SECURITY ANALYSIS OF AODV, ARAN AND IMPROVED ARAN MOBILE ADHOC NETWORK ROUTING PROTOCOLS

Dissertation submitted to the Central University of Punjab

For the Award of

Master of Technology

In

Computer Science and Technology

By

Ruby Goel

Supervisor

Er. Meenakshi

Centre for Computer Science & Technology
School of Engineering & Technology
Central University of Punjab, Bathinda

September, 2014

DECLARATION

I declare that the dissertation entitled "**SECURITY ANALYSIS OF AODV, ARAN AND IMPROVED ARAN MOBILE ADHOC NETWORK ROUTING PROTOCOLS**" has been prepared by me under the guidance of Er. Meenakshi, Assistant Professor, Centre for Computer Science & Technology, School of Engineering & Technology, Central University of Punjab. No part of this dissertation has formed the basis for the award of any degree or fellowship previously.

(Ruby Goel)
Centre for Computer Science & Technology
School of Engineering & Technology
Central University of Punjab
Bathinda- 151001.

Date: September, 2014

CERTIFICATE

I certify that RUBY GOEL has prepared her dissertation entitled "**SECURITY ANALYSIS OF AODV, ARAN AND IMPROVED ARAN MOBILE ADHOC NETWORK ROUTING PROTOCOLS***"*, for the award of M.Tech degree of the Central University of Punjab, under my guidance. She has carried out this work at the Centre for Computer Science & Technology, School of Engineering & Technology, Central University of Punjab.

(Er. Meenakshi)
Supervisor
Centre for Computer Science & Technology,
School of Engineering & Technology,
Central University of Punjab,
Bathinda- 151001

Date: September, 2014

ABSTRACT OF DISSERTATION

Security Analysis of AODV, ARAN and Improved ARAN Mobile Adhoc Network Routing Protocols

Name of student : Ruby Goel

Registration Number : CUPB/M.Tech/SET/CST/2012-13/04

Degree for which submitted : Master of Computer Science & Technology

Name of supervisor : Er. Meenakshi

Centre : Centre for Computer Science & Technology

School of Studies : School of Engineering & Technology

Key words : AODV, ARAN, Blackhole, IP-Spoofing, DDOS, GloMoSim-2.03.

Wireless networks use wireless connections to provide a communication environment between the communicating devices using their radio transmission range. Wireless network doesn't require any pre-established infrastructure. Adhoc network is an infrastructure-less network which allow nodes to communicate beyond their direct wireless transmission range by introducing cooperation in mobile nodes. Wireless communication is guided by routing protocols. Wireless routing protocols come under different categories like- On-demand, Table-driven and secure routing protocols. Wireless networks face many challenges due to limited resources, dynamic topologies and lack of physical security, due to which variety of attacks have been identified that target both the on-demand and table-driven routing protocols. By attacking the routing protocols attacker can absorb network traffic, or can inject the false traffic in the network. Due to this attacks like- Blackhole, IP-Spoofing, False message fabrication, Denial of service, etc. are possible in adhoc networks. Many secure routing protocols have been developed that can deal with these attacks. One of them is Authenticated Routing for Adhoc Network (ARAN) which introduces authentication, message integrity and non-repudiation as part of its security policy and provides security against various network attacks like- Message modification, false message fabrication and impersonation attack. But ARAN is vulnerable to Distributed Denial of Service (DDOS) attack because legitimate nodes can send large amount of unnecessary packets in the network and can create congestion and thus prevent other legitimate nodes to access the network.

In this research work security aspects of ARAN have been analyzed with respect to Adhoc On-Demand Distance Vector (AODV) routing protocol under Blackhole and IP-Spoofing attack. Further a technique has been proposed for ARAN to resist DDOS attack by limiting the number of packets per unit of time each node can send in the network and this enhanced ARAN in this research work is called as improved ARAN (i-ARAN). By implementing the proposed technique i-ARAN is able to prevent DDOS attack. Various performance metrics like- Packet Delivery ratio, Average Path Length, Average end-to-end delay and Throughput;

are calculated under Glomosim-2.03 simulator. Results show that ARAN is safe against Blackhole and IP-Spoofing attack, but AODV is highly vulnerable to both the attacks. Also results of i-ARAN under DDOS attack show that the attack can be prevented by the proposed technique as it provides constant Packet delivery ratio from all the source nodes and throughput of i-ARAN is also approximately constant. By using i-ARAN there is no congestion in the network so average end-to-end delay of i-ARAN is less than the ARAN.

(Ruby Goel) (Supervisor- Er. Meenakshi)

ACKNOWLEDGEMENTS

I would like to express my gratitude to all those who gave me the possibility to complete this dissertation report. I am extremely grateful to my guide, Er. Meenakshi, for having spent her valuable time reviewing the draft of this dissertation report and excellent feedback and suggestions that helped a lot. She is always being there with his encouraging words and excellent guidance through the course of this dissertation work. Without her keen professional insight and critical suggestions, this dissertation work would not have been possible.

I would also like to extend my sincere appreciation to Prof. Dr. A.K. Jain COC of Centre for Computer Science & Technology, the staff of Centre for Computer Science & Technology for providing a great academic environment.

This acknowledgement would be incomplete if I don't mention emotional support, love, blessings and inspiration provided by my family and friends. Words are insufficient to express my gratitude to my family and friends for their unfailing encouragement.

Finally I bow to the almighty, who gave me strength to carry out this work with sincerity and dedication.

(Ruby Goel)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

Sr. No.	Full Form	Abbreviation
1.	Adhoc On-Demand Distance Vector	AODV
2.	Authenticated Routing for Adhoc Network	ARAN
3.	Bootstrap Router Protocol	BSR
4.	Clusterhead Gateway Switch Routing Protocol	CGSR
5.	Destination Sequenced Distance Vector Protocol	DSDV
6.	Dynamic Source Routing	DSR
7.	Error	ERR
8.	Flow-Oriented Routing Protocol	FORP
9.	Global Mobile Information System Simulator	GloMoSim
10.	Hierarchical State Routing Protocol	HSR
11.	Internet Protocol	IP
12.	Location Aided Routing	LAR
13.	Media Access Control	MAC
14.	Mobile Adhoc Networks	MANETs
15.	Network Simulator	NS-2
16.	On-Demand Multicast Routing Protocol	ODMRP
17.	Optimized Link State Routing	OLSR
18.	PARallel Simulation Environment for Complex systems	PARSEC
19.	Parallel Computing Laboratory	PCL
20.	Personal Digital Assistants	PDAs
21.	RREQ_Accept_Limit	RAL
22.	Route Discovery Packet	RDP
23.	Reply	REP
24.	Route Error	RERR
25.	Secure Efficient Ad hoc Distance vector routing protocol	SEAD
26.	Server Routing Protocol	SRP
27.	Scalable Source Routing	SSR
28.	Source Tree Adaptive Routing	STAR
29.	Temporally Ordered Routing Algorithm	TORA

Sr. No.	Full Form	Abbreviation
30.	University of California Los Angeles	UCLA
31.	Vehicular Adhoc Networks	VANETs
32.	Wireless Routing Protocol	WRP
33.	Wireless Sensor Networks	WSNs

CHAPTER 1

INTRODUCTION

1.1 Networking: An Overview

As discussed by (Goyal & Gaba, 2013), networking is an emerging technology that allows users to communicate with each other to access information and services electronically. Network can be wired or wireless. Wireless networking offer many advantages than wired; as wired networking requires pre-established infrastructure whereas wireless networks doesn't have such a requirement. Also wired network consists of cables which are not suitable for long distance communication whereas wireless network offers distant communication. Due to these reasons much advancement are taking place in wireless networking. Wireless networks are of two types: Infrastructured and Infrastructure-less. In Infrastructured wireless networks, at the time of communication nodes can move, the base stations are fixed and nodes can communicate within the range of base stations. In Infrastructure-less wireless network or Adhoc network, at the time of communication nodes can move, no fixed base stations are there in the network and the nodes in the network act as routers. Adhoc networks are further classified in different categories as shown in Figure 1.1. Mobile Adhoc Networks (MANETs) consists of mobile nodes in which basic networking functions like- routing and packet forwarding are done by wireless interface and communicates with other nodes by multihop routing. Network of vehicles forms Vehicular Adhoc Network (VANET). WSN is the Wireless Sensor Networks that are used to collect real-time data from the collection of embedded sensor devices.

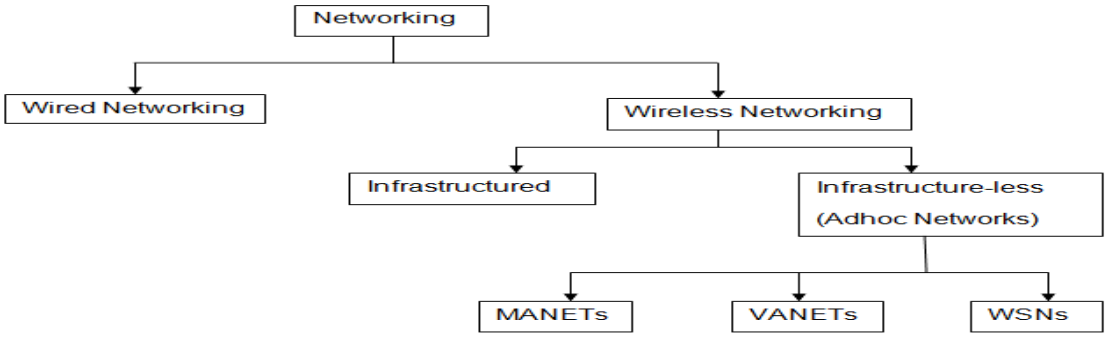

Figure1.1: Networking types

This research work focuses on infrastructure-less wireless network which are also known as Ad-hoc networks. (Goyal & Gaba, 2013) states that ad hoc literally means- for this, i.e. for this purpose only and thus temporary. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. As shown in Figure 1.2, an adhoc network consists of various nodes which communicate with each other by their transmission ranges.

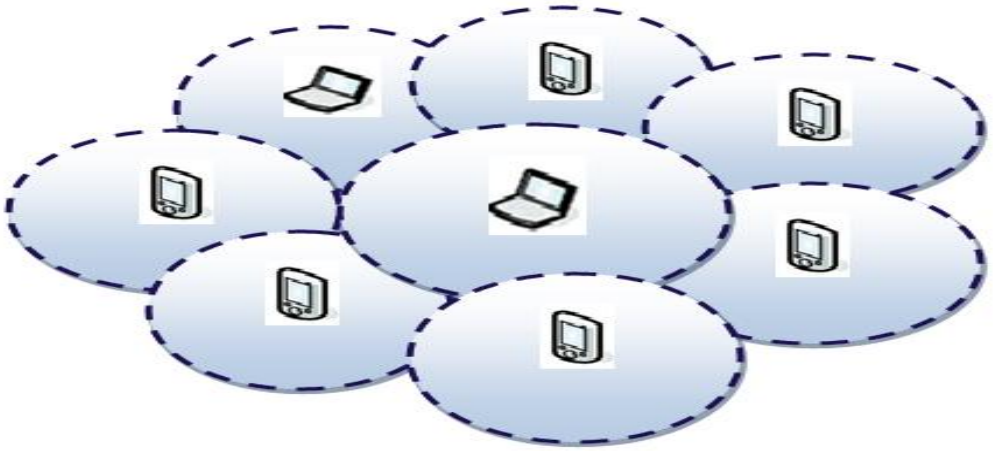

Figure 1.2: An Adhoc Network

This research work deals with Mobile Adhoc Networks (MANETs). As discussed by (Kumar, Kulkarni, & Gupta, 2010) MANETs have several advantages over traditional wireless networks including ease of deployment, speed of deployment, and decreased dependence on a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. Each wireless node can function as a sender, a receiver or a router. When the node is a sender, it can send messages to any specified destination node through some route. As a receiver, it can receive messages from other nodes. When the node functions as a router, it can send the packet to the next node in the route. When necessary, each node can buffer packets awaiting transmission. Whenever a packet has to be transmitted to a destination, a routing protocol is needed. Routing protocols define rules to deliver the packet to the correct destination by finding route for the packet.

1.2 Applications of MANETs

According to (Mahmoud, Sameh, & El-Kassas, 2005) and (Goyal & Gaba, 2013), wireless ad-hoc networks can be deployed in areas where a wired network

infrastructure may not be possible due to reasons of cost or convenience. MANETs can be deployed rapidly to support emergency requirements, short-term needs, and coverage in undeveloped areas. Ad hoc networks have self-organizing capability. As a result, some well-known ad hoc network applications are:

- **Tactical Network**: MANET can be used for emergency services, battlefields and military communication because they are easy to establish without any pre-installed infrastructure. The Ad-hoc networks are very important area where people wish to have quick and secure information.
- **Crisis-management Applications**: Natural disasters disorder the entire communications infrastructure, so it is essential to restore communications quickly. By using ad hoc networks, a communication channel could be set up in few hours.
- **Sensor Networks**: Each node collects sample data, and then forward data to centralized host for processing. Sensor network can be used inside the home (smart sensors embedded in electronics devices such as fire alarm, security alarm, etc.), body area networks, data tracking of environmental conditions etc.
- **Home and Enterprises**: Wireless networking is used in home or office, conferences, meeting rooms, and personal area networks.
- **Commercial and civilian environment**: It supports Vehicular services like in road maps, accident guidance, weather conditions and inter-vehicle networks.

1.3 Mobile Ad Hoc Networks Challenges

As discussed in (Gowda & Hiremath, 2013) and (Goyal & Gaba, 2013), MANETs have several challenges. They are as follows:

- **Dynamic topologies**: Nodes are mobile and can move arbitrarily in MANETs. The network topology may change at unpredictable times. When nodes move out of the range, network has to realign itself and has to update dynamic link information. Breakage of link has to be controlled by some route maintenance procedure.
- **Absence of security infrastructures on wireless links**- Mobile wireless network are more vulnerable to physical security threats as compared to wired cable network because wireless medium is accessible to both genuine network

users and malicious or selfish attackers. Due to this open access to the wireless links various attacks like- Blackhole, IP-spoofing, Traffic analysis and denial-of-service are possible.

- **Limited Resources**: Each Mobile node in the network has limited power, storage capacity and processing capability. Limited number of applications and services are supported by mobile node due to limited energy and processing power.
- **Bandwidth-constrained links**: Wireless links have significantly lower capacity. The limited capacity of frequency band offer low data rates and it has become a challenge for mobile ad hoc networks.
- **Energy-constrained operation**: Some or all of the nodes in a MANET rely on batteries for their energy. So for network's better performance some scheme is needed to conserve energy for these nodes.

1.4 Routing Protocols

As discussed by (Mahmoud, Sameh, & El-Kassas, 2005), routing protocols come under different categories like:

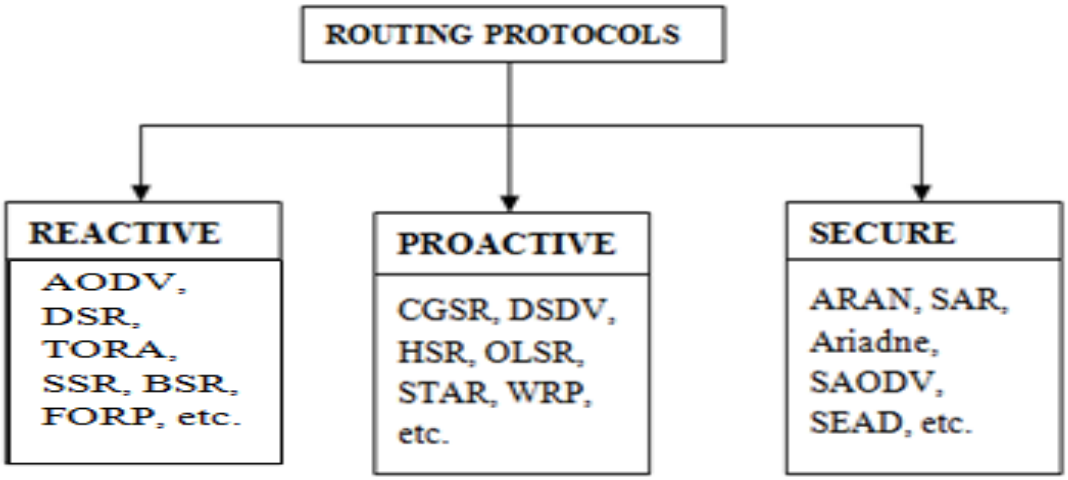

Figure 1.3: Types of Routing Protocols

- **Reactive or on-demand**- here routes are only generated when they are needed by any source node to send the packets to another node.
- **Proactive or table driven**- here routes to all destinations are kept in tables which are regularly updated with changes in topology.

Reactive protocols found to be more efficient than proactive protocols because they use lower bandwidth for maintaining routing tables, and they are more energy-efficient and have effective route maintenance.

As discussed in Section 1.3 MANETs are subject to various security challenges due to which Reactive and Proactive protocols are subject to various attacks like- IP Spoofing, Blackhole, Eavesdropping, Traffic Analysis, and Denial of service, etc.

- **Secure protocols-** To provide security against these types of attacks secure protocols have been developed.

1.5 Efficient Routing Requirements

In the field of mobile ad hoc networks routing, there are lot of problems to be tackled such as Quality of service, power awareness, routing optimization and security issues. A routing protocol has to follow the following conditions for providing efficient routing:

- Routing Protocol should not be vulnerable to the attacks.
- Routing Protocol must be aware of network resources which are limited.
- Quality of Service should be considered in routing protocol.

In this research work security issues related to routing protocols in MANETs are focused. Security in MANETs is an essential component for basic network functions like- packet forwarding and routing; otherwise network operation can be easily degraded if countermeasures are not embedded into these basic network functions. According to (Sanzgiri, LaFlamme, Dahill, Levine, Shields, & Belding-Royer, 2005), a widely used protocol AODV is prone to many network attacks (like Blackhole attack, IP-spoofing, Message modification, Denial-of-Service attack, etc.) and to prevent these attacks various secure protocols are developed (like ARAN, SAODV, Ariadne, etc.). ARAN protocol has been found to be very secure that detects and protects various malicious actions carried out by third parties and peers in the ad hoc environment, but is vulnerable to DOS attack.

1.6 Problem Statement

AODV performs very basic security functions but does not provide protection against network attacks like message modification, impersonation, and

false message fabrication attacks. The study shows that AODV is vulnerable to Blackhole and IP-Spoofing attack because of hop count and sequence number parameters, which can be easily modified in AODV. But ARAN is resistant to these attacks because these two parameters are not used in ARAN.

But ARAN is vulnerable to DDOS attack as the legitimate node can send large number of route request or data packets to the victim node. So it is required to find out a method by which ARAN can become resistant to DDOS attack.

1.7 Objectives

The main objective of this research work is to analyze security aspects of AODV and ARAN against Blackhole and IP-Spoofing attacks and to find out a technique to make the ARAN protocol resistant to DDOS attack. This objective can be divided into the following sub-objectives:

1. To set the simulation environment for AODV and ARAN to analyze them against Blackhole and IP-Spoofing attacks and then measure their effects on both the protocols.
2. To set the simulation environment to perform DDOS attack on ARAN protocol.
3. To implement the new technique on ARAN protocol to prevent DDOS attack i.e. by limiting the number of packets a node can send per unit of time in the network.
4. To perform DDOS attack on improved ARAN.
5. To compare the results of both ARAN and improved ARAN protocol.

1.8 Organization of the Dissertation

Organization of the dissertation work is organized as follows: Chapter 2 gives the literature review. In Chapter 3 discusses AODV and ARAN routing protocol and attacks (Blackhole, IP-Spoofing and DDOS). Chapter 4 then discusses the proposed work, the simulator used and the methodology of evaluation presenting different simulation parameters and various metrics that are measured in the simulations. In Chapter 5, simulation results are discussed. In Chapter 6, conclusion about the results and the future work is discussed.

CHAPTER 2

REVIEW OF LITERATURE

Von Mulert, Welchn, & Seah, 2006 stated that among the many routing protocols that have been developed to allow self-configuring and self-maintaining routing in MANETs, the Ad-hoc On-demand Distance Vector (AODV) protocol is one of the most popular. This protocol was developed under the assumption that all nodes in the network are friendly and cooperative. Consequently, there are many attack vectors in AODV which allow attackers to disrupt its route discovery and packet forwarding processes. In AODV control messages can be easily manipulated and AODV has no mechanism for dealing with malicious manipulation of these messages.

Mehla, Gupta, & Nagrath, 2010 have stated that there are many routing protocols that are in used in MANET but many of these routing protocols are not secure. One of the most common used routing protocol is AODV that handles the routing functions well but does not performs basic security functions. AODV does not satisfy the requirements of certain discovery, isolation or Byzantine robustness. AODV allows for many different types of attacks like-message modification, impersonation, and message fabrication. With these attacks, attacker can absorb network traffic, can inject false information in the path between source and destination and thus can control network traffic. Therefore secure routing protocols are developed that can resist these attacks. This paper firstly presents various attacks on AODV and then discusses a secure protocol Authenticated Routing for Adhoc Networks (ARAN) that can prevent many of the network attacks. Finally it stated that active attacks can be avoided by the use of stringer authentication methods as used by ARAN protocol.

Ning, & Sun, 2005 have done the security analysis of AODV protocol and concluded that it is not surprising to find the security attacks against the AODV protocol, since this protocol was not designed with security as a goal. It also stated that achieving security is not as simple as combining generic security mechanisms with a target application such as the AODV protocol. Protocol and application designers must pay special attention to the security requirements, the risks and

threats, as well as the semantics of the specific protocols and applications to have truly secure and dependable solutions. Providing security in MANET is a quite challenging task, particularly due to the fact that mobile nodes in MANET are subject to capture and compromise. It also suggested that additional mechanism such as intrusion detection should be used along with prevention based security mechanisms such as authentication and encryption to accommodate possible failures of the prevention based mechanisms.

Sanzgiri, et al., 2005 have stated that initial work in ad hoc routing field has considered only the problem of providing efficient paths in dynamic networks, but doesn't considered the security aspects. There are many exploits against ad hoc routing protocols like modification, impersonation and fabrication. They introduced ARAN or authenticated routing protocol that detects and protects against malicious actions by third party and peers in ad hoc network. ARAN provides secure routing. ARAN uses cryptographic certificates to prevent most of the attacks presented above. Only authorized nodes participate at each hop between source and destination and the routing messages are authenticated before passing to the other node in the network. In this paper it has been concluded that ARAN is as effective as AODV in discovering and maintaining routes but the cost of ARAN is larger because of the cryptographic computations done during the routing of packets in the network.

Mahmoud, Sameh, & El-Kassas, 2005 have stated that security in MANET is essential because network operation will not perform well if security countermeasures are not embedded into basic network routing functions. Paper stated that there are basically two types of security threats to a routing protocol, external and internal attackers. An external attacker injects false information into the network and degrades the routing functions. The internal attacker is a compromised node of the network that is in control of some external attacker. Different attacks that are possible in a network are eavesdropping, modification, replication, deletion, etc. To provide security in an ad hoc network numbers of requirements have to be fulfilled. These requirements are: availability, confidentiality, integrity, authentication and non-repudiation. As a result of which many security protocols has been proposed like SEAD, SAODV, ARAN, SRP, ARIADNE, etc. On comparing these protocols it has been concluded that ARAN

satisfies almost all the security requirements except DOS (denial of service) attack and selfish node behavior which may not allow packets to reach to the destination. So here author gave a new reputation-based scheme to be integrated with one of the secure routing MANET protocol, ARAN, to make it detect and defend against selfish nodes and their misbehavior.

Ullah, & Rehman, 2010 have done the analyses of blackhole attack on various MANET routing protocols (AODV and OLSR). In black hole attack, a malicious node provides a fake route reply message to advertise itself for having the shortest path to the destination node. It provides minimum hop count and the maximum sequence number to ensure the freshness of the route. By evaluating various performance metrics, it has been concluded that that AODV is more vulnerable to Black Hole attack than OLSR.

Benetti, Merro, & Vigano, 2010 have stated that ad hoc routing protocols are exposed to a number of different attacks. A number of efficient tools have been implemented for security protocol falsification (i.e., detecting attacks) and/or verification (i.e., proving the protocols correct). They discovered three attacks- a route disruption, a route diversion, and a creation of incorrect routing state. ARAN does not have any mechanism that deals with wormhole attack, Denial of service attack. It has also been concluded that a node being selfish can drop the packets for no reason so ARAN is also said to be vulnerable to Blackhole attack.

Dokurer, 2006 has worked upon Blackhole attack in AODV protocol. It has explained that AODV protocol code can be modified to launch blackhole attack as malicious node tries to deceive nodes sending a modified RREP packet. Highest sequence number of AODV protocol is 4294967295, 32 bit unsigned integer value. Values of RREP packet that malicious node will send are: The sequence number is set to 4294967295 and hop count is set to 1. The false RREP message is then sent to the source node. After the simulations performed on NS-2 simulator it concluded that the percentage of data loss of the Black Hole AODV is increased more than the normal AODV network simulations in all scenarios. Further it stated that all other routing protocols are expected to give different results of packet loss.

Vigna, Gwalani, Srinivasan, Belding-Royer, & Kemmerer, 2004 have described the IP Spoofing attack. In this attack, attacker is using the identity of a

distant computer. Then attacker uses the identity of some other node and sends messages to a victim computer indicating that the message has come from a trusted system. To the victim system that it appears that the packets are coming from the trusted system. It has been stated that AODV is vulnerable to the spoofing attack whereas ARAN is secure against it.

Sanzgiri, et al., 2005 and Garg, & Beniwal, 2012 have stated that ARAN uses a central certification authority server for node authentication and neighbor node authentication in route discovery. Though ARAN prevents from many network attacks like modification, impersonation and offers non-repudiation for false message fabrication but Denial-of-service attacks are possible with selfish nodes. Participating selfish nodes can broadcast unnecessary route requests or data packets across the network. Because packets are broadcasted and forwarded across the network, an attacker can cause widespread congestion and power-loss to all nodes in the network. Also it is hard to differentiate between legitimate and malicious RREQs.

Sinha, Singh, Pandey, & Sahu, 2013 and Reddy, Kundra, Babu, & Kumar, 2012 have stated that the networks are particularly vulnerable to denial of service (DOS) attacks launched through compromised nodes or intruders. The DOS attack is commonly launched by sending enormous amount of packets in the network. In this attack a malicious attack sends bulk route request (RREQ) or data packets so that all links get overloaded and all bandwidth is consumed and the valid communication cannot be kept. Legitimate users are not able to use network resources such as a website, web service, or computer system. Another form of DOS attack is Distributed Denial of Service (DDoS) attack, which is launched indirectly through many compromised nodes of the network to target a given system which is known as primary victim. The compromised systems used to launch the attack are called as the secondary victims. DDOS is more dangerous because here secondary victims actually perform the attack and it is difficult to track down the real attacker.

Specht, & Lee, 2004 have proposed various taxonomies of DDoS attack, various tools used to cause the attack, to define the scope of the DDoS problem. This paper also discussed various countermeasures to facilitate more

comprehensive solutions. But there are many DDoS attack tools that are available to attackers and are easy to implement and can have disastrous effects. The paper concluded that though there are methods to prevent the attack from succeeding, but new techniques of attack are still being developed. So it is required to make some more comprehensive solutions and countermeasures to DDoS attacks.

Kataria, Dhekne, &Sanyal, 2006 proposed a method by which malicious flooding of route requests can be effectively controlled to prevent DOS attack. They set a parameter RREQ_ACCEPT_LIMIT (RAL) which is equal to the number of RREQs that a node can accept and process per unit time from each of its neighbors. If the number of RREQs sent by a neighbor per unit time exceeds this value, the neighbor is assumed to be acting malicious and is blocked. So it can be concluded from this paper that if some limit is set on the number of packets a node can send to the other node per unit of time, DOS attack can be prevented in ARAN.

CHAPTER 3

ROUTING PROTOCOLS & ATTACKS

MANET consists of mobile nodes that are connected in an arbitrary manner and as the node moves from one place to another their connections keeps on changing dynamically. Nodes of MANET can behave as sender, receiver and router. As a router a node can take part in route discovery and route maintenance to establish a reliable route for other nodes of the network. In an Ad-hoc network, a station can transfer data to another one by using intermediate nodes. In (Mahmoud, Sameh, & El-Kassas, 2005) it has been stated that Ad hoc routing protocols are generally classified as Proactive or Reactive. But these protocols lack security aspects, so secure protocols are developed which are known as security protocols.

3.1 Protocols chosen for the Research work

AODV and ARAN protocols are chosen for analysis because literature review shows that AODV is a widely used protocol in adhoc networks but is vulnerable to number of network attacks; and ARAN is the most secure protocol which can prevent most of the network attacks. Both the protocols are discussed below:

3.1.1 AODV (Adhoc On-demand Distance Vector) Routing Protocol

According to (Zhou, 2007) AODV can be called as a pure on-demand routing protocol i.e. routes are not built until certain nodes intend to communicate or transmit data to other node. AODV consists of two important stages: Route Discovery procedure and Route Maintenance procedure.

a) In Route Discovery procedure- when source node intent to communicate with other node then it broadcasts Route Request (RREQ) packets to all its neighboring nodes. The RREQ packet consists of following parameters:

<s_addr, id, s_seq, d_addr, d_seq, hop_count>

(Zhou, 2007) stated that s_addr and d_addr denotes the IP address of source node and the destination node, id is the broadcast ID, s_seq represents the source node's sequence number and d_seq is the destination node's sequence number, hop_count indicates the number of nodes the message have passed. On receiving the RREQ packet, the intermediate nodes rebroadcast this RREQ to its neighbors and increase hop_count by 1. Intermediate nodes also set up a Reverse Path Pointer for the node from which they receive the RREQ. When RREQ reaches the destination node, the destination node would unicasts a Route Reply packet (RREP) to the source node along the reverse path as set by the intermediate nodes. The RREP contains the following parameters:

<s_addr, d_addr, d_seq, hop_count, lifetime>

(Zhou, 2007) stated that s_addr, d_addr are directly copied from RREQ, also hop_count is reset to zero and counted again. Every intermediate node will increase the hop_count by 1 and send it according to Reverse Path Pointer. As soon as the source node receives the RREP, a path is set and data packets are then sent over this route. Also if intermediate nodes have the route to the destination node, they can also send a RREP to the source node. As shown in Figure 3.1, when S (source node) wants to send data to D (destination node) it broadcasts the RREQ packet to all neighboring nodes which will further broadcasts the packet until the destination is reached. After all the RREQ packets reach the destination node D, it unicasts the RREP packet upon the path with shortest hop count. So the RREP packet is sent through node I3 and being the shortest route S-I3-D path is selected.

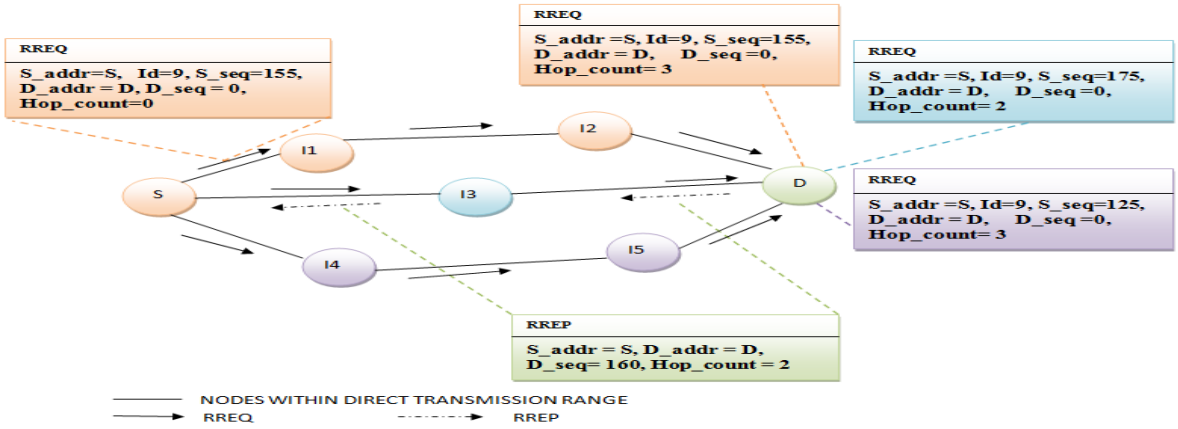

Figure 3.1: Route discovery process in AODV

b) In Route Maintenance procedure-all nodes of the network keeps on checking the active routes available and in order to detect possible link failure nodes broadcast HELLO message to all of its neighbors periodically. If a link failure is detected all active routes through that link would not work, so a Route Error message (RERR) is send to inform the other nodes on that link. The RERR message contains the following items:

< d_addr, new d_seq, hop_count=∞ >

(Zhou, 2007) stated that new d_seq is bigger than the maximum d_seq of all the RREQ or RREP the node have received, also hop_count is set to an infinite number which means the destination node is now unreachable.

As shown in Figure 3.2 node I1 sends Route error (RERR) message to source node S for the broken link.

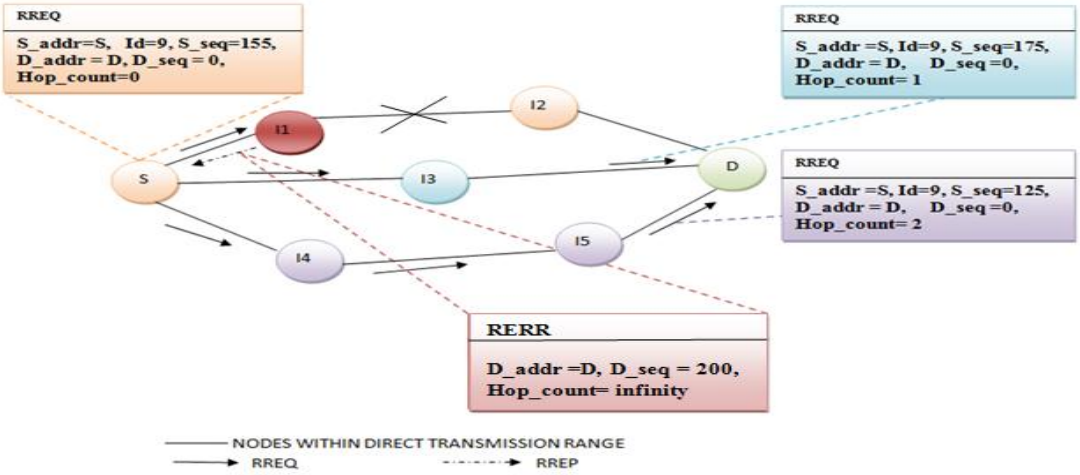

Figure 3.2: Route maintenance process in AODV

3.1.1.1 Security analysis of AODV

The study shows that all the parameters that are used in AODV (like d_seq, hop_count, s_addr and d_addr) are not protected and can be easily modified, so AODV is vulnerable to variety of attacks that can be conducted by malicious, compromised and selfish nodes. These attacks can be like- message modification, impersonation and false message fabrication attacks. Therefore, it is requires to enhance the security in AODV protocol or to develop a security protocol to prevent from the attacks done by malicious, compromised and selfish nodes.

3.1.2 ARAN(Authenticated Routing for Adhoc Networks) Routing Protocol

According to (Sanzgiri, et al., 2005) the ARAN secure routing protocol is a protocol that detects and protects against malicious actions carried out by third parties and peers in the ad hoc environment. (Sanzgiri, et al., 2005) also stated that ARAN introduces authentication, message integrity and non-repudiation as part of minimal security policy for the ad hoc environment and consists of a preliminary certification process, a mandatory end-to-end authentication stage. This protocol adopts dual authentication i.e. public key certificate and private key signature. Thus, it effectively ruled out the hidden danger of illegal nodes participating in routing. ARAN doesn't record the total number of hops in the route discovery. Each legitimate node only records the IP address of its precursor nodes and successor nodes. This ensures the security of the network topology information. ARAN protocol consist four steps: Certificate application, route discovery, route establishment, route maintenance.

a) Certification of Authorized Nodes

ARAN uses cryptographic certificates to fulfill its security policy. ARAN uses trusted certificate server 'T'(or multiple servers may be used) to certify all nodes of the network. The public key of the trusted server 'T' is provided to all valid nodes. These certificates are used by the nodes to authenticate themselves to other nodes of the network during the exchange of routing messages. Before entering the ad hoc network, each node requests for the certificate and receives exactly one certificate from T.

As discussed by (Sanzgiri, et al., 2005), a node 'A' receives a certificate from T as follows:

$$T \rightarrow A: \text{cert } A = [IPA, KA+, t, e]\ K\ T- \quad (1)$$

The certificate contains: the IP address of 'A' (IPA), the public key of 'A' (KA+), a timestamp 't' indicating when the certificate was created, and a time 'e' at which the certificate will expire. All these variables are signed by T. Table 3.1 summarizes these notations.

Table 3.1: Table of notations and their description (Sanzgiri et al., 2005)

NOTATIONS	DESCRIPTION
KA+	Public key of node A
KA-	Private key of node A
[d]KA-	Data d digitally signed by node A
CertA	Certificate belonging to node A
E	Certificate expiration time
NA	Nonce issued by node A
IPA	IP address of node A
RDP	Route discovery packet identifier
REP	Reply packet identifier
T	Timestamp

b) Authenticated Route Discovery

To send data from source to destination a route is required and end-to-end authentication process of ARAN helps to obtain a secure path. The source node, S, begins route discovery process to destination 'D' by broadcasting a route discovery packet (RDP)to all its neighbors:

S -> broadcast: [RDP, IPD, NS] KS- , certS (2)

The RDP includes a packet type identifier ("RDP"), the IP address of the destination (IPD), S's certificate (certS) and a nonce (NS), all these are signed with S's private key. Nonce is used to uniquely identify an RDP coming from a source. Each time a node performs route discovery, it increases its nonce value.

Every time when a node receives an RDP message, it sets up a reverse path back to the source from which it has received the RDP. The receiving node uses S's public key, which it extracts from S's certificate, to validate the signature and verify that S's certificate has not expired. The receiving node also checks the (NS, IPS) tuple to verify that it has not already processed that RDP otherwise the RDP is not forwarded.

Now the receiving node signs the contents of the message, sends its own certificate, and broadcasts the message to its neighbors. Let ‘I1’ be a neighbor that has received the RDP broadcast from S. The rebroadcasted message from ‘I1’ is:

I1->broadcast: [[RDP, IPD, NS]KS-]KI1-, certS, certI1 (3)

Next the node I1's neighbor I2 validates the signatures for both source S, and its neighbor I1. Node I2 then removes I1's certificate and signature, records I1 as its predecessor, signs the contents of the message and appends its own certificate and then rebroadcasts the RDP. Each intermediate node repeats these steps until the destination is reached.

I2->broadcast: [[RDP, IPD, NS] KS-]KI2-, certS, certI2 (4)

c) Authenticated Route Setup

When the RDP message is received by the destination D, it replies to the first RDP that it received from the source and the given nonce. After receiving the RDP, the destination unicasts a Reply (REP) packet back along the reverse path to the source. Let the first node that receives the REP sent by D be node I3.

D->I3: [REP, IPS, NS] KD- ,certD (5)

The REP includes a packet type identifier (“REP”), the IP address of S (IPS), and the nonce sent by S. As discussed by (Sanzgiri, et al., 2005) nodes that receive the REP forward the packet back to the node from which they received the original RDP. Each node along the reverse path back to the source signs the REP and appends its own certificate before forwarding the REP to the next hop. Let I3's next hop to the source is node I2.

I3->I2: [[REP, IPS, NS]KD-]KI3- , certD, certI3 (6)

I2 validates I3's signature on the received message, removes the signature and certificate, then signs the contents of the message and appends its own certificate before unicasting the REP to I1.

I2->I1: [[REP, IPS, NS]KD-]KI2- ,certD, certI2 (7)

Finally when REP reaches source node S, it verifies the destination's signature and the nonce returned by the destination.

As shown in Figure 3.3 node I1 verifies the signature of node S; I2 of I1; I3 of I2 and D of I3 while sending RREQ packet and I3 verifies D node signature; I2 of I3; I1 of I2 and S of I1 while receiving RREP packet. Finally after all the verification a route is established between S and D.

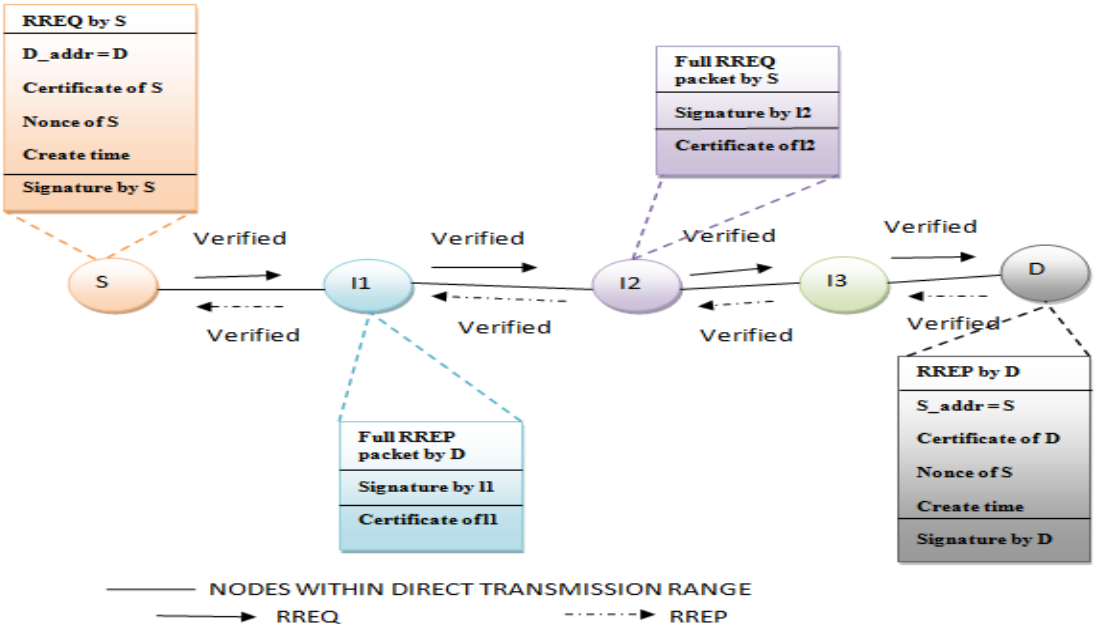

Figure 3.3: Route discovery in ARAN

d) Route Maintenance

ARAN is an on-demand protocol. (Sanzgiri, et al., 2005) stated that when no traffic has occurred on an existing route for that route's lifetime, the route is de-activated in the route table. An Error (ERR) message is sent for the inactive routes. ERR messages are also used to report the broken links due to node movement. In ARAN all ERR messages are signed.

For a route between source S and destination D, a node I2 generates the ERR message for its neighbor I1 as follows:

I2->I1: [[ERR, IPS, IPD, NI2] KI2-, certI2 (8)

This message is forwarded to the source node without any modification.

In Figure 3.4 Route Maintenance process is shown, where a link between node I2 and I3 is broken, so a route error message (RERR) is sent by node I2 to source node S.

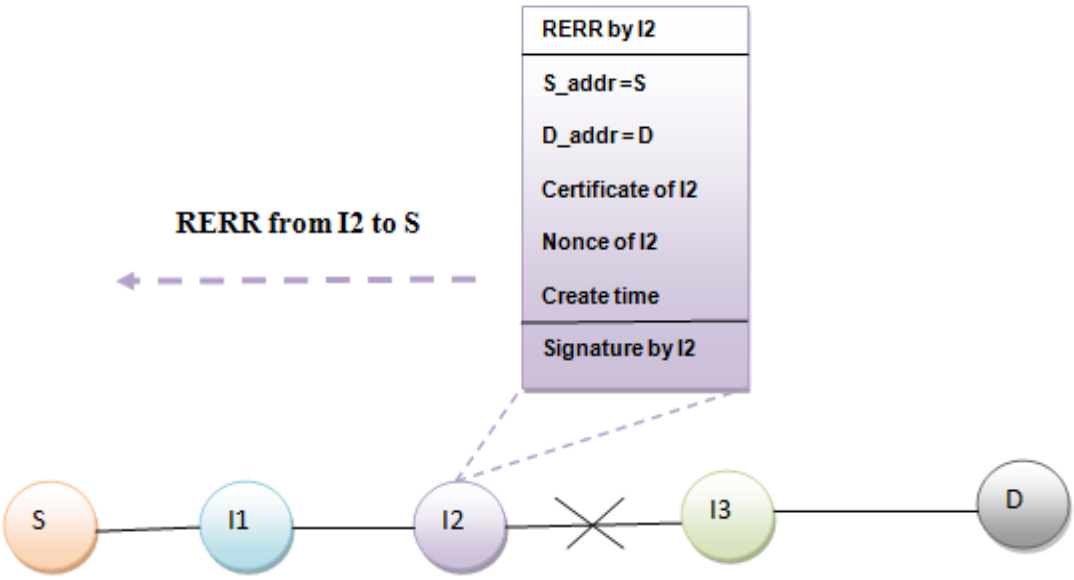

Figure 3.4: Route maintenance in ARAN

3.1.2.1 Security analysis of ARAN (Sanzgiri et al., 2005)

- In ARAN all nodes are authenticated by a trusted certificate server. So it prevents impersonation attacks because in ARAN no node can impersonate another node's identity.
- Nodes can fabricate false messages in the network but by the non-repudiation policy of ARAN, that node can be detected and may be excluded from the network.
- But Denial-of-service attack is possible in ARAN if the authenticated nodes having valid certificates send large amount of unnecessary route requests packets in the network. By this there will be a widespread congestion in the network and all nodes will suffer from power-loss by processing these unnecessary route requests. Valid nodes will not be able to access the network resources.

3.2 Routing Attacks

Due to network challenges discussed in Section 1.3 networks are vulnerable to various routing attacks caused by malicious or selfish nodes. Malicious nodes can modifying routing information, can fabricate false routing information or can impersonate other node's identity so as to disrupt the correct functioning of a routing protocol. Also selfish nodes may not participate in the network routing process by not forwarding the packets passing by them. These types of nodes can highly degrade network's performance.

In the research work Blackhole, IP-Spoofing and DDOS attacks are chosen for analysis under AODV and ARAN and are discussed as below:

3.2.1 Blackhole Attack

As discussed by (Dokurer, 2006), In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the target destination node or to the node where it wants to intercept the packets by sending fake replies to the target node. This blackhole node advertises itself for having a fresh route to the destination node by sending a fake route reply packet. This reply from malicious node will be received by the requesting node before the genuine reply from other actual nodes of the network; hence a fake route is created. When this fake route by the blackhole node is established, all the packets passing through it will be dropped and none of the packets will reach the destination node. Blackhole attack can be of two types depending on the method by which malicious node fits in the data routes (Kamra, Singh, & Singh, 1996):

- **Internal Blackhole attack**- here the malicious node is the part of the network and it provides fake route replies and thus does not allow packets to reach to its destination by simply dropping the packets passing through it.
- **External Blackhole attack**- here node stays outside the network and compromises the nodes of the other network.

In ARAN, each node is provided with a certificate so only authenticated nodes can participate in routing; no external node can enter in the network. So to compare AODV and ARAN, we are dealing with only internal blackhole attack.

3.2.1.1 Blackhole in AODV

As discussed in (Ullah & Rehman, 2010)blackhole attack can be conducted by modifying count and sequence number and a node then start behaving as a malicious node, which on receiving the RREQ packet sends a fake RREP packet of minimum hop count and maximum sequence number. Finally the packets which passed through this node would be dropped.

As shown in Figure 3.5, where node I1 acts as a blackhole node which sends an immediate reply to source node's(S) route request with a RREP packet, where it sets hop_count = 1 and D_seq = 4294967295 (Ullah & Rehman, 2010). Another genuine RREP packet is sent by node I3 but source node will not accept the RREP packet from node I3 as it has higher hop_count and lower D_seq number as compared to the reply coming from malicious node I1. After this the source node starts sending packets to I1, being the malicious node I1 will drop all the packets without making them to reach to the destination node.

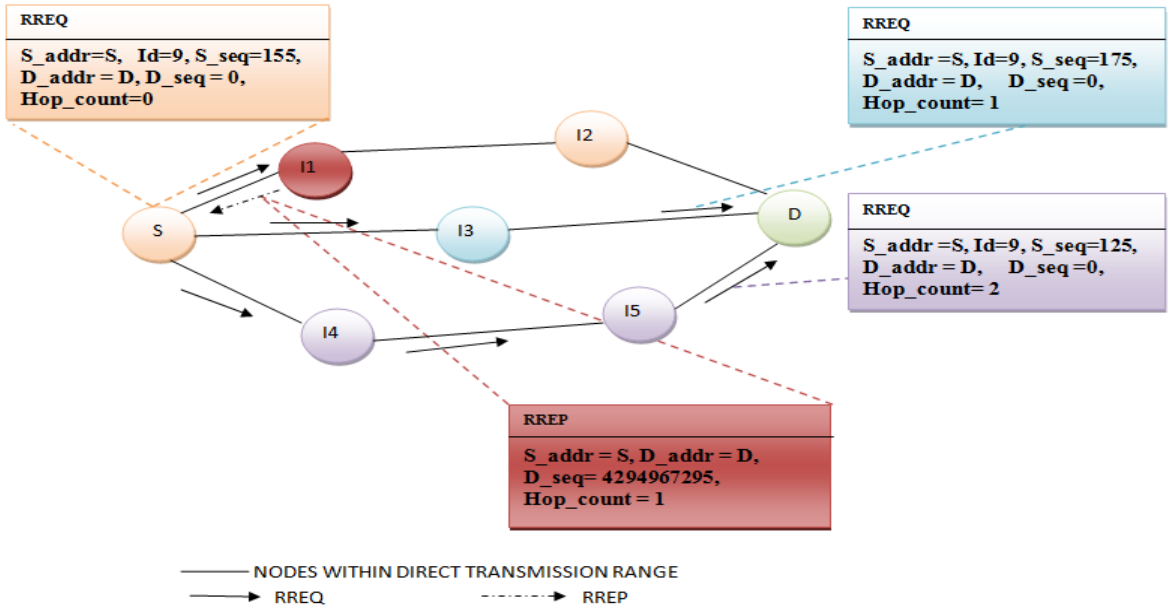

Figure 3.5: Blackhole attack in AODV

3.2.1.2 Blackhole in ARAN

In ARAN there are no such parameters like hop count or sequence number, for route discovery process. Therefore in ARAN Blackhole attack is not feasible unless selfish nodes drop the packets (Kamra, Singh, & Singh, 1996).

3.2.2 IP-Spoofing Attack

As discussed by (Vigna, 2004), IP spoofing is a method of attacking a network in order to gain unauthorized access. Internet communication between nodes which are placed far apart from each other is handled by routers. These routers generally find the route for communication by finding the destination node's address only, and ignore the originating node's address. So any node can use another node's address and send packets in the network.

In IP-Spoofing attack, the intruder by "spoofing" the IP address of a trusted system can send wrong messages to some another node of the network and thus indicates that the message has come from a trusted system. Now to the victim node it appears that the packets are coming from the trusted system.

3.2.2.1 IP-Spoofing in AODV

AODV doesn't check the source node's address while routing the packets in the network. So if source node's address is spoofed with some other node's address, packets will reach the destination with the spoofed node address.

3.2.2.2 IP-Spoofing in ARAN

In ARAN at every step precursor node's and successor node's address is verified before forwarding the packet to the next node. So ARAN resists IP-Spoofing attack.

3.2.3 DOS and DDOS attack

As discussed by (Reddy, Kundra, Babu, & Kumar, 2012),MANETs have several salient characteristics, such as Dynamic topologies, Bandwidth-constrained, variable capacity links, Energy-constrained operation, Limited physical security, etc. due to which MANETs are vulnerable to different types of network attacks like- DOS, Blackhole, IP-Spoofing, False message fabrication, etc. Denial-of-Service (DOS) is one the major attack which is used to deny the network access to other nodes in the network.DOS attack is launched through compromised or malicious nodes or selfish nodes which prevent other legitimate nodes to access various network resources.

When launched through a single node it is called single source DOS attack and when multiple nodes are used to launch the attack it is known as Distributed Denial-of-Service (DDoS) attack (Abliz, 2011). In DDOS attack unwanted traffic is sent over the network which prevents legitimate traffic to reach the destination. The victim system is made unable to process legitimate node's requests.

3.2.3.1 DDOS on ARAN

In this research work DDOS attack has been discussed on ARAN protocol, where the attack is caused by selfish nodes which sends large amount of unnecessary packets in the network, so that all bandwidth is consumed. This makes the victim system processing speed slow and network bandwidth is fully occupied, so now the legitimate users are not able to access the network resources.

In the simulation for DDOS attack nodes N1, N3, N5, N7 and N8 are taken as selfish nodes and node N6 as genuine node. As shown in Figure 3.6 nodes N1, N3, N5, N7 and N8 send unnecessary data in the network to create congestion in the network, and don't allow the data of node N6 to reach the destination node D. So in DDOS attack a legitimate node cannot access the services of another legitimate node.

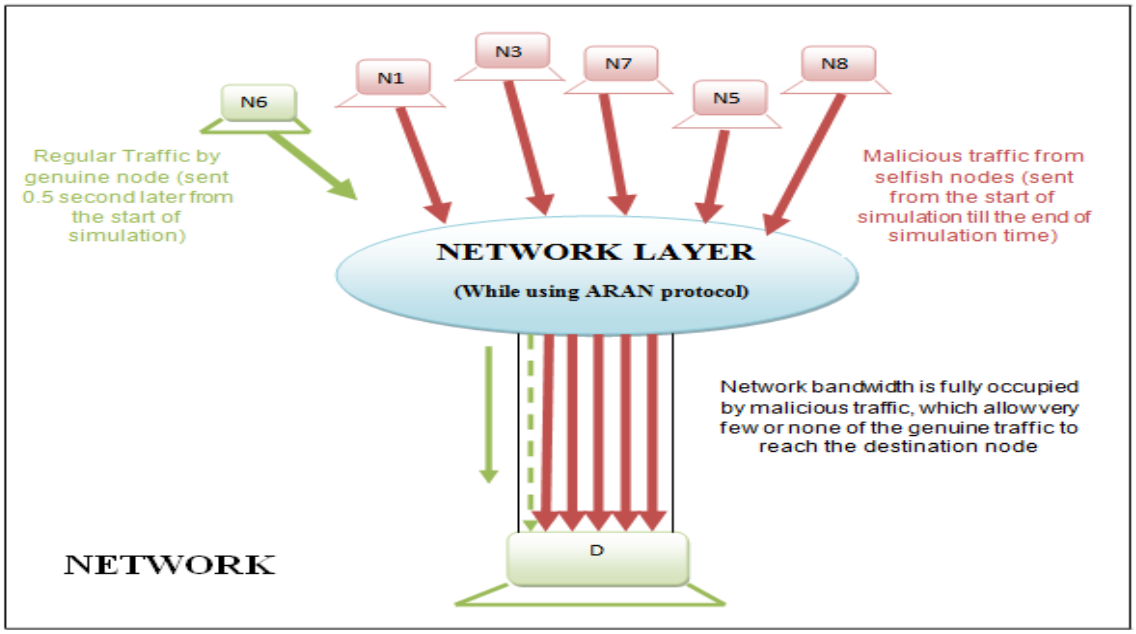

Figure 3.6: DDOS attack

3.3 Chapter Summary

In this chapter a detailed working of an on-demand routing protocol AODV has been discussed. Security analysis shows that the protocol is vulnerable to many network attacks. Afterwards, a discussion is given about how ARAN defends various attacks like- spoofing, false message fabrication and modification of protocol message. By the study of both the protocols it has been observed that ARAN provides much more security features than AODV. But it has also been proven that the ARAN protocol does not defend against Distributed Denial of Service (DDOS) attack which is performed by authenticated selfish nodes. Table 3.2 summarizes the security analysis of AODV and ARAN protocols.

Table 3.2: Attacks possible in AODV and ARAN

Attacks	**AODV**		**ARAN**	
	YES/NO	**REASON**	**YES/NO**	**REASON**
Blackhole	YES	Hop count and Sequence number can be easily modified.	NO	Hop count and Sequence number does not exist. But it is possible if selfish node drops the packets passing through them.
Message Modification	YES	No check on message contents.	NO	Digital signature by the sender.
IP- Spoofing	YES	Source address is not verified.	NO	Source address is verified by sender's digital signature.
False Route Errors	YES	Can be sent by any node by using IP-spoofing.	YES	Can be sent by any node but sending node can be detected.
DOS or DDOS	YES	Congestion can be created by using IP-spoofing.	YES	Congestion can be created by legitimate nodes.

CHAPTER 4

PROPOSED WORK AND SIMULATION ENVIRONMENT

4.1 Introduction

ARAN prevents from various types of attack like- message modification, impersonation and false message fabrication but cannot prevent from selfish node behavior. ARAN is vulnerable to DDOS attack where authenticated selfish nodes can send unnecessary large number of packets in the network. Whole network bandwidth will be full of the packets sent by the selfish nodes. The communication bandwidth and other resources (like storage capacity and battery power) are exhausted in processing of these packets. Now with enormous amount of packets in the same interval of time, the bandwidth will be fully occupied and legitimate nodes cannot get the bandwidth to send data.

4.2 Problem Definition

As shown in Figure 3.6 DDOS can be launched by selfish nodes which sends large amount of unnecessary packets in the network, and thus preventing other legitimate node's packets to reach the destination.

4.3 Main Idea for prevention of DDOS attack in ARAN by introducing i-ARAN

As shown in Figure 4.1 a technique has been designed to prevent the DDoS attack and is called as Improved ARAN (i-ARAN). Overall working of i-ARAN is similar to that of ARAN except that in i-ARAN each node can send only the limited amount of packets per second in the network. If the rate exceeds the threshold values, packets will not be forwarded in the network and are dropped.

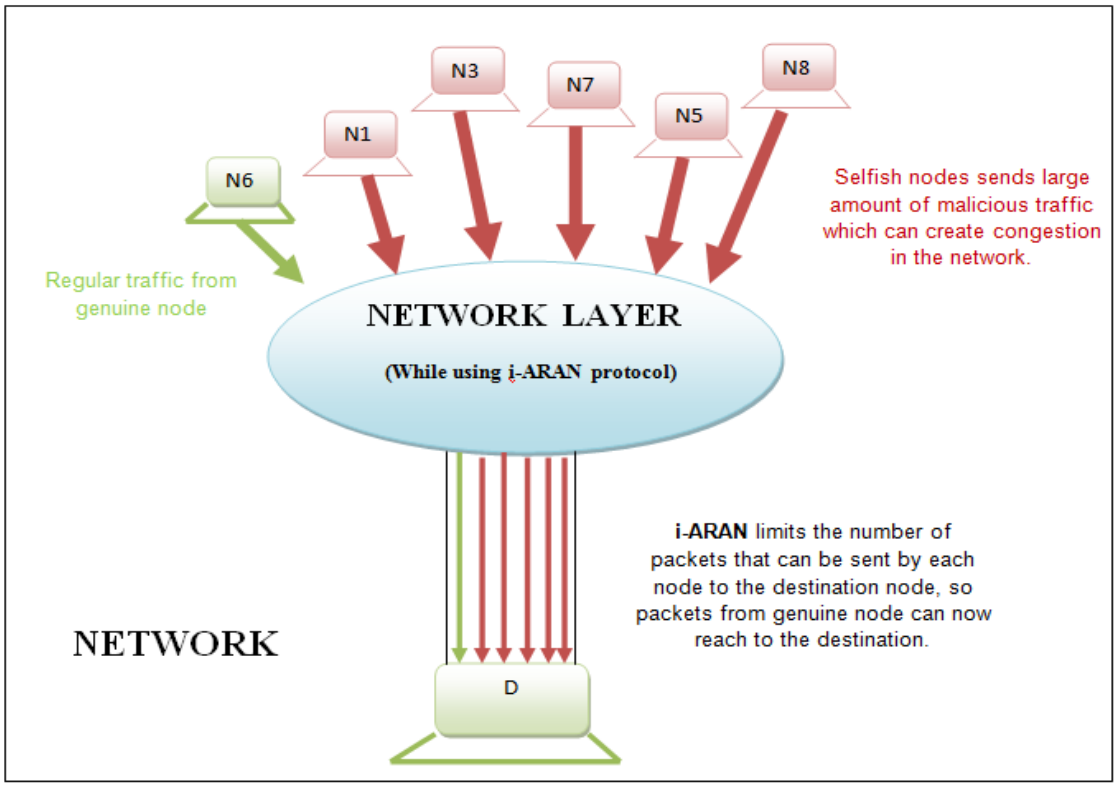

Figure 4.1: DDOS attack prevention scheme by using i-ARAN

The overall process followed by i-ARAN is described by Algorithm 1.

Algorithm 1:

1. Include the cbr_client.h file in aran.pc code file.
2. Get the session start time and end time of the traffic sessions from "cbr_client.h" file into aran.pc file.
3. Convert the clocktype values of start time and end time into integer values.
4. Now apply the threshold values (like th1, th2, th3) on the number of packets every node can send in the network per unit of time in the routing function of aran.pc, as:

- If (end time – start time >= 3 seconds)
- <th1> number of packets can be sent;
- If (packets to be sent are more than <th1>) then
- Return;
- Else if(end time – start time > 1 second and end time – start time <= 2)
- <th2> number of packets can be sent;
- If(packets to be sent are more than <th2>) then
- Return;

- Else if (end time – start time > 0 and end time – start time <= 1)
- <th3> packets can be sent;
- If(packets to be sent are more than <th3>) then
- Return;
- Else
- Forward the packets;

4.4 Analysis of the Proposed Technique

In this research work it has been assumed that each node will send packets at the rate of 50 packets per second and threshold values have been taken as: th1=39, th2=26 and th3=13. By limiting the number of packets each node can send in the network, congestion in the network is prevented and thus packets from all the legitimate nodes will reach the destination.

4.5 Introduction to GloMoSim Simulator

Global Mobile Information System Simulator(GloMoSim) as discussed by (Nilsson, 2002) is a popular network simulation tool, which is used in the study of the behavior of large-scale hybrid networks that include wireless, wired, and satellites based communications networks. It is freely available without any fee for educational and research institutes. It can be easily installed and used. Glomosim supports various multi-hop ad hoc network protocols like- AODV, DSR, Fisheye, LAR, ODMRP and WRP.(Nilsson, 2002) stated that GloMoSim is built using the OSI seven layer network architecture and standard APIs are used between the different simulation layers.

In (Bajaj et al., 1999) it has been discussed that Glomosim uses Parsec, which is a C-based simulation language developed by PCL at UCLA, for sequential and parallel execution of discrete-event simulation models. PARSEC runs on several platforms, including UNIX and Windows. An object or set of objects (also called as physical process) in the physical system are represented by a logical process. Interactions among physical processes (events) are modeled by time-stamped message exchanges among the corresponding logical processes.

(Bajaj et al., 1999) also stated that PARSEC has the ability to execute a discrete-event simulation model on a variety of parallel architectures using different asynchronous parallel simulation protocols. PARSEC is designed to hide the description of a simulation model from the simulation protocol being used.

In this research work Glomosim has been installed on RedHat Linux 9 operating system.

4.6 Installation of Glomosim-2.03 on Redhat Linux 9

Steps to be used for installing GloMoSim simulator in RedHat Linux are given as under:

a) Firstly download GloMoSim-2.03 and java jdk1.5.0_07 07-linux-i586-rpm.bin for Linux.
b) Open RedHat Linux with root user and copy GloMoSim-2.03 and jdk1.5.0_07 in root folder of Linux. To install JDK just double click its icon and then click “run in terminal”, it will install JDK at directory /usr/java/jdk1.5.0_07.
c) Now open the terminal of Linux and change directory to home and create Parsec folder by typing following commands:
    - cd home
    - mkdir parsec
d) Copy the files of glomosim-2.03\parsec\redhat-7.2 in new parsec folder in home directory.
e) Close the terminal and reopen it and run the following command:
    - vi ~/.bash_profile
f) A file will appear , press ‘insert’ from keyboard to insert in the file and write there:
    - JAVA_HOME=/usr/java/jdk1.5.0_07/bin/java
    - PCC_DIRECTORY=/home/parsec
    - PATH=$PATH:$HOME/bin:/usr/java/jdk1.5.0_07/bin:/$PCC_DIRECTORY/bin
    - BASH_ENV=$HOME/.bashrc
    - USERNAME=“root”

- export USERNAME BASH_ENV PATH PCC_DIRECTORY JAVA_HOME

Now press Esc button and do :w and then :q.

g) Now change directory to main folder of GloMoSim as:
   - cd /glomosim-2.03/glomosim/main

h) Now type the following commands to start the GloMoSim:
   - make clean
   - make
   - cd ../bin
   - ./glomosim config.in

If it gives output glomosim is properly installed.

4.7 Installation of Visualization Tool of GloMoSim

For installation of visualization tool of glomosim following steps are to be followed:

a) Copy all files of glomosim\bin to glomosim/java_gui.
b) Now open the terminal and change directory to java_gui of glomosim as:
   - cd /glomosim-2.03/glomosim/java_gui
c) Type the commands:
   - javac *.java
   - java GlomoMain

A glomosim visualization screen will appear and it is successfully done.

4.8 Addition of ARAN protocol in Glomosim-2.03

Addition of a new routing protocol in GloMoSim is quite easy. To add ARAN protocol some files have to be edited. GloMoSim by default supports AODV protocol. To add ARAN protocol in GloMoSim, files of AODV has to be replaced with ARAN. Following steps have to be followed to add the routing protocol. Firstly check for the two files, the new protocol code must have files- .pc and .h, i.e., ARAN protocol code must have aran.pc and aran.h files. Check that both the files

(aran.pc and aran.h) must have two functions “void RoutingARANInit()” and “void RoutingARANFinalize()”.Files that are to be modified in GloMoSim-2.03 are:

a) Makefile (in main folder)
    - SIM_HDRS=.../network/**aran.h**…
    - PAR_FILES=…/network/**aran.pc**…

b) Application.pc (in application folder)
    - Void GLOMO_AppInit(GlomoNode *node, constGlomoNodeInput *nodeInput)

      {

      ….

      Else if (strcmp(buf, “**ARAN**”) == 0)

      {

      }

      …..

      }

c) Nwcommon.h (in include folder)
    - # define IPPROTO_**ARAN** 123

d) Network.h (in include folder)
    - Typedefenum {

      ….

      ROUTING_PROTOCOL_**ARAN**

      ….

      }

      NetworkRoutingProtocolType;

e) Nwip.pc (in network folder)
    - Include “**aran.h**” in header files.

- Make the following changesin the function static void ProcessPacketForMeFromMac()

  Switch (IpPROTOCOL){

  …..

  Case IPPROTO_**ARAN**:{

  Routing**Aran**HandleProtocolPacket(node, msg, sourceAddress, destinationAddress, ttl);

  break;

  }…..}

- Make the following changes in the function voidNetworkIPLayer(GlomoNode *node, Message *msg)

  ……..

  case ROUTING_PROTOCOL_**ARAN**: {

  RoutingAranHandleProtocolEvent(node, msg);

  break;

  }

  ……

- Make the following changes in the function void NetworkIpInit(GlomoNode* node, constGlomoNodeInput* nodeInput)

  ……..

  else if (strcmp(protocolString, "**ARAN**") == 0) {

  ipLayer->routingProtocolChoice= ROUTING_PROTOCOL_**ARAN**;

  Routing**Aran**Init(node,(GlomoRouting**Aran****)&ipLayer->routingProtocol, nodeInput);

}

……

- Make the following changes in the function void NetworkIpFinalize(GlomoNode *node)

……

case ROUTING_PROTOCOL_**ARAN**:

Routing**Aran**Finalize(node);

break;

……

Save the changes. Then go to the terminal and type:

- cd/glomosim-2.03/glomosim/main
- make clean
- make

If no error appears that means ARAN has successfully been added in the GloMoSim simulator.

4.9 Configuration file of GloMoSim

The configuration file of GloMoSim simulator provides a number of predefined parameters which are used to configure it.Various configuration parameters used for the simulation are like:

- SIMULATION TIME- It is adjusted according to the time period simulations are made to run.
- TERRAIN-DIMENSIONS- The units are in metres. It is used to vary the average node density.
- NUMBER-OF-NODES- This parameter provides the total number of nodes that are to be simulated in the network.

- NODE-PLACEMENT- The nodes are usuallyplaced uniformly or randomlyin the simulated area. Otherwise nodes can be placed manually by using nodes.input file of Glomosim.
- MOBILITY- Mobility For static networks is to set to NONE. Otherwise for mobility, GloMoSim uses the Random Waypoint mobility model, in which nodes move with a speed which is specified by its limits, also pause time is also used where nodes pause for some time.
- ROUTING-PROTOCOL- GloMoSim supports following protocols by default: Bellman Ford AODV, DSR, LAR1, WRP, Fisheye, ZRP.

Now to run a simulation a traffic scenario and the types of applications used by the nodes is to be defined by the user. This is done by a application file (app.conf).

app.conf file defines three types of traffic that can be generated by a node, FTP, TELNET and CBR (Constant Bit Rate). The syntax used to generate these different types of traffic are:

- FTP <source node><dest node><amount sent><start time>
- TELNET <source node><dest node><duration><start time>
- CBR <source node><dest node><items to send><item size><interval><start time><end time>

  Now simulation can be done by typing:

  ./glomosim config.in

Finally the results of simulation are collected in “glomo.stat” file which is used later for analysis.

4.10 Methodology of Evaluation

For performance evaluation of ARAN and AODV, both the protocols are run under identical mobility and traffic scenarios as described in Table 4.1 under GloMoSim simulator.

Step 1.All simulation experiments are developed and simulated on an Intel machine using Linux Red Hat 9.0 and the network simulator Glomosim-2.03.

Step 2. Blackhole and IP-Spoofing attack is implemented and both the protocols are analyzed under the attacks.

Step 3. DDOS attack is performed on ARAN and its effect is analyzed on the protocol.

Step 4. Proposed technique to prevent from DDOS attack has been implemented in ARAN and is called as i-ARAN. i-ARAN is analyzed under DDOS attack again.

4.11 Simulation Environment Setup for Blackhole and IP-Spoofing attack

Here the simulation setup which is used to measure the performance of AODV and ARAN protocols under Blackhole and IP-Spoofing attack is discussed. GloMoSim-2.03, which provides a scalable simulation platform for wireless networks, is used to perform the simulations. The common parameters that have been used in the simulations are given in Table 4.1. Simulations are done on an Intel (core i3) machine using Linux Red Hat 9.0.

Table 4.1: Simulation environment setup

Simulation parameter	**Value**
Simulator	GloMoSim-2.03
Simulation Time	100 seconds
Routing Protocols	AODV and ARAN
Traffic	CBR packets
Mobility Model	Random Waypoint
Traffic Sessions	6
Number of nodes	10, 30, 50 and 70
Number of internal Blackhole node	1
Node speed	0, 5, 10 and 15m/s
Terrain Area	500*500, 750*750, 1000*1000 and 1250*1250
Packet size	512 bytes
Performance Metrics	Packet Delivery ratio, Average Path Length , Average end-to-end Delay and Throughput

- **Traffic**: Constant bit rate (CBR) packets are sent over the network.
- **Mobility Model**: Random Waypoint Model is used to simulate MANETs where the mobile nodes can move randomly in any direction constrained with the speed specified in MOBILITY-WP-MIN-SPEED and MOBILITY-WP-MAX-SPEED parameters of GloMoSim. Also MOBILITY-WP-PAUSE defines the pause time a node pauses before moving randomly further (Nilsson, 2002).
- **Traffic Sessions**: To generate traffic 6 nodes are selected as source nodes and 6 nodes as the receiver nodes. All these sending nodes send packets of 512 bytes at the rate of 10 packets per second. Total 100 packets are sent

from each node. All the simulations for a particular number of nodes are carried out for different speeds- 0m/s (no mobility), 5m/s, 10m/s and 15m/s.

- **Terrain areas for different number of nodes**: Simulations are done for different number of nodes which are randomly allocated in different terrain areas. For simulation of 10 numbers of nodes the terrain area is given as 500*500; similarly for 30 nodes it is 750*750; for 50 nodes it is 1000*1000 and for 70 nodes it is given as 1250*1250.
- **Number of internal Blackhole node**: To evaluate AODV under blackhole attack only one node is taken as malicious node which advertises itself of having shortest path to the destination node by sending fake route replies by modifying hop count and sequence number parameters. But in ARAN no such parameters exist so a single selfish node is taken which simply drops the packets passing through it.
- **Performance Metrics:**
  a) **PDR (Packet Delivery ratio)**: This metric indicates the fraction of data packets that reached the destination and is calculated as: Total Packets Received/Total Packets sent (Sanzgiri et al., 2005).
  b) **Average Path Length** - This is the average length of the paths discovered by the protocol. It is calculated as: Total data packets/Total hops taken(Sanzgiri et al., 2005).
  c) **Average end-to-end Delay**- This is the average delay between the sending of the data packet by the constant bit rate source and its receipt at the corresponding constant bit rate receiver (Mahmoud et al., 2005). It is calculated by taking average of Total end-to-end delay at each receiving node.
  d) **Throughput**- This value represents the ratio of the total bits of data packets that reach their destination, to the total time it takes to reach to the destination. It is calculated by taking average of Throughput at all receiving nodes.

Finally results are obtained by collecting the above mentioned performance metrics from “glomo.stat” file by using various Linux shell scripts. The shell scripts are run by the command: sh<shell script><stat file>. These shell scripts are given in appendix D.

4.12 Simulation Environment Setup for DDOS attack

To generate traffic 6 nodes has been selected as source nodes and a single node as the receiver nodes. All these sending nodes send packets of 512 bytes at the rate of 50 packets per second. All the simulations for a particular number of nodes are carried out for different speeds- 0m/s (no mobility), 5m/s, 10m/s and 15m/s. Here five nodes have been considered that will act as selfish nodes sending large amount of data at the start of the simulation till the simulation end time is reached and node 6 is the genuine user which starts sending packets after 0.5 second of the start of simulation time. By that time, bandwidth of the network is fully occupied by the other selfish nodes.

In the simulations, effect of DDoS attack has been studied under the following conditions:

- Different simulation time- for 1, 2 and 3 seconds;
- Different node mobility.

4.13 Chapter Summary

In this chapter the proposed technique for prevention of DDOS attack on ARAN protocol has been discussed. Then installation of Glomosim-2.03 simulator on RedHat Linux 9 has been discussed. Afterwards the evaluation methodology gives the simulation approach followed. The description of the simulation environment used and the different chosen simulation parameters is given and followed by the shell scripts used for analyzing the results.

CHAPTER 5

SIMULATION RESULTS & DISCUSSION

5.1 Security analysis of AODV and ARAN under Blackhole (BH) Attack

Experiment 1: Blackhole attack simulation results using 10 nodes in 500*500 area

Objective: To find out which protocol perform better under blackhole attack by evaluating- Packet Delivery ratio, Average Path Length, Average end-to-end Delay and Throughput for AODV and ARAN using total 10 nodes at varying node speeds.

Results: The results obtained in this scenario are given in Table 5.1 and 5.2.

Table 5.1: Simulation results of AODV using 10 nodes

Node Speed ⟶ / Performance Metric ↓	0m/s	5m/s	10m/s	15m/s
Packet Delivery Ratio	0.166667	0.166667	0.166667	0.166667
Average Path Length	3	3	3	3
Delay	4.709	4.709	4.709	4.709
Throughput	6896.5	6896.5	6896.5	6896.5

Table 5.2: Simulation results of ARAN using 10 nodes

Node Speed ⟶ / Performance Metric ↓	0m/s	5m/s	10m/s	15m/s
Packet Delivery Ratio	0.833	0.833	0.833	0.833
Average Path Length	1.166	1.166	1.166	1.166
Delay	13.056	12.783	12.504	12.244
Throughput	34668.33	34684.5	34665.5	34687.17

(i) Packet delivery ratio

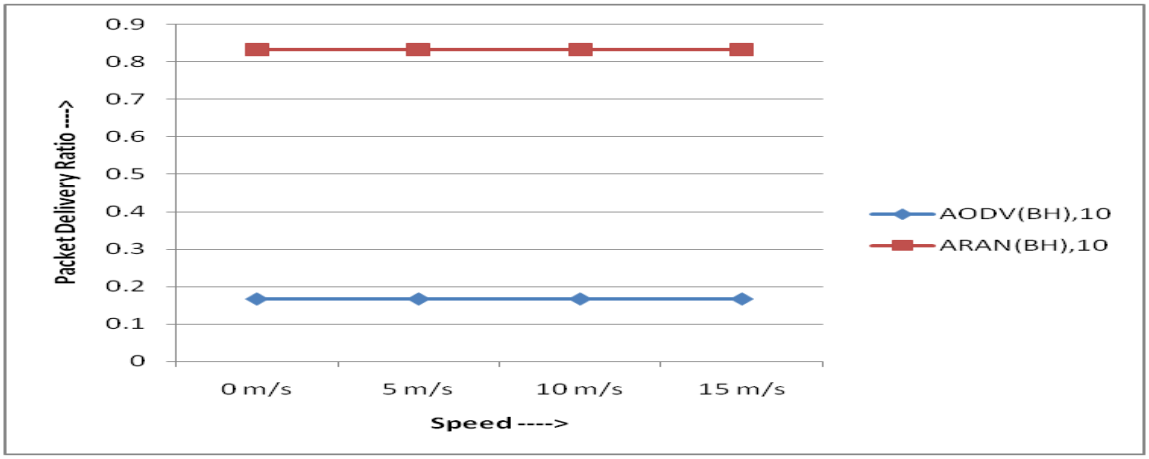

Figure 5.1: Packet Delivery Ratio of AODV and ARAN at varying speeds for 10 nodes

Analysis:

- It has been observed that the packet delivery ratio decreases more under AODV as compared to ARAN. The packet delivery ratio is 16% while using AODV but ARAN provides nearly 83% PDR in same scenario.
- The decrease in PDR in AODV is due to the blackhole node which can cause maximum data packets to pass through it by giving fake route reply and finally drops the packets. But in ARAN selfish node cannot send such a reply, so only those packets which pass through the selfish node are simply dropped.

(ii) Average Path Length

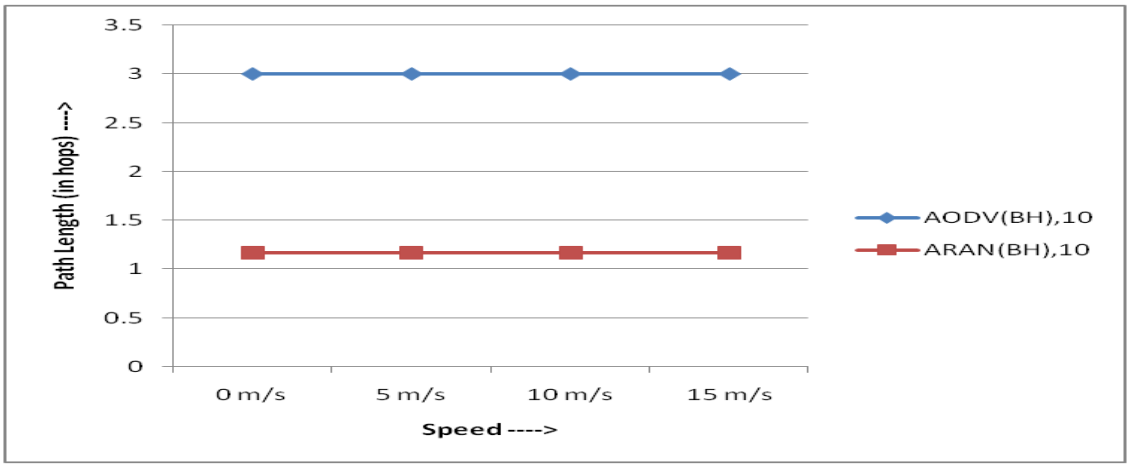

Figure 5.2: Average Path Length of AODV and ARAN at varying speeds for 10 nodes

Analysis:

- AODV has been observed of having a longer route path in presence of malicious node than ARAN.
- In AODV malicious node can set a longer route path for the packets passing by it. ARAN provides authenticity due to which malicious nodes can't modify contents of the routing packets. Secure routes are selected and there is no adverse effect on the Average Path Length.

(iii) <u>Average end-to-end delay</u>

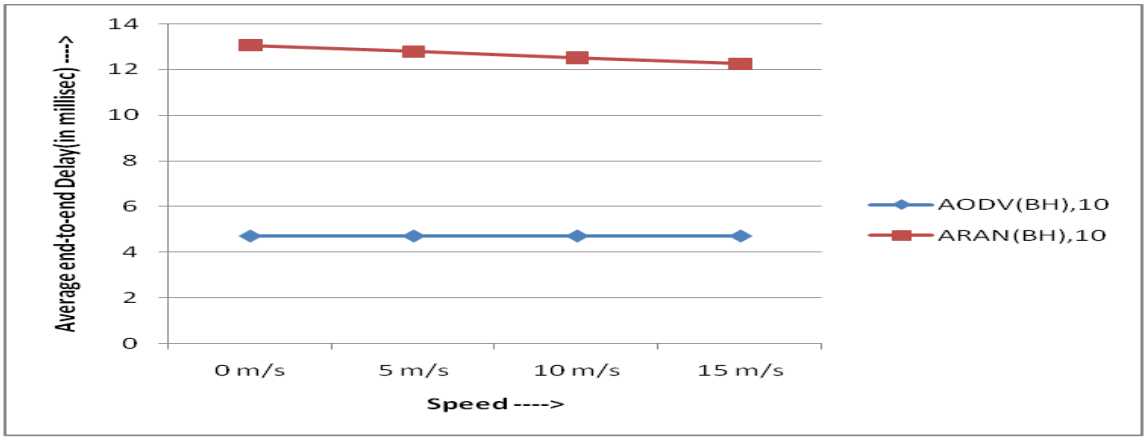

Figure 5.3: Average end-to-end Delay of AODV and ARAN at varying speeds for 10 nodes

Analysis:

- Delay of AODV is less although there is an increase of Average Path Length as shown above in Figure 5.2; this can be due to very less packet delivery ratio of AODV while using 10 nodes (as shown in Figure 5.1) due to which average end-to-end delay decreases. Also delay in ARAN is more due to cryptographic calculations.
- Average end-to-end delay depends upon Packet Delivery ratio as well as on Average Path Length.

(iv) Throughput

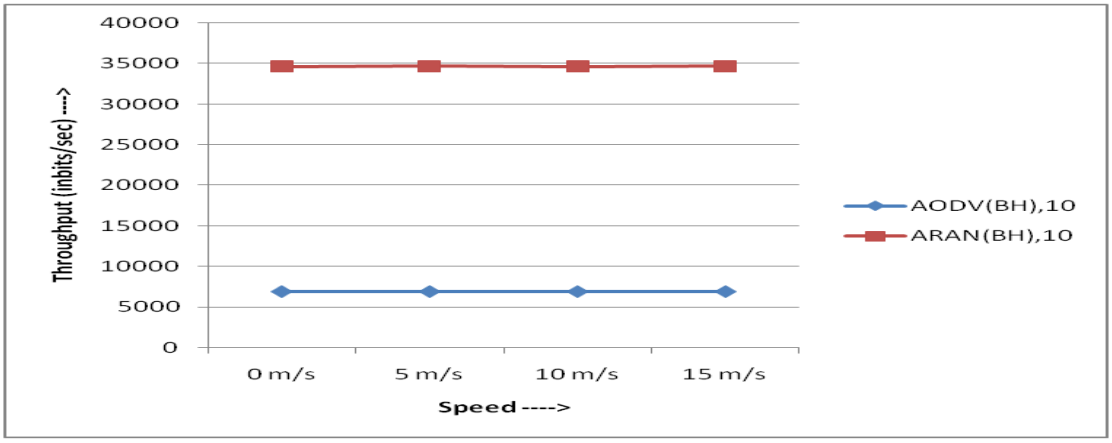

Figure 5.4: Throughput of AODV and ARAN at varying speeds for 10 nodes

Analysis:

- The throughput of AODV is less as compared to that of ARAN.
- This effect is because of the decrease in Packet Delivery Ratio, as there is a decrease in total number of data bits received so throughput of AODV is less than that of ARAN.

Experiment 2: Blackhole attack simulation results using 30 nodes in 750*750 area

Objective: To find out which protocol perform better under blackhole attack by evaluating- Packet Delivery ratio, Average Path Length, Average end-to-end Delay and Throughput for AODV and ARAN using total 30 nodes at varying node speeds.

Results: The results obtained in this scenario are given in Table 5.3 and 5.4.

Table 5.3: Simulation results of AODV using 30 nodes

Node Speed → / Performance Metric ↓	0m/s	5m/s	10m/s	15m/s
Packet Delivery Ratio	0.50	0.50	0.50	0.50
Average Path Length	1.4	1.4	1.8	1.8
Delay	15.976	15.86	15.663	15.8
Throughput	21016.5	21055.3	21069.33	21056.66

Table 5.4: Simulation results of ARAN using 30 nodes

Node Speed → / Performance Metric ↓	0m/s	5m/s	10m/s	15m/s
Packet Delivery Ratio	0.833	0.833	0.833	0.833
Average Path Length	1.16667	1.16667	1.16667	1.16667
Delay	13.559	13.722	13.555	13.416
Throughput	34895.16	34893.66	34902.66	34896.16

(i) Packet Delivery Ratio

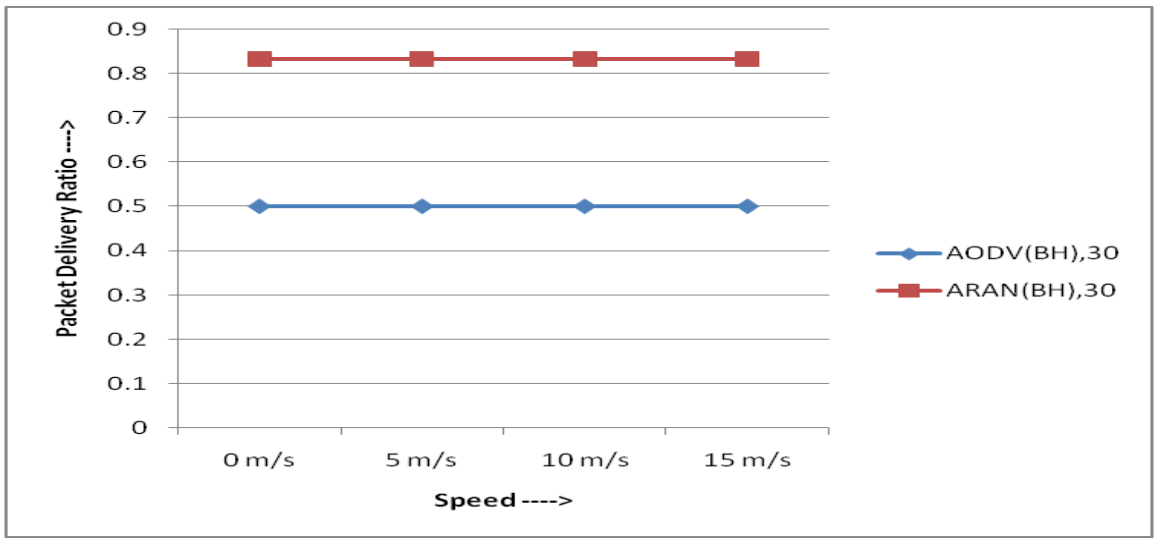

Figure 5.5: Packet Delivery Ratio of AODV and ARAN at varying speeds for 30 nodes

Analysis:

- The packet delivery ratio is 50% while using AODV but ARAN provides nearly 83% PDR in same scenario.
- The decrease in PDR in AODV is due to the blackhole node which can drop maximum data packets.

(ii) Average Path Length

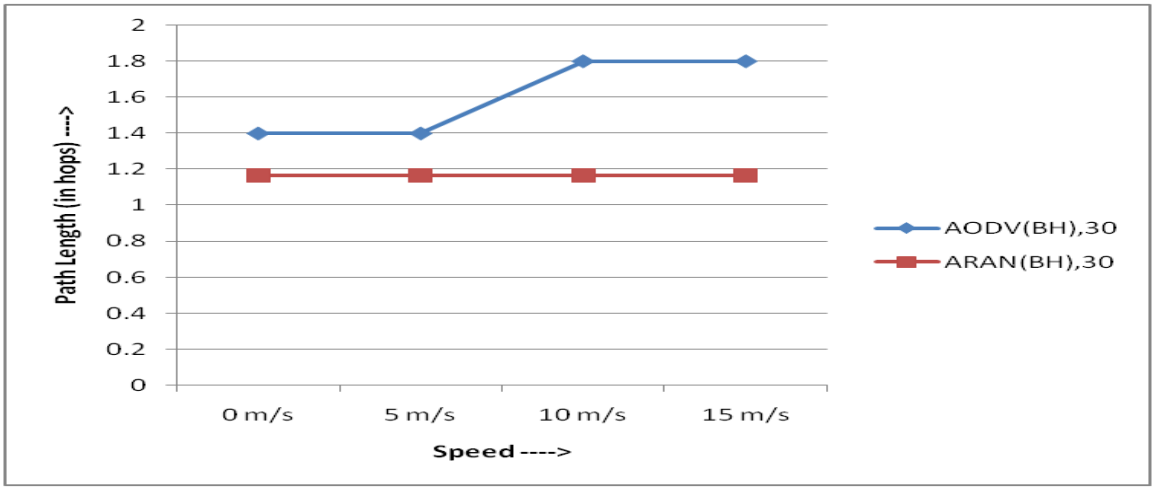

Figure 5.6: Average Path Length of AODV and ARAN at varying speeds for 30 nodes

Analysis:

- AODV has been observed of having a longer route path in presence of malicious node than ARAN.

(iii) Average end-to-end Delay

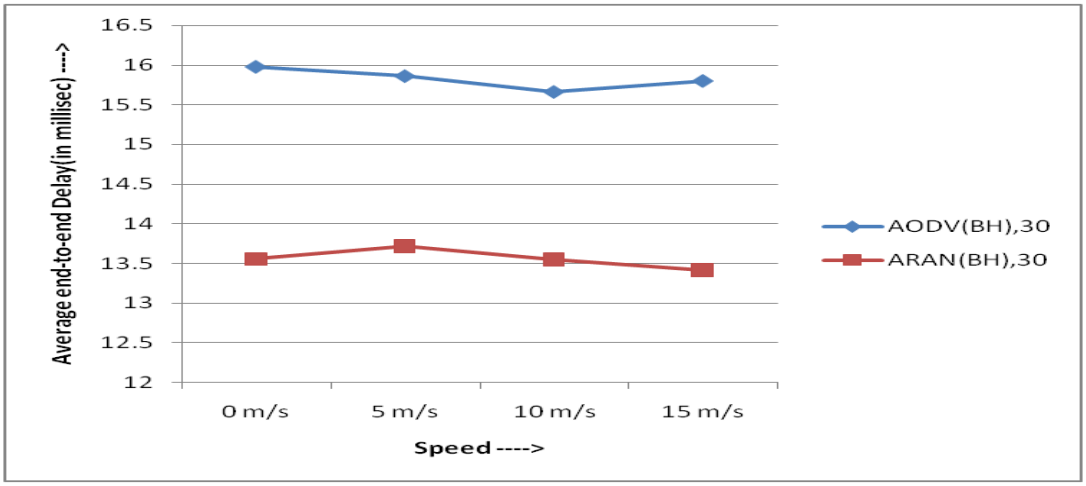

Figure 5.7: Average end-to-end Delay of AODV and ARAN at varying speeds for 30 nodes

Analysis:

- Delay of AODV is more than ARAN because there is an increase in Average Path Length.

(iv) Throughput

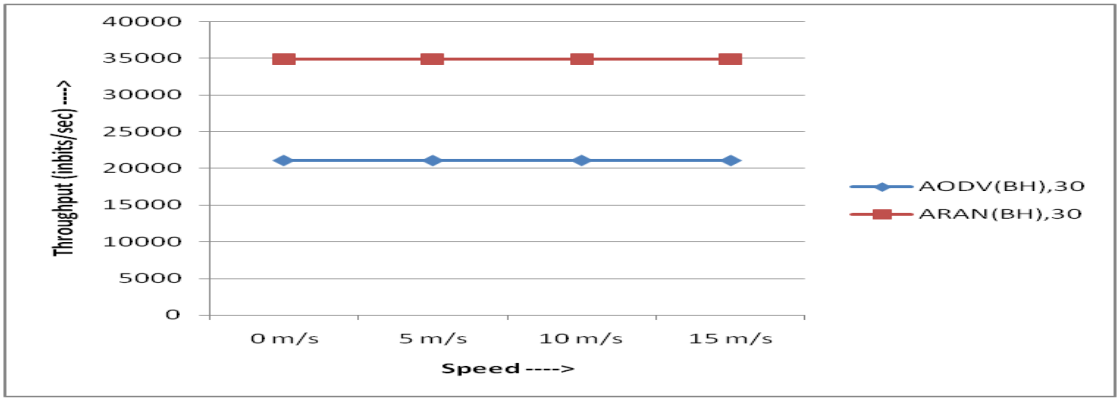

Figure 5.8: Throughput of AODV and ARAN at varying speeds for 30 nodes

Analysis:

- The throughput of AODV is less as compared to that of ARAN because of the decrease in Packet Delivery Ratio as shown in Figure 5.5.

Experiment 3: Blackhole attack simulation results using 50 nodes in 1000*1000 area

Objective: To find out which protocol perform better under blackhole attack by evaluating- Packet Delivery ratio, Average Path Length, Average end-to-end Delay and Throughput for AODV and ARAN using total 50 nodes at varying node speeds.

Results: The results obtained in this scenario are given in Table 5.5 and 5.6.

Table 5.5: Simulation results of AODV using 50 nodes

Node Speed → / Performance Metric ↓	0m/s	5m/s	10m/s	15m/s
Packet Delivery Ratio	0.166667	0.166667	0.385	0.385
Average Path Length	1	1.31	1.5	1.5
Delay	5.994	7.023	32.7547	32.7785
Throughput	6960.33	6956	25844.83	25882

Table 5.6: Simulation results of ARAN using 50 nodes

Node Speed → / Performance Metric ↓	0m/s	5m/s	10m/s	15m/s
Packet Delivery Ratio	0.995	0.9933	0.991667	0.8316667
Average Path Length	1.003778	1.00479	1.00485	1.147817
Delay	16.293	16.881	20.682	17.045
Throughput	42002	41914.5	42078.83	35015.17

(i) Packet Delivery Ratio

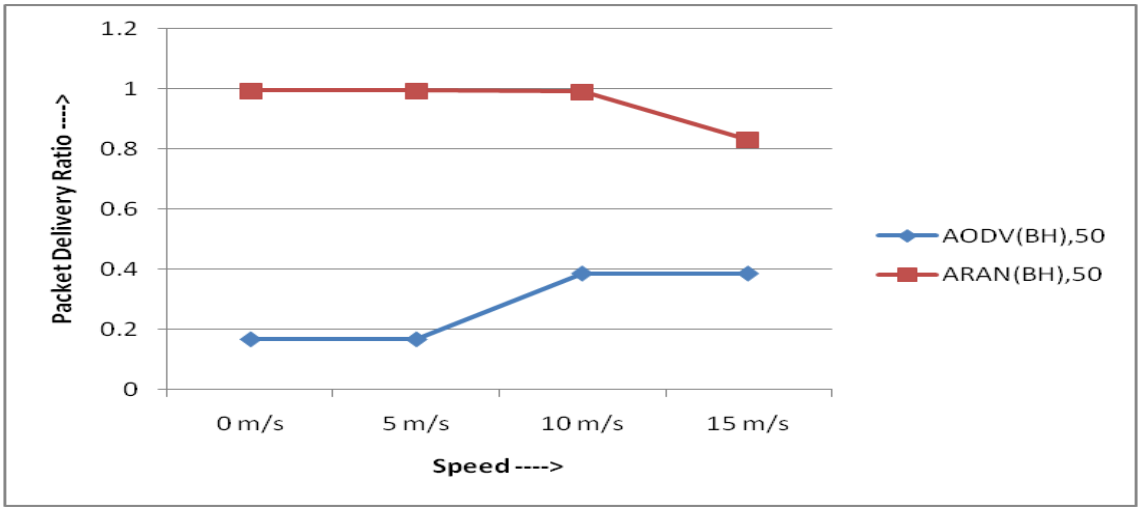

Figure 5.9: Packet Delivery Ratio of AODV and ARAN at varying speeds for 50 nodes

Analysis:

- Here also due to blackhole effect Packet Delivery ratio of AODV is much lesser than ARAN.

(ii) Average Path Length

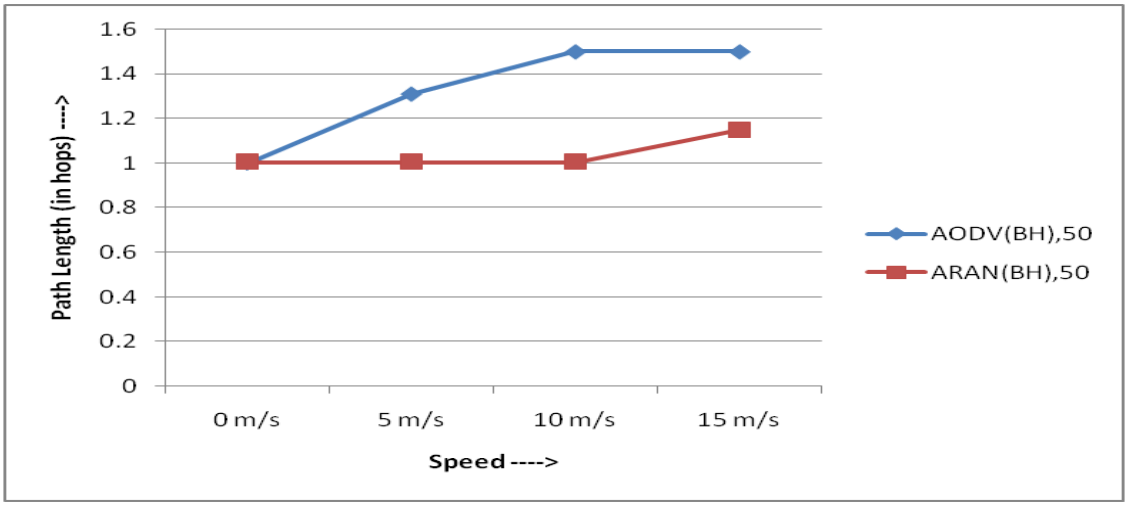

Figure 5.10: Average Path Length of AODV and ARAN at varying speeds for 50 nodes

Analysis:

- Here also AODV has larger Average Path Length due to the presence of malicious node than ARAN.

(iii) Average end-to-end Delay

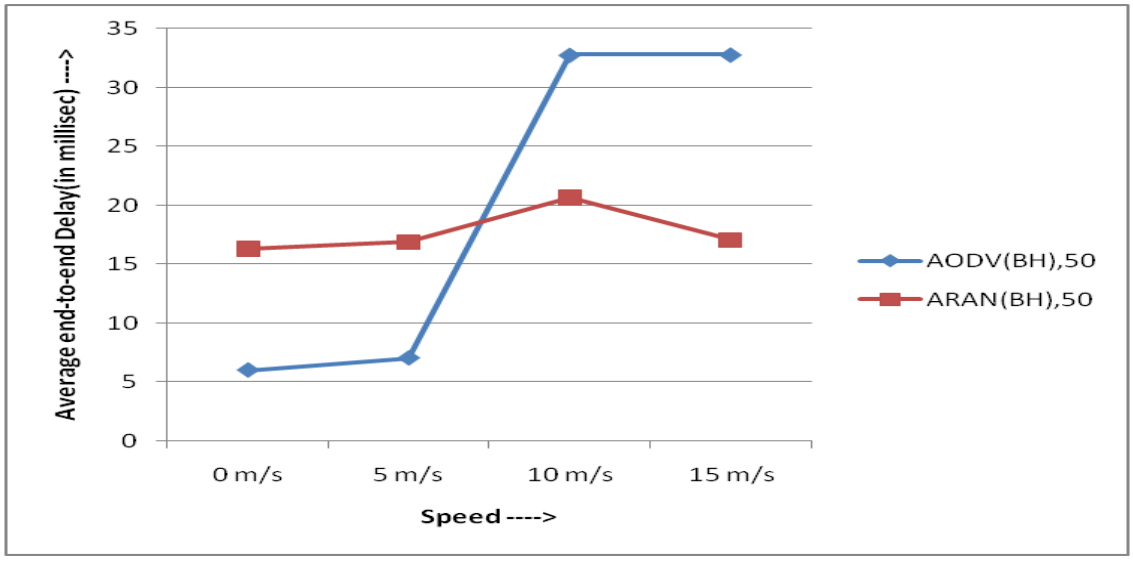

Figure 5.11: Average end-to-end Delay of AODV and ARAN at varying speeds for 50 nodes

Analysis:

- At 0m/s ARAN shows higher delay than AODV because here Average Path Length is same but packet delivery ratio of ARAN is much higher, due to which end-to-end delay increases.
- Similarly at 15m/s, though Average Path Length of AODV increases but the packet delivery ratio is much less.
- At speeds of 10-15m/s there is a high increase in Average Path Length of AODV due to which delay also increases.

(iv) <u>Throughput</u>

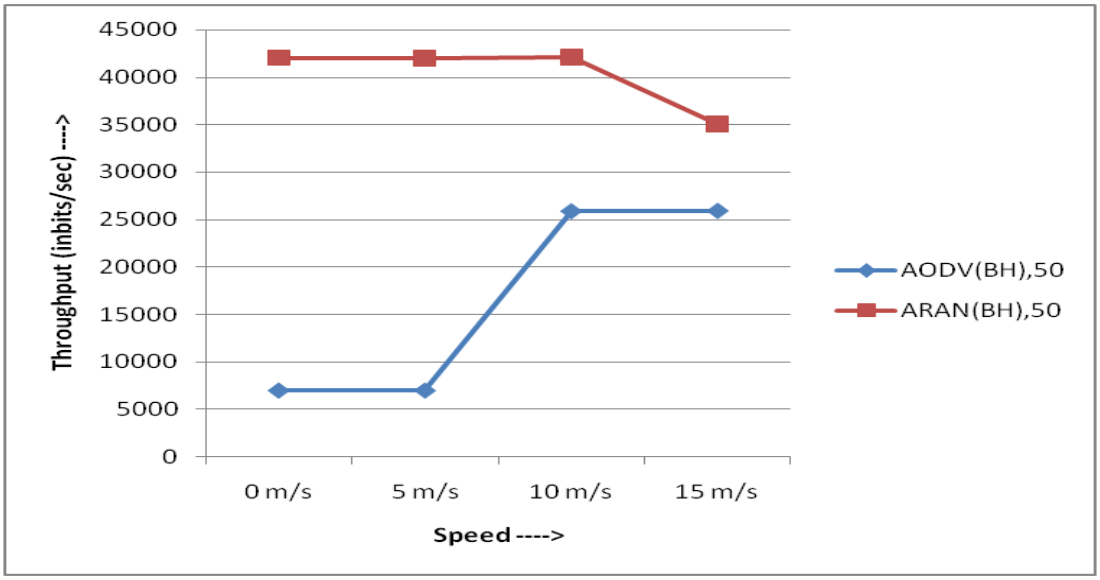

Figure 5.12: Throughput of AODV and ARAN at varying speeds for 50 nodes

Analysis:

- Throughput of ARAN is higher than AODV because of higher packets delivery ratio.

Experiment 4: Blackhole attack simulation results using 70 nodes in 1250*1250 area.

Objective: To find out which protocol perform better under blackhole attack by evaluating- Packet Delivery ratio, Average Path Length, Average end-to-end Delay and Throughput for AODV and ARAN using total 70 nodes at varying node speeds.

Results: The results obtained in this scenario are given in Table 5.7 and 5.8.

Table 5.7: Simulation results of AODV using 70 nodes

Node Speed → / Performance Metric ↓	0m/s	5m/s	10m/s	15m/s
Packet Delivery Ratio	0.833	0.666667	0.666667	0.435
Average Path Length	1.125	1.11	1.223	1.3
Delay	20.4459	22.092	22.154	24.8223
Throughput	40220.33	28497.16	28497.83	32848.17

Table 5.8: Simulation results of ARAN using 70 nodes

Node Speed → / Performance Metric ↓	0m/s	5m/s	10m/s	15m/s
Packet Delivery Ratio	1	1	0.84	0.985
Average Path Length	1	1	1.011	1.011509
Delay	15.063	17.167	18.322	16.114
Throughput	42207.16	42223	35295	35765.33

(i) Packet Delivery Ratio

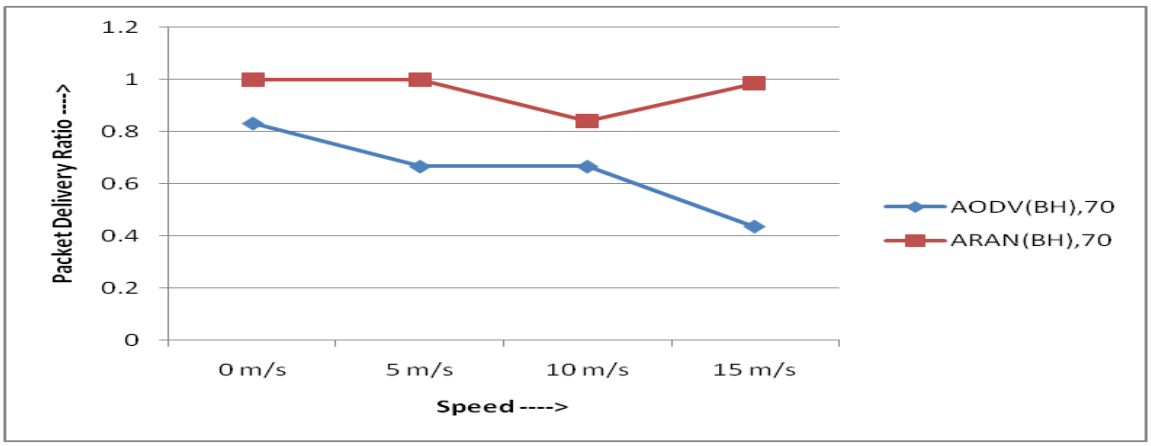

Figure 5.13: Packet Delivery Ratio of AODV and ARAN at varying speeds for 70 nodes

Analysis:

- Blackhole node affects AODV much adversely than ARAN as Packet Delivery Ratio is much lesser in AODV.

(ii) Average Path Length

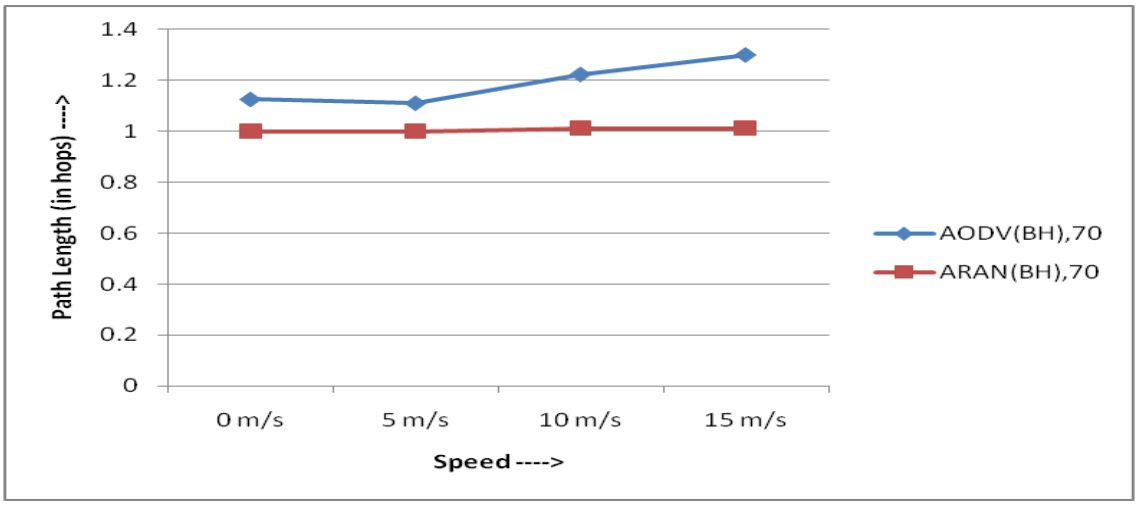

Figure 5.14: Average Path Length of AODV and ARAN at varying speeds for 70 nodes

Analysis:

- Due to malicious effect of blackhole node Average Path Length of AODV is greater than ARAN.

(iii) Average end-to-end Delay

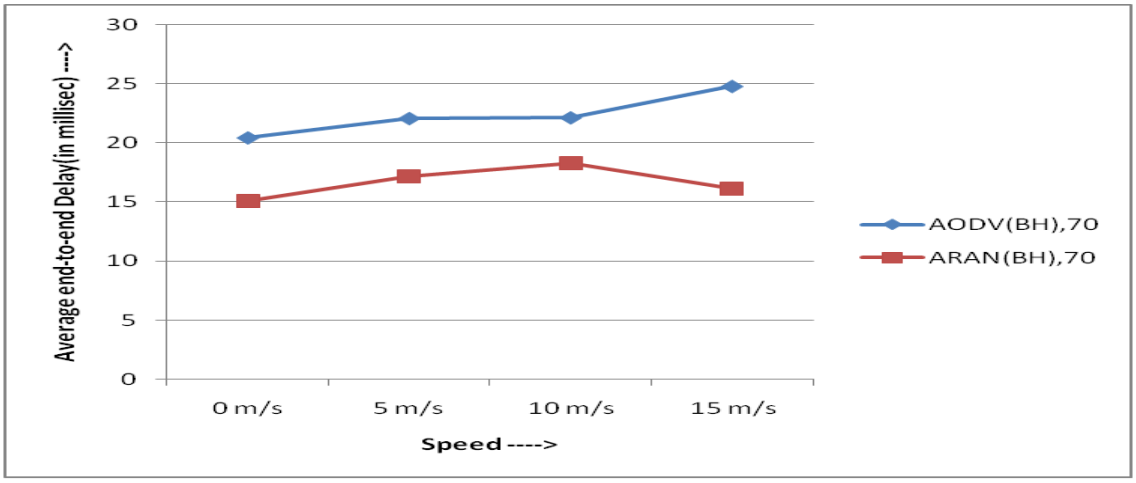

Figure 5.15: Average end-to-end Delay of AODV and ARAN at varying speeds for 70 nodes

Analysis:

- The increase in delay is due to increase of Average Path Length in AODV as discussed in above Figure 5.14.

(iv) <u>Throughput</u>

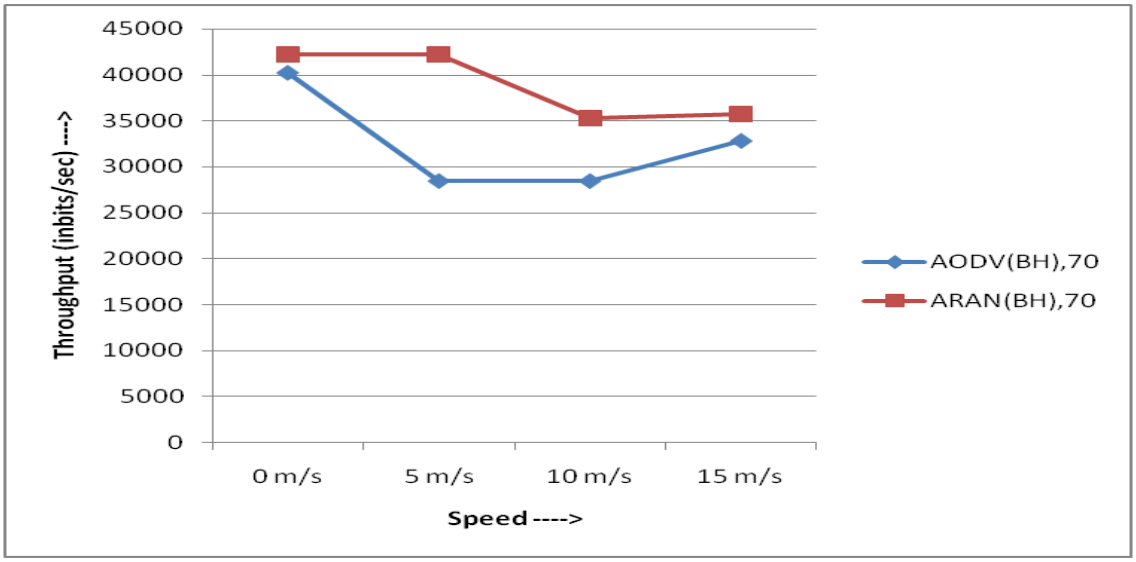

Figure 5.16: Throughput of AODV and ARAN at varying speeds for 70 nodes

Analysis:

- Throughput depends purely on Packet Delivery Ratio, due to which AODV throughput is lesser than that of ARAN.

5.1.1 Discussion

- **<u>Packet Delivery Ratio</u>**: Figures5.1, 5.5, 5.9, 5.13 shows the effect of Blackhole attack on Packet Delivery Ratio (PDR) for AODV and ARAN protocol. It is observed there is not much variation in the PDR parameter at various speeds. It is measured that the packet delivery ratio of AODV decreases at much higher rate than ARAN as the packet delivery ratio of ARAN is between83 to 99%. It is because ARAN can't make the packets to pass through the selfish node, only the packets which have taken the route the selfish node are dropped. But due to effect of fake replies sent by the Blackhole node in AODV packet delivery ratio is between to 16 to 65% because large number of packets are made to pass through the blackhole node and are dropped.

- **Average Path Length:** Figures 5.2, 5.6, 5.10, 5.14 shows the effect of Blackhole attack on Average Path Length for AODV and ARAN protocol. Blackhole node can exploit AODV by creating a fake reply of an extremely short route. Because of the immediate reply sent by the blackhole node, a fake is created. The blackhole node now can set longer route path for the packets that are directed to pass through it. So path elongation is observed in AODV under the blackhole attack. Simulation results show that the maximum Average Path Length while using AODV goes to 3, but ARAN provides shorter Average Path Length approximately between 1 and 1.5. As the speed is increased it is measured that there is a slight increase in path length, it may be due to the change in topology that nodes are constantly changing their positions.
- **Average end-to-end Delay:** Figures 5.3, 5.7, 5.11, 5.15 shows the effect on average end-to-end delay measured for the AODV and ARAN protocol under Blackhole attack. It has been observed that, delay is directly proportional to packet delivery ratio and average path length; so the average delay varies depending upon these values. Also when measured at different speeds delay shows the same variations.
- **Throughput:** Figures5.4, 5.8, 5.12, 5.16 shows the effect of Blackhole attack on the network throughput. When measured at different speeds slight variations are observed in throughput value. Throughput is directly proportional to the bits received and inversely to the time. So depending upon PDR and delay parameters, throughput shows the variation. The throughput of the network decreases more in AODV than ARAN due to decrease in Packet Delivery ratio.

5.2 Security analysis of AODV and ARAN under IP-Spoofing (IPS) Attack

IP-Spoofing on AODV and ARAN is explained in Appendix B.

Experiment 5: Packet Delivery Ratio

Objective: In this simulation, Packet Delivery ratio has been measured for the AODV and ARAN by implementing IP-Spoofing attack.

Results: The results obtained for AODV and ARAN under the attack in this scenario is given in Table 5.9

Table 5.9: Packet delivery Ratio of AODV and ARAN under spoofing attack

Protocol → / Node Speed ↓	AODV(IPS)	ARAN(IPS)
0 m/s	0.998	0
5 m/s	0.992	0
10 m/s	0.988	0
15 m/s	0.99	0

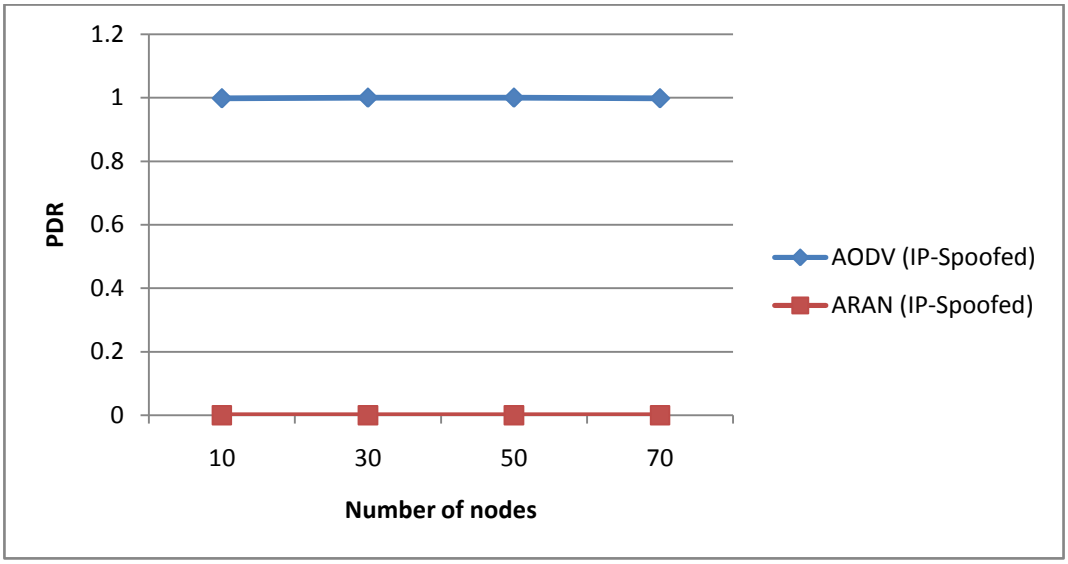

Figure 5.17: Packet delivery ratio of AODV & ARAN under IP-Spoofing attack.

Analysis:

- While using AODV protocol it has been found that nearly 99.9% of spoofed packets reach the destination. Thus AODV is vulnerable to spoofing attack. But in similar simulation environment under ARAN protocol all the spoofed packets are dropped i.e. no packets reach the destination. Thus ARAN is safe against spoofing attack.

5.2.1 Discussion

- AODV is highly vulnerable to IP-Spoofing attack as compared to ARAN which is safe against the attack. It is because in AODV a node can easily send packets in the network using some other node's identity, but in ARAN protocol, each node checks the identity of its adjacent node from which it is receiving some information. If any fault is detected in verification process, all the packets are dropped without reaching the destination.

5.3 Security Analysis of ARAN and Improved ARAN (i-ARAN) under DDOS Attack

Experiment 6: Packets Delivered

Objective: Total number of packets delivered by ARAN and improved ARAN has been compared for three simulation time- 1, 2 and 3 seconds at 15m/s mobility.

Results: Results are shown in Figure 5.18.

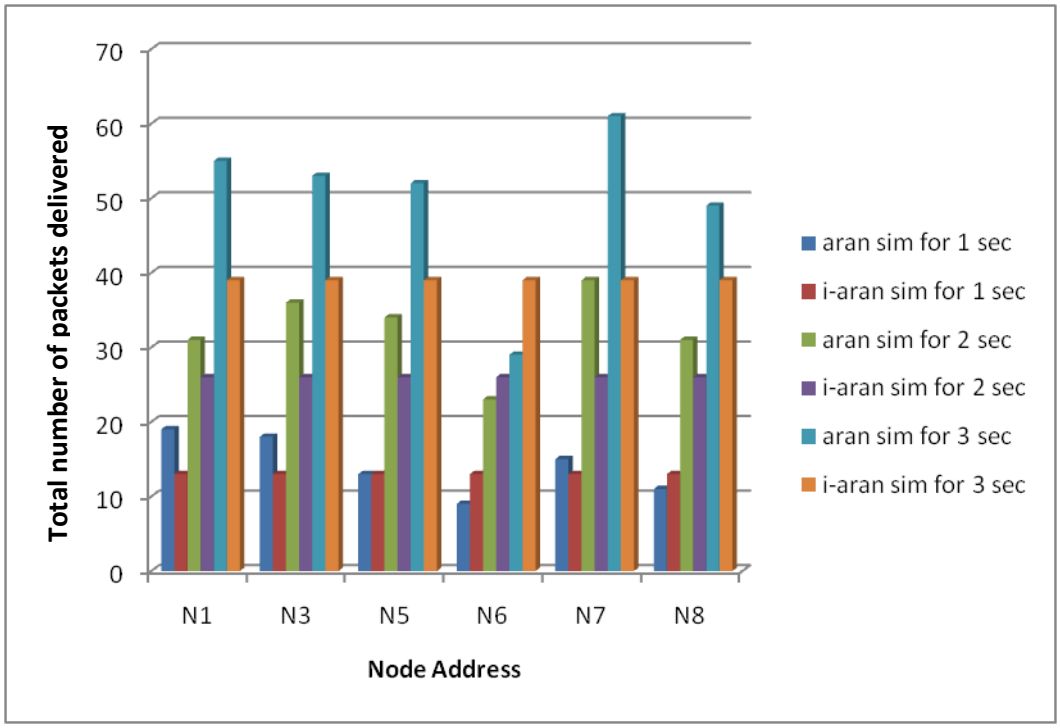

Figure 5.18: Packets delivered by ARAN and i-ARAN under DDOS attack

Analysis:

- Under DDOS attack on ARAN few packets are received from genuine node 6at the destination because of the congestion created by other selfish nodes in the network.
- Packet Delivery Ratio of improved ARAN (i-ARAN) for all the nodes is constant. By limiting the number of packets sent in the network congestion can be prevented, and packet delivery ratio from all the nodes is kept constant. Due to this node 6 packets can now reach the destination.

Experiment 7: Average end-to-end delay

Objective: Average end-to-end delay of ARAN and improved ARAN has been compared for three simulation time- 1, 2 and 3 seconds at 15m/s mobility.

Results: Results are shown in Figure 5.19.

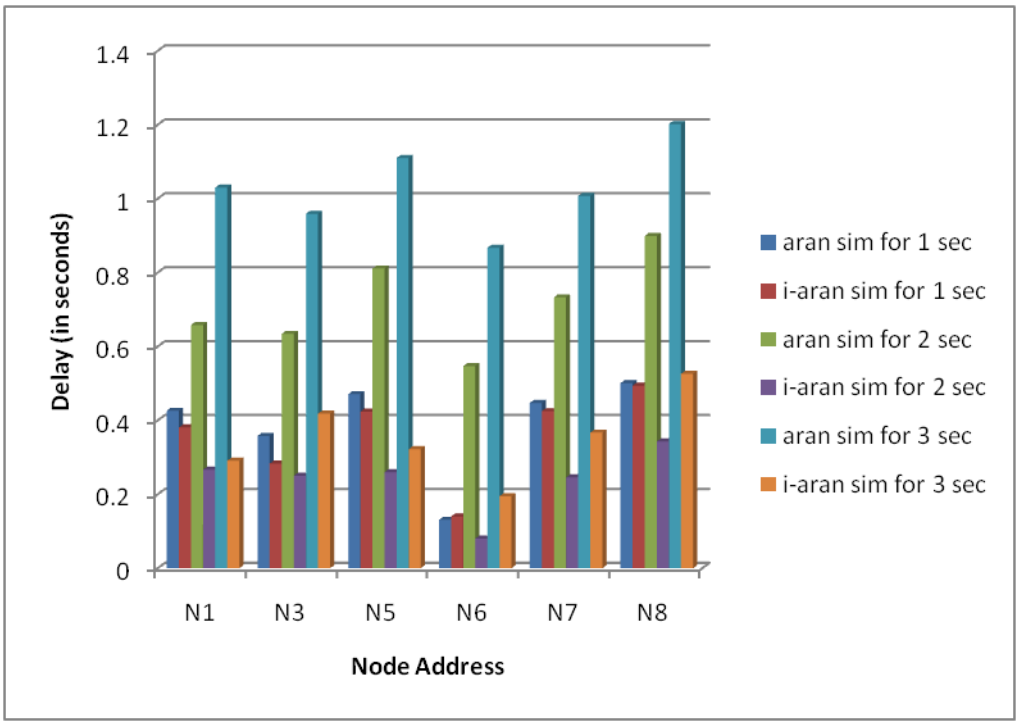

Figure 5.19: Average end-to-end delay for ARAN and i-ARAN under DDOS attack

Analysis:

- Average delay for improved ARAN is lesser than that of the ARAN. Except in case of 1 second simulation time for node 6, where delay is slight more than in ARAN. It is due to the delivery of packets from node 6 at the destination node while using i-ARAN; which was very less while using ARAN.
- Average end-to-end delay for improved ARAN decreases as number of packets reaching the destination is now limited by the threshold value. So there is no congestion in the network and the packets can reach the destination node fast.

Experiment 8: Throughput

Objective: Throughput of ARAN and improved ARAN has been compared under DDOS attack for three simulation time- 1, 2 and 3 seconds.

Results: Figure 5.20 shows the Throughput of the network under same scenario.

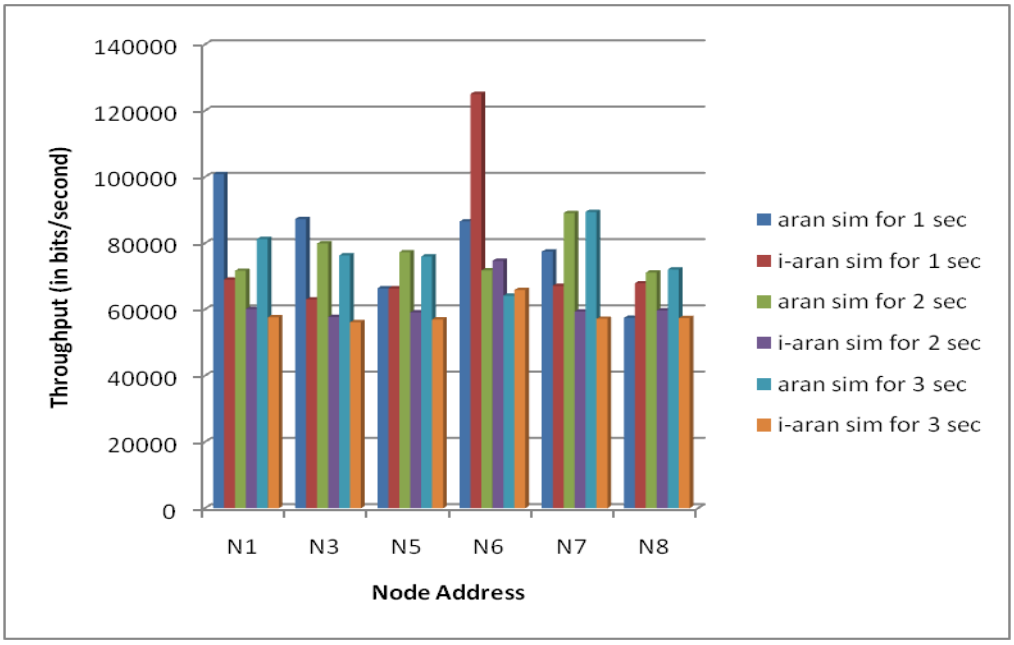

Figure 5.20: Throughput for ARAN and i-ARAN under DDOS attack

Analysis:

- Net throughput of i-ARAN is 100% because limited packets are sent per second by each node in the network and these all packets reaches the destination.
- In ARAN there is no such limit; any node can send large number of packets. So overall throughput of the network of ARAN may appears to be greater than the i-ARAN but ARAN denies the services of other legitimate nodes (like node 6).
- Throughput depends directly on number of packets received and depends inversely on the delay in receiving these packets. So in some cases throughput from node 6 of i-ARAN is more as compared to ARAN depending upon these two metrics.

5.3.1 Discussion

- **Packet Delivered:** Figures 5.18 shows the effect of DDOS attack on total number of packets delivered for ARAN and i-ARAN at15m/s mobility at various simulation times. Results at speeds of 0m/s, 5m/s and 10m/s are shown in Appendix C. Simulation results show that while using ARAN there is congestion in the network due to which only few packets from the genuine node 6 are able to reach to the destination node. But by providing the threshold limit constant numbers of packets are received from each node and there is no congestion in the network.

- **Average end-to-end Delay:** Figures 5.19shows the effect of DDOS attack on average end-to-end delay for ARAN and i-ARAN at 15m/s mobility at various simulation times. Results at speeds of 0m/s, 5m/s and 10m/s are shown in Appendix C. Simulation results show that delay of ARAN is higher than i-ARAN because of the large number of packets sent from the selfish nodes which creates congestion in the network. So with limited packets sent in i-ARAN there is no congestion in the network and delay is lesser. But in some cases at node 6, delay of i-ARAN is more than that of ARAN. It is because earlier there was very less Packet delivery ratio from legitimate node 6, but with i-ARAN packets can now reach the destination node.
- **Throughput:** Figures 5.20 shows the effect of DDOS attack on throughput for ARAN and i-ARAN at 15m/s mobility at various simulation times. Results at speeds of 0m/s, 5m/s and 10m/s are shown in Appendix C. Simulation results show that the net throughput of i-ARAN is 100% because limited packets are sent per second by each node in the network and these all packets reaches the destination.
- **Energy Consumption:** It has been observed that under DDOS attack when simulation time is of 1 second, energy consumption for ARAN is .263 mWhr and for i-ARAN is .262 mWhr while in normal condition it is .256 mWhr. While at 2 seconds of simulation time it is .525 mWhr for ARAN and .520 mWhr for i-ARAN while in normal condition it is .509 mWhr. Similarly for 3 seconds using of simulation time it is .786 mWhr for ARAN and .778 mWhr for i-ARAN while in normal condition it is .761 mWhr. After analysis it is concluded that i-ARAN can resists the DDOS attack without any increase in the energy consumption as compared to ARAN under DDOS attack.

5.4 Chapter Summary

In this chapter simulation results for AODV and ARAN under Blackhole and IP-Spoofing attacks are presented and discussed. Analysis of results shows that ARAN is more secure against both the attacks than AODV protocol. Since ARAN is safe against blackhole attack unless selfish nodes are present, so ARAN has been made secure against DDOS attack by introducing i-ARAN. Further ARAN and i-ARAN are analyzed under the DDOS attack.

CHAPTER 6

CONCLUSION AND FUTURE WORK

Variety of attacks are possible on Ad hoc network routing protocols, through modification of routing message or fabrication of false messages or impersonation of other node's identity, thus allow attackers to influence a victim's selection of routes and cause dropping of packets without making them to reach to the destination. In this research work it has been observed that Blackhole attack can exploit the AODV routing protocol much adversely than the ARAN. Blackhole attack in ARAN is only limited to the selfish nodes which may not forward the packet passing through them in the network and simply drops them. Also it has been observed that ARAN is safe against IP-Spoofing attack but AODV is highly vulnerable to the attack. Finally by analyzing the results it has been concluded that ARAN provides secure routing as compared to AODV against both the attacks.

It has been studied that though ARAN prevents from many attacks like message modification, impersonation attack and non-repudiation for false message fabrication, but is vulnerable to DDOS attack by the authenticated selfish nodes. A technique was proposed and implemented to prevent ARAN from DDOS attack. The technique has been analyzed against DDOS attack and results of ARAN and i-ARAN have been compared and it shows that i-ARAN performs well under DDOS attack compared to ARAN. Results show that constant Packet Delivery ratio is obtained. Since there is no congestion in the network, Average end-to-end Delay decreases and Throughput is approximately constant for all the nodes. Also the energy consumption of i-ARAN is nearly same as that of ARAN under DDOS attack. It signifies that i-ARAN doesn't consume more energy as compared to ARAN under DDOS attack.

As ARAN spends longer time in verifying signatures and additional energy is spent during ARAN's cryptographic operations, so for the future work ARAN may be checked by applying other public key cryptographic schemes which may reduce signature verification delay time and energy costs.

REFERENCES

Abliz, M. (2011). Internet denial of service attacks and defense mechanisms.Technical Report TR-11-178.University of Pittsburgh.

Bajaj, L., Takai, M., Ahuja, R., Tang, K., Bagrodia, R., andGerla, M. (1999). Glomosim: A scalable network simulation environment. *UCLA Computer Science Department Technical Report, 990027*, 213.

Benetti, D., Merro, M., and Vigano, L. (2010, September). Model checking ad hoc network routing protocols: Aran vs. endaira. In 8th IEEE International Conference on *Software Engineering and Formal Methods (SEFM),* pp. 191-202, 2010.

Dokurer, S. (2006).*Simulation of Black hole attack in wireless Ad-hoc networks*: Atılım University.

Garg, A., and Beniwal, V. (2012).A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks. *International Journal of Advanced Research in Computer Science and Software Engineering*, ***2*****(9)**:145-148.

Goyal, N., and Gaba, A. (2013).A Review over MANETS Issues and Challenges.*International Journal of Enhanced Research in Management & Computer Applications, **2**:*16-28*.*

Gong, C., Wu, S., and Jing, Y. (2012, October).ARAN protocol analysis and improvement.Proceedings of theSystem Science, Engineering Design and Manufacturing Informatization (ICSEM) 3rd International Conference, Vol 2, pp. 347-350.

Gowda, S. R., and Hiremath, P. S. (2013).Review of Security Approaches in Routing Protocol in Mobile Adhoc Network. *International Journal of Computer Science Issues (IJCSI)*, ***10*****(1)***.*

Kamra, P., Singh, T.P., and Singh, R.K. (2013).Preventing Black hole Attacks in Mobile adhoc Networks: A Review.Proceedings of the Intl. Conf. on Recent Trends In Computing and Communication Engineering – RTCCE.

Kataria, J., Dhekne, P. S., and Sanyal, S. (2006, December). A Scheme to Control Flooding of Fake Route Requests in Ad-hoc Networks.Proceedings of theInternational Conference on Computers and Devices for Communications, CODEC-06.

Kathirvel, A., & Srinivasan, R. (2009).Global Mobile Information System Simulator in Fedora Linux. ACM online Computer Communication Review.

Kumar, J., Kulkarni, M., and Gupta, D. (2010, December).Secure routing protocols in ad hoc networks: A review. Special Issue of IJCCT, 2(2), 3.

Mahmoud, A., Sameh, A., and El-Kassas, S. (2005). Reputed authenticated routing for ad hoc networks protocol (reputed-ARAN). Proceedings of the International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.

Mehla, S., Gupta, B., and Nagrath, P. (2010).Analyzing security of Authenticated Routing Protocol (ARAN).*International Journal on Computer Science and Engineering,* **2(3):**664-668.

Nilsson, T. (2002).A Tutorial on GloMosim. *Department of Computing Science.University of Umea*.

Ning, P., and Sun, K. (2005). How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols*. Ad Hoc Networks,* **3(6):** 795-819.

Reddy, D., Kundra, K., Babu, M. R., and Kumar, L. P. (2012). Prevention of Routing Attack in Mobile Ad-Hoc Networks: A comparative study. *IJRCCT,* **1(5)**:228-237.

Ruiz, J.-C., Friginal, J., de-Andrés, D., and Gil, P. (2008). Black Hole Attack Injection in Ad hoc Networks. *Fault Tolerance Systems Group (GSTF).*

Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., and Belding-Royer, E. M. (2002).A secure routing protocol for ad hoc networks*.* Proceedings of the 10th IEEE International Conference on Network Protocols.

Sanzgiri, K., LaFlamme, D., Dahill, B., Levine, B. N., Shields, C., and Belding-Royer, E. M. (2005).Authenticated routing for ad hoc networks. *IEEE Journal on Selected Areas in Communications,* **23(3):**598-610.

Sinha, S. K., Singh, R., Pandey, K., and Sahu, M. K. (2013). Distributed Denial of Service attack Prevention using Critical Link Method in MANET. *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE),* **2(3):** pp: 325-328.

Specht, S. M., and Lee, R. B. (2004). Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures*.*Proceedings of the ISCA PDCS.

Ullah, I., and Rehman, S. U. (2010).Analysis of Black Hole attack on MANETs Using different MANET routing protocols. Master Thesis, School of Computing Blekinge Institute of Technology, Sweden*.*

Vigna, G., Gwalani, S., Srinivasan, K., Belding-Royer, E. M., and Kemmerer, R. A. (2004).An intrusion detection tool for AODV-based ad hoc wireless networks*.* Proceedings of the Computer Security Applications Conference.

Von Mulert, J., Welch, I., and Seah, W. K. (2012). Security threats and solutions in MANETs: A case study using AODV and SAODV. *Journal of Network and Computer Applications,* **35(4):**1249-1259.

YAU, P., Hu, S., and Mitchell, C. J. (2007). Malicious attacks on ad hoc network routing protocols. *Information Security Group*.

Yi, P., Dai, Z., Zhang, S., and Zhong, Y. (2005). A new routing attack in mobile ad hoc networks. *International Journal of Information Technology,* **11(2):**83-94.

Zhou, Z. (2007). Security enhancement over ad-hoc AODV routing protocol.Tsinghua University, Beijing.

APPENDIX A

BLACKHOLE ATTACK

According to (Dokurer, 2006) implementation of the attack is done by considering the RREQ function because Black Hole behavior is carried out as the malicious node receives an RREQ packet. The blackhole node will then send the RREP packet having sequence number set to 4294967295 and hop count set to 1. The following changes have been made in **aodv.pc** file of glomosim:

```
voidRoutingAodvHandleRequest(GlomoNode *node, Message *msg, intttl)

{….

RoutingAodvReplaceInsertRouteTable(

rreqPkt->srcAddr,

        4294967295,                    //highest sequence number

            1,                         //hopcount

rreqPkt->destAddr,          //dest IP address

        simclock() + ACTIVE_ROUTE_TO,

          TRUE, TRUE,

&aodv->routeTable);

…….}
```

In ARAN protocol there is no such parameters used like sequence number. In the ARAN code blackhole packet dropping effect can be observed by giving the number of malicious nodes. Here is the code that was used in **aran.pc** file of glomosim:

```
//Setting the selfish nodes' percentage

MaliciousNodesPercentage=20;

//Setting the malicious nodes
```

```
aran->isMalicious = 0;
if(maliciousNodesPercentage>= 10)
   {
if(node->nodeAddr % 10 == 5)
aran->isMalicious = 1;
   }
if(maliciousNodesPercentage>= 20)
   {
if(node->nodeAddr == 6)
aran->isMalicious = 1;
   }
if(maliciousNodesPercentage>= 30)
{ if(node->nodeAddr % 10 == 7)
aran->isMalicious = 1;
   }
if(maliciousNodesPercentage>= 40)
   {       if(node->nodeAddr % 10 == 8)
aran->isMalicious = 1;}
If(aran->isMalicious)
{return;}
Else{ forward the packet;}
```

APPENDIX B

IP-SPOOFING ATTACK

In spoofing attack RREQ is send by modifying the source address to any other's node address (here node 3 address is used by attacking nodes as the source node's address).

- Code of **aodv.pc** file that has been modified is shown as below:

```
voidRoutingAodvInitiateRREQ(GlomoNode *node, NODE_ADDR destAddr)
    {…
    rreqPkt->srcAddr = 3;
    …..}
    voidRoutingAodvRetryRREQ(GlomoNode *node, NODE_ADDR destAddr)
    {….
    rreqPkt->srcAddr = 3;
    ……}
```

- For ARAN protocol code of **aran.pc** has been modified as:

```
voidRoutingAranHandleData(GlomoNode *node, Message *msg,
NODE_ADDR destAddr)
{…..
NODE_ADDR sourceAddress = ipHeader->ip_src = 3;
…}
voidRoutingAranInitiateRDP(GlomoNode *node, NODE_ADDR destAddr)
{….
if(DEMO) printf("ARAN: Node %d: Initiating RDP\n", 3);
…}
```

APPENDIX C

SECURITY ANALYSIS OF ARAN AND i-ARAN UNDER DDOS ATTACK

C.1 Results at the speed of 0m/s (no mobility)

(i) Packet Delivered

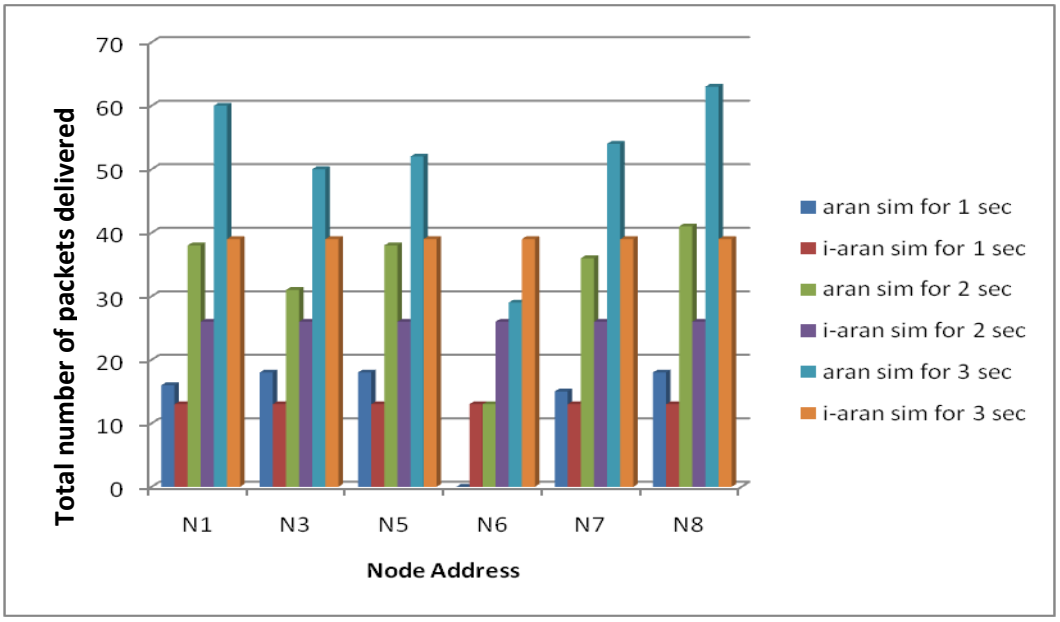

Figure C.1: Total number of packets delivered by ARAN and i-ARAN at 0m/s

(ii) Average end-to-end Delay

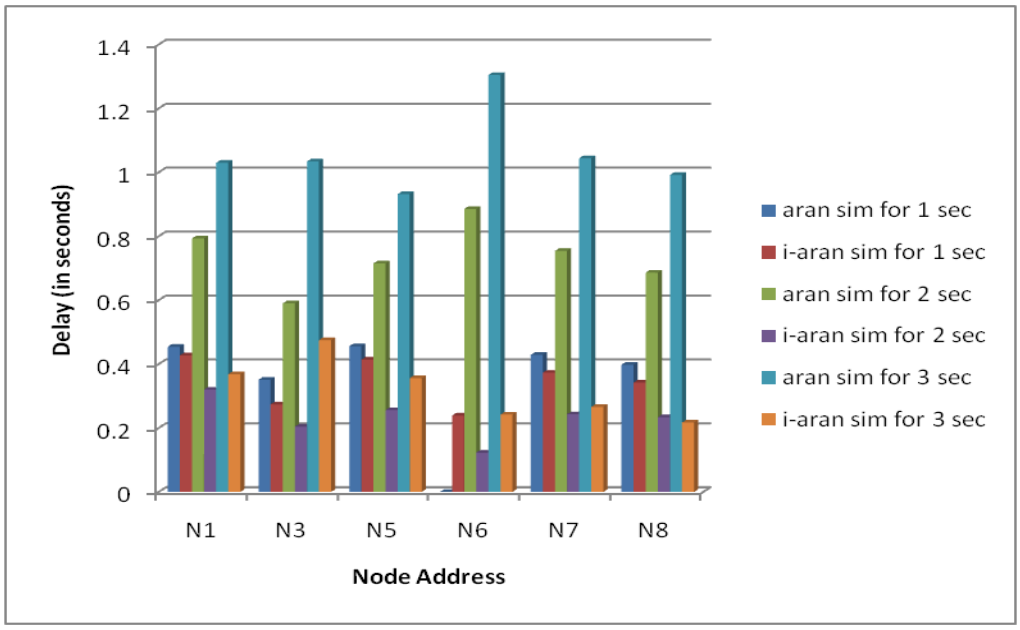

Figure C.2: Average end-to-end Delay of ARAN and i-ARAN at 0m/s

(iii) Throughput

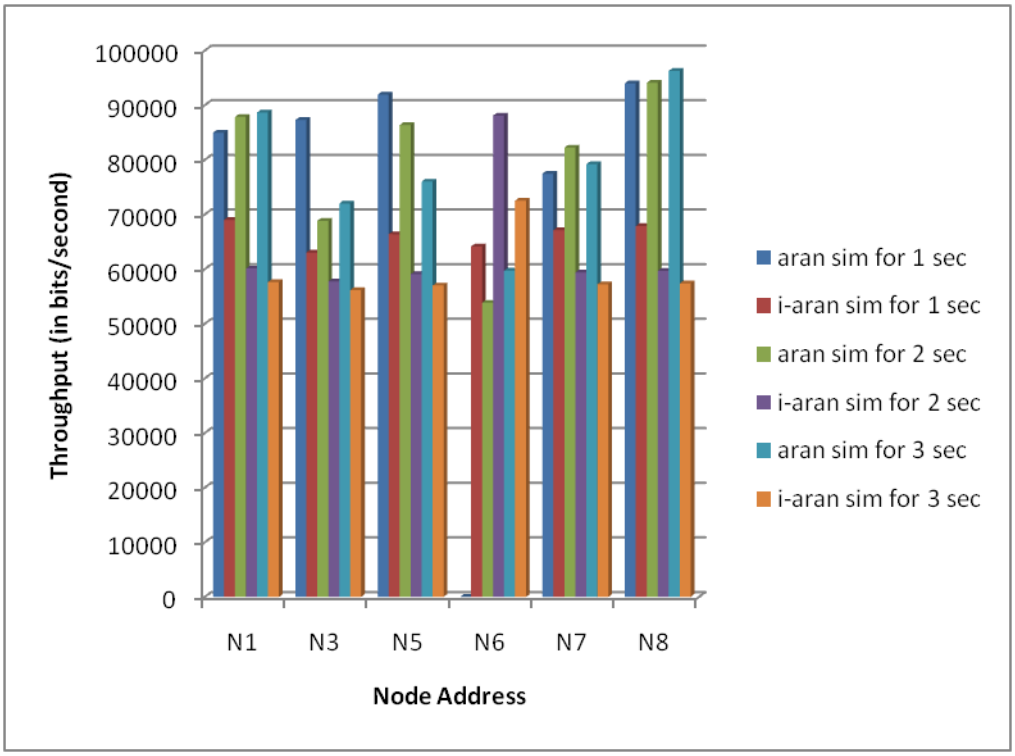

Figure C.3: Throughput of ARAN and i-ARAN at 0m/s

C.2 Results at the speed of 5m/s

(i) Packets Delivered

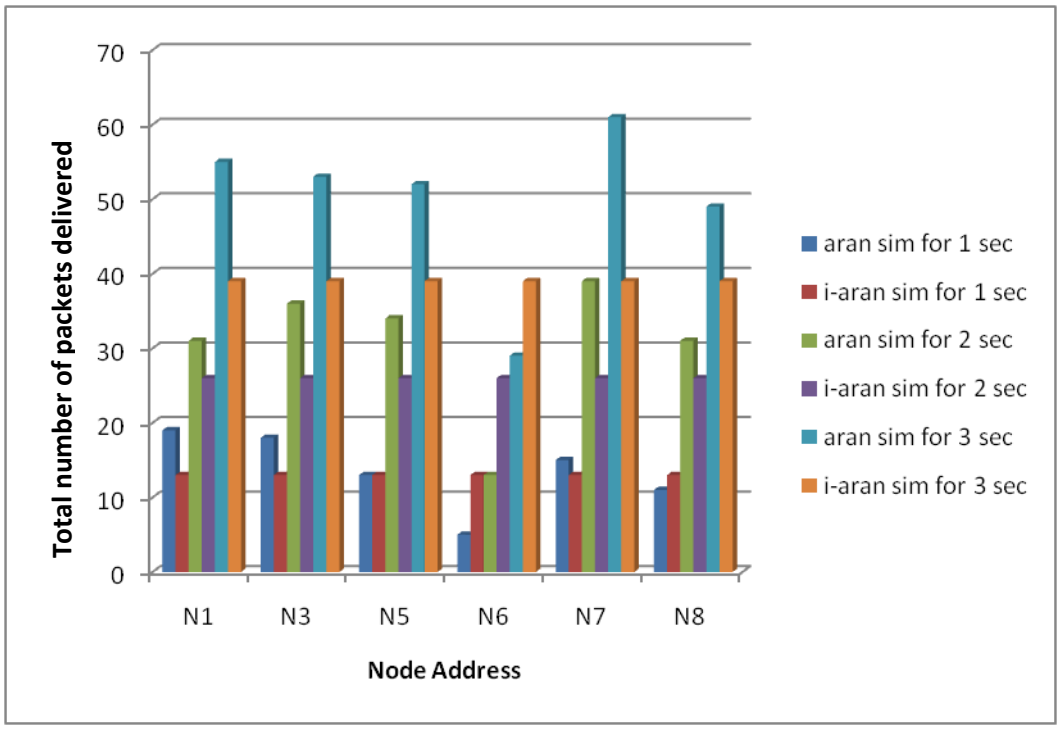

Figure C.4: Total number of packets delivered by ARAN and i-ARAN at 5m/s

(ii) Average end-to-end Delay

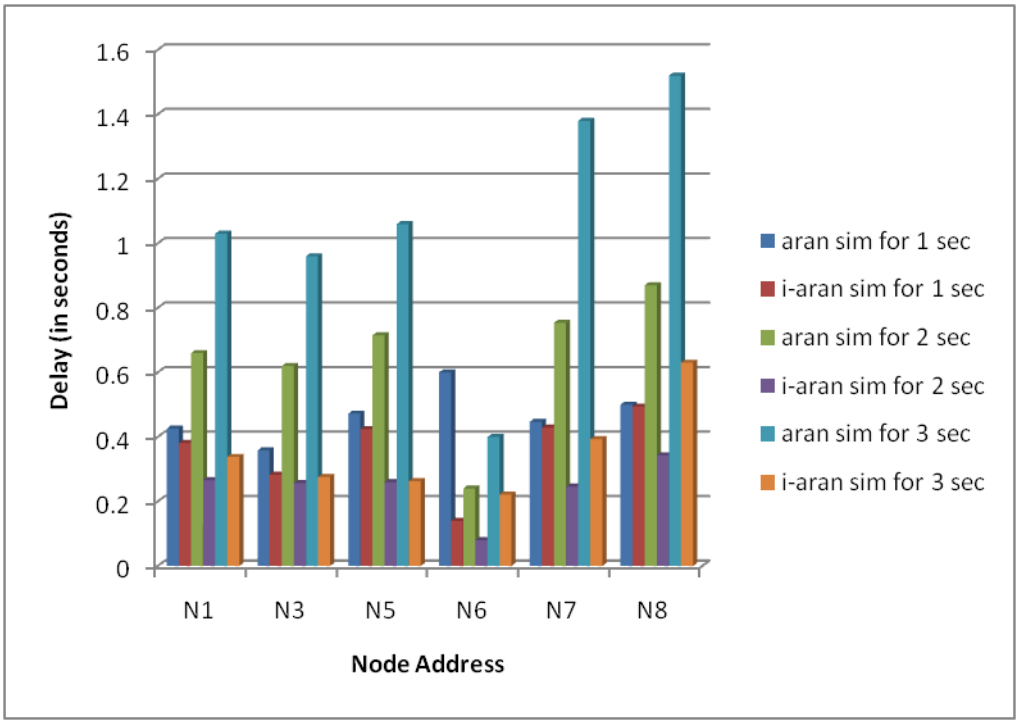

Figure C.5: Average end-to-end Delay of ARAN and i-ARAN at 5m/s

(iii) Throughput

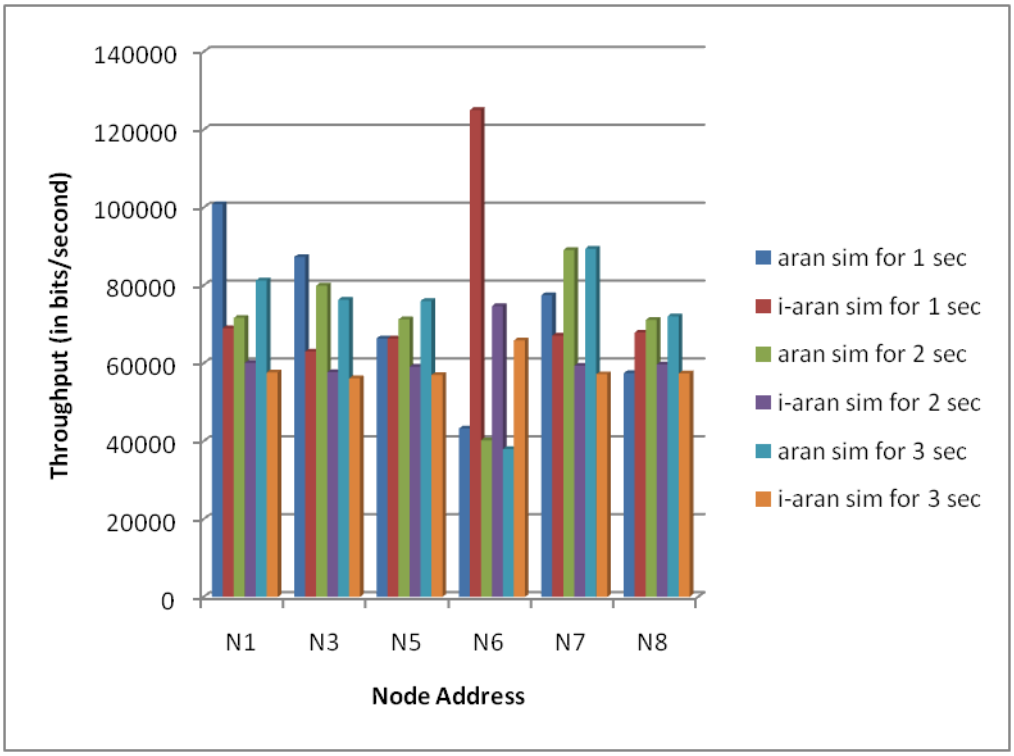

Figure C.6: Throughput of ARAN and i-ARAN at 5m/s

C.3 Results at the speed of 10m/s

(i) Packet Delivered

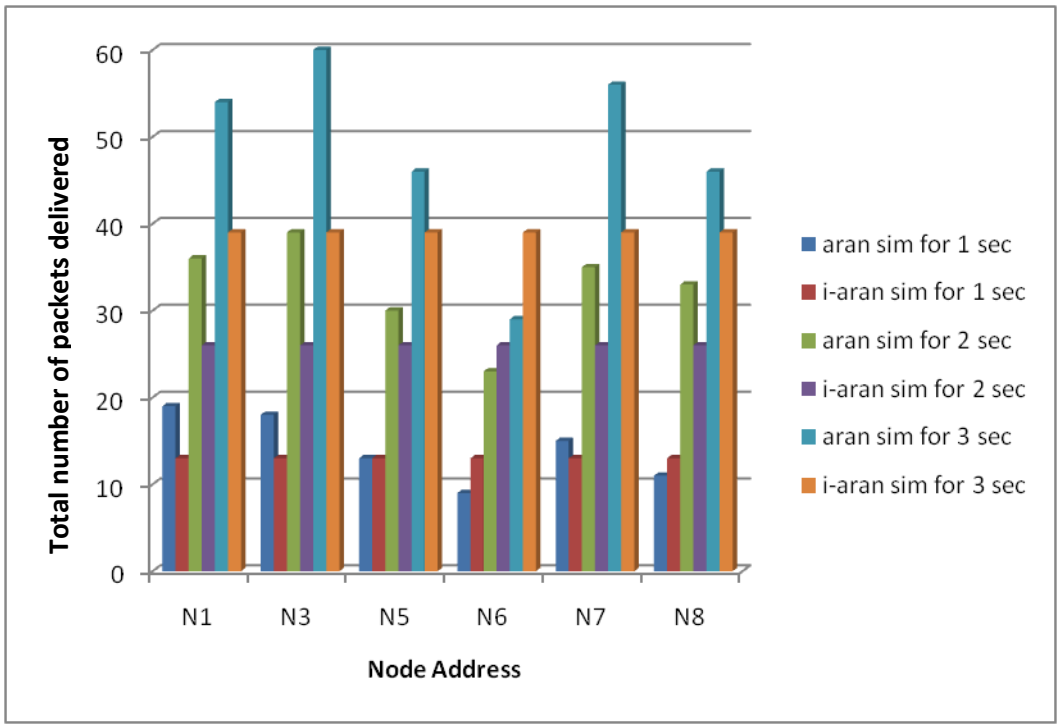

Figure C.7: Total number of packets delivered by ARAN and i-ARAN at 10m/s

(ii) Average end-to-end Delay

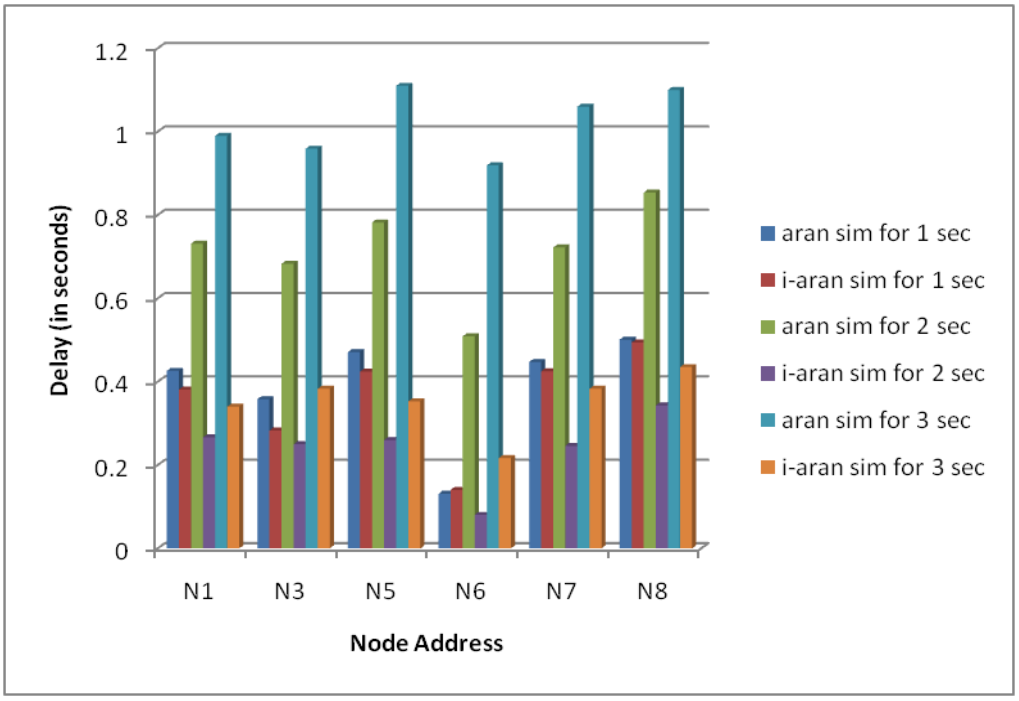

Figure C.8: Average end-to-end Delay of ARAN and i-ARAN at 10m/s

(iii) Throughput

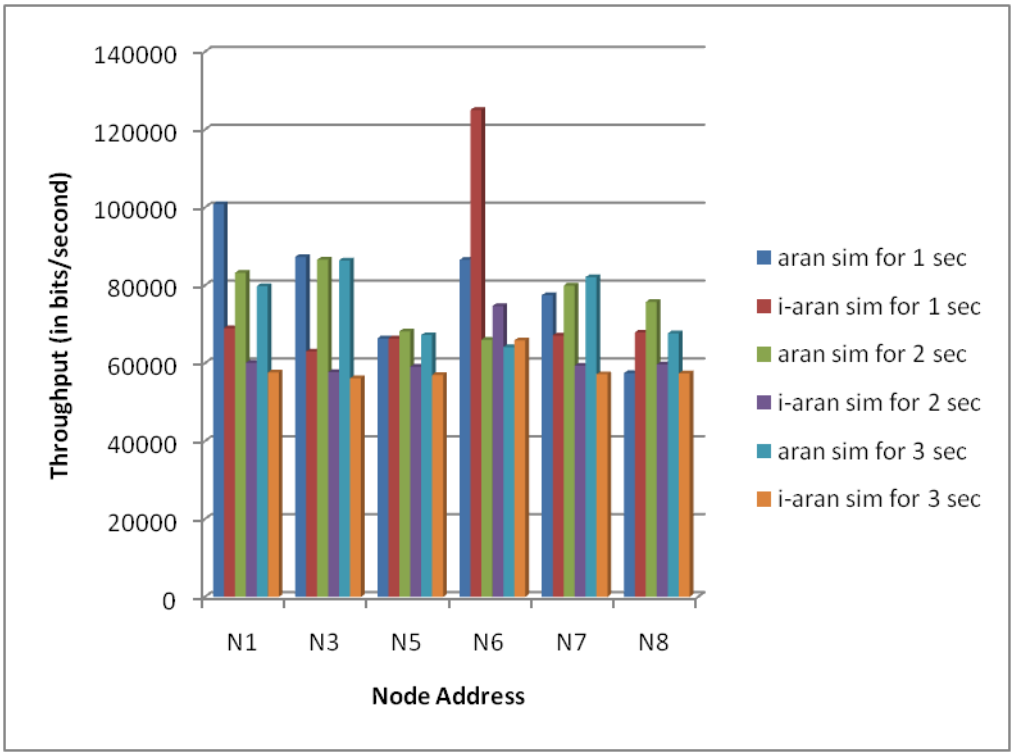

Figure C.9: Throughput of ARAN and i-ARAN at 10m/s

APPENDIX D

SCRIPTS USED

D.1 Packet Delivery Ratio

This shell script pdr.sh file is used to measure the packet delivery ratio. The Glomosim output file, glomo.stat is being passed to this shell script to collect values related to this metric. As stated by (Kathirvel, &Srinivasan, 2009) the shell script that can be used is:

```
Cat $1 | grep App | grep Total | grep packets | awk –f pdr.awk
```

Then, the results of this shell script are redirected to another Linux AWK script to do the actual calculation. Its content is as follows:

pdr.awk:

```
BEGIN { sumcountrcv = 0;

sumcountsent=0 }

{

if ($4=="AppCbrServer," && $10=="received:"){sumcountrcv+=$11}

if ($4=="AppCbrClient," && $10=="sent:"){sumcountsent+=$11}}

END { printf("Packet received = %d \n",sumcountrcv);

printf("Packet sent = %d \n",sumcountsent);

printf("PDR = %f \n",sumcountrcv/sumcountsent)}
```

Now the output can be collected by using the command: **sh pdr.sh glomo.stat**

D.2 Average Path Length

This shell script pl.sh file is used to measure the Average Path Length metric. The Glomosim output file, glomo.stat, is being passed to this shell script to

collect values related to this metric. As stated by (Mahmoud, Sameh, & El-Kassas, 2005) the shell script that can be used is:

```
Cat $1 | grepRoutingAran | awk –f pl.awk
```

Then, the results of this shell script are redirected to another Linux AWK script to do the actual calculation. Its content is as follows:

pl.awk:

```
BEGIN { sumdatapktshops = 0;

sumdatapkts = 0 }

{if ($4=="RoutingAran," && $7=="Data" && $8=="Txed")

{sumdatapkts+=$10}

if ($4=="RoutingAran," && $7="Data" && $9=="Hops")

{sumdatapktshops+=$11}}

END { if (sumdatapktshops>0)

{printf("Routing Data Packets Hops = %f \n",sumdatapktshops);

printf("Routing Data packets = %f \n",sumdatapkts);

printf("Average Path Length  = %f \n",sumdatapkts/sumdatapktshops)}}
```

Now the output can be collected by using the command: **sh pl.sh glomo.stat**

D.3 Average end-to-end Delay

This shell script file delay.sh is used to measure the average end-to-end delay metric. The Glomosim output file, glomo.stat, is being passed to this shell script to collect values related to this metric. As stated by (Kathirvel, &Srinivasan, 2009) the shell script that can be used is:

```
cat $1 | grepAppCbrServer | grep end-to-end | grep delay | awk -f delay.awk
```

Then, the results of this shell script are redirected to another Linux AWK script to do the actual calculation. Its content is as follows:

delay.awk:

```
BEGIN{sumdelay=0;

countdelay=0;}

{sumdelay +=$10;

countdelay++;}

END{printf("Average Delay = %f \n",

sumdelay/countdelay);}
```

Now the output can be collected by using the command: **sh delay.sh glomo.stat**

D.4 Throughput

This shell script th.sh file is used to measure the throughput metric. The Glomosim output file, glomo.stat, is being passed to this shell script to collect values related to this metric

```
Cat $1 | grepAppCbrServer | awk –f th.awk
```

Then, the results of this shell script are redirected to another Linux AWK script to do the actual calculation. Its content is as follows:

th.awk:

```
BEGIN{Th=0;}

{If($6=”Throughput”)

Th+=$12;}

END{Printf(“Throughput: %f”, th/6);}
```

Now the output can be collected by using the command: **sh th.sh glomo.stat**