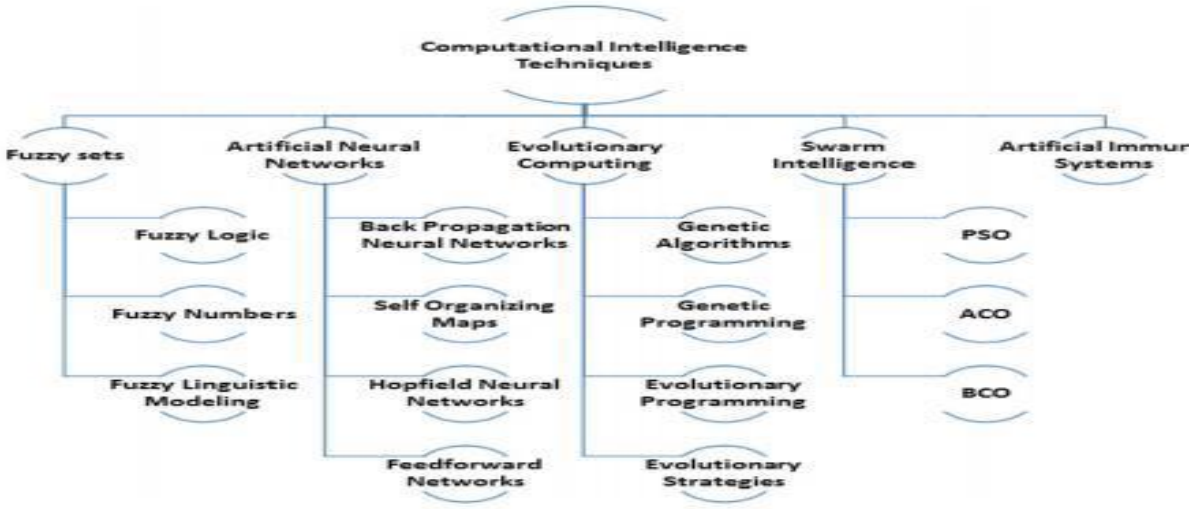

Figure 2.9: Classification of Computational Intelligence (CI) Techniques (Abbas et al., 2015)

CI is defined as the computational ideals and implements of intelligence with the ability of inputting raw numerical sensory data directly, analysing them by manipulating the representational parallelism and pipelining the problem, generating trustworthy and robustness (Kulkarni., *et al* 2011). The properties of basic computational intelligence is shown in Table 2.1.

Table 2.1: Properties of Basic Computational Intelligence (Kulkarni *et al.,2011*)

CI Techniques	**Computational requirement**	**Memory requirement**	**Flexibility**	**Optimality**
Fuzzy Logic	Medium	Medium	Medium	High
Artificial Immune System	Medium	Problem	High	Near Optimal
Neural network	Medium	Medium	Low	Optimal
Evolutionary Algorithm	Medium	Medium	High	Optimal
Swarm Intelligence	Medium	Medium	High	Optimal

2.2.6.1 Neural Networks (NNs)

Inspired by the human brain thinks, learn, analyse and generalise, comprising of multiple network connecting to each other. Each neuron receives signals through synapses. NN works on three components (Abbas et al., 2015):

i. The connection that provide weights hi to the m input of kth neuron.

ii. An aggregation function that add the weighted input to compute the input to the activation function. An activation function that maps the output value of the neuron. Perhaps, NN comprises of neurons that controlled input, hidden and output layer. This is shown in Figure 2.10

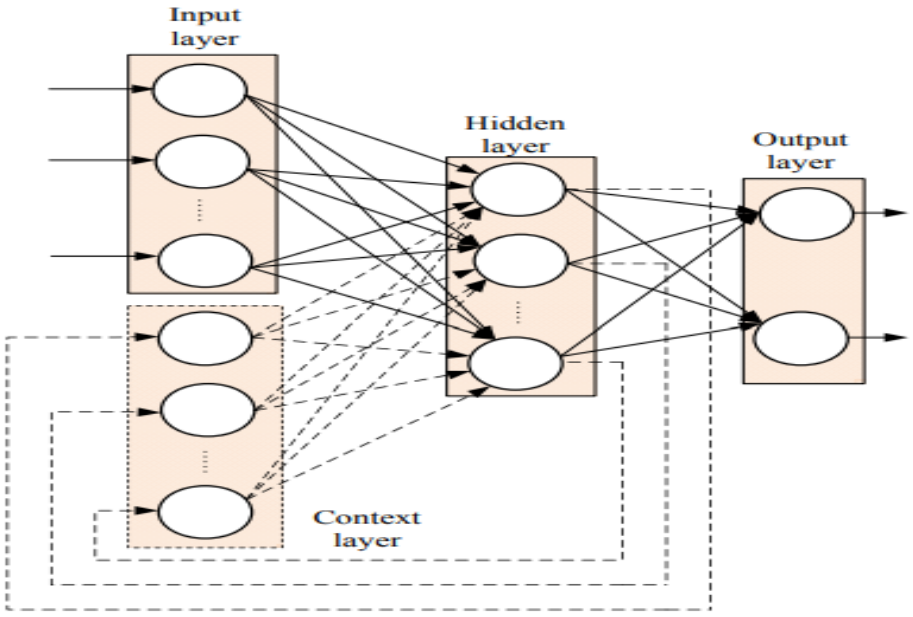

Figure 2.10: Structure of Neural Networks (Abbas et al., 2015)

2.2.6.2 Swarm Intelligence (SI)

SI emerged from the study of combined behavior of group of biological species, such as flocks of birds, shoals of fish and colonies of ants (Karaboga & Akay, 2009). SI is a possession of a system where by collective behaviors of simple agents socializing locally

with their environment leads to clear functional global patterns to emerge (Karaboga & Akay, 2009).

2.2.6.3 Evolutionary Algorithm

Evolutionary algorithm is a representation of natural evolution, by using steps of adaptation to improve the survival tendency of next generation (Kulkarni *et al*., 2011). These steps include natural selection, survival of the fittest, reproduction, mutation and competition. Evolutionary algorithm is based on random selection of candidates called chromosomes. Each chromosome present peculiar characteristics, the idea is to weigh and select the best through the process of reproduction, usually an offspring with high transformed genetics to fit into the next generation are selected and the rest are discarded (Kulkarni *et al*., 2011).

2.2.6.4 Artificial Immune Systems

Natural immune system protects the body against attack (pathogens), such as bacteria or virus. This immune system consists of three different levels which are (Kulkarni *et al*., 2011)

i. Anatomic barrier
ii. Non- specific immunity
iii. Specific immunity

Both specific and non-specific immunities have effect on each other, specific immunity facilitate an order of responses of humeral immunity. While non-specific immunity is assigned on any pathogen. However, if the pathogen withstands the non-specific immunity, system assign defense against specific known class of pathogen (Kulkarni *et al*., 2011).

2.2.6.5 Fuzzy Logic

Fuzzy logic is an attempt to imitate human behavior into a computer system to approximate human decision based on natural language terms *(*Bih, 2006*)*. Fuzzy logic is an extension of

conventional logic, where decision is based on approximate value rather than exact. Fuzzy logic is acquired from fuzzy sets with range of values that extend between 0 and 1 rather than true or false (Hemba & Islam, 2017). The idea of fuzzy logic was proposed by Lotfi-Zadeh in 1965. Fuzzy logic is centred on human observation, actions, behaviour, and selection which are realised with the help of membership functions and fuzzy rules which have the ability to deal with uncertainty (Sharma & Johari, 2017). This research use fuzzy logic because it computationally efficient, guaranty continuity of output, are intuitive, widespread of acceptance, and highly flexible.

2.2.7 Fuzzy Inference Systems (FIS)

Fuzzy inference systems (FIS) are among the most notable application of fuzzy logic and fuzzy sets theory. FIS performs optimally to achieve off-line process simulation, process control, classification task, and online decision support tools. FIS are identified on two perspectives, the ability to handle linguistic terms and universal approximators capable of accomplishing nonlinear mapping between input and output (Serge Guillaume, 2001). Fundamentally, there are five steps to be followed in FIS (Naaz *et al*., 2011) which consist of:

i. **Fuzzification:** This is the process of exchanging the data input to a membership function that obeys the natural behavior of the system position.
ii. **Rules Processing:** Computing and manipulation of the response input from the system based on the initial defined rules.
iii. **Inference:** Calculating fuzzy rules for each incident.
iv. **Composition:** Combining all the fuzzy output into a single entity for defuzzification.

v. **De-fuzzification**: The process of converting fuzzy output. This process of FIS is shown graphically in Figure 2.11.

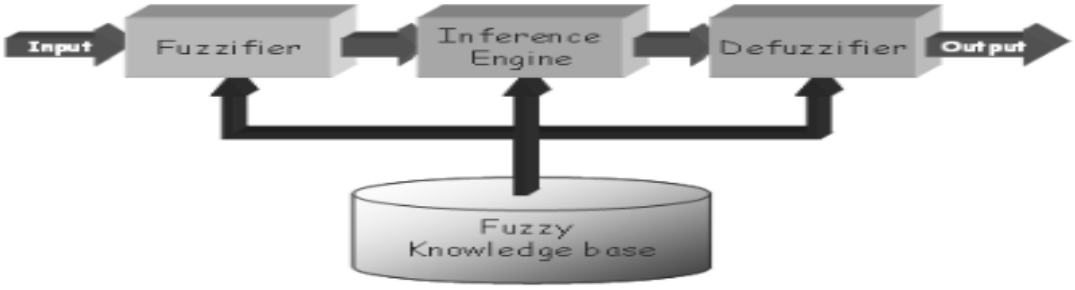

Figure 2.11: Fuzzy Inference System (Naaz *et al.*, 2011)

2.2.8 Inference Mechanisms: Mapping input to output in fuzzy logic, inference mechanism includes membership functions, logical operations, and if-then rules. Two forms of inference mechanism are basically Mamdani and Sugeno (Kaur & Chopra, 2006).

Mamdani Method: The output membership function in Mamdani is not linear in nature, these rules are written as:

R1: if x is A1 and y is B1 then z is C1

R2: if x is A2 and y is B2 then z is C2

Sugeno Method: In this method, the output membership functions are either linear or constant and are written as:

R1: if x is A1 and y is B1 then z is Z1 = a1x1 + b1y1

R2: if x is A2 and y is B2 then z is Z2 = a2x2 + b2y2

2.2.9 Defuzzification Techniques

Basically, there are four techniques used for defuzzification which are as follows (Husain et al., 2017):

i. **Centroid defuzzification method**: It is also known as centre of gravity method and the defuzzifier in this method is used to determine the centre of gravity that uses the value as an output of the fuzzy logic system.

ii. **Maximum decomposition method**: In this method, the defuzzifier observes the sum total of the fuzzy output and choose the one with high degree of fulfilment.

iii. **Centre of maxima**: The centre of maxima in fuzzy region is determined by taking the highest plateau along with the next higher plateau and then the centre point between them is chosen.

iv. **Bisector method**: The region is divided into two equal part using bisector method which is a vertical line. It is not always that it corresponds with the centroid line.

2.3.1 Membership Functions

A membership function is necessary to determine how each term in the input is mapped according to the degree of membership based on binary range 0 and 1 (Husain *et al.*, 2017). There are basically six types of fuzzy membership functions (Husain *et al.,* 2017).

i. Triangular

ii. Trapezoidal

iii. Z-shape

iv. S-shape

v. Sigmoid

vi. Gaussian

Membership function of fuzzy is graphically represented in Figure 2.12.

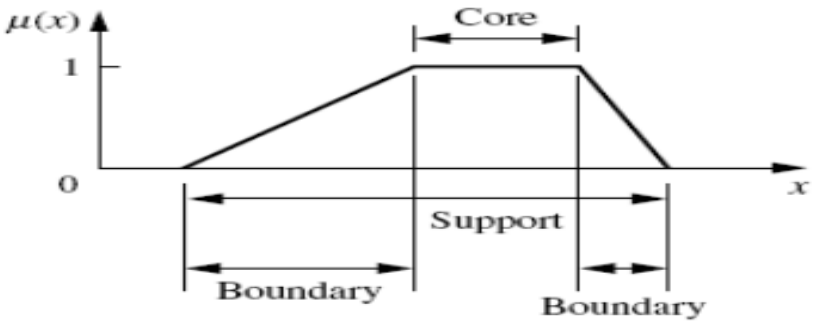

Figure2.12: Fuzzy Membership Function (Husain *et al.*, 2017)

2.3.2 Network Simulator -2 (NS-2)

In an area comprising of network research that encompasses multiple computers, routers and data links will attract high cost of implementation. In this kind of situation, simulators are used in order to save cost and time for accomplishing this type of task (Pan, 2011). However, network simulation is an effort to model the real-world scenario. The main idea is to arrange the system in such away that it can be model so that the features can easily be manipulated and analyzed (Siraj & Gupta, 2012). Primarily, NS-2 is an object-oriented separate event simulator that was first developed at the University of California- Berkely. It uses two set of programming languages that is C++ and OTcl (Object oriented tool command). The reason for hybridization of these programming languages was that C++ has poor visual and graphics, in order to obtain efficient design and implementation for easy usage of descriptive language, NS-2 was design in such a way that control path implementation is separated from data path implementation. To minimize packet lost and time delay, the network object component in the data path are written and collected using C++. While OTcl is responsible for the network topology and control of traffic from source to destination (Pan, 2011). Figure 2.11 shows the users view of NS-2

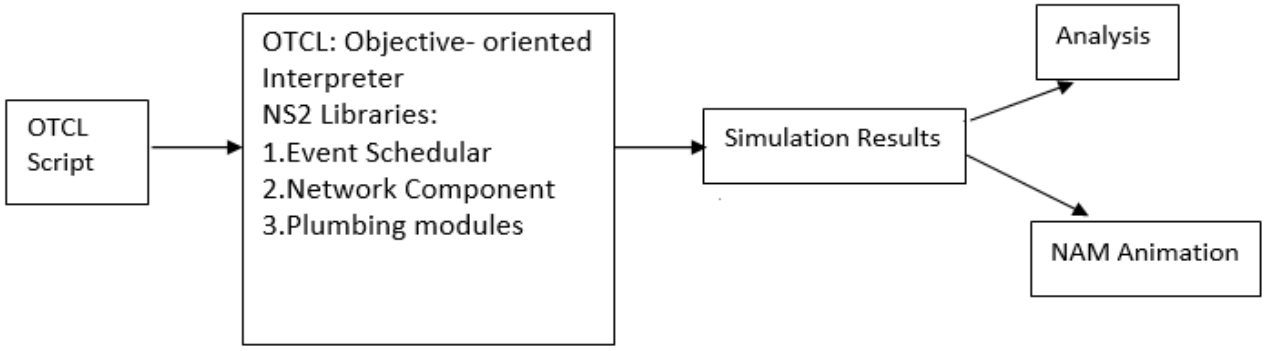

Figure 2.13: Simple view of Network Simulator-2 (Pan, 2011).

2.3.3 Performance Metrics

The following performance metrics were used to analyze the performance of the modified scheme.

2.3.3.1 Network Overhead

Network overhead is the total number of control packets generated by the node in the network. Mathematically it is given (Gurung & Chauhan, 2018) as:

$$\mathbf{NO} = \sum_{i=1}^{k} \boldsymbol{R\ i} \qquad (2.1)$$

where;

NO denotes Network Overhead

R is the number of control packets

i is the number of nodes generating control packet

k is the number of applications

2.3.2.2 Throughput

Throughput is the number of bytes that is successfully transmitted or received per unit time. Throughput is given as (Vangili & Thangadurai, 2015).

$$\mathbf{TP} = \frac{\sum_{i=1}^{n} X_i^r}{\sum_{i=1}^{n} Y_i^s} \qquad (2.2)$$

Where;

TP is the throughput

X_i^r is the average receiving packet for the application

Y_i^s is the average sending packet for the application

n is the number of applications

2.4.3 Packet Delivery Ratio (PDR)

Packet delivery ratio is simply the ratio of the total number of packets received by the node to the total number of packets transmitted by the node (Vangili & Thangadurai, 2015). Mathematically,

$$\mathbf{PDR} = \frac{\sum_{i=1}^{n}(P_i^s P_i^r)}{\sum_{i=1}^{n} P_i^s} \quad (2.3)$$

Where;

P_i^s is the packet send

p_i^s is the packet received

n is the number of applications

It an evidence from literatures that were reviewed, MANETs is a dynamic network whose topology is constantly changing, as nodes in this network are free to move around without restriction. To deal with the uncertainty surrounding MANETs and to detect malicious nodes during data transmission, it requires an accurate and flexible technique to be able to mitigate these attacks. Hence among the computational intelligence techniques, fuzzy logic is flexible and needs no intricate mathematical models. Only a practical understanding of the overall system behavior. Fuzzy also deals with degrees of truth and degrees of membership.

2.3.3 Trust-based Scheme

Trust in MANET is surrounded with lot of uncertainty, trust can be applied to measure and analyze the future behavior of node in the network (Xia *et al*., 2013). Trust in MANET is used to determine the relationship between two adjacent nodes in terms of reliability, timeliness, and data integrity. Hence, trust shows the degree at which node offers a definite service (Xia *et al*., 2013). A node measures the direct trust of its adjacent node by direct computation using the relation (Jain *et al*., 2018):

$$\mathbf{T\ (C, D)} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} (\boldsymbol{x_k y_k}(\boldsymbol{C}, \boldsymbol{D})) \qquad (2.4)$$

where x_k is the parameter to weigh the trust by node C about D and y_k (C, D) is the ith parameter observed by C about D.

2.3.4 Modified TRUST- based Scheme

To achieve the modified trust-based scheme, nodes weigh the trust of one another after a given transmission using a trust evaluator. If found that the trust level of a node is less-than the threshold (with acceptability between 0.6-1.0), then request for second information about the node, then compute the value and take the average. AODV is adopted so that devices interact only with trusted neighbor, fuzzy logic takes in the input and grouped it based on the degree of membership, processed and forwarded to inference mechanism to convert it back to true values at the output. Modified trust-based scheme protocol is shown in Figure 2.13.

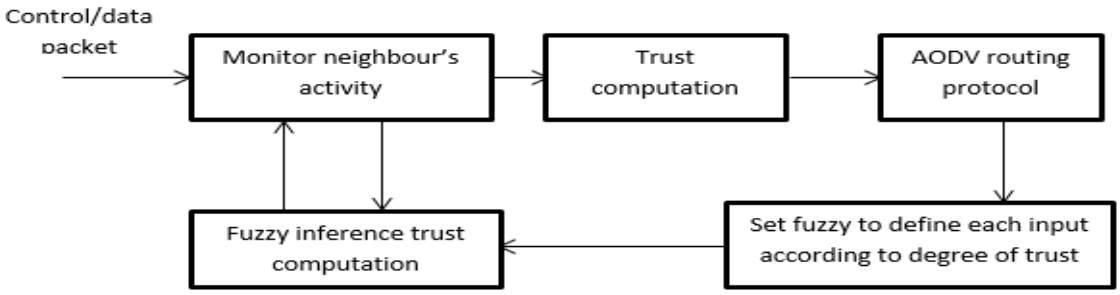

Figure 2.13: Modified Trust based Scheme Routing Protocol

Modified trust based equation is shown in equation 2.5

$$\mathbf{T_1(C,D)} = [[\sum_{k=1}^{n} (x_k y_k(C, D))], [k_1 k_2]] \quad (2.5)$$

Where K_1 is the first fuzzy operation based on immediate acknowledgement and K_2 is the second fuzzy operation based on intermediate acknowledgement.

2.3.5 Flowchart of Shaikh and Rajan (2018)

The IDS protocol is described in Figure 2.14, the protocol is made up of source node, intermediate node, destination node, and IDS nodes deployed into the network. The IDS were set to monitor the participating nodes to report malicious act. The identity of the suspicious node is stored in the routing table to avoid further transmission.

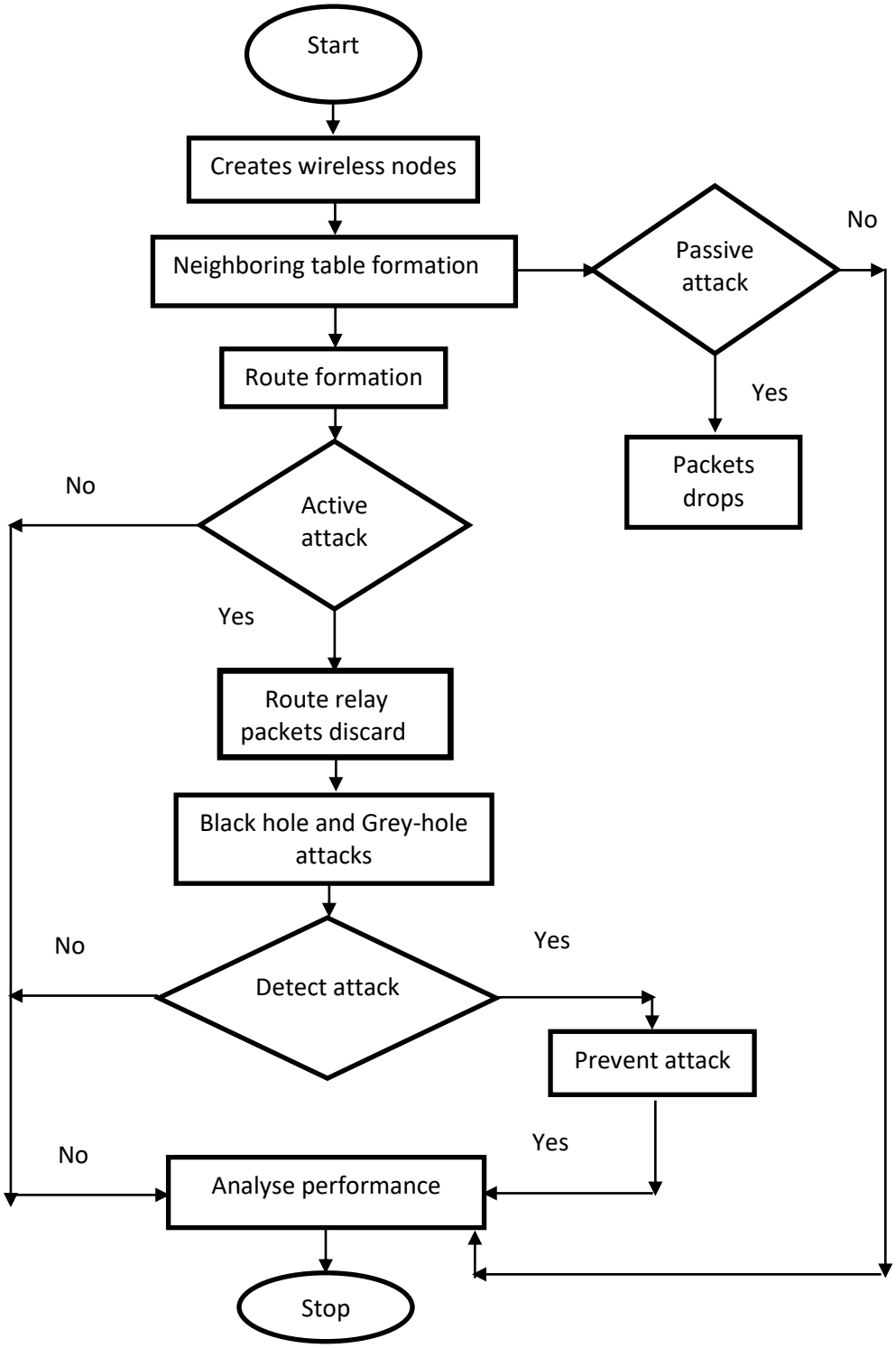

Figure 2.14: Flowchart of Shaikh & Rajan, (2018)

2.3.6 Basic Flowchart of Trust-based Scheme

Trust based scheme was adopted to suite the aim of this work that led to a better performance to a better performance when compared with the existing protocol. The active flowchart is discussed in Figure 2.15 that describes the algorithm, the main sequence of this algorithm are as: first is deployment of nodes in an unrestricted environment. The second phase is monitoring and accountability of neighbor activity. Last part is weighing the trust to ensured node performance is within the desirable threshold, otherwise node is discarded.

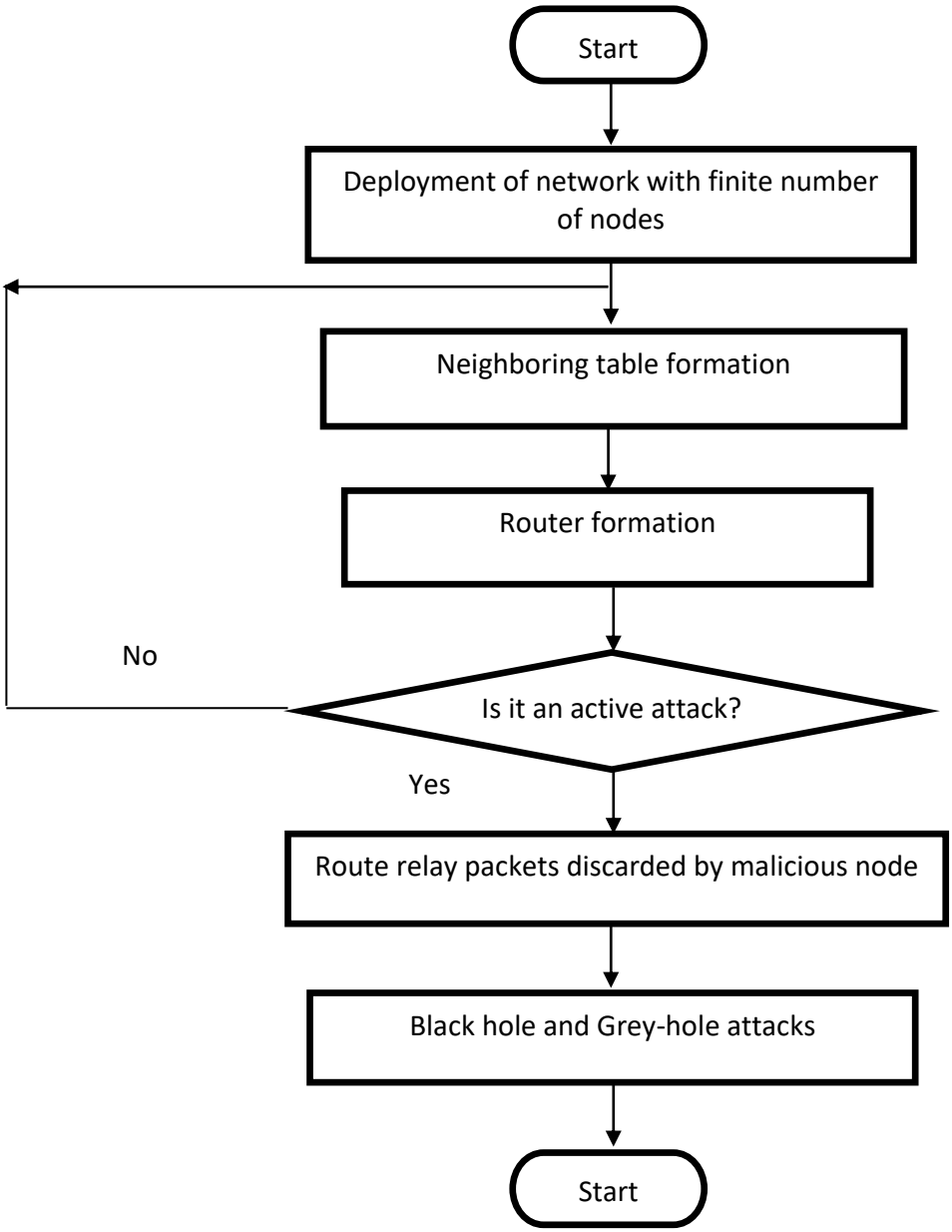

Figure 2.15: Basic Flowchart of Trust based Scheme (Luo *et al*., 2014)

2.5.2 Review of Similar Work

This sub-section discusses a review of some relevant works carried out and published by other researchers. This gives an indication of the extent of the work in this area of research and the techniques or mechanisms and tools used to resolve the same problem. With this knowledge, a better tool and method will be identified and used to give better results.

Chandure (2011) developed a protocol to recognize and eradicate grey-hole attack based on confidentiality and integrity. Two major stages were taken: the first stage was to come up with a technique to tackle malicious nodes in the network. The second stage was carried out to implement grey-hole attack so as to understand the implication of such attack in the network as malevolent activity might cause severe damage to network performance as it was difficult to detect. It caused a node that carried such kind of attack behave as a normal node and later switched to its malicious activity. The result was obtained using Network Simulator (NS-2) that showed better performance when compared with conventional Ad hoc on Demand Distance Vector (AODV) routing protocol. The short-coming of this work was that the network required more computation that led to delay as a result of different stages taken to identified malicious nodes.

Enhanced route discovery for AODV (ERDA) was proposed by **Jalil *et al*. (2011)** to mitigate the issue of security vulnerability such as black hole in AODV routing protocol. The aforementioned issue was tackled by incorporating new conditions in the routing table update process and also by adding simple destructive node equalization and separation process to the AODV route device. Furthermore, to examine the capability of the proposed method, a simulation method was developed. An important enhancement to the network performance when ERDA was implemented in the AODV in comparison to the traditional protocol was

demonstrated by the simulation results. The ERDA scheme was able to address black hole attack on a single node only and hence the issue of coordinated black hole attack and other possible attacks (grey worm, spoofing) formed the major constraints of the ERDA technique.

Choudhury *et al*. (2015) investigated wait time and request reply algorithm to enhance the performance of AODV routing protocol in the presence of black hole attack. The algorithm was implemented by incorporating pre receive reply, RREP table, and wait time as against the conventional AODV routing protocols. All the RREPs were kept in a fresh table for a given period of time in order to screen out destructive nodes since all the routes have an exclusive sequence number in accordance with the algorithm. Hence destructive nodes were isolated and the source node chose a route with the highest sequence number. In addition, the simulation result showed a significant improvement in throughput, Packet Delivery Ratio (PDR), and end-to-end delivery in contrast to the standard AODV protocol when a destructive node was introduced into the network. More memory buffer was required as all the RREP had to be stored for a period of time. This led to poor performance as the participating nodes had low memory capacity.

Vishnu Balan *et al*. (2015) investigated fuzzy based intrusion detection systems in MANET to observe the malevolent activity of nodes in the network using fuzzy logic to verify the type of attack and any further transmission of the node by discarding the node from network. The aforementioned technique made the network vigorous enough to identify and verify the type of attack (black hole or grey hole attack) and this made communication within nodes in the network more reliable. Intrusion Detection System (IDS) was used to monitor the activities of nodes in the network in order to identify destructive nodes by removing any malevolent node from the network. When IDS identified any node with suspicious activities, it quickly

notified other nodes by sending an alarm message with the identity of the malevolent node. AODV routing protocol was adopted for Route Request (RREQ) and Route Reply (RREP) for efficient communication. An IDS used added to network overhead and jitter due to route modification were some of the undesirable limitations of this work.

Vangili & Thangadurai (2015) analyzed detection of black hole attack in mobile ad hoc networks using ant colony optimization. Motivated by nature to transform the performance of Ad hoc on Demand Distance Vector (AODV) routing protocol. This was achieved by incorporating each node with an ant that was used to calculate the pheromone value. Nodes with higher pheromone concentrations (high forwarding ratio) were considered as cooperative nodes and those with less concentration (low forwarding ratio) were taken as malevolent nodes. However, the results were obtained using simulation where the modified AODV showed better performance by increasing the packet delivery ratio, throughput, and reduction in end to end delay. Nevertheless, computational complexity of the algorithm was high as it required long time training of the nodes and eventually led to delay.

Singh (2016) studied hybrid technique to reduce the effect of cooperative black hole attack in order to provide secure and reliable information in the military operation against enemies. The technique was able to identify malicious soldiers by flooding the network with false Routing Request (RREQ) packets, those that respond at first instant by generating and sending back Route Reply (RREP) packets without checking their routing table in order to drop the packets. Identification number of those nodes were added into the black hole list, the results was obtained using simulation that showed a better performance as compared with the conventional MANET. Packet Delivery Ratio (PDR) and throughput of the network improved in comparison with traditional AODV protocol. But the suggested technique

achieved improvement in PDR and throughput at the expense of more delay that eventually led to buffer overflow.

Trust based security model for identifying black hole and grey hole attacks in military based Mobile Ad hoc Network (MANETs) was investigated by **Sivagurunathan & Prathapchandran (2016)**. The mentioned method integrated trust identity to each soldier in order to be able to distinguished between cooperative and suspicious soldier, based on the following; stereo trust, situational awareness and current trust. Each soldier's performance was computed based on first-hand information, second hand information and soldiers current trust. Result of the proposed technique was obtained using simulation which showed better performance as compared with the conventional technique. However, the technique used dynamic source routing (DSR) protocol for data communication, this protocol can only support small networks which form a major constraint in cases where a large network is required.

Hiremath (2016) worked on Fuzzy Inference System (FIS) to identify and avoid supportive black hole attacks in Mobile Ad hoc Networks (MANETs). This was achieved by setting the source node to investigate all nodes activities by using Data Access Table (DAT), DAT mainly keeps all node to node information through hello acknowledgement. If a node consistently work below threshold, it was declare as a black hole and is been blocked from participating in the network activities. Network simulator-2 (NS-2) was used to obtained the results which showed a better performance as compared with the conventional Ad hoc on demand Distance Vector (AODV) routing protocol in terms of throughput, end-to-end delay and packet delivery ratio. However, in this technique, more memory space will be required as

data access table was used to store information of the entire devices in the network. Also periodic updates by intermediate devices increased the network overhead.

Sharma & Johari (2017) analyzed a technique using fuzzy logic to reduce the effect of coordinative black hole attack in AODV routing protocol in mobile ad hoc network (MANETs). The aforementioned technique was realized using two conditions, to fully understood and differentiate between nodes that were distrustful but not destructive and nodes that were distrustful and destructive to avoid discarding non-destructive node within the network. Set of rules were used in identifying coordinative black hole attack. Hence, the source node can effectively stop collaborative black hole. Result of the proposed technique was compared with that of traditional AODV in the presence of malevolent node, it showed an improvement in terms of throughput, network overhead and Packet Delivery Ratio (PDR) through simulation. But due to a set of rules placed for node verifications, the system was encountered by high computational complexity.

Singh (2017) studied a technique called Hybrid and Secure Clustering Technique (HSCT) to minimize the effect of black hole attack in Mobile Ad hoc Network (MANETs) using AODV routing protocol. The technique used Reply Time (RT) and Waiting Time (WT) so that if RT of a specific node is less than WT, another step was used to clearly identify the neighboring node if destructive. It was then added to malevolent table so that any further route reply from that node was ignored or removed. But in the case where RT was equal to WT, a further step was taken by equating the identifications (IDs) of that node with those in the malevolent table to be sure whether it was destructive node or not. Furthermore, if the distrustful node was not in the list, then another stage was taking by computing distance, which was expected to be least and equate with the expected total. When conditions were satisfied, RREP was kept in

the destination table, else node identification number and sequence number were kept in the malevolent table. As soon as all certified were updated in RREP table, then a cluster head was chosen by considering node with the highest order in the table and the result was achieved using simulation (NS2.3 simulator). However, further analyses needs to be done for identification of malicious node as other factors such as buffer overflow or geographical location can cause packet drop by node that may be mistaken for malicious node.

Gurung & Chauhan (2017) suggested Mitigating Grey hole Attack Mechanism (MGAM), the aforementioned technique was used to mitigate smart base grey hole attack in Mobile Ad hoc Network (MANETs) routing protocol. The technique was achieved by introducing an exceptional node into the network called Grey hole-Intrusion Detection System (G-IDS), they were used to avoid destructive nodes attacks using passive acknowledgement to sense any node with malicious act, the G-IDS sends an alert to the entire nodes in the network with the identity of that node in order to stop the malevolent node from accessing the network resources. Network simulator (NS-2.35) was used to authenticate the suggested technique; hence, the result showed an improvement as compared with current pattern of smart grey-hole attack. But an introduction of IDS into the network leads to an increased in overhead as many packets were been transmitted within the network.

Jain *et al* (2018) analyzed fuzzy-based trust computation protocol (FTCP) to minimize the impact of black hole attack using AODV routing protocol. This technique was built on trust upon which was impulsive. Each node calculates the trust of one another and has to be active as the network was highly mobile and the topology changes rapidly. Fuzzy logic was used to validate the technique by setting a range of trust in order to identify and discard a malevolent node in the network. Moreover, an improvement was observed in terms of Packet Delivery

Ratio (PDR), end- to- end delay and throughput as compared with the traditional AODV. The result was obtained using simulation (NS2 simulator). Hence, if trust rate was less-than threshold value, it was considered as destructive node. But only a single information was used to finalize node activity where by a node may be suspicious not malicious as a result of the network mobility thereby isolating those nodes may degrade the network performance.

Jeevamaheswari et al. (2018) studied Modified Ad hoc On demand distance Vector routing protocol (MAODV) using Association Based Data Routing Information (AB-DRI) to provide secure routing protocol against packet drop attacks. This type of attack was very difficult to detect as the node carried out malicious act and later switched to it normal activity during transmission of data packet. The protocol aim at mitigating grey-hole attack using trust base technique to weigh the trust value of each node in the network according to the packet delivered by the node during transmission based on the threshold. This was set to identify malevolent node from normal nodes. Furthermore, the proposed technique shows improvement in terms of packet delivery ratio when compared with the conventional AODV. However, some of the malicious node behaves normally during route discovery, but as soon as they received packet, they switched to their malicious activities which forms the major constrained in this work.

Shaikh & Rajan (2018) investigated Intrusion detection and avoidance of black and grey hole attacks using AODV protocol-based MANET to mitigate the effect of these threats in order to improve the network performance. In this technique, Intrusion Detection System (IDS) was used to monitor's the network activities by listening to each node transmission, in case of any suspicious act carried out by any node within the network, when observed by the IDS node, an alarm was broadcasted to other nodes to avoid any further transmission to that

malevolent node. Hence, each node updates its routing table by storing the IP address of that node in its black list. Network simulator (NS2) was used to obtained the result and found an efficient improvement in terms of packet delivery ratio, end to end delay and network overhead as compared with the conventional AODV. However, the scheme used an IDS node to monitor the network activity is subject to false positive, demand more network overhead in order to coordinate different devices in the network.

From the reviewed literatures, it is evident that mitigation of black hole and grey-hole attacks in MANET is an on-going research challenge. Several mitigation techniques were proposed ranging from mobile agent, fuzzy logic, and genetic algorithm etc. However, nodes in MANET shared wireless bandwidth and topology is constantly changing as a result of nodes mobility, hence obtaining an optimal path for data transmission that is free from attacks is difficult. This research proposed a trust based scheme to mitigate the effect of these attacks and also by adopting fuzzy logic to be able to identify and group each node according to its behavior, this will also help to be able distinguish between malicious node and suspicious node by setting up a threshold base on first hand and second hand information.

CHAPTER THREE

MATERIALS AND METHOD

3.1 Introduction

In this chapter, the material, procedures and methods employed for the successful completion of this research work are discussed. The mitigating of black hole and grey-hole attacks on Mobile Ad hoc Network (MANET) AODV routing protocol using a modified trust-based scheme was simulated using network simulator-2 (NS-2 2015) simulation environment.

3.2 MATERIALS USED FOR THE RESEARCH WORK

The materials used for the research work are as follows:

i. Network simulator-2 (NS2)
ii. Visio 2016
iii. Microsoft word 2016
iv. Literature materials

3.3 METHODOLOGY

The following methodology was adopted in carrying out the research work:

i. Replication of the work of Shaikh and Rajan (2018) using these steps:
   a. Setting up classical AODV routing protocol in mobile ad hoc network.
   b. Deploying 41 nodes into the network in a random way pattern.
   c. Creation of neighboring tables through hello acknowledgement.
   d. Formation of routing tables to store the information of nodes by source node.
   e. Tracking and prohibition based on packet forwarding of node
   f. Implementation of IDS using Network Simulator-2 (NS-2)

ii. Development of a modified trust-based scheme using these steps:

   a. Adaptation and modification of trust-based scheme using fuzzy logic

   b. Implementation of the modified trust-based scheme in ii (a) using Network Simulator-2 (NS-2)

iii. Validation of the result is done by comparing the result obtained from the modified trust-based scheme with those of Shaikh and Rajan (2018) using packet delivery ratio, network overhead and throughput as performance metrics.

3.4 Replication of Shaikh and Rajan, (2018)

The steps followed in the replication of the work of Shaikh and Rajan, (2018) are discussed in this sub section.

3.4.1 Setting up classical AODV Routing Protocol on Mobile Ad Hoc Network

AODV represents the routing protocol, which was used in this scheme to transmit packet from source node to destination node. The routing protocol is on demand, it only established route based on request. The pseudocode for implementing AODV is given as:

a. : *AODV_RREQ-0 // sends RREQ packets for route discovery*

b. : *AODV_RREP-1// Receives RREP packets for route establishment*

c. : *AODV_RERR-2// Generate RERR packet for link breakage*

d. : *AODV_MSG-3// Select message with fresh and shortest path to the target node*

e. : *data pkt-4// Transmission of data packets*

3.4.2 Deploying Forty-One Nodes into the Network in a Random Pattern

Specific number of nodes were deployed into the network using network simulator 2 (NS2) to simulate and model Mobile Ad hoc Network (MANET). The nodes are constantly moving round the network with the source node sending RREQ packet to the destination node using

Ad hoc on demand Distance Vector (AODV) routing protocol. These nodes are grouped into source nodes, intermediates nodes and destination nodes. The aim is to establish connection between the source node and destination node, create a link between them taking into consideration security attacks by malicious nodes. 41 mobile nodes are deployed covering an area of 1500m by 1000m. The pseudo code for random movement of nodes is:

a. : *$topo load_flatgrid 1500 1000// setup a topology covering 1500m by 1000m*

b. : *create-god $val(nn)//create general operation directors for storage of information*

c. : *global ns_tracefd // set global information about the state of the nodes*

d. : *$n($i) random-motion 1 // Nodes are set to move randomly within the network*

3.4.3 Creation of Neighboring Tables

Neighboring tables are formed through gathering of hello messages. The message is updated periodically to ensure presence of neighbor, otherwise, it generate Route Reply Error (RRER) to inform the source node about link breakage. Hence, source node search for an alternative route to destination. The pseudocode for realizing neighboring table is given as:

a. : *nsaddr_t neighbour;// the previous hop*

b. : *log Hello packets // Initialising hello message*

3.4.4 Formation of routing tables

The path of a particular destination is stored in the routing table. If node performs below expectation, the identification number of that node is send to the source node in order to discard that particular node from taking part during data transmission. It also contains the information of topology changes. The pseudocode for actualizing the formation is given as:

a. : *$ns node-config-adhocRouting $val(rp)// create routing table by providing node ID*

b. : *routerTrace ON // Keep routing information of nodes*

3.4.5 Tracking and Prohibition based on Packets Forwarding

IDS nodes did tracking and the prohibition was carried out by source node through the following procedure. Firstly, RREQ packet was flooded into the network for route discovery from source to destination. Once that is established, RREP packet is generated and send back to the source node along with the Id address of that particular node for route establishment. All the Id addresses of nodes in that particular path are collected and stored in the routing table of source node. If node is found dropping packet, the Id address of that node is sent to the source node from where it checked it routing table and block such node from taking part in data transmission. Pseudocode for tracking is given as:

a. *: stats[nbid] // data packet count by IDS*
b. *: Drop(packet *p) // node drops packet*
c. *: ATTACKER_node // declare node malicious*
d. *: invalid packet \n // terminate node from transmission*

3.4.6 Implementation of IDS using Network Simulator-2 (NS-2)

Figure 2.14 is the flow chart of Shaikh and Rajan (2018) that serve as a guide in writing the NS-2 program codes for simulation. Network Simulator-2 is used to simulate the system model.

Total of 41 nodes are deployed into the network covering an area of 1500m by 1000m. wireless channel is modelled in two ray ground with a frequency of 2.4GHz and a maximum range of 100 meters. Omni directional antenna is used for transmission and reception of signals, while AODV routing protocol is used. The script with for the process are as follows:

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)         200                             ;# max packet in ifq
set val(nn)              41                             ;# number of mobilenodes
set val(rp)              AODV                                   ;#ruting protokol
set val(x)              1500                            ;# x coordinate of topology
set val(y)              1000                            ;# y coordinate of topology
set val(energymodel)    EnergyModel                     ;# Energy consumption
        set val(n_ch)           chan_1
```

The model was simulated in Network Simulator-2 (NS-2) using the parameters shown in Table 3.1

Table 3.1: Simulation Parameters of IDS Protocol (Shaikh & Rajan., 2018)

Parameter	**Value**
Mobile Nodes	39
Coverage Area	1500m × 1000m
Various Traffic	CBR
Model of Propagation	Two Ray Ground
Mac Layer	802.11
Packet Size	512
Type of Antenna	Omni
Malevolent Node	2
Routing Protocol	AODV

The obtained results are presented in a graphical form and are used in the comparison of the two protocols as a basis for validation of the developed protocol.

3.5 Development of a Modified Trust-based Scheme (MTS)

The stages involved in the modification of trust based scheme is detailed in this section.

3.5.1 Adaptation and Modification of Trust-based Scheme using Fuzzy Logic

The model system of trust-based scheme was adopted and modified to group nodes based on their individual performance after they carried out a particular task. Nodes in this model were

incorporated with trust evaluator, where by nodes were able to monitor the activities of the adjacent node and vice versa. This reduces number of control packet into the network as no special nodes were deployed to monitor the network, this in return reduces network overhead. Threshold was set and fuzzy logic was used to group these nodes according to their membership group. This improved packet delivery ratio through classifying a group of nodes that performs averagely (that is, between the cooperative and non-cooperative). The model has high mobility support, this reduces un-necessary packet drop and subsequently increases throughput using equation (2.2). The set of threshold used for the fuzzifier is shown in Table 3.2

Table 3.2: Analysis of Trust using Fuzzy Logic

Threshold (Number of nodes delivered)	**Fuzzy steps**	**Trust Level**
0.0-0.2	Very small	Malicious
0.3-0.5	Small	Suspicious
0.6-0.8	Large	Medium
0.9-1.0	Very large	Cooperative

3.5.1 Implementation of the Modified Trust-based Scheme

Model equations and the algorithm of trust-based scheme are developed in the simulation environment, Network Simulator-2 (NS-2) version. The parameters used for the simulation are shown in table 3.3

Parameter	Value
Simulator	NS-2 version 2.35
Simulation time	150s
Propagation model	Two- ray ground
Routing protocols	AODV
MAC	802.11
Traffic source	CBR, FTP
Antenna	Omni Antenna
Packets size	512 bytes/packet
Link layer (LL) type	Logical Link (LL)
Mobility model	Random waypoint model
Pause time type	0.05s
Area of network	1500m x 1000m
TTL	7
Velocity of mobile nodes	0-20m/s
Number of nodes	41 nodes
Initial energy of node	15J
Transmission and receiving power	600mW, 300mW
Transmission range	250m
Queue type	Drop-tail

To compute the trust of every node based on their performance, they are grouped and analyzed using two sets of information. The pseudocode are as follows:

1: nsaddr_t monitoringNode // Set trust evaluator

2: nsaddr_t neighbour // monitor neighbour

3: AODV_MSG // record packet forwarded by node

4: if (index>= 0 && < = 0.2) // malicious node

5: else

6: strcmppktType, "RREP" // discard the node

The obtained results are presented are presented in Chapter four of this report. The results obtained are presented graphical form and are used in the comparison with the IDS protocol developed by Shaikh & Rajan, (2018) as the basis for validation of the modified algorithm.

3.6 Evaluation and Comparison of the Developed Protocol with the work (Shaikh & Rajan, 2018) for Validation.

3.6.1 Validation of the Modified Protocol

The simulation environment where IDS protocol was applied developed by Shaikh & Rajan (2018) was also used to simulate the modified protocols. The modified trust-based scheme was compared with IDS protocol to ensure conformity.

3.6.2 Performance Evaluation

The performance of the Modified protocol and the IDS protocol developed by Shaikh & Rajan (2018) was evaluated using packet delivery ratio, network overhead, and throughput as performance matrices. The percentage improvement was evaluated sing equation (3.2).

$$\text{Percentage improvement} = \frac{MTS - IDS}{MTS} \times 100\%$$

where, MTS is the modified trust-based scheme and IDS is the intrusion detection system

3.6.3 Flowchart of Modified Trust-based Scheme

The operational flowchart of modified trust-based scheme is analyzed in Figure 2.16. In the modified algorithm, fuzzy logic was incorporated with conventional trust-based scheme that aid in analyzing these devices by grouping them into different classes. Two set of acknowledgements were used to come-up with node performance that is first acknowledgement from immediate node was analyzed and computed. If it is within the threshold, node is treated as a true node otherwise further analysis is been made by tracking the node previous performance from intermediate node (second acknowledgement) before final decision was made.

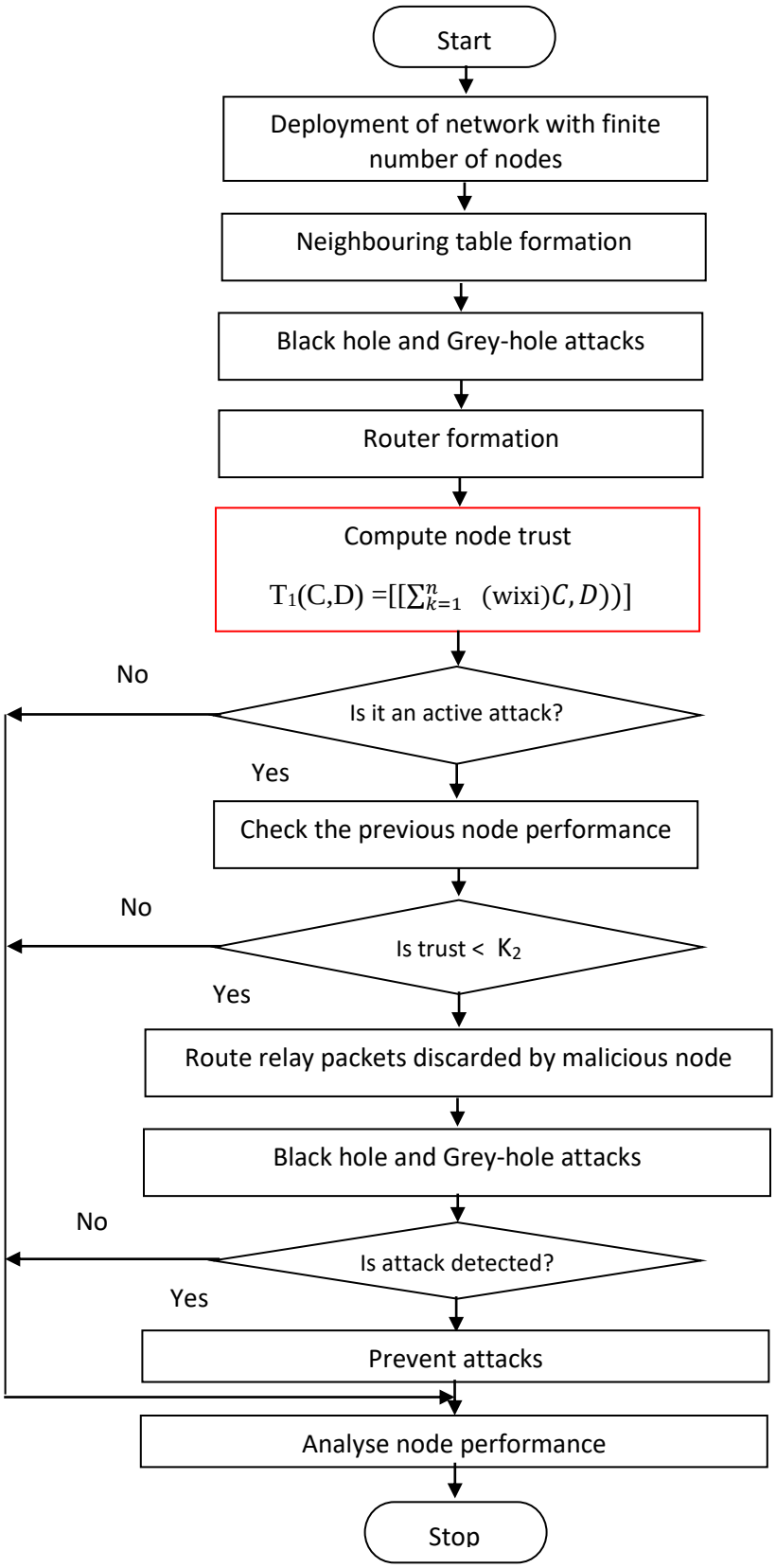

Figure 3.1: Flowchart of Modified Trust Based Scheme

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Introduction

In this chapter, the results obtained are presented and discussed based on trust-based scheme by using fuzzy logic to analyze the performance. Results obtained are also compared with the work of Shaikh and Rajan, (2018) for validation. Finally, the performance of the trust-based scheme using fuzzy logic was evaluated using Packet Delivery Ratio (PDR), network overhead and throughput as performance metrics.

4.2 Packet Delivery Ratio versus Mobility Speed for IDS and MTS

Figure 4.1 is a plot of packet delivery ratio against node speeds for both protocols (IDS and MTS). It was observed that during the simulation when mobility of the nodes is increased, packet delivery ratio decreases a bit as illustrated in Figure 4.1. This is as a result of constant mobility of the intermediate node that drops data packet due to collision, change of location or as a result of link breakage. When there is a malevolent node, packet delivery ratio gets even lower because the destructive node pretends to have a valid path to the destination without checking its routing table. In this case, as soon as the malicious node receives the data packets, it either dropped the entire packets or drops some of the packets base on random selection. However, the simulation result in the Figure 4.1 shows that the performance of MTS outperforms IDS in terms of packet delivery ratio. Although there was a decrease with an increase in node speed, but is not as severe as IDS. This is because of better operation of MTS in analyzing the destructive nodes and also to screen them out to avoid any further transmission or reception of data packets from them. Table 4.1 shows the performance of the two protocols with respect to Figure 4.1. It is also observe that from the

table PDR dropped woefully at 25m/s and start to increase at 30m/s, it's mainly because destructive nodes changes location rapidly at higher speed that led to risen and fallen of PDR values.

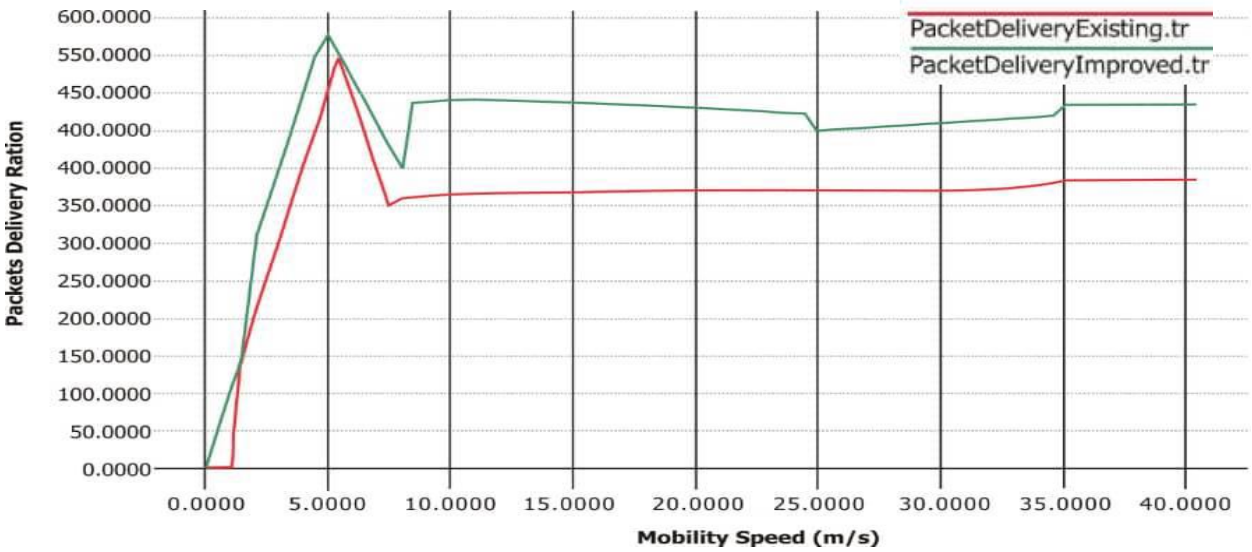

Figure 4.1: Plot of Packet Delivery Ratio for the two Protocols against Mobility Speed

Table 4.1: Percentage Improvement of Packet Delivery over IDS of Shaikh & Rajan (2018)

Mobility Speed (m/s)	Modified protocol (PDR)	IDS of Shaikh & Rajan (2018) (PDR)	PDR Improvement (%)
5.0	570	450	21.5
10	440	370	15.9
15	435	375	13.8
20	430	375	12.8
25	400	375	6.3
30	410	375	8.5
35	435	385	11.5
40	435	390	10.3

The average percentage improvement is given as

$$P = \frac{\text{Sum of percentage improvement}}{\text{Number of variables}} \quad (4.1)$$

$$\frac{21.5 + 15.9 + 13.8 + 12.8 + 6.3 + 8.5 + 11.5 + 10.3}{8} \text{ x } 100\% = 12.6\%$$

The results were obtained using equation (2.3) and the average packet delivery ratio was improved by 12.6% as compared IDS of Shaikh & Rajan (2018) using equation (4.1) considering a range of values from 0 – 40m/s.

4.3 Network Overhead versus Mobility Speeds (m/s) for IDS and MTS

Figure 4.2 is a plot of network overhead against mobility speed (m/s) that shows the result for the performance of IDS and MTS in terms of network overhead against mobility speed (m/s). During simulation, nodes were allowed to move randomly by adopting Random Way Point (RWP) mobility model. The network overhead is determined using equation (2.1). Trust that is required for each node to monitor its neighbor during transmission of data packets is given by equation (2.4). For both protocols, it was observed that as the speed increases, the network overhead increases. This is because at high speed, malicious node generates more control packets in the network and drops the packets resulting in a very high routing overhead. At lower speed, destructive nodes are easily identify and blocked from participating in the network activities. With an increase in mobility speed and number of nodes in the network, it is difficult to fish out the destructive node. The simulation result in Figure 4.2 shows a reduction in network overhead of MTS over IDS. This is because MTS was able to reduced number of un-wanted packets. Threshold was used to sought out the malicious node and prevented them from taking part in the network. Unlike IDS, where special nodes are been deployed into the network to monitor their activities and eventually led to an increase in network overhead. It is as a result of unnecessary control packets generated by those nodes

within the network. Table 4.2 shows the network performance of the two protocols with respect to Figure 4.2. At 20m/s, there was a significant reduction (45.5%) of overhead from the existing protocol, which occurred as a result of low generation of control packets by the IDS nodes. However, from 30m/s upward, the network attained stable state for both protocols. This is because at higher speeds, destructive nodes attacks can only be minimized to the barest level but cannot be completely avoided.

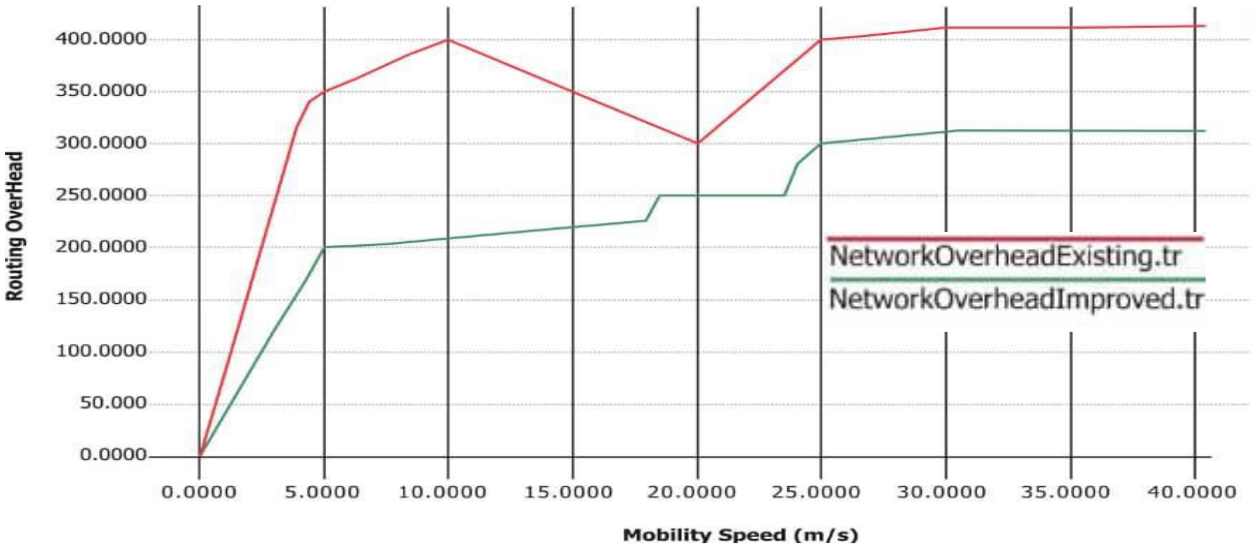

Figure 4.2: Plot of Network Overhead for the Two Protocols against Mobility Speed

Table 4.2: Percentage Reduction of Network Overhead over IDS of Shaikh & Rajan (2018)

Mobility Speed (m/s)	Modified Protocol (Network overhead)	IDS of Shaikh and Rajan (2018) (Network Overhead)	Network Overhead Reduction (%)
5.0	200	350	-75
10	210	400	-90
15	225	350	-55.6
20	250	300	-20
25	300	400	-33.3
30	315	410	-30
35	315	410	-30

The average percentage reduction is given as

$$R = \frac{\text{Sum of percentage reduction}}{\text{Number of variables}} \quad (4.2)$$

$$\frac{-75 - 90 - 55.6 - 20 - 33.3 - 30 - 30 - 30}{8} \text{x } 100\% = 45.5\%$$

Results for network overhead was obtained using equation (2.1), while the average network overhead was reduced by 45.5% as compared with the IDS of Shaikh & Rajan (2018) using equation (4.2).

4.4 Throughput versus Mobility Speed for IDS and MTS

Figure 4.3 is a plot of throughput against mobility speed, it shows the result of the performance of IDS and MTS. The throughput is calculated using equation (2.2). Random Way Point (RWP) mobility model was used for the network simulation. It was observed that an increase in speed does not necessarily increase or decrease the throughput. This is as a result of the random nature of the network. Despite that, MTS was able to improve IDS, this is because MTS has high mobility support as compared with IDS. At 10m/s both protocols attained the maximum throughput. This is because malicious node was not present at that point in time. From Figure 4.3, it showed that the MTS protocol outperforms IDS protocol. Table 4.3 showed the network performance of the two protocols with respect to Figure 4.3. It is also observed that there was a stability from 35m/s for both protocols, this is a result of link breakage, change of location, and buffer overflow that led to packet drop and subsequently reduced the throughput.

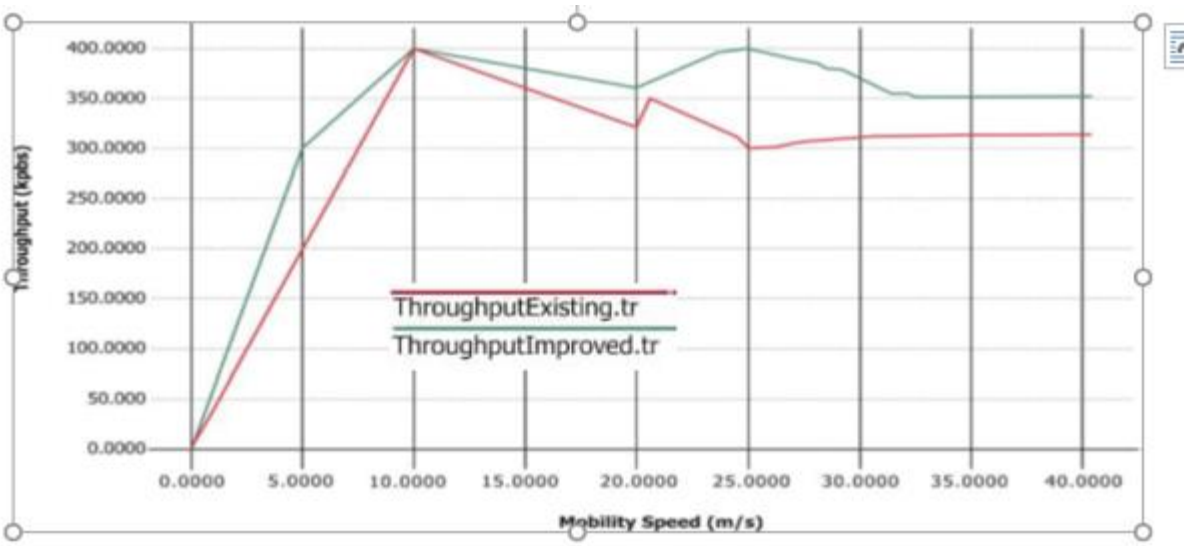

Table 4.3: Throughput improvement over IDS of Shaikh & Rajan (2018)

Modified Protocol (Throughput in Kbps)	IDS of Shaikh & Rajan (2018) (Throughput in Kbps)	Throughput Improvement (%)
300	200	33.3
400	395	1.25
375	360	4.0
365	325	11
400	300	25
370	315	14.9
350	315	10

The average percentage improvement is given as

$$T = \frac{\text{Sum of percentage reduction}}{\text{Number of variables}} \quad (4.3)$$

$$\frac{33.3 + 1.25 + 4 + 11 + 25 + 14.9 + 10 + 10}{8} \text{x } 100\% = 13.7\%$$

Throughput was obtained through equation (2.2) and the average throughput of 13.7% was gotten over the IDS of Shaikh & Rajan (2018).

4.5 Summary of Results

From the simulation results obtained from Modified Trust-base Scheme (MTS) using fuzzy logic. The average improvement in throughput, Packet Delivery Ratio (PDR), and network overhead outperforms that of Intrusion Detection System (IDS). The improvement happened as a result of incorporating the participating nodes with trust evaluator that enables them to monitor and evaluate the performance of its neighbor without necessarily deploying special nodes into the network. This then reduced network overhead and improves Packet Delivery Ratio (PDR) and throughput. However, in this scheme two sets of information were used (Information from adjacent node and recommendation from other nodes) to evaluate the node performance base on the threshold set. This helps in distinguishing between suspicious node and malicious node. Results obtained from simulation showed that MTS reduced the network overhead by 45.5% as a function of mobility speed over IDS protocol. MTS was also able to improve Packet Delivery Ratio (PDR) by 12.6% as a function of mobility speed over IDS protocol. Throughput was also improved by 13.7% with MTS as a function of mobility speed as against IDS protocol.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 INTRODUCTION

This chapter presents a conclusion of the work done, significant contributions achieved in this research. Recommendations for further research work are also made.

5.2 CONCLUSIONS

Black hole and Grey-hole attacks are considered as the major drawback of all routing protocol in Mobile Ad hoc Network (MANET) because it limits their expected routing ability. Several mitigation techniques such as mobile agent, fuzzy logic, genetic algorithm, cross layer cooperation, clustering algorithm, route redundancy, and message parameters, etc. have been introduced in different literatures to address the problem of internal attack (such as black hole and grey-hole attacks). This research work focused on Intrusion Detection System (IDS) in the IDS protocol, where special nodes were deployed to supervise the nodes performance. Hence, this protocol is prone to overhead due to excess flooding of control packets and is subjected to false positive leading to low Packet Delivery Ratio (PDR) and low throughput. Modified Trust based Scheme (MTS) was modified using fuzzy logic where to sets of information were used to ensure detection of black hole and grey-hole attacks was done with minimal error. Also threshold was used to ensure that suspicious node were not mistaken for malicious node which improved the network in terms of throughput. In this protocol, trust evaluator was incorporated into the participating node, hence no special nodes were needed in the network that reduced the network overhead significantly. The performance of Modified Trust based Scheme (MTS) was evaluated using network overhead,

packet delivery ratio, and throughput as performance metrics and the results showed that the modified technique was effective.

5.3 SIGNIFICANT CONTRIBUTIONS

A Modification of Trust-based Scheme (MTS) was used to mitigate the effect of black hole and grey-hole attacks in AODV routing protocol, the MTS when compared with IDS protocol was able to:

i. Reduce Network overhead by 45.5%,
ii. Improve Packet Delivery Ratio (PDR) by 12.6%.
iii. Improve throughput by 13.7%.
iv. By varying the speed from 0 to 40m/s

5.4 RECOMMENDATIONS

Although the aim of this research, which was to mitigate the effect of black hole and grey-hole attacks using the modified trust-based scheme to enhance the performance of MANET, was achieved, the following areas could be studied to further improve this scheme:

i. The work can be further studied to find the effect of increased number of nodes and coverage area on the improved scheme.
ii. Other routing protocols may be considered such as Destination-Sequence Distance Vector (DSDV) and Dynamic Source Routing (DSR) to observe their impact on the improved scheme.
iii. Other attacks, such as wormhole, spoofing may be considered to observe their impact on the improved scheme.

REFERENCES

Abbas, A., Zhang, L., & Khan, S. U. (2015). A survey on context-aware recommender systems based. https://doi.org/10.1007/s00607-015-0448-7 Journal of Software Engineering and Applications

Ali, N. Z., Ahmad, R. B., & Aljunid, S. a. (2008). International Conference on Electronic Design. *Link Availability Estimation for Routing Metrics in MANETs : An Overview*, 1–3. https://doi.org/10.1109/ICED.2008.4786686 international Conference on Computing, Communication and Automation (ICCCA)

Bih, J. (2006). Paradigm shift - An introduction to fuzzy logic. *IEEE Potentials*, *25*(1), 6+21. https://doi.org/10.1109/MP.2006.1635021

Chandure, O. V. (2011). A Mechanism for Recognition and Eradication of Gray Hole Attack using AODV routing protocol in MANET, *2*(6), 2607–2613. (IJCSIT) International Journal of Computer Science and Information Technologies.

Choudhury, D. R., Ragha, L., & Marathe, N. (2015). Implementing and improving the performance of AODV by receive reply method and securing it from Black hole attack. *Procedia Computer Science*, *45*(C), 564–570. https://doi.org/10.1016/j.procs.2015.03.109

Devi, V. U. (2017). A State-of-the-Art Survey on MANET Protocols, *116*(10), 471–480.

Eldein, D., Ahmed, M., & Khalifa, O. O. (2017). An Overview of MANETs : Applications, Characteristics , Challenges , and Recent Issues. International Journal of Engineering and Advanced Technology (IJEAT).

Gurung, S., & Chauhan, S. (2017). A dynamic threshold based approach for mitigating black-hole attack in MANET. *Wireless Networks*, 1–15. https://doi.org/10.1007/s11276-017-1514-1

Gurung, S., & Chauhan, S. (2018). A novel approach for mitigating gray hole attack in MANET. *Wireless Networks*, *24*(2), 565–579. https://doi.org/10.1007/s11276-016-1353-5

Hemba, S., & Islam, N. (2017). Fuzzy Logic : A Review, (2), 61–63 Journal of Vibro engineering, Vol. 21.

Hiremath, P. S. (2016). Adaptive Fuzzy Inference System for Detection and Prevention of Cooperative Black Hole Attack in MANETs, 245–251 2016 International Conference on Information Science (ICIS).

Husain, S., Ahmad, Y., Sharma, M. M., & Ali, M. S. (2017). Comparative Analysis of Defuzzification Approaches from an Aspect of Real life problem, *19*(6), 19–25. https://doi.org/10.9790/0661-1906031925 IOSR Journal of Computer Engineering (IOSR-JCE).

Jain, A. K., Tokekar, V., & Shrivastava, S. (2018). Security enhancement in MANETs using

fuzzy- based trust computation against black hole attacks. *Advances in Intelligent Systems and Computing*, *625*, 39–47. https://doi.org/10.1007/978-981-10-5508-9_4 IEEE Communications Surveys & Tutorials (Volume: 14, Issue: 2, Second Quarter 2018)

Jalil, K. A., Ahmad, Z., & Manan, J. A. (2011). Mitigation of Black Hole Attacks for AODV Routing Protocol. *International Journal on New Computer Architectures and Their Applications (IJNCAA)*, *1*(2), 336–343.

Jeevamaheswari, M., Jothi, R. A., & Palanisamy, V. (2018). AODV Routing Protocol to Defence Against Packet Dropping Gray Hole Attack In MANET, *4*(2), 1464–1471. Computer science international journal of scientific research in science and technology.

Karaboga, D., & Akay, B. (2009). A survey: Algorithms simulating bee swarm intelligence. *Artificial Intelligence Review*, *31*(1–4), 61–85. https://doi.org/10.1007/s10462-009-9127-4 IEEE international conference.

Kaur, A., & Chopra, V. (n.d.). Fuzzy Model for Optimizing Strategic Decisions using Matlab, 270– 282. IEEE Transactions on Systems.

Kulkarni, R. V, Member, S., Förster, A., Venayagamoorthy, G. K., & Member, S. (2011). Computational Intelligence in Wireless Sensor Networks : A Survey, *13*(1), 68–96 IEEE Communications Surveys & Tutorials 13(1):68 - 96

Naaz, S., Alam, A., & Biswas, R. (2011). Effect of Different Defuzzification Methods in a Fuzzy Based Load Balancing Application. *International Journal of Computer Science Issues (IJCSI)*, *8*(5), 261–267. https://doi.org/1694-0814

Nath, S., Banik, S., Seal, A., & Sarkar, S. K. (2017). Optimizing MANET routing in AODV: An hybridization approach of ACO and firefly algorithm. *Proceedings - 2016 2nd IEEE International Conference on Research in Computational Intelligence and Communication Networks, ICRCICN 2016*, 122–127. https://doi.org/10.1109/ICRCICN.2016.7813643

Ochola, E. O., Eloff, M. M., & Poll, J. A. Van Der. (2017). Manet Reactive Routing Protocols Node Mobility Variation Effect In Analysing The Impact Of Black Hole Attack ., *108*(June), 80–91 SAIEE Africa Research Journal.

Pan, J. (2011). A Survey of Network Simulation Tools : Current Status and Future Developments, 1–13. *International Journal of Computer Science Issues (IJCSI).*

Shaikh, U., & Rajan, A. P. (2018). Intrusion detection and avoidance of black and grey hole attacks using AODV protocol based MANET, *7*, 110–116 International journal of engineering & technology.

Sharma, A., & Johari, P. K. (2017). Eliminating Collaborative Black-hole Attack by Using

Fuzzy Logic in Mobile Ad-hoc Network, (5) International Journal of Computer Sciences and Engineering.

Singh, B., Srikanth, D., & Kumar, S. C. . (2016). Mitigating effects of Black hole Attack in Mobile Ad-hoc Networks: Military Perspective. *IEEE International Conference on Engineering and Technology (ICETECH)*, (March).

Singh, H. (2017). Available Online at www.ijarcs.info HSCT: A Hybrid and Secure Clustering Technique for Detection of Black hole Attack in Mobile Adhoc Networks, *8*(4), 2017 International Journal of Advanced Research in Computer Engineering & Technology (IJARCET).

Siraj, S., & Gupta, A. K. (2012). Network Simulation Tools Survey, *1*(4), 201–210 International Journal of Advanced Research in Computer and Communication Engineering.

Sivagurunathan, S., & Prathapchandran, K. (2016). Trust Based Security Model To Withstand Against Black Hole and Grey Hole Attacks in Military Based Mobile Ad Hoc Networks. *International Journal of Mobile Network Communications & Telematics (IJMNCT)*, *6*(1), 1–14. https://doi.org/10.5121/ijmnct.2016.6101

Sun, Y. L. (2004). Trust Modeling and Evaluation for Ad Hoc Networks, (20041017).

Vangili, A., & Thangadurai, K. (2015). Detection of Black Hole Attack in Mobile Ad-hoc Networks using Ant Colony Optimization – simulation Analysis. *Indian Journal of Science and Technology*, *8*(13). https://doi.org/10.17485/ijst/2015/v8i13/58200

Vishnu Balan, E., Priyan, M. K., Gokulnath, C., & Usha Devi, G. (2015). Fuzzy based intrusion detection systems in MANET. *Procedia Computer Science*, *50*, 109–114. https://doi.org/10.1016/j.procs.2015.04.071

Vu, C. H., & Soneye, A. (2009). An Analysis of Collaborative Attacks on Mobile Ad hoc Networks, *146*(14), 42–45 IEEE Communications Magazine.

Xia, H., Jia, Z., Li, X., Ju, L., & Sha, E. H. M. (2013). Trust prediction and trust-based source routing in mobile ad hoc networks. *Ad Hoc Networks*, *11*(7), 2096–2114. Elsevier.

Loo et al.,(2016) wireless communication standards: A study of IEEE 802.11. Published by standard information network IEEE press. 2016

S. Guillaume. Designing fuzzy inference systems from data: an interpretability-oriented review. IEEE Transactions on Fuzzy Systems, Institute of Electrical and Electronics Engineers, 2001, 9 (3), pp.426- 443.

APPENDIX A

Implementation of the General Model of the Simulation

We begin our script with list of defined parameters as shown:

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) 200 ;# max packet in ifq

set val(nn) 35 ;# number of mobilenodes

set val(rp) AODV ;#ruting protokol

set val(x) 500 ;# x coordinate of topology

set val(y) 500 ;# y coordinate of topology

set val(energymodel) EnergyModel ;# Energy consumption

set val(n_ch) chan_1

The next step is to create an instant of the simulator

set ns [new Simulator]

Then set-up trace support by opening by opening file as follows:

set f0 [open execute/Throughput-Existing.tr w]

set f1 [open execute/Throughput-Improved.tr w]

set f2 [open execute/NetworkOverhead-Existing.tr w]

set f3 [open execute/NetworkOverhead-Improved.tr w]

set f4 [open execute/PacketsDelivery-Existing.tr w]

set f5 [open execute/PacketsDelivery-Improved.tr w]

set tracefd [open trust.tr w]

$ns trace-all $tracefd

$ns use-newtrace

set namtrace [open sim12.nam w]

$ns namtrace-all-wireless $namtrace $val(x) $val(y)

Next create a topology object that keeps track of movement mobile nodes within the topological boundary.

set topo [new Topography]

$topo load_flatgrid $val(x) $val(y)

Next we create the object GOD (General Operations Director) is used to store global information about the state of the environment.

create-god $val(nn)

set chan_1 [new $val(chan)]

Nodes Configuration

We need to create nodes before we can configure them, simulation for the configured nodes is

as follows:

**$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) **

**-channel $chan_1 **

**-topoInstance $topo **

**-agentTrace ON **

**-routerTrace ON **

**-macTrace ON **

**-movementTrace OFF **

**-channel $chan_1 **

**-energyModel $val(energymodel) **

**-rxPower 0.3 **

**-txPower 0.6 **

-initialEnergy 90

APPENDIX B

Simulation Code for Source and Destination Node

Appendix B present the code for setting up communication between the source node and the destination node.

```
for {set i 0} {$i < 10} { incr i } {
set n($i) [$ns node]
$n($i) random-motion 1
$n($i) color red
$ns at 0.0 "$n($i) color red"
$ns initial_node_pos $n($i) 20
}
for {set j 10} {$j < 20} { incr j } {
set n($j) [$ns node]
$n($j) random-motion 1
$n($j) color green
$ns at 0.0 "$n($j) color green"
$ns initial_node_pos $n($j) 20
}
for {set k 20} {$k < 30} { incr k } {
set n($k) [$ns node]
$n($k) random-motion 1
$n($k) color blue
$ns at 0.0 "$n($k) color blue"
```

```
$ns initial_node_pos $n($k) 20
   }
for {set l 30} {$l < 35} { incr l } {
set n($l) [$ns node]
$n($l) random-motion 0 ;
$n($l) color black
$n($l) shape box
$ns initial_node_pos $n($l) 25
$ns at 0.0 "$n($l) color black"
$ns at 0.0 "$n($l) label attacker"
Antenna/OmniAntenna set X_ 0
Antenna/OmniAntenna set Y_ 0
Antenna/OmniAntenna set Z_ 1.5
Antenna/OmniAntenna set Gt_ 1.0
Antenna/OmniAntenna set Gr_ 1.0
Phy/WirelessPhy set CPThresh_ 20.0
Phy/WirelessPhy set CSThresh_ 2.0589e-11
Phy/WirelessPhy set RXThresh_ 6.258e-10
Phy/WirelessPhy set Rb_ 3*1e6
Phy/WirelessPhy set Pt_ 8.2818
Phy/WirelessPhy set freq_ 1028e+6
Phy/WirelessPhy set L_ 3.0
}
```

Random Motion

The random movement of nodes is enable here, as we are going to provide node position and movement (speed and direction) directives.

#

 # Provide initial (X,Y, for now Z=0) co-ordinates for node_(0) and node_(1)

#

$node_(0) set X_ 5.0

$node_(0) set Y_ 2.0

$node_(0) set Z_ 0.0

$node_(1) set X_ 390.0

$node_(1) set Y_ 385.0

$node_(1) set Z_ 0.0

Produce some node movement

#

 # Node_(1) starts to move towards node_(0)

#

$ns_ at 50.0 "$node_(1) setdest 25.0 20.0 15.0"

$ns_ at 10.0 "$node_(0) setdest 20.0 18.0 1.0"

 # Node_(1) then starts to move away from node_(0)

$ns_ at 100.0 "$node_(1) setdest 490.0 480.0 15.0"

Next set-up traffic flow between the two nodes

set udp0 [new Agent/UDP]

$ns attach-agent $n(10) $udp0

set sink0 [new Agent/LossMonitor]

$ns attach-agent $n(1) $sink0

$ns connect $udp0 $sink0

set cbr0 [new Application/Traffic/CBR]

$cbr0 set packetSize_ 512

$cbr0 set rate_ 600kb

$cbr0 set interval_ 0.05

$cbr0 set random_ 1

$cbr0 set maxpkts_ 10000

$cbr0 attach-agent $udp0

set udp1 [new Agent/UDP]

$ns attach-agent $n(20) $udp1

$ns at 0.0 "$n(20) label SOURCE"

set sink1 [new Agent/LossMonitor]

$ns attach-agent $n(4) $sink1

$ns at 0.0 "$n(4) label DESTINATION"

$ns connect $udp1 $sink1

set cbr1 [new Application/Traffic/CBR]

$cbr1 set packetSize_ 512

$cbr1 set rate_ 600kb

$cbr1 set interval_ 0.05

$cbr1 set random_ 1

$cbr1 set maxpkts_ 10000

$cbr1 attach-agent $udp1

set udp2 [new Agent/UDP]

$ns attach-agent $n(25) $udp2

set sink2 [new Agent/LossMonitor]

$ns attach-agent $n(16) $sink2

$ns connect $udp2 $sink2

set cbr2 [new Application/Traffic/CBR]

$cbr2 set packetSize_ 512

$cbr2 set rate_ 600kb

$cbr2 set interval_ 0.05

$cbr2 set random_ 1

$cbr2 set maxpkts_ 10000
$cbr2 attach-agent $udp2

set udp3 [new Agent/UDP]

$ns attach-agent $n(3) $udp3

$ns at 0.0 "$n(3) label SOURCE"

set sink3 [new Agent/LossMonitor]

$ns attach-agent $n(6) $sink3

$ns connect $udp3 $sink3

set cbr3 [new Application/Traffic/CBR]

$cbr3 set packetSize_ 1000

$cbr3 set rate_ 600kb

$cbr3 set interval_ 0.05

$cbr3 set random_ 1

$cbr3 set maxpkts_ 10000

$cbr3 attach-agent $udp3

Set-up traffic flow via malicious nodes

proc ATTACKER_node { $ATTACKER_app ack* RREP* RREQ* data* $CPThresh_

$CSThresh_ $RXThresh_ $ini_Thresh} {

set $ack $RREP | $RREQ

if { $ack > $data } {

set Thresh_ $CPThresh_ | $CSThresh_| $RXThresh_

set $Thresh > $ini_Thresh || $Thresh < $ini_Thresh

$transmit $ack($n($i))

}

}

Stop Time

We define stop time when the simulation ends and command mobile nodes to reset.

#

 # Tell nodes when the simulation ends

#

for {set i 0} {$i < $val(nn) } {incr i} {

$ns_ at 150.0 "$node_($i) reset";

}

$ns_ at 150.0001 "stop"

```
$ns_ at 150.0002 "puts \"NS EXITING...\" ; $ns_ halt"

proc stop {} {

global ns_ tracefd

close $tracefd

}
```

APPENDIX C

MTS Simulation on NS-2

Appendix C present the simulation codes for Modified Trust Scheme (MTS).

Each node is set to monitor its neighbour activities

```
/* log message */

void

AODV::writeMsg(Packet *p) {

struct hdr_ip *ih = HDR_IP(p);

FILE *fp;

nsaddr_t monitoringNode;

nsaddr_t neighbor;    // the previous hop

/* log Hello packets */

monitoringNode = index;

neighbor = ih->saddr();

if ((fp = fopen(TRACE_FILE, "a+")) != NULL)

  {

// my neighbor SENDs out a message

fprintf(fp, "s %.9f %d %d MESSAGE\n",

CURRENT_TIME,

monitoringNode,

neighbor);

fclose(fp);

}
```

```
   return;
   }
AODV::logDrop(Packet *p)
  {
struct hdr_cmn *ch = HDR_CMN(p);
struct hdr_ip *ih = HDR_IP(p);
struct hdr_mac802_11 *mh = HDR_MAC802_11(p);
struct hdr_aodv *ah;
struct hdr_aodv_request *rq;
struct hdr_aodv_reply *rp;
FILE *fp;
char op = 'D';
nsaddr_t neighbor;
char pktType[10];
char neigh_path[100];
char nodeid[10];
sprintf(nodeid,"%d",ch->prev_hop_);
strcpy(neigh_path, CURRENT_DIR );
strcat(neigh_path, nodeid);

                if ( (fp = fopen(neigh_path, "a+")) == NULL)
{
        fprintf(stdout, "logDrop: open neighbor profile %s failed\n", neigh_path);
```

```
        return;
        }
//      if ( (DATA_PACKET(ch->ptype())) && (ih->saddr() != index))
        if (((ch->ptype()==PT_TCP)||(ch->ptype()==PT_CBR))&&(ih->saddr()!=index))
        {
// Data packet
fprintf(fp, "%c %.9f %d %d %s %d\n",
op,
Scheduler::instance().clock(),
ch->prev_hop_,
index,
packet_info.name(ch->ptype()),
ch->size());
}
fclose(fp);
// drop a AODV packet
if (ch->ptype() == PT_AODV)
        {
ah = HDR_AODV(p);
switch(ah->ah_type){
case AODVTYPE_RREQ:
rq = HDR_AODV_REQUEST(p);
neighbor = ih->saddr();
```

```
strcpy(pktType, "RREQ");
break;
case AODVTYPE_RREP:
rp = HDR_AODV_REPLY(p);
neighbor = rp->rp_src;
strcpy(pktType, "RREP");
break;
case AODVTYPE_RERR:
neighbor = ch->prev_hop_;
strcpy(pktType, "ERROR");
break;
if ( neighbor != index ) {
char neigh_path[100];
char nodeid[10];
sprintf(nodeid,"%d",neighbor);
strcpy(neigh_path, CURRENT_DIR );
strcat(neigh_path, nodeid);
if ( (fp = fopen(neigh_path, "a+")) != NULL)
        {
fprintf(Scheduler::instance().clock(),neighbor, index, pktType);
        }
else{
fprintf( neigh_path);
```

```
return;
        }
fclose(fp);
        }
}
```

APPENDIX D

Membership Group

Fuzzy logic was used to group the nodes based on their performance

```
AODV::getProfileNode(double records[][FLOWNUM][MSNUM], double
stats[][PKTNUM][FLOWNUM][MSNUM], int totalNodes){
/* for each node -
*       s -0, r-1, f-2, d-3,
        *  AODV_RREQ-0, AODV_RREP -1, AODV_RERR -2, AODV_MSG -3 , data
pkt -4
        */
FILE *fp;
char line[MAXLINE];
char op;                                /* r, s, f, D*/
int nodeid;                             // monitoring node
int nbid;                               // neighbor
double mean;                            //mean
double stdDev;                          //standard deviation
char pktType[10];                       /* RREQ, RREP, ERROR, MSG, tcp,*/
char* charEof;
if ( (fp = fopen(PROFILE_FILE, "r")) != NULL)
{
        //skip first 8 lines
```

```
for(int i = 0; i < 8; i++){
fgets(line, MAXLINE, fp);
//printf("skip line: %s", line);
}
while(1)
{
charEof = fgets(line, MAXLINE, fp);
if ( charEof != NULL )
        {
sscanf(&op, &nodeid, &nbid, pktType, &mean, &stdDev);
if (nodeid == index)
{
/****************************** COOPORATE ************************/
if (index >= 0 && <= 0.2)
{
if (strcmp(pktType, "RREQ") == 0)
{
stats[nbid][0][0][0] = mean;
stats[nbid][0][0][1] = stdDev;
        }


else if (strcmp(pktType, "RREP") == 0)
```

```
{
stats[nbid][1][0][0] = mean;
stats[nbid][1][0][1] = stdDev;
}
else if (strcmp(pktType, "ERROR") == 0)
{
stats[nbid][2][0][0] = mean;
stats[nbid][2][0][1] = stdDev;
}
        else if (strcmp(pktType, "ATTACK") == 0)
{
stats[nbid][3][0][0] = mean;
stats[nbid][3][0][1] = stdDev;
}
// data packet size
else if( (strcmp(pktType, "DATA") == 0) )
{
records[nbid][0][0] = mean;
records[nbid][0][1] = stdDev;
}
// aodv
else if ( (strcmp(pktType, "AODV") == 0))
{
```

```
stats[nbid][5][0][0] = mean;
stats[nbid][5][0][1] = stdDev;
}
// data packet count
else if ( strcmp(pktType, "DATANUM") == 0)
{
stats[nbid][4][0][0] = mean;
stats[nbid][4][0][1] = stdDev;
}
else {
                    fprintf(stdout, "AODV::getProfileStats: invalid
packet \n");
        exit(1);
}
}
/***** MEDIUM ********************************************/

        else if (index >= 0.3 && <= 0.5)
        {
        if (strcmp(pktType, "RREQ") == 0)
{
stats[nbid][0][0][0] = mean;
stats[nbid][0][0][1] = stdDev;
```

```
}
else if (strcmp(pktType, "RREP") == 0)
{
stats[nbid][1][0][0] = mean;
stats[nbid][1][0][1] = stdDev;
}
else if (strcmp(pktType, "ERROR") == 0)
{
stats[nbid][2][0][0] = mean;
stats[nbid][2][0][1] = stdDev;
}
else if (strcmp(pktType, "ATTACK") == 0) {
stats[nbid][3][0][0] = mean;
stats[nbid][3][0][1] = stdDev;
}
// data packet size
else if( (strcmp(pktType, "DATA") == 0) )
{
records[nbid][0][0] = mean;
records[nbid][0][1] = stdDev;
}
// aodv
else if ( (strcmp(pktType, "AODV") == 0))
```

```
{
stats[nbid][5][0][0] = mean;
stats[nbid][5][0][1] = stdDev;
}
// data packet count
else if ( strcmp(pktType, "DATANUM") == 0)
{
stats[nbid][4][0][0] = mean;
stats[nbid][4][0][1] = stdDev;
}
        else {
                                                fprintf(stdout, "AODV::getProfileStats:
invalid packet \n");
        exit(1);
        }
        }

/******** *SUSPICIOUS ***************************************/
else if (index >= 0.4 && <= 0.7)
{
        if (strcmp(pktType, "RREQ") == 0)
        {
stats[nbid][0][0][0] = mean;
```

```
stats[nbid][0][0][1] = stdDev;
        }
else if (strcmp(pktType, "RREP") == 0){
        stats[nbid][1][0][0] = mean;

        stats[nbid][1][0][1] = stdDev;
}
else if (strcmp(pktType, "ERROR") == 0)
{
stats[nbid][2][0][0] = mean;
stats[nbid][2][0][1] = stdDev;
}
else if (strcmp(pktType, "ATTACK") == 0)
{
stats[nbid][3][0][0] = mean;
stats[nbid][3][0][1] = stdDev;
}
// data packet size
else if( (strcmp(pktType, "DATA") == 0) )
{
records[nbid][0][0] = mean;
records[nbid][0][1] = stdDev;
}
```

```
// aodv
else if ( (strcmp(pktType, "AODV") == 0))
        {

stats[nbid][5][0][0] = mean;
stats[nbid][5][0][1] = stdDev;
}
// data packet count
else if ( strcmp(pktType, "DATANUM") == 0)
{
stats[nbid][4][0][0] = mean;
stats[nbid][4][0][1] = stdDev;
}
else {
                                        fprintf(stdout,
   "AODV::getProfileStats: invalid packet \n");
        exit(1);
        }
}
/************************** MALICIOUS ************************/

else if (index >= 0.8 && <= 1)
{
```

fprintf(stdout, "AODV::getProfileStats:

invalid packet \n");

exit(1);

}

fclose(fp); `