Evaluation of AODV and DSR Performance Using Jellyfish Delay Variance Attack with Self-Cooperative Trust Scheme

Thesis submitted in partial fulfilment of the requirements for the award of degree of

Master of Technology

in

Computer Applications

Submitted By

Deepika

(601634006)

Under the supervision of:

Dr. Sharad Saxena

Associate Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY

PATIALA – 147004

June 2018

CERTIFICATE

I hereby certify that the work, which is being given in this thesis, entitled **"*Evaluation of AODV and DSR Performance Using Jellyfish Delay Variance Attack With Self-Cooperative Trust Scheme*"**, in partial fulfilment of the requirements submitted in Computer Science & Engineering Department of **Thapar Institute of Engineering and Technology**, Patiala for the award of **Master of Technology** in Computer Science and Engineering is a bona fide record of my own work completed under the supervision of ***Dr. Sharad Saxena.*** I have additionally referred to the reference about the text(s)/figure(s)/table(s) from where they have been taken.

The issue introduced in this thesis is not been submitted anywhere else for the honour of some other degree or recognition from any organization.

Signature: _____

Deepika

This is to guarantee that the above explanation made by the competitor is right to the best of our insight.

Signature: _____

Dr. Sharad Saxena

Associate Professor

CSED

ACKNOWLEDGEMENT

I acknowledge my debt to those who have contributed significantly to my efforts in this research work and dissertation. I would like to express deep sense of gratitude to **Dr. Sharad Saxena,** Associate Professor, CSED who have been a great source of inspiration, guidance and moral support for me. It would never be possible for me to continue this study without their constant support, encouragement and positive attitude. It has been a great pleasure and experience working with them.

I am also grateful to **Dr. Maninder Singh**, Head, CSED for his inspiration. He sets high principles for his students and motivates and guides them to meet those principles.

I would also like to thank PG coordinator **Dr. Sanmeet Bhatia,** my parents, friends and other staff members for their love, motivation, support and blessings. They have been a constant source of love, concern, support and strength for me all these years.

Finally I would like to thank the management of Thapar Institute of Engineering & Technology for providing me a great opportunity for learning, not just in academics but also in many other creative things.

Deepika

(Deepika)

Roll No. 601634006

ABSTRACT

In applications with low infrastructural elements, a MANET becomes highly vulnerable to security attacks. These attacks can be active or passive in nature. Active attacker including 'Black-hole', 'Grey-hole' and 'Worm-hole'; can modify, listen and inject messages in communication channel. Whereas, a passive attacker does not alter the information; but secretly listens to valuable information i.e. spoofing. Jellyfish attack is one of the illustrations of a passive attack. Jellyfish conforms to all routing and forwarding protocol specifications. A Jellyfish attacker possesses the property that it is difficult to detect until after the sting. Jellyfish attacker targets closed loops and misguide the packets to adversely affect the network performance. A Jellyfish attack can attack the network in 3-ways Jellyfish-reorder-attack, Jellyfish-periodic-dropping-attack and Jellyfish-delay-variance-attack. In Jellyfish Delay Variance (JFDV) attack, attacker node receives the packets from source side and adds delay while forwarding the packets to receiver. This leads to automatic performance degradation in both sender and receiver perspective. JFDV attack causes delayed ACK and sender assumes that packet has been lost and begins to retransmit the packet leading to congestion in the network. Routing protocols specifies the ways to establish the route from source to destination. The established route belongs to reactive and proactive category. AODV and DSR fall under the category of reactive routing protocol or on demand routing protocol. The AODV routing protocol is based on DSDV and DSR. In AODV, each packet carries the destination path, whereas in DSR each packet carries full routing information. Moreover AODV is adaptive to highly dynamic network.

The present work has been implemented on network simulator, NS 2.35. It is a discrete set of terms and protocol settings for network lay-outing and configurations. The present work has taken 2-routing protocols AODV and DSR; on which JFDV attack has been implemented. The impact of varying number of jellyfish attacker nodes 1, 3, 6 and 9 has been compared in both the protocols. AODV outperforms DSR protocol for several performance parameters, which include "*Throughput*" and "*End to End Delay*" with JFDV detection algorithm. The Algorithm provides better identification and removal in AODV protocol.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

JF	Jellyfish
MANET	Mobile Ad hoc Network
AODV	Ad hoc on Demand Distance Vector
DSR	Dynamic Source Routing
QOS	Quality of Service
RREQ	Route request
RREP	Route reply
TCP	Transmission Control Protocol
ACK	Acknowledgment
ESCT	Evolutionary Self-Cooperative Trust
E2E	End to End
JFDV	Jellyfish Delay Variance
N	Number of Nodes
AP	Access Point

CHAPTER 1
INTRODUCTION

With the improvement of network and communication innovation, a problem of wired connections are reduced by wireless networks as it has wide viewpoint and practicability in the zone of disaster recovery, defence, emergency situations and special event management. A wireless local area network that uses assigned frequency radio waves rather than wires or physical connections to communicate between networks enabled devices. Every second is crucial in large scale developments and wireless technology increases the output by providing high mobility of nodes and easier network expansion. It works in two modes named as Infrastructure based network and ad-hoc systems. Infrastructure mode organize is comprised of settled and wired network nodes and gateways, network services conveyed with the assistance of preconfigured frameworks. For instance, cell net-works are foundation based systems worked from PSTN backbone as switches, MSCs, BSs, and portable hosts. Every node has its particular obligation in the system, and association foundation takes after a strict signalling grouping among the nodes. However in ad-hoc systems, nodes are uncomfortable with a topology of their systems. Rather, it needs to investigate on regular basis based on the mechanisms of different protocols. Every node contacts its neighbours using best routes. There are many ways to select the routes like hop count, bandwidth and delay.

1.1 Mobile Ad Hoc Network (MANETs)

Presently a-days gadgets are becoming compact, less expensive and easier to understand. MANET is included by arrangement of quick moving remote nodes. Because of the absence of the organization also, the adaptability of nodes, each node in the system contributes in coordinating activity by monitoring system network and topology changes. MANETs are self-surrounding and self-recovering, enabling companion level correspondence between portable nodes without dependence on infrastructure and any centralize device. In MANET, every node can behave as router to forward a protocol throughout the specific network. These credits empower MANETs to convey critical advantages in basically any situation that incorporates a unit of exceptionally mobile clients or stages, a solid need to share IP-based data, and an

environment in which settled system framework is unreasonable, weakened, or unimaginable. Four core functions of MANETs include Path Generation, Path Selection, Data Forwarding and Path Maintenance[2]. Key applications of Ad-hoc networks incorporate catastrophe recuperation, overwhelming manufacturing, data mining, transport, guard, and unique occasion administration.

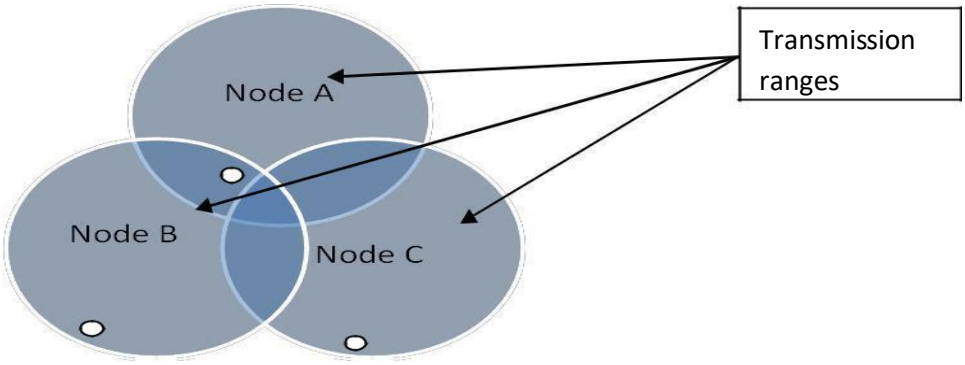


Fig.1.1. Mobile Ad-hoc Network

MANET with three nodes named as node A, node B, and node C is shown in Figure 1.1.

1.1.1 Characteristics of MANETs

An ad-hoc system is a gathering of mobile nodes framing an instantaneous system without settled topology and centralized system. Various Characteristics of MANETs are described as:

- **Autonomous Behaviour:** Every mobile node in MANET can go about as both host and router exhibiting autonomous conduct.
- **Multi hop Radio Relaying:** When any origin node and goal node is out of radio range, the MANET is equipped for multi-hop transferring. Multi hop relaying is a type of communication in which network coverage is larger than the coverage area of single node. Therefore, a node can use other nodes as relays to reach a specific destination.
- **Less Secure:** A Centralized firewall is absent in the network making the ad-hoc network as less stable and secure.
- **Dynamic Topology:** The node can connects or disconnects the network at any time making a network topology varying continuously.
- **Less Human Intervention:** Mobile and spontaneous behaviour of nodes tend to result in minimum human intervention to configure in network.

- **High User Density**: Large numbers of users can get the benefit of the network.

1.1.2 MANET Applications

MANET found applications in various fields

- **Military Battlefield:** It enables the military to exploit ordinary system innovation to trade data between warriors, vehicles and military data central command.
- **Commerce Level:** Specially appointed systems can be utilized as a part of crisis/save activities for calamity alleviation endeavours in surges or quake like circumstances. It can be helpful where existing network got damaged and fast organization of new correspondence arranges is required. Data is shared by various team members over a small hand held.
- **Local level:** Ad-hoc systems can independently connect a moment and brief media arrange utilizing notebook PCs or palmtop PCs to spread and offer data among members at e.g. gathering or classroom or may be domestic network where these devices can interconnect straight in controlling household appliances.
- **Personal Area Networking:** Too much wired links are replaced with remote associations with connects.

1.2 Ad-hoc Routing Protocol

A protocol is an arrangement of predefined rules that needs to be followed while communication in end points of a network. Networks are made to follow these rules for successful transmission of data. Every rule is characterized in various terms and is assigned out a specified name. Protocols give point by point information on forms associated with information transmission. Such procedures incorporate kind of task, process nature, information stream rate, and information type and device administration. A single procedure can be dealt with by in excess of one protocol. Routing Protocol describes how routers communicate with each other to send the information packet from source to goal. Routing protocols indicates the specified route to be chosen by nodes as the nodes are not familiar with the topology of the system; instead they need to find it [1].

1.2.1 Classification of Ad-hoc Routing Protocols

In view of the conveyance of packets from source to destination, Classification of routing protocols should be possible as unicast and Multicast routing protocols. In unicast routing protocol single source and single destination is involved for communication forming one-to-one relationship. In multicast routing protocols, information or data is delivered to number of receivers simultaneously utilizing the most advantageous and effective procedure. Additionally directing protocols are categories as, Proactive, Reactive and Hybrid routing protocol as shown in Figure 1.2.

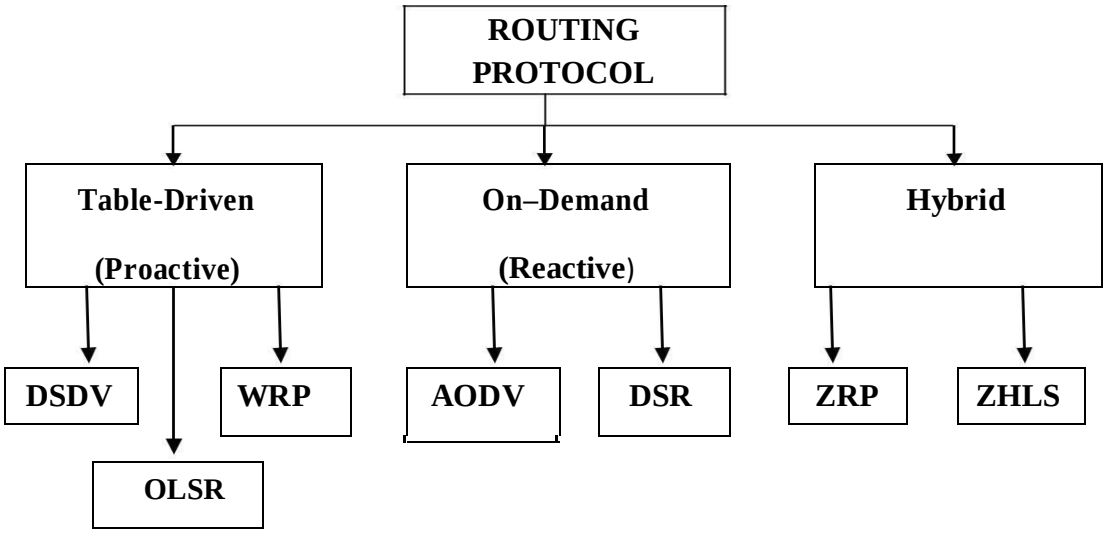


Fig.1.2.Routing Protocols

1.2.1.1 Proactive (Table-Driven) Routing Protocols

In table driven routing protocols route is computed prior to request. Periodic updating and distribution of routing information takes place in it. Proactive protocols consume more bandwidth as it holds a routing table throughout the transmission. The merits of proactive protocol is that a route can be chosen instantly without waiting for hold up yet keeping up vast measure of information for routing data with higher transmission capacity and moderate response on failing and attacks are real setbacks. Ex: DSDV, OLSR, WRP.

- **DSDV (Destination Sequence Distance Vector Routing):** In this, every mobile node which is participating in a system need table maintenance. Every routing table maintains a record of all possible routes and hop count to reach the destinations. These tables are update either periodically or driven by an event. Each node advertises its own routing

table to the neighbouring nodes by broadcasting or multicasting.

- **WRP (Wireless Routing Protocol):** WRP keeps up a Distance table, a Routing table, a Link Cost table and a message retransmission to rout. WRP lessens the quantity of cases in which directing circle get built up. It utilizes intermittent refresh message transmission to the neighbouring nodes. The nodes in the reaction list send affirmations as ACK. On the off chance that there is no change with the last refresh, at that point nodes in respond list sends idle hi message to guarantee availability.
- **OLSR (Optimized Link State Routing):** OLSR protocol is an advancement of pure connection state routing protocols for MANETs. Firstly, it proclaims just a subset of link with their neighbours rather if all connections in this manner lessening the extent of control protocols with the utilization of multi point transfer selectors. Besides, it limits the flooding of activity by utilizing chosen nodes called multi point transfers, to send messages in the system. It utilizes hi and Topology Control (TC) messages to get and after that spread connection state data all through the system.

1.2.1.2 Reactive (On Demand) Routing Protocols

Routes are found, when requested by flooding route request in reactive routing protocols. There is no need of distribution of routing information. Reactive routing protocols ensure less bandwidth and compelling in route however requires high time route foundation and at times exorbitant flooding may prompt system congestion. Ex: AODV, DSR.

- **AODV (Ad-hoc On Demand Distance Vector):** it intended for remote as well as portable computer systems. This protocol defines up routes to objectives on request and backings both uni-cast and multi-cast routing, an on-request calculation and does not make any additional movement for correspondence along links. The routes are kept up for whatever length of time that they are required by the sources. In AODV, systems are quiet until the point when associations are set up. System nodes that need associations communicate a request for association. The rest of the AODV nodes precedes the protocols and list the node that requested an association. In this way, they make a progression of brief routes back to the requesting node.
- **DSR (Dynamic Source Routing):** The Dynamic Source Routing protocol (DSR) is a straightforward and productive routing protocol planned particularly for use in multi-hop remote specially appointed systems of mobile nodes. DSR speaks to on-Demand directing utilizing source-route. DSR enables the system to be completely self-sorting out

and self-arranging, without the requirement for any current system framework or organization. DSR is an on request source directing protocol which demonstrates that the information packets contain a list of nodes speaking to the route to be taken after and routes are made at whatever point a source node requests to send information to the goal node[3]. By utilizing source routing, packet directing is permitted to be inconsequentially circle free, stays away from the requirement for up and coming routing data in the middle of the relay nodes through which packets are sent, and permits nodes sending or catching packets to reserve the routing data in them for their own particular future utilize.

1.2.1.3 Hybrid Protocols

Hybrid protocol is formed by mixture of useful features of reactive and proactive routing protocols. Productivity of hybrid protocols may change with number of nodes and measure of movement chooses the response to request, Ex: ZRP.

- **ZRP (Zone Routing Protocol):** ZRP is a hybrid protocol for mobile ad hoc systems which separates the nodes into sub-networks (zones). Inside each zone, proactive protocol is adjusted to expand the speed of correspondence and on-demand routing is used in inters zone communication to reduce unnecessary links.
- **ZHLS (Zone Based Hierarchical Link State Routing Protocol):** ZHLS depends on various levelled structure in which the system is isolated into non-covering zones. Every node has one of a kind node ID and a zone ID, which are computed utilizing topographical data.

1.3 Security Issues in MANETs

The security issues are to be considered in MANETS as a result of its qualities like vulnerability of mobile nodes, nonappearance of infrastructure and progressively evolving topology. In MANETs, a mobile node has a few restrictions regarding data transmission, power of computation, and battery that can prompt application-particular trade-offs amongst security and resource utilization of the cell phone. In any case, to do this middle of the relay node accomplishes no advantages.

So there might be a probability that a few nodes decline to forward packets and consequently diminish the effectiveness of the system in term of throughput and protocol delivery ratio.

In MANETs, there are different type of attacks that belongs to different network layers such as physical layer, data link layer, network layer and transport layer. Some major goals of security are Confidentiality, Availability, Authentication, Integrity, Non-repudiation, detection and isolation. Compromised nodes and no central management are responsible for security issues[4]. Security incorporates a heap of security works that guarantee dependable correspondence. The significant security objectives can be clarified as:

- **Authentication:** guarantees that before sending and getting the information utilizing the framework, the beneficiary and sender character should be confirmed. N have Authentication is sometimes called as origin integrity. It is a way of measuring the degree of trust that one can have while sending or receiving data. Authentication should be measurably precise and definite. Information must not be shared, vulnerable to loss, forgery, duplication, Guessing and masquerading.
- **Availability:** enables the sender to use any path in the event that required number of nodes is available in the system.
- **Confidentiality:** means that only the authenticated receiver or node can interpret the control message. As MANETs do not have centralized administration and securing the information in such a network is challenging task. If private information got exposed to anyone other than intended node could cause a privacy and confidentiality breach.
- **Integrity:** indicates that the protocols should arrive in same order at the receiver end as they were sent by sender and conveyed information is guaranteed to be free from any adjustment.
- **Non-Repudiation:** infers that neither the sender nor the recipient can forgery and intentionally deny that they have sent a specific message.

1.4 Security Attacks in MANETs

Attacks against routing protocols can be ordered into inner and outer attacks. An outside attack starts from a router that does not participate in a routing procedure but rather carries on as confided in router. These attacks can be avoided by utilizing standard security mechanism, for example, encryption methods and firewalls.

An inner attack originates from concession, misconfigured, faulty or malicious routers. Since the assailants are now part of the system as approved nodes, interior attacks are more serious and hard to distinguish when contrasted with outside attacks. Any attack on Ad-hoc systems can likewise be classified as dynamic and inactive attacks described in Table 1.1.

Table 1.1 Attackers at Different Layers

Layer	Example of attacks
Application Layer	Repudiation, Data Corruption, Viruses, Worms
Transport Layer	Session Hijack, SYN Flood, Jellyfish Attack
Network Layer	Sybil Attack, Black-hole Attack, Gray-hole Attack, Wormhole Attack, Spoofing, Selfish Misbehaviour, Byzantine Attack , Route Table Overflow
Data Link Layer	ARP Spoofing
Physical Layer	Eavesdropping

In a dynamic attack, the acting up node effectively aggravates the typical task of the system with endeavours to change or destroy the information being traded in the system. In inactive attack the malignant substance just tunes in to the movement without disturbing appropriate task of the system. An attacker is likewise ready to decipher the information accumulated through snooping to damage privacy necessity.

1.4.1 Application Layer Attacks

Various attacks that affect application layer are

- **Repudiation Attack:** A repudiation attack happens when an application or system does not check or track the log user actions. Thus new actions cannot be identified and malicious nodes got permission to forge the system. It is the ability of system to deny that specific tasks or actions are performed by them.

- **Data Corruption:** Corruption can affect the communication in various ways. Sometimes a complete file can got deleted. It can either drop all database tables or change the database record.
- **Viruses:** Virus is a type of software which attack itself to a program and moves ahead through the system by copying itself. Once a virus is executing, it can affect the performance by performing deletion of all files and programs.
- **Worms:** A system worm spread like a virus but it is independent program rather than hidden inside another program. It is standalone malware which uses computer network to spread itself and relies on the security failures of the target computer system.

1.4.2 Transport Layer Attacks

The following attacks prevail in transport layer

- **Session Hijack:** Attack consists of misuse of the web session control mechanism. The mechanism is generally managed for a session token. In any http communication, token is a most common method to identify every user's connection. Attack comprises of misuse of the web session control instrument. The system is by and large overseen for a session token. In any hypertext transfer protocol correspondence, token is a most common method to identify every user's connection. Web server sends tokens to the customer program after a successful event validation. The session hijack attack contains a session token by taking or anticipating a substantial session token to increase unapproved access to internet browser.
- **SYN Flooding:** In this type of attack, a false node sends a lot of SYN packets to a victim node, spoofing the arrival locations of the SYN packets. The SYN ACK packets are conveyed from the casualty directly after it gets the SYN packets from the attacker and afterward the victim waits for the reaction of ACK parcel. Except if reaction is gotten from ACK packets, the information structure stays in the victim node. On the off chance that the victim node stores these half-opened associations in a settled size table while it anticipates the ACK of the three-way handshake, these pending associations could flood the buffer, and the victim node would not have the capacity to acknowledge some other true endeavours to open an association. Regularly there is a timeout related with a pending association, so the half-open associations will in the end lapse and the victim node will recover. Notwithstanding, a malicious nodes can just keep sending packets that

demand new associations continuously than the termination of pending associations.

- **Jellyfish Attack:** Jellyfish attack affects the network by behaving in three ways named as Jellyfish protocol reordering attack, Jellyfish periodic dropping of protocol attack and jellyfish random delay variance attack [5]. This type of attack is the main focus in this work.

1.4.3 Network Layer Attacks

This layer is affected by the following attacks

- **Sybil Attack:** A Sybil assailant can either make in excess of one character on a single working device with a specific end goal to launch a planning attack on system. It can switch characters keeping in mind the end goal to debilitate the location procedure, along these lines advancing absence of responsibility in the system. In remote sensor organizes, a Sybil assailant can change the entire accumulated perusing result by contributing ordinarily as confided in node. In Voting based Systems, a Sybil attacker can be utilize various virtual ID's to control the outcome by gear the polling procedure. In Vehicular specially appointed systems, Sybil attacker can make a discretionary number of virtual non-existent vehicles and transmit bogus intimation of movement blockage and redirection of the traffic.
- **Black Hole Attack:** In this sort of attack, an assailant endeavours to keep legitimate and approved clients from the administrations offered by the system. A Black Hole Attack can be done from numerous points of view. The great route is to flood packets in the system with the goal that administrations gave be halfway node is not any more accessible to other taking an interest nodes in the system, because of which the system never again working in the way it was intended to work. This may prompt a disappointment in the conveyance of ensured administrations to the end clients. Because of the one of a kind qualities of MANETs, there exist numerous more approaches to organize a Black Hole Attack in such a system. Black Hole Attack attacks can be propelled against any layer in the system protocol stack. On the physical and MAC layers, an attacker could utilize jamming signs which upset the on-going transmissions on the remote channel. On the IP layer, an attacker could participate in the directing procedure and adventure the routing protocol to upset the typical working of the system.

For instance, an enemy node could take part in a session yet essentially drop a specific number of packets, which may prompt corruption in the Quality of Service being offered by the system. On the higher layers, an attacker could cut down basic administrations by Low Rate Black Hole Attack.

- **Gray Hole Attack:** Dark entire attack is a functioning kind of attack, which prompt dropping of messages. Attacking node initially consents to forward packets and after that neglects to do as such. At first the node carries on accurately and replays genuine RREP messages to nodes that start RREQ message by which it assumes control over the sending packets. A short time later, the node just drops the packets to dispatch Black Hole Attack. On the off chance that neighbouring nodes that endeavour to send packets over attacking nodes lose the association with goal then they might need to find a route once more, communicating RREQ messages. Attacking node builds up a route, sending RREP messages. This procedure goes ahead until the point when vindictive node succeeds its point of lessening execution of system. This attack is known as Routing Misbehaviour attack. A Gray Hole assailant shows malicious conduct in various ways. It might drop the originating from certain particular nodes; it might carry on non-legitimately for quite a while, and after that change to normal conduct. Subsequently recognition of gray hole attack is troublesome assignment.
- **Wormhole Attack:** Wormhole aggressor node pick up the classification of the sender by faking the MAC address from the sender and furthermore by getting the entire information sent by sender by means of making a passage and by not letting the sender to send information to valid goal.
- **Spoofing:** When an attacker tries to access computer or system by behaving as a trusted source.
- **Selfish Misbehaviour:** Whenever the selfish node feels that protocol requires lot of sources, the malicious node does not forward it in network. Node misbehaviour and failures causes isolation problem. However, selfish nodes can still make the communication with all other nodes. Selfish nodes are of three types: No protocol forwarding, No participation, Partial protocol forwarding with energy saving [6].
- **Byzantine Attack:** Byzantine attack is characterized as attack against routing protocol, in which at least two routers conspire to drop, manufacture, alter or misroute packets trying to exploit the directing services. It is an example of internal attack.

- **Route Table Overflow:** Attacker attempts to create routes to non-existing nodes and prevents creation of new routes. Proactive protocols are more affected by this attack.

1.4.4 Data Link Layer Attacks

Attack related to this layer is given below

- **ARP spoofing:** Address resolution protocol is a protocol used to map IP address to a physical machine. At whatever point a host machine needs to discover a MAC address for an IP address, it communicate ARP ask. The host machine answers with ARP answer message. Each time a host gets an ARP answer from another host, despite the fact that it has not sent an ARP ask for, it will acknowledge ARP answer passage and updates its ARP Cache. The way toward adjusting target has, ARP reserve with manufacture passage is known as ARP spoofing.

1.4.5 Physical Layer Attack

Attack affecting physical layer is

- **Eavesdropping:** An attacker can tune in to any remote system to comprehend what is happening in the system. It initially tunes in to control messages to deduce the system topology to see how nodes are found or are speaking with another. It gathers useful data about the system before attacking. It might likewise tune in to the data that is transmitted utilizing encryption despite the fact that it ought to be classified having a place with upper layer applications. Eavesdropping is additionally a risk to area security.

1.5 Challenges in MANET

MANET atmospheres have to fight against the limitations and inabilities for generating maximum efficiency. The challenges include:

- **Transmission Impediments:** like path loss, fading, high number of routing overheads which resists the performance of MANETs.
- **Hidden Terminal Issue:** happens when a terminal is noticeable from a remote passage (APs), yet not from different nodes speaking with that AP. This circumstance drives the troubles in medium access control sub layer over remote systems administration. Hidden terminal problem issue happens in MANETS because of its remote nature. Hidden nodes are those nodes which are out of scope of different nodes. When any two nodes are not

visible to each other then there is a chance of collision and protocol loss. Consider a remote systems administration, every node at the far edge of the access point range, which is known as A, can see the access point, yet it is improbable that a similar node can see a node on the contrary end of the access point range, C. These nodes are known as covered up. The issue is when nodes A and C begin to send packets all the while to the access point B. Since the nodes A and C are out of scope of each other thus can't recognize a crash while transmitting, transporter sense different access with impact identification does not work, and crashes happens, which at that point degenerate the information got by the access point.

- **Exposed Terminal Problem:** also comes in the way of communication in wireless networks. In this case, when node B is sending data to A then C senses this transmission and needlessly stops its own transmission towards B. However data transmission between B and C cannot create collision at B. This unnecessary termination of transmission results in exposed terminal problem as shown in Figure 1.3.

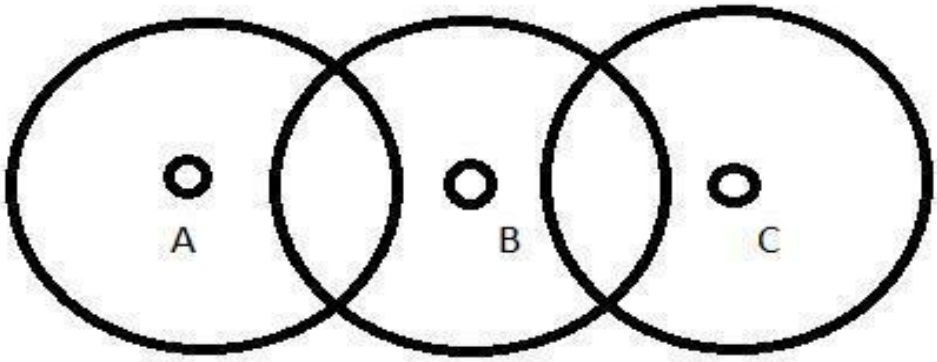


Fig.1.3. Nodes Representation in Exposed and Hidden Terminal Problem

- **Lower Link Capacity:** In this, channel limit is frequently less than a radio's most extreme transmission rate with the goal that the acknowledged throughput of remote communications in the effects of numerous accesses, blurring, noisy, and impedance conditions, and so on. As MANETs are autonomous systems of mobile nodes. Mobile nodes can move arbitrary in any direction thus network topology may change in random and arbitrarily at unusual time intervals. A random moment of the nodes leads to network partitioning and topology can change without any prediction pattern.

- **Battery Life:** is another aspect on which mobile nodes in MANETs depends. The problem with battery life is unavoidable because once the battery got exhausted; node cannot receive or send any data thus affecting the throughput of the network.
- **Security Attacks:** in MANETs affects the different network layers of OSI model.
- **Routing Attacks:** also emerge as an issue when information is sent from sender to receiver.

1.6 Thesis Organization

The objective of thesis is to evaluate the performance of the Ad-hoc routing protocols in the presence of various security attacks in the MANET. The layout of thesis is discussed below:

In Chapter 1, introduction about MANET, its advantages, and characteristics, routing protocols, Security attacks in MANET and various challenges. A literature review of the important papers has been discussed in Chapter 2. In Chapter 3, problem statement is given. A proposed framework for detection and removal of jellyfish attack present in the network has been presented in Chapter 4. Chapter 5, demonstrates the simulation outcomes accomplished. Chapter 6, discusses conclusion and future work.

CHAPTER 2
LITERATURE SURVEY

The different methods and techniques for detection and removal of various security attacks are discussed to amplify the lifespan of a network. This survey includes theoretical review on MANET, security attacks, MANET routing protocols, methods used in detection and prevention of attacks and other techniques on the basis of which performance of mobile network is examined in presence of attack. A brief summary on behaviour of jellyfish attack has been carried out in this section.

2.1 Reactive Routing Protocols

Routing is a way toward moving data over a system from a source node to a goal node. Along the way, more than one relay node commonly is experienced. It is additionally refer to carry out two main tasks, first is to determine optimal path through which data flows and second is to send the protocols through this best path from sender to receiver. The routing algorithm is the part of the network layer software responsible for deciding which output line an incoming packet should be transmitted. Routing protocols use metrics to evaluate what path will be the best for a packet to travel from source to Destination node. The metrics used in deciding the routing path can be hop count, reliability, delay etc. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which contain route information [3].

AODV is Ad-hoc on demand routing mechanism. It is a reactive category of protocol. This type of protocol can be most suitable for the network where topology is very dynamic. In MANET there are various mobile nodes moves from one position to other position. While moving they goes from one nodes neighbour list to other nodes neighbour list. So each time node moves from one position to other position, the node will get change to another nodes neighbour list. So every interval of time a node needs to transmit protocol it has to establish a route from sender to the receiver. Previous route will be left and new route is to be established. Sometimes it
may be possible that route get failed in single communication. That means for full communication the new path will be required. AODV has to minimize the quantity of dynamic routes between dynamic source and goal. AODV establish various routes amongst source and goal. Be that as it may, just a single route must be selected. This selection depends on least number of Hops amongst source and goal. It is always difficult to manage multiple routes in to the buffer. In that situation when one

route will be failed another route will be selected from the previously formed path list. AODV discover the route as and when it will be required. It does not maintain the route from source to destination. Routes are managed just as long as it is required [5]. After the requirement is completed the previous route will be left and when there is a requirement new route will be established. Each node keeps up monotonically expanding sequence number. It will increase the sequence number every time it sees the change in the topology of the network. AODV uses the routing tables to store directing data. Routing table will be required for both unicast and multi-cast routes.

Dynamic Source Routing protocol (DSR) is an on-request source routing protocol which indicates that the information packets contain a list of nodes tells the route to be utilized and the routes are made at whatever point there is need of data transmission from sender node to receiver node. It verifies the route from sender to receiver. It does not buffer the path. Rather will use the path by selecting one path out of many paths. Unlike AODV there will be no periodic exercise of any kind. In AODV hello messages will be sent on regular basis. It is to check the neighbour list. But rather in DSR the new path will be established dynamically. Each time route request will be forwarded neighbour are identified at that time. So, no extra work or energy has to be wasted while building the path list [7].The summary of reactive routing protocols is given in Table 2.1.

Haleem et al. in [10] designed secure reactive protocol for MANETs, called TRIUMF MANETs, called TRIUMF (Trust Based Routing Protocol with Controlled Degree of Selfishness for anchoring MANET against packet dropping attack). In the protocol, trust among nodes is spoken to by trust esteem, which contains coordination score, self-trust and cooperative trust of the considerable number of nodes.

Ali et al. in [26], provides examination on diverse QoS measurements of diverse receptive protocols. The measurements utilized while thinking about nodes thickness and form of IEEE 802.11g WLAN Standard are Network Load, Retransmission Attempts, End to End Delay, Media Access Deferral, Throughput, and so on. Accordingly, we discovered that AODV beats alternate protocols as far as media get to delay, stack, delay, information drop retry, and retransmission endeavours. In any case, DSR had been exhibiting better outcomes than others as far as throughput and routing activity send. Along these lines, the conclusion demonstrates that each protocol acts uniquely in contrast to others under various conditions in light of the fact that there are distinctive parameters that have been varied under shifted circumstances. Along these lines, as indicated by our simulation comes about; we can state that AODV beats others. Dynamic system of Mobile Ad-hoc Network, its topology is unusual and indeterminate.

This paper is proposed to think about and dissect QoS parameters of different receptive directing protocols while thinking about fluctuating node thickness.

Bai et al. in[27] proposed two principle kinds of the MANET directing protocols, proactive and responsive composes, are looked at and dissected no holds barred in view of different routing setups. Test comes about showed that the AODV calculation of the responsive type performs better as far as throughput and normal E2E delay, while the DSR of the responsive kind is somewhat better among the routing algorithm as far as packet conveyance proportion. As the span of the system builds, the receptive protocols (particularly the AODV routing protocol) wind up overwhelming in all execution classifications, while the impact of the packet measure is unimportant.

Nayak et al. in [28] exhibits a top to bottom investigation of AODV and DSR receptive directing protocols thinking about both arbitrary way point and random walk model. NetSim Simulator has been utilized as the simulation instrument to test the execution measurements of these protocols. A few parameters, for example, E2E delay, throughput, packet conveyance proportion, routing overhead and system lifetime has been considered as the execution measurements to check the behaviour of these protocol. Simulation comes about show that (amongst DSR and AODV) DSR is superior to AODV as far as packet conveyance proportion and throughput though AODV has less normal end to end postpone than DSR. Once more, with expanding no. of nodes AODV and DSR deliver nearly steady throughput. In any case, the routing overhead backings DSR furthermore overhead is more in AODV if there should be an occurrence of irregular portability display and almost rise to if there should be an occurrence of random walk model.

Patel et al. in [29] Looks on fundamental part of correspondence protocols in MANET. The plan of the protocols is driven by particular objectives and prerequisites in light of separate presumptions about the network properties. In this overview he attempts to survey run of the review receptive routing protocols and uncover the attributes and exchange offs. Every one of the protocols considered performs well now and again and has certain disadvantages in others.

Karthikeya et al. in [30] Objectives to accomplish with multipath routing was to have a superior unwavering quality. There might have been even a vastly improved execution, i.e., a superior throughput, Average end-to-end delay, Routing overhead furthermore, Route securing time for the multipath directing protocols. Overhead is vital too in systems as it is a factor which expresses the effectiveness of a system. In AODV, there are clearly less sent control packets, since each copy is disposed of by arrival. Especially in quick moving systems time is an essential factor as there may be a great deal of route breaks.

The summary of on different Routing Protocols (AODV and DSR**)** is given in Table 2.1.

Table 2.1 Summarized Literature Survey on Different Routing Protocols (AODV and DSR)

Year	**Title**	**Author**	**Proposed Work**
2017	Comparing and Analysing Reactive Routing Protocols (AODV, DSR and TORA) in QoS of MANET	*Ali et al.*	• Studied performance under different protocols like AODV,DSR,TORA.
2017	Performance Comparison and Evaluation of the Proactive and Reactive Routing Protocols for MANETs	*Bai et al.*	• Compare the performance of both reactive and proactive protocols.
2014	A Survey of reactive protocols in MANET	*Patel et al.*	• It has studied the different reactive routing protocols.
2014	Analysis of Reactive AODV Routing Protocol for MANET	*Karthikeya et al.*	• Studied different reactive routing protocols.
2013	Analysis of Random Way Point and Random Walk Mobility Model for Reactive Routing Protocols for MANET Using Net Sim Simulator	*Nayak et al.*	• Compare the performance of the different mobility models.
2011	TRIUMF: Trust based routing protocol with controlled degree of selfishness for securing MANET against packet dropping attack	*Haleem et al.*	• it has used trust based scheme for detection of the selfish node.

2.2 Various Attacks in MANETs

Ming Yu et al. in [7] exhibited an incorporated protocol called Secure Route against Collision (SRAC) that makes decision by checking the trust value of the neighbouring nodes and detect the internal attack named Byzantine attack.

Abbas et al. in [8] proposed a light weight plan to identify the new characteristics of Sybil attacker nodes with no utilization of outsider or any additional equipment as a hardware. Broad simulations and experiments are able to detect the Sybil attacker even in the presence of mobility.

Gupta et al. in [9] solves the problem of wormhole attack by utilizing Cryptography and electronic signature as MANETs are prone to digital attacks as instead of other attacks.

Sen et al. in [11] proposed a component which includes both local and coordination recognition to distinguish any malicious gray hole node in the system. The plan works in four consecutive steps in particular Neighbourhood information accumulation, Local anomaly discovery, Cooperation anomaly discovery and worldwide alarm raiser [11].

Jain et al. in [31] managed investigation and attainability of reactive routing protocol in MANETs. Attack is normal in MANET because of shared error prone remote channel. The presence of malicious nodes in MANET was too researched. The outcomes were plainly depicting AODV as a better responsive directing protocol when contrasted with DSR. In any case, packet drop of DSR is not as much as AODV in the presence of malicious nodes in MANET. The summary of different attacks in MANETs is described in Table 2.2.

Among the survey our focus is on Jellyfish attack. JF attack support acceptance with two scenarios like control and information protocols. Because it acts compliant to both data and control protocol which make it difficult to detect and prevent. Therefore Jellyfish attacker is difficult to detect until after the sting [21].Firstly, the rushing attack is implemented by jellyfish attacker to gain the authorization to a routing mesh. In the event that end up effective, it at that point defers every one of the packets by an arbitrary timeframe [22]. As there is no improvement among mobile nodes in MANETs, a relay node can present a basic vulnerability for TCP clog Control system. There are various variant of the jelly fish type of attack.

2.2.1 Jellyfish Reordering Attack

As itself name implies attacker nodes rearranges protocols before being forwarded to the immediate next node in its neighbour. As ACKs of some of the rearranged protocols are not gotten in

time, the source will considers that these packets have been dropped in the network and will re-forward them. Receiver will receive the packets again and their will re-generation of the ACK. frame. This results in the formation of more than one ACK for single packet. TCP initiate the control of flow to control these copy ACK packets, when these ACK packets exceed the threshold. The reordering protocols can be performed in two ways. First is by reordering packets in clusters of k packets each. This process is performed in three essential advances. 1. Reorder current cluster of k packets, 2. Forward the rearranged group, 3. Wait for next group. Secondly reordering is done by use of sliding window of k measure and each time a packet is sent, this window is developed by one packet. Reordering is started on accessible k packets each time a packet is going to leave the reordering buffer [23] as shown in Figure 2.1.

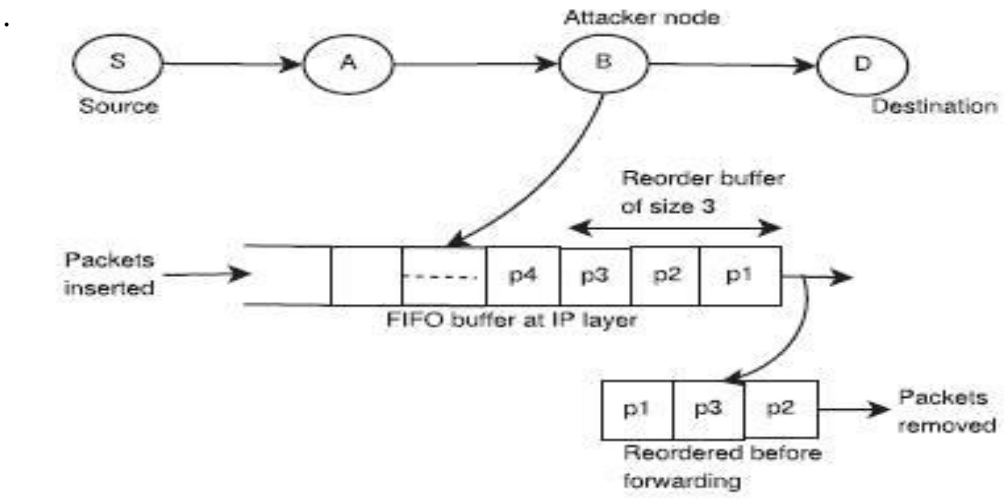


Fig.2.1. Reordering Attack [23]

2.2.2 Jelly Fish Periodic Protocol Drop Attack

In this attack, a JF node randomly disposes of a few packets received over the specific timeframe. JF attacker node may drop a small amount of packets or every one of the packets in a predetermined time. For example if 5 percent packets, then it has received 100 packets it will drops the 5 packets. This dropping of the packets can be the indication of congestion in the network. TCP will try to control the disturbed flow in specific period of time. Later on jellyfish attacker node chooses another time period to starts dropping the packets which will again disturb the flow. That means this type of exercise is performed after certain period of time resulting in decreased network performance as shown in Figure 2.2.

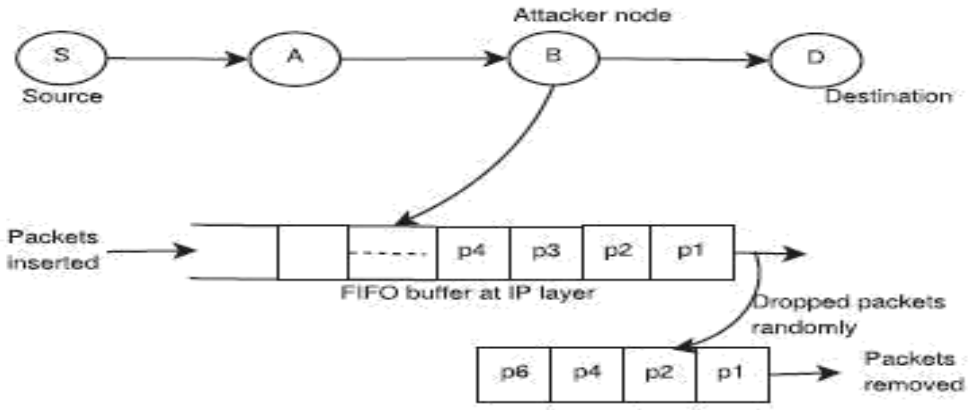


Fig.2.2. Periodic Dropping Attack [23]

2.2.3 Jelly Fish Delay Variance Attack

JF delay variance attack is a one which follows all protocol rules and hence hard to recognize. Jellyfish is a passive attack as the attacker disrupts the network from within. JF attacker becomes the part of routing mesh and introduces some amount of delay before forwarding the packets. When ACK is deferred then the source will not get the acknowledgement within particular amount of time. Source node will assume that packets are lost and start retransmitting the packets. It leads to increased congestion and reduced throughput. Jellyfish attack targets closed loop flows because of which flow is affected by packet loss and delay [9] as shown in Figure 2.3.

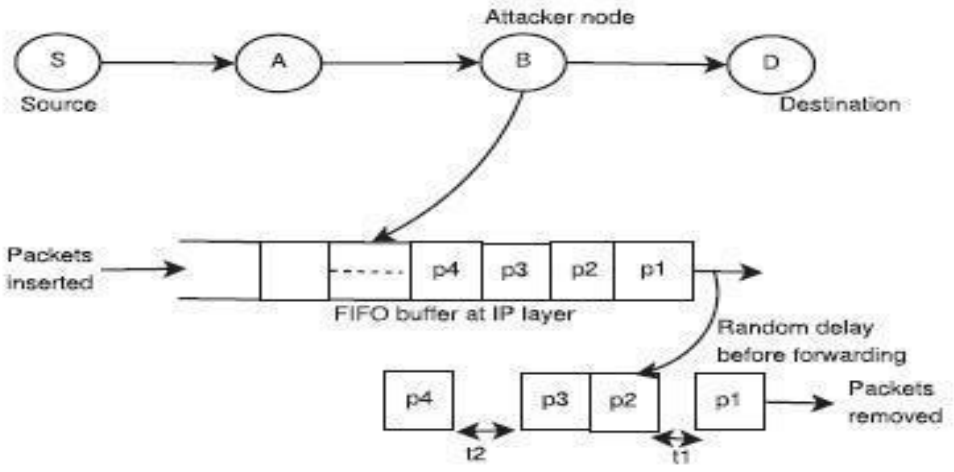


Fig.2.3. Delay Variance Attack [23]

Hence in JF delay variance attack, the malicious node upsets the ordinary working of the protocol and presents undesirable deferrals in sending information packets in the system. It causes TCF traffic to be sent in bursts and chances of collisions and losses are higher. It increases RTO value and also results in wrong estimation of the accessible transmission capacity in clog control protocols in view of packet delays.

Kumar et al. in [14] proposed a procedure for AODV routing protocol, to detect jellyfish delay variant attacker node. Sending time and sequence number is noted before sending the packets. When the packets reaches the destination and ACK is received, then difference between the previous values of time as well as ACK getting interval of all the nodes was compared to the ideal time taken by all the nodes. When the value was greater than the maximum value then the receiver was assumed to be a Jelly Fish attacker node and flag value was set to 1. This maximum value is based on the propagation delay, link delay etc. This process continued for every node until it was known that which node caused delay of the packet. Once the jellyfish attacker was identified, no path will use these attacker nodes has been explained in this work.

Garg et al. [15] gives routing protocol called Enhanced AODV is detect the JF delay variance attack and also removes attacker node. A threshold value of time was chosen initially. After certain timeframe every node sends an ordinary packet in EAODV at that point check which node among its neighbouring nodes was causing delay in the information packet transmission by time more than the threshold time of system. Any node founded guilty was discarded and alternate path was chosen.

Wazid et al. in [12] gives Cluster based Intrusion Detection and prevention procedures for JF reorder attack (CBIDPT) and Super cluster based Intrusion detection and prevention procedures for reorder attack (SCBIDPT) are two techniques proposed for jellyfish reorder attack. Cluster head choose based on decency and proficiency of the taking an interest. In CBIDPT, source node and middle nodes make enter into FIFO queue. The Buffer advances the information parcel to its neighbour node. Source node and middle node sends same FIFO support to group head moreover. Sequence number of FIFO queue and is contrasted with the sequence number of every single middle node. In the event that any reordering is found in sending information packet, group head consequently precludes that Intruder node based on their ID which is as of now put away in bunch head. At that point group set searches toward other ideal route which has no any kind of intruder node. Be that as it may, in SCBIDPT, super group is built by gathering numerous groups. SCBIDPT is used to find and remove the fake cluster head from the network.

Wazid et al. in [14] explained that Jellyfish delay variance attack defers the information packet during sending the information packet to the goal. Because of the deferral in packet sending, ACK is likewise postponed and sender expect that the parcel has been lost. Sender expects that parcel has been lost and begins retransmission, prompting blockage in the system. If the group head time is equivalent to middle of relay node support enter tie then proficient TCP otherwise not. Efficient TCP protocol protects JFDV attack by making invisible quick transmission of malicious information packets and empowering particular ACK .As the network performance was improved, therefore named as Efficient-TCP.

Khirasariya et al. [16] explained that Jellyfish attack comes into existence after rushing attack. When the attacker got the hold of sending protocols, then attacker begins dropping and postponing information packets by certain period of time.

Sharma et al. in [17] proposed Non-cryptography approach is work essentially on defer threshold time. Defer threshold time was a measure of timeframe limit of all en-route nodes of sending information packets. The approach works in two stages, initially all information packets was broke down and watched what specific information among them postponing the packet at en-route nodes. Any trouble during investigation proclaims the node as a JF node. At that point exchange ideal way is chosen with the assistance of re-routing if the distinction between time of current sending information packet and their past sent packet have higher deferral than threshold.

Dahiya et al. in [18] modifies TCP and AODV system to handle the jelly fish periodic dropping attack, the jellyfish protocol reordering attack and the jelly fish delay variance attack. The system uses the E_TCP of the existing system along with the modified AODV routing to get the effective results. In the E_TCP protocol the buffer stores the sequence number and the acknowledgement time while in the NAODV_ETCP protocol the forwarding ratio is stored in buffer.

Kaur et al. [19] presented a technique in order to detect and prevent abnormal behaviour of JF attacker node, the proposed scheme aims to work in the following way. At the point when the source node gets the route replies, it will store every one of the ways in its cache memory. Whole data was sliced in three parts and sent to destination by three different routes. When the goal node will receive packets, it will compare the number of received packets with the threshold value where the threshold value will be set at 80 percent to the number of packets sent. Detection procedure was initiated on the path containing low threshold value to check the count of packets received and transmit by every node of that path. If again packet delivery rate of a particular node tends to drop below the threshold value, then that particular node will be detected as malicious. ID of the suspected node will be as a

broadcasted to all the nodes in the paths to prevent communication with that malicious node and thus shall benefit the performance.

Sachdeva et al. in [20] indicates that the existence of Jellyfish attacker node deteriorate the network performance like throughput and E2E delay. A plan is proposed to identify and keep JF attacker node from deteriorating the system and adequacy of plan is assessed on ns2 simulator. JFDV attack on AODV is examined by JFDV detection algorithms that investigates packet deferring , mischief of nodes and identifies different JFDV attacker nodes. The summary of different techniques of jellyfish is described in Table 2.2.

Table 2.2 Summarized Literature Survey on Different Types of Attacks in MANETs

Year	Title	Author	Proposed Work
2017	Performance Comparison and Evaluation of the Proactive and Reactive Routing Protocols for MANETs	*Bai et al.*	• Compare the performance of both reactive and proactive protocols.
2017	Detection and prevention of JFPD attack in MANETs using NBA Technique	*Kaur et al.*	• NBA based technique is used for the detection of the jellyfish attacker node
2016	Design and implementation of NAODV-ETCPtohandle jellyfish attack	*Dahiya et al.*	• NAODV-ETCP based technique has been used for the detection of the jellyfish attack.
2016	Detection and Analysis of Jellyfish Attack in MANETs	*Sachdeva et al.*	• TY-AODV based scheme is used for the detection of the jellyfish attacker node.
2016	Detection and prevention of jellyfish Attack in AODV routing protocol in MANET	*Kumar et al.*	• this paper has used buffer based technique for detection of the attacker node.
2016	Wormhole attack in MANET	*Gupta et al.*	• It has detected the

			wormhole attack by sending the route request.
2014	Non-Cryptographic Detection approach and countermeasure for JFDV attack	*Sharma et al.*	• It used Non. Cryptography based scheme for the detection of the jellyfish attacker node.
2014	Enhanced AODV protocol for defense against jellyfish attack on MANETs	*Garg et al.*	• Enhancement of the protocol is taken place for the jellyfish attacker node.
2013	Analysis and Feasibility of Reactive Routing Protocols with Malicious Nodes in MANETs	*Jain et al.*	• This has studied different routing protocols of reactive protocol to study the feasibility for the malicious node.
2013	Simulation study of jellyfish attack in MANET using AODV routing protocol	*Khirasariya et al.*	• this paper has studied the performance effect while having jellyfish node in the network under AODV protocol.
2013	E-TCP for efficient performance of MANET under JF delay variance attack	*Wazid et al.*	• E-TCP based scheme is used for the detection of the jellyfish attacker node
2012	Lightweight Sybil attack detection in MANETs	*S. Abbas et al.*	• It has used the false request scheme for detection of Sybil attack.
2012	Comparative performance analysis of routing protocols in	*Wazid et al.*	• This research paper has proposed a scheme for

	mobile Ad Hoc networks under Jelly Fish Attack		the detection and compare the performance of various techniques for the jellyfish detection
2009	A secure routing protocol against byzantine attack for MANETs in adversarial environments	*Ming Yu et al.*	• Used acknowledgement based method for detection of byzantine attack.
2007	Mobile ad-hoc networks	*Sen et al.*	• It has studied the complexities lies into MANET type of network.

2.3 Summary

In this chapter, works and researches done by various researchers on reactive routing protocols and various attacks in MANET s especially jellyfish attack in last few years have been presented. The objective of the thesis work is to compare the execution of routing protocols, DSR and AODV under the impact of jellyfish attacker. Hence many techniques of jellyfish attacker detection and prevention were studied and discussed briefly in this chapter.

CHAPTER 3
PROBLEM STATEMENT

In this chapter, problem statement, research gaps and research objectives are given. Research on Ad-hoc has expanded excessively consistently. Usually the attack is either application layer attacks or the physical layer or the network layer attack. JF type of attack specially is for multiple layers. This jelly fish attack is hard to detect and remove. In current research our focus is on the jelly fish attack. Where the ESCT based technique for identifying the jelly fish has been applied on while attack process and during attack we applied detection and removal algorithm for jellyfish node.

So because of MANET as infrastructure less network due to no prior configuration, hostile environments and regular change in topology, it becomes very necessary to save network of nodes to improve the network duration as it is extremely hard to maintain security in MANET due to various types of attacks present in it. Routing protocols AODV and DSR both are of reactive type so in this it is difficult to find change in network which is caused by presence of malicious node in the network .So to avoid this malicious node to cause any change in the network communication between sender and receiver we are proposing algorithm for detection and removal of attacker node specifically in Jellyfish attack. Network maintainability and lifetime are the key issues for the contemporary examinations in MANET. Subsequently, this method can, effectively, increment lifetime of different network and applications, for example, commercial application, tactical network, workplaces, PAN, producing conditions, military systems.

Numerous papers have talked about JF attacks and its effect on MANET organize alongside the count of performance parameters like throughput under Jellyfish attackers. Yet, there is no work done as of not long ago about the level of Jellyfish attackers a network can tolerate. In this we focused on E2E delay, Throughput of network. Again less measure of look into work has been done on the analysis of performance of MANET in presence of changing number of Jellyfish attackers by taking before, while, after assumptions.

3.1 Research Gaps

A lot of study has been done in the area of MANET and on various types of its security attacks but still some exploration holes were seen which are discussed below:

- The approach proposed by M.Yu[7] et. al is limited to before the communication , not taken any consideration while communication .
- A comparison of AODV and DSR routing protocol in the presence of jellyfish nodes is required.
- There is no consideration of transport and network layers attack as collective attack by D. Tedia [4] et al only single layer attack is taken into focus.
- By DSR routing protocol various attacks are examined except jellyfish attack by A.Halan [10] et. al.
- Trust based scheme is used for both AODV and DSR which gives accurate solutions but has not considered detection and removal algorithm by S. Garg [15] et. al.
- A comparison is presented on two different AODV and DSR protocol by A. Sharma [17] et. al. but not taking the performance parameters like throughput and end to end delay under jellyfish attack.
- M. Wazid [13] et. al. assuming the existing memory buffered existing path list but it do not mark the trust value of the neighbours.
- After effect of the jellyfish detection is not considered. there is the increase in end to end delay by P. Dahiya [18] et al.
- By I. Aad[20] et. al there is no consideration of multiple jellyfish attackers.

3.2 Research Objectives

Security being one of the significant difficulties for MANETs is the principle focal point of this work. The work centres around the jellyfish delay variance attack on reactive routing protocols.

- To detect and remove jellyfish node in the MANET using detection and removal algorithm and ESCT by considering different parameters.

- To compare the performance of proposed work with existing research.
- To compare the performance of AODV and DSR protocols under jellyfish attack by taking variable number of attacker nodes.

CHAPTER 4

PROPOSED WORK

4.1 Proposed Trust Based Algorithm

In MANET, nodes speak with one another and on hop-by-hop premises. In the attacker node detection and removal technique, each node transmits packet to its nearby neighbours nodes with Time to Live(TTL)=1 and neighbouring node IP address as goal IP address after a settled timeframe and timer is set to monitor deferred packets. A counter is utilized to avoid false decisions and every node is twice given an opportunity not to set a malicious node inaccurately. Timer sets in a way that it takes threshold value .Threshold delay chosen relies upon the packet delivery time.

Algorithm: 1 Trust Based Algorithm for Detection and Removal of Attacker Node.

```
BP: Broadcast packets
Counter: = 2
TF: Timeframe
    For every node
    {
        Build a packet BP
        Transmit the bundle to all close-by neighbour nodes}
            For every node
            {
                If (BP received)
                {
                    If (TF lapsed)
                    {
                        JF malicious node suspected
                        Counter = Counter -1
                        If (Counter < 0)
                            Node is a declared as JF
                    }
                }
            }
```

```
                For every node
                {
                    While (route disclosure)
                      {
                          If (RREPLY from JF attacker)
                              Reject RREPLY
                      }
                }
}
```

Packet delivery time is collectively taken by the sum of handling delay at every router, queuing delay presented by relay nodes, packet transmission time and propagation delay. When the node sends a communicate protocol and gets back a packet from any other neighbour node, at that point the timeframe is checked. If the time frame set is observed to be lapsed then node is suspected to be Jelly Fish node and the estimation of counter is subtracted and if the estimation of counter falls less than zero then node is affirmed as JF attacker node. Once the node gets recognized, its address is saved in a malicious node list and re-routing is started to keep the attacker node from participating in the system. However, it has been investigated only for AODV, whereas in this work we have implemented and compared it on NS-2 platform under different scenarios for DSR as well.

4.2 ESCT

ESCT is the approach used in two basic steps one is the self-detection and other is the neighbour detection. Under self-detection each node detects itself and broadcast the information to its neighbours. This self-detection is followed by the cooperative detection. In cooperative detection node will send the hello message to the neighbouring node, so that each node on receiving the hello messages detect itself and its neighbours [25] as shown Figure 4.1 and Figure 4.2.

All these steps which are mentioned below we are applying before the attack occurs in the network to suspect the malicious nodes. Through these steps we are finding the trust value of nodes by taking the advantage of self and cooperative detection technique. As our network is infrastructure less so it is keep on changing the topology so it is necessary to do that. Trust values are maintaining in the list so accordingly by finding history and replies we are keep on the

increasing trust value of nodes. If node is having high trust value then we will consider it as legitimate node otherwise declare it as malicious.

Step1: Node x sends the hello messages to its neighbours.

Step2: On receiving the request protocol neighbours y checks for the history. If the neighbour history has the number of requesting node x, it will reply to the x. and increase the trust value of x.

Step3: On receiving the route reply the node x checks for the replied node and if the number is found that will increase the trust value of y.

Step4: This cooperative trust based scheme will be followed at each occasion before the actual transmission will be taken place.

Step5: End.

Every node additionally keeps up the accompanying five kinds of attributes:

- Sending History Record (SHR): storage for no. of packets it delivered or sent along a particular routing way.
- Receiving History Record (RHR): storage for no. of packets it receives as an goal along a particular routing way.
- Self-Analysis Record (SAR): stores agreeable and uncooperative no. of peer nodes. These two numbers store the confirmation for trust level calculation executed in self discovery.
- Neighbour judgment record (NHR): stores the nearest neighbour ids and the latest trust information that is shared by these neighbours.
- Trust Information Record (TIR): stores the trust levels of various nodes and the benefit level of each piece of trust in information.

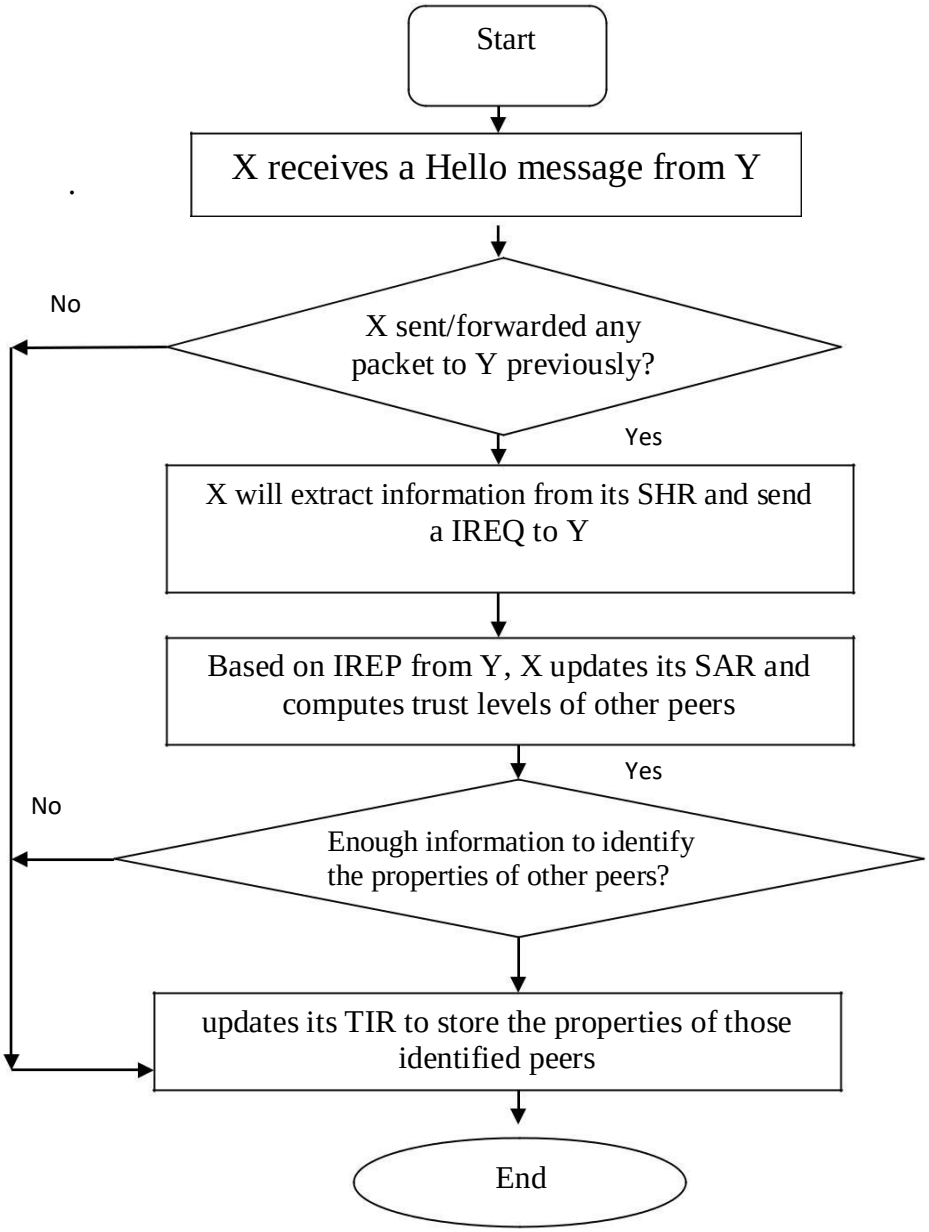


Fig. 4.1 Self-Detection Procedure

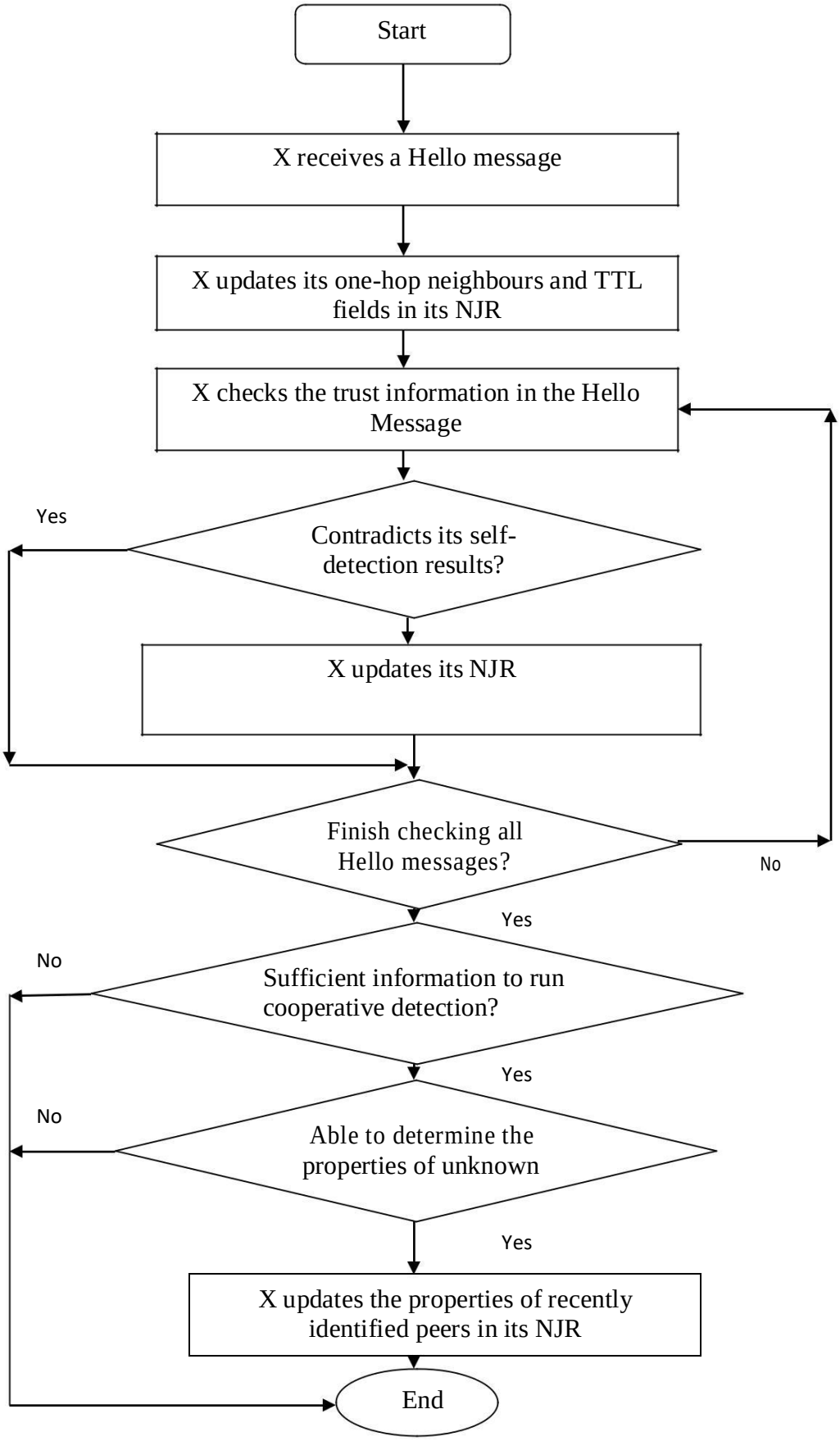


Fig. 4.2 Cooperative-Detection Procedure

CHAPTER 5

IMPLEMENTATION AND RESULTS

Based on parameters taken for simulations, both AODV and DSR routing protocols are being implemented in NS for identifying the based parameters like throughput and E2E delay.

5.1 Simulation Scenario

The simulation situation and parameters utilized for performing out the point by point examination is depicted beneath. This aspect tells that how the performance parameters have been examined to simulate the protocols. Following advances have been utilized for simulation.

- Inputs to Simulator: - Scenario File having development of nodes, traffic pattern record, and simulation TCL document.
- Outputs File from Simulator: - Trace record file, Network Animator.
- Output from Trace Analyser: - xgr record.

Table 5.1 Simulation Parameters

SIMULATION PARAMETERS	
COVERAGE AREA	1000m x 1000m
PROTOCOLS	AODV,DSR
NUMBER OF NODES	50
SIMULATION TEST TIME	100 seconds
RANGE OF TRANSMISSION	250m
MODEL OF MOBILITY	RANDOM WAY POINT MODEL
LOAD	5 Kb-UDP Protocols
MOBILITY SPEED(variable)	(80,90.100,150)Seconds
TRAFFIC PATTERN TYPE	CBR,UDP,FTP,TCP
PROTOCOL SIZE	512 Kbps
PAUSE TIME	10 ms

5.2 Network Topology

The evaluation of routing protocols is examined using NS2 network simulator. Firstly, conduct of AODV under jellyfish attacker node is studied. Then DSR routing protocol is taken and analysed. Further comparison of AODV and DSR is done based on performance parameters, for example, throughput and E2E delay.

In this work, NS2 (Network Simulator version 2) is used to study the effect of Jellyfish attack namely Jellyfish Delay Variance Attack (JFDV) on reactive routing protocols. The protocols taken in this work are well known protocols, AODV and DSR. The behaviour of both AODV and DSR compared using the algorithm that detects and removes the jellyfish attacker node. Performance of routing protocols is evaluated using parameters like throughput and end to end delay. Today, many network simulators are present that can simulate the ad-hoc remote systems. There are three protocol systems, which are utilized for breaking down the performance of wired and remote systems: Analytical method, Computer simulation and Physical method and test bed estimation. Among these, simulation is the most commonly used way of developing and testing the new protocols of any wireless network. For this evaluation purpose NS2 is used shown in Figure 5.1.

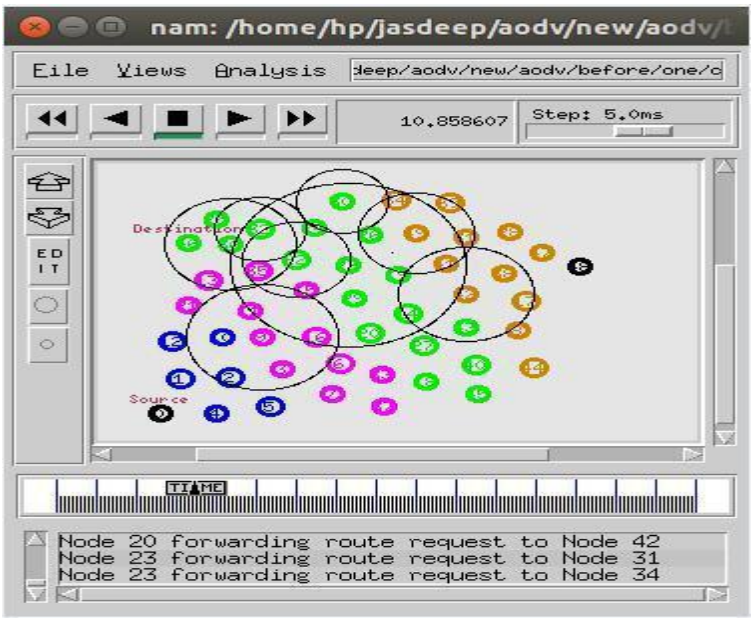


Fig.5.1.Network Animator Window

5.3 Results

Results have been carried out by comparing AODV with DSR under jellyfish attack by varying number of attacker nodes in the network.

5.3.1 AODV under Jellyfish Attack

In this section E2E delay and throughput is evaluated for AODV routing protocol under impact of Jellyfish attack.

5.3.1.1 E2E Delay for AODV under Jellyfish Attack

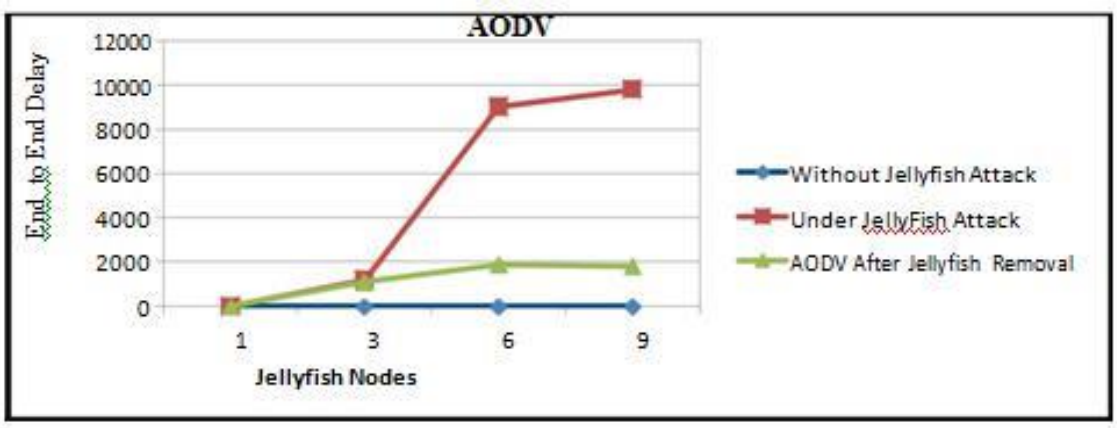


Fig.5.2. AODV E2E Delay under Jellyfish Attack

Normal E2E delay for network under AODV routing protocol is taken to understand the effect of jellyfish attack. Three scenarios are taken with varying number of nodes as 1, 3, 6 and 9. Firstly simple AODV protocol is implemented without any attack. It is noted that there is no delay in transmission. In second case, behaviour of AODV is seen under varying jellyfish attacker nodes. As the count of attacker nodes increases, End to End delay keeps on increasing. Afterwards, the attacker identification and removal algorithm is applied to the network and results are shown in Figure 5.2. It is found that performance in terms of E2E delay improves substantially especially at higher number of attacker nodes.

5.3.1.2 Throughput for AODV under Jellyfish Attack

Throughput under AODV routing protocol is analysed under the impact of jellyfish attack. Three scenarios are used with varying number of attacker nodes as 1, 3, 6 and 9. In the first scenario, AODV gives maximum throughput as no attacker is present in this case.

Afterwards throughput decreases significantly with increasing number of attacker nodes, when the protocol got affected by jellyfish attackers. Further after the implementation of the attacker detection and removal algorithm, significant increase in throughput is observed. The following figure represents the behaviour of AODV routing protocol as shown in Figure 5.3.

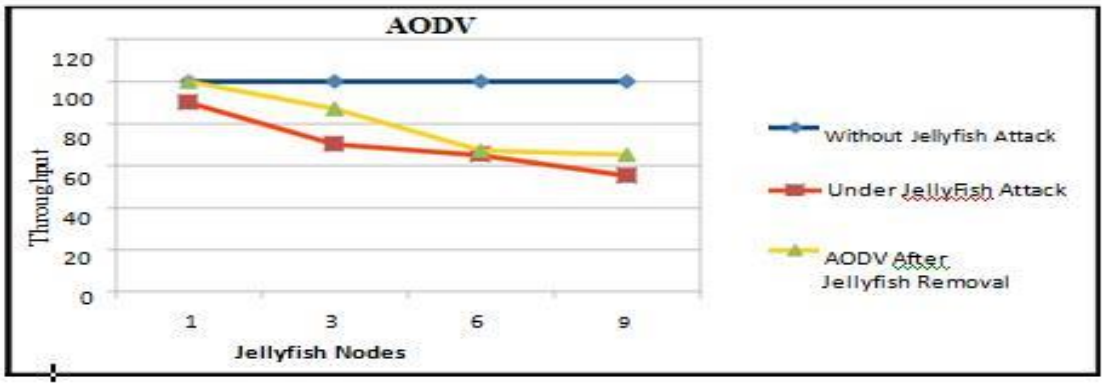


Fig.5.3.AODV Throughput under Jellyfish Attack

5.3.2 DSR under Jellyfish Attack

In the section, E2E delay and throughput is evaluated for DSR routing protocol under impact of jellyfish attack.

5.3.2.1 E2E Delay for DSR under Jellyfish Attack

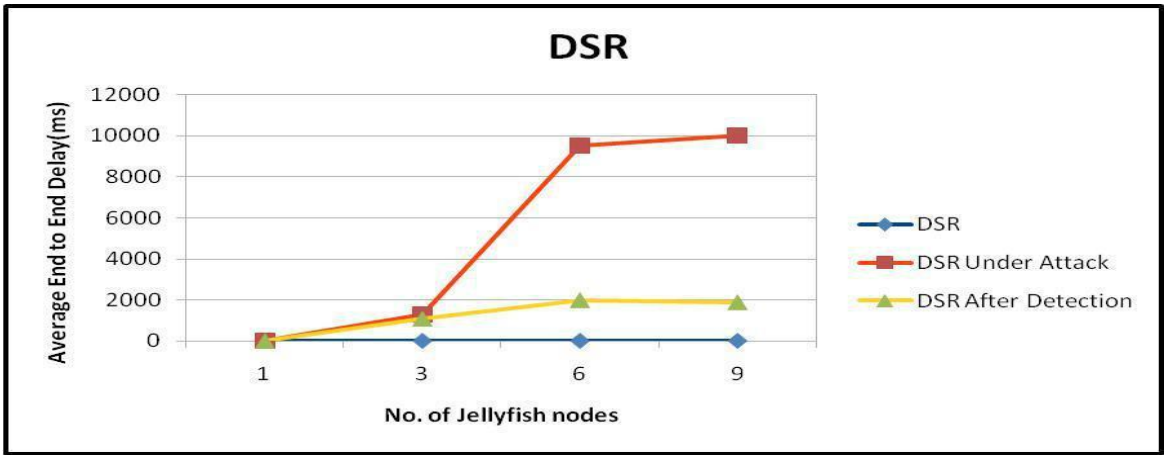


Fig.5.4.DSR E2E Delay under Jellyfish Attack

Average E2E Delay (ms) for system in DSR protocol undergoing the impact of jellyfish attack is shown in the figure. The framework includes three cases under varying attacker nodes as 1, 3, 6 and 9. There is no delay in simple DSR. The behaviour of DSR protocol changes as the count of attacker nodes varying from 1 to 9.The average E2E delay get enhanced substantially under the effect of jellyfish attack. Further after the execution of attacker detection and removal technique, End to End delay decreases as shown in Figure 5.4.

5.3.2.2 Throughput for DSR under Jellyfish Attack

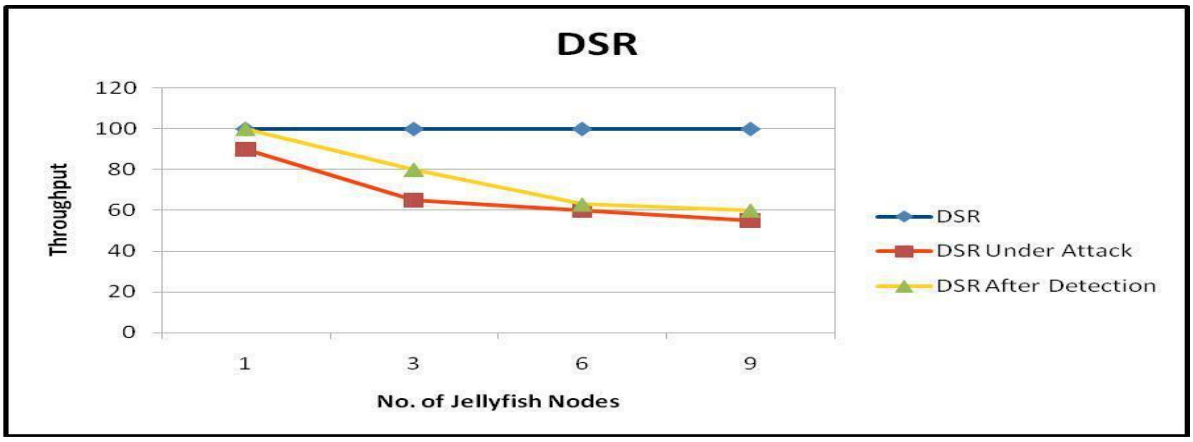


Fig.5.5. DSR Throughput under Jellyfish Attack

Throughput in DSR routing protocol is studied under the impact of jellyfish attack. Three Scenarios are shown by this figure with varying attacker nodes 1, 3, 6 and 9. Throughput is highest under the absence of attacker nodes. As the attacker nodes increase, throughput decreases significantly. Further after the implementation of attacker detection and removal technique, performance got improved in terms of throughput shown in Figure 5.5.

5.4 Comparison of AODV and DSR under Jellyfish attack

Comparison results have been carried out by comparing AODV with DSR under jellyfish attack by varying number of attacker nodes in the network.

5.4.1 E2E Delay

It is the average time taken by a data packet to arrive at the destination. It includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC and propagation transfer times.

$$D=\Sigma (Tr - Ts) / \Sigma \text{ No. of Connections} \quad (5.1)$$

Where Tr =received time

Ts =sent time.

(A)Comparison under 1 Attacker

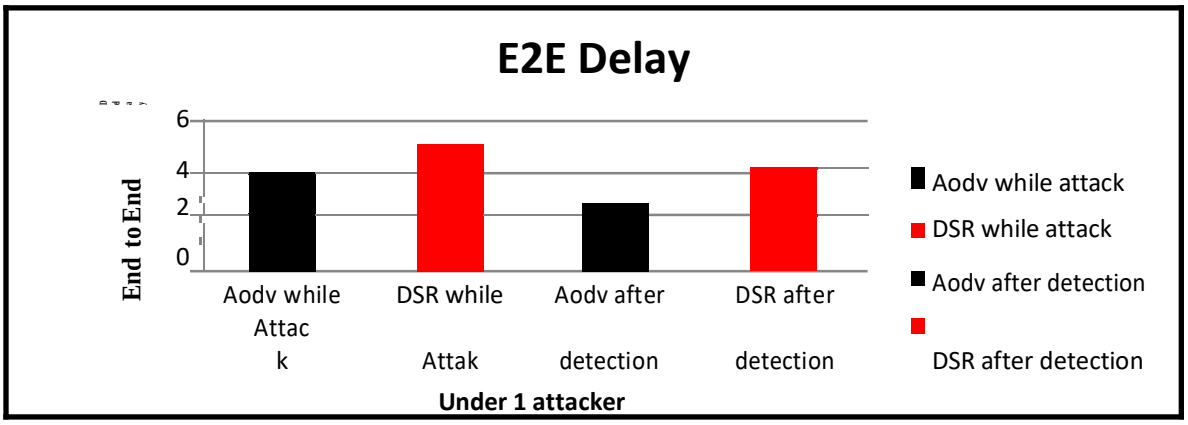


Fig.5.6.Delay in AODV, DSR for 1 Attacker under Jellyfish Attack

(B) Comparison under 3 Attackers

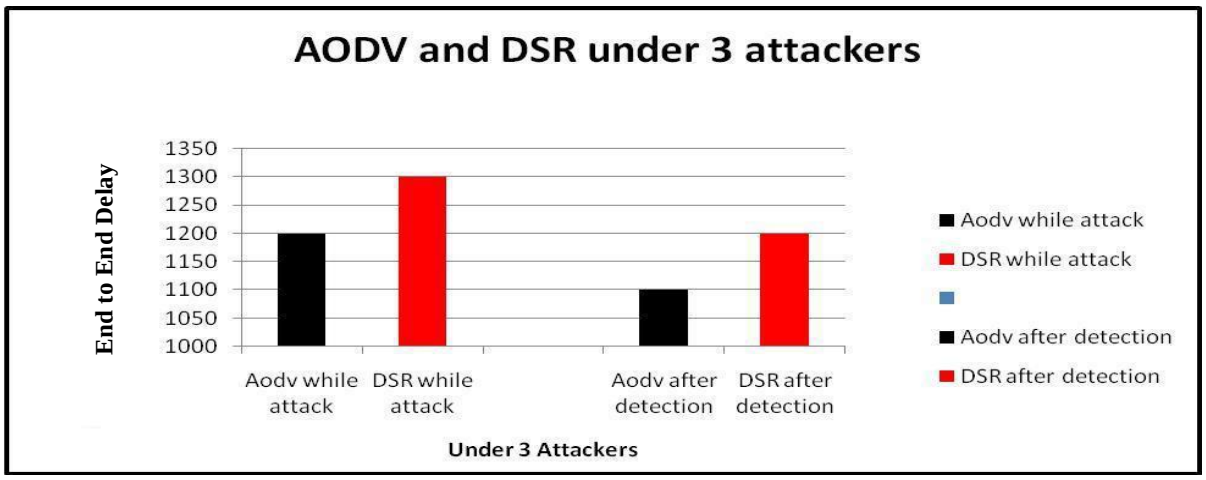


Fig.5.7.Delay in AODV, DSR for 3 Attackers under Jellyfish Attack

Comparison between AODV and DSR is done under 3 jellyfish attacker nodes in the figure shown above. AODV and DSR are compared with and without attacker nodes, after these JF nodes have been detected and removed. At first, it is noted that AODV is less affected by jellyfish attack in terms of End to End delay as compared to DSR. When attack detection and removal algorithm is applied, then AODV shows more improvement than DSR, which indicates

that AODV preferable outcomes over DSR under impact of jellyfish attack as shown in Figure 5.6 and Figure 5.7.

(C) Comparison under 6 Attackers

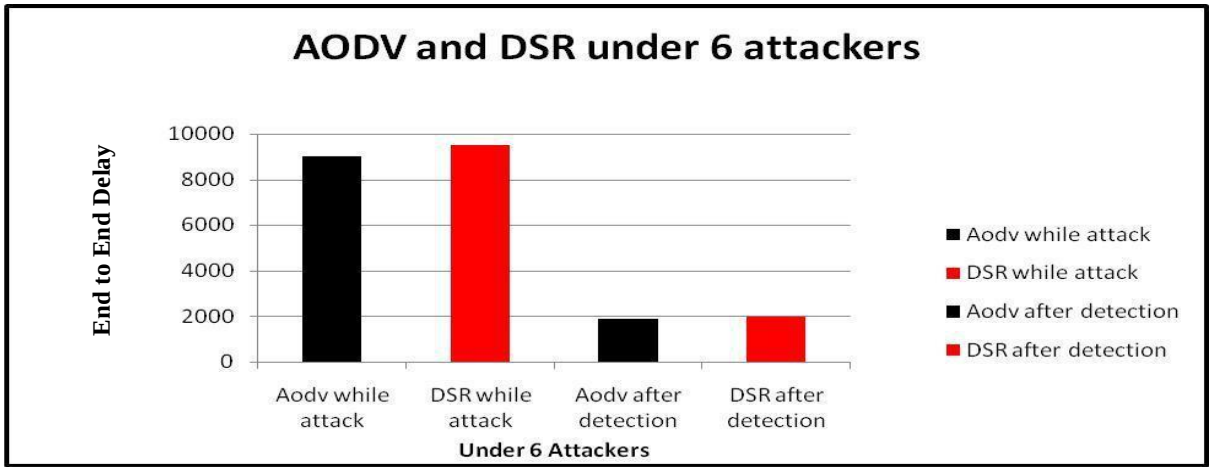


Fig.5.8.Delay in AODV, DSR for 6 Attackers under Jellyfish Attack

AODV and DSR protocols are compared under 6 jellyfish attacker nodes in two scenarios. While attack is performed AODV got less affected than DSR. Moreover, after the implementation of attack detection and removal algorithm, the execution of AODV indicates preferable outcomes over DSR regarding E2E delay as shown in Figure 5.8.

(D) Comparison under 9 Attackers

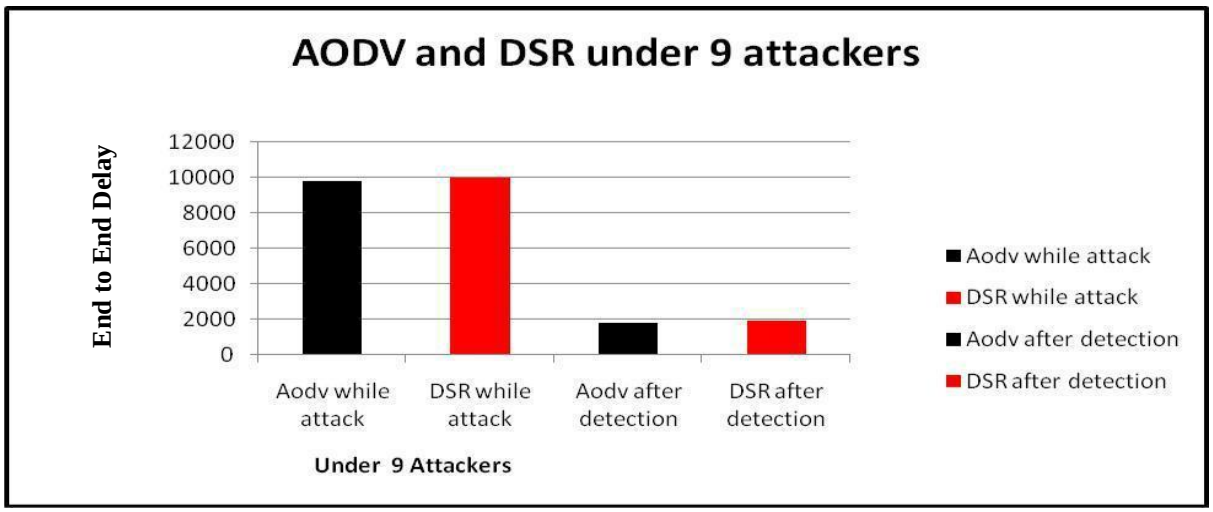


Fig.5.9.Delay in AODV, DSR for 9 Attackers under Jellyfish Attack

Comparison of AODV and DSR under 9 Jellyfish attacker nodes is done using NS2. AODV performs better than DSR under 9 attacker nodes also and gives reduced End to End delay as shown in Figure 5.9.

5.4.2 Throughput

It is the average rate of successful message delivery over a communication channel. It is also called as packet sent per unit interval of time. The throughput is usually measured in bits per second or data packets per time slot.

Throughput=Total packet received / Total time (5.2)

(A) Comparison under 1 Attacker

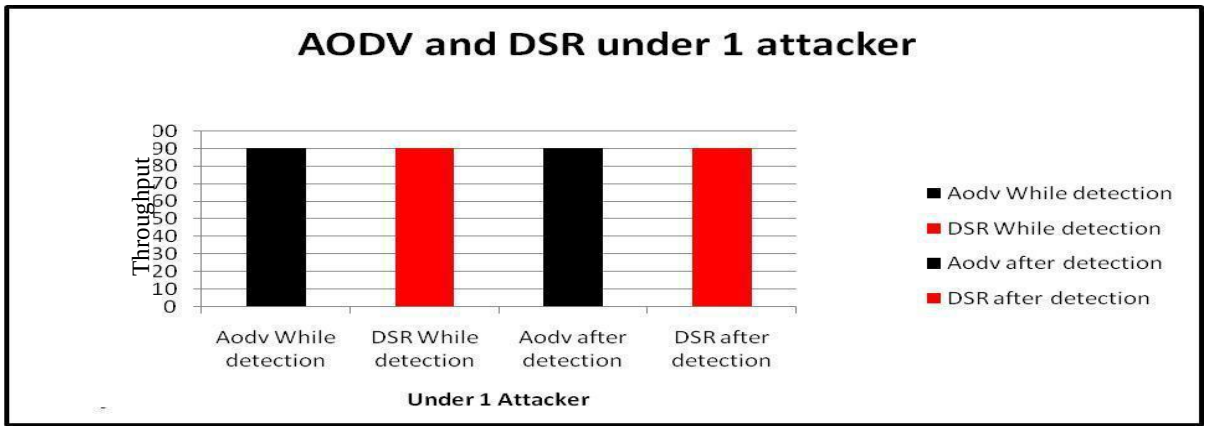


Fig.5.10.Throughput in AODV, DSR for 1 Attacker under Jellyfish Attack

Comparison of AODV and DSR is done under 1 jellyfish attacker node in the Figure 5.10. One attacker node does not vary the performance in terms of throughput in both the protocols. Both AODV and DSR remain unaffected by 1 jellyfish attacker node.

(B) Comparison under 3 Attackers

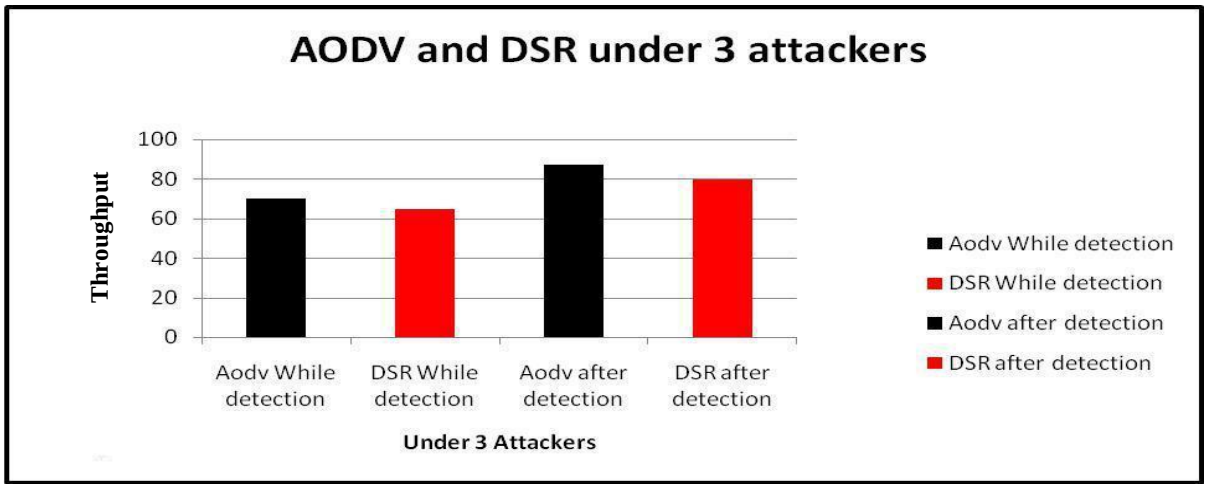


Fig.5.11. Throughput in AODV, DSR for 3 Attackers under Jellyfish Attack

Under the impact of 3 jellyfish attacker nodes, both AODV and DSR routing protocols are compared. Two scenarios are shown in the above Figure 5.11. It is noted that throughput reduces more in DSR than AODV. Further after the implementation of attacker detection and removal algorithm AODV shows more improvement than DSR in terms of throughput.

(C) Comparison under 6 Attackers

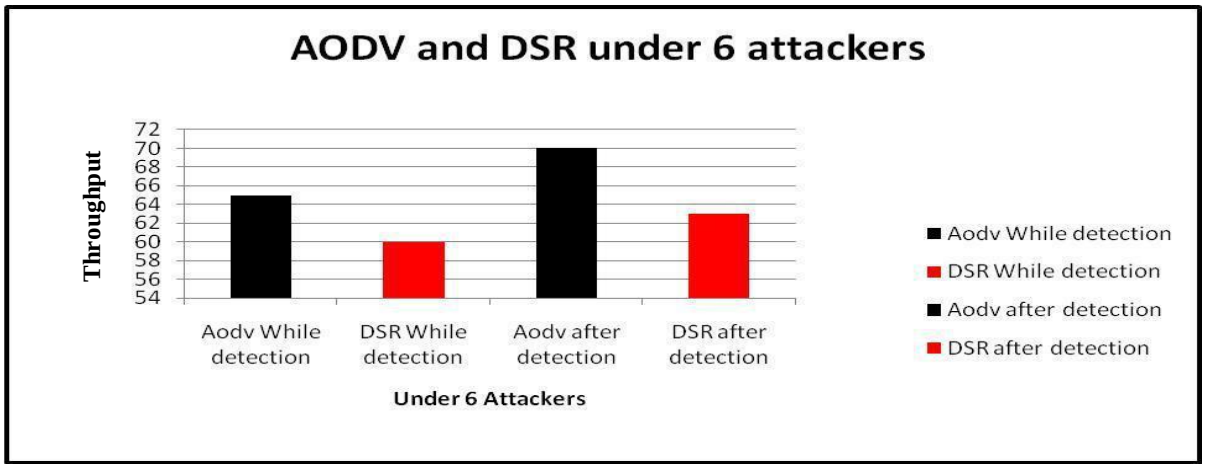


Fig.5.12.Throughput in AODV, DSR for 6 Attackers under Jellyfish Attack

Comparison of AODV and DSR under 6 jellyfish attacker nodes is analysed. It is noted that AODV has detected and removed jellyfish attacker nodes better than DSR and gives high throughput as shown in Figure 5.12.

(D) Comparison under 9 Attackers

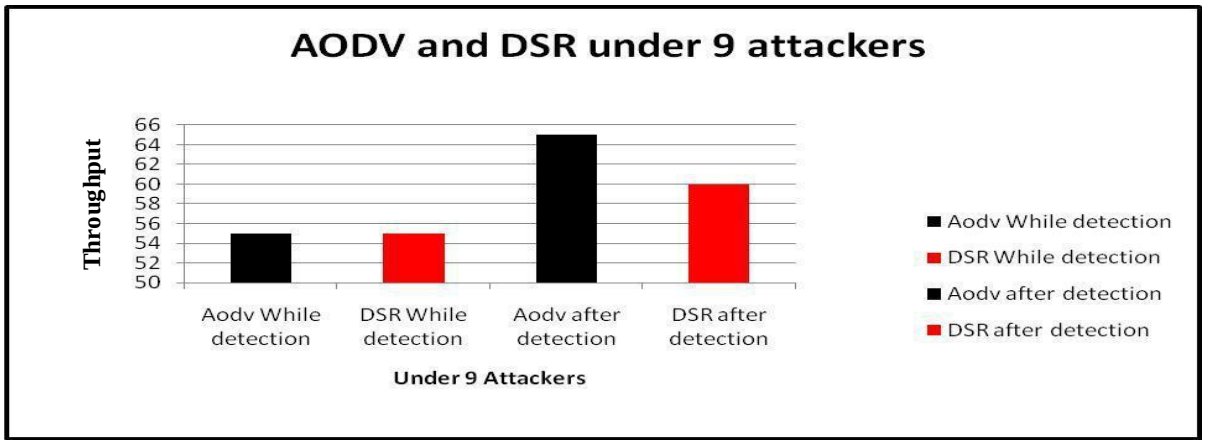


Fig.5.13.Throughput in AODV, DSR for 9 Attackers under Jellyfish Attack

Comparison of AODV and DSR is done under the impact of 9 jellyfish attacker nodes. It is shown that after the implementation of attack detection and removal algorithm, AODV shows more improvement than DSR in terms of throughput shown in Figure 5.13.

5.5 Summary

In this chapter on-demand based protocols, AODV and DSR are studied under the effect of jellyfish attack. The simulator used to carry out all the results is NS2. JF delay variance attack affects both AODV and DSR Performance of AODV and DSR is analysed as far as performance measurements, E2E delay and throughput using NS2 simulator. Afterwards both AODV and DSR protocols are looked at by taking fluctuating number of attacker nodes. It is analysed that attacker detection and removal technique makes more improvement in AODV than DSR. Hence, AODV protocol is less affected by jellyfish attack than DSR protocol.

CHAPTER 6
CONCLUSION AND FUTURE WORK

MANET is emerging as a useful technology in mobile computing and has found many applications in different fields. MANET supports various routing protocols, which helps the user to communicate in wireless system. Because of the decentralized nature as well as ability of nodes to move freely in any direction, MANET is highly prone to security attacks. Security is major issue in MANETs as it supports dynamic topology and any malicious node can enter the system and affect its normal functioning. Various types of attackers are present that intend to ruin the performance of network. One such attacker that affects the routing protocols is JF delay variance attack (JFDV). In Jellyfish attack, JF attacker becomes the part of routing mesh and introduces some amount of delay before forwarding the protocols. As it behaves more like an ordinary node, it is exceptionally hard to identify its essence. As discussed in literature survey, numerous procedures have been utilized to overcome the jellyfish attack in AODV routing protocol. In this work, emphasis is made on impact of jellyfish attack in DSR routing protocol. Further comparison is made between AODV and DSR routing protocols under the effect of differing count of jellyfish nodes. The quantity of attacker nodes included is 1, 3, 6 and 9. The execution measurements utilized are E2E delay and Throughput. AODV and DSR protocols are assessed with expanding number of attacker nodes increments range 1 to 9.

6.1 Conclusion

Major conclusions drawn on the basis of simulation results on NS-2 platform are-

- Jellyfish attacker node considerably affects the performance (Throughput and E2E delay) for both AODV and DSR routing protocols.
- Algorithm used for detection and removal of JF attacker nodes can significantly improves the performance of routing protocols.
- Throughput of AODV routing protocol is more able to support itself in comparison to that for DSR in the presence of JF attacker nodes. Further, after the detection and removal of attacker node, AODV routing protocol shows higher improvements than DSR.

- E2E delay has smaller value in AODV routing protocol than DSR. Moreover, after the detection and removal of jellyfish attacker node, AODV routing protocol indicates preferred outcomes over DSR as far as E2E delay.

6.2 Future Work

This examination can be stretched out by concentrate other two kinds of jellyfish attacks to be specific JF periodic dropping attack and JF reorder attack. This work can also be improved by considering other proactive protocols like OLSR, WRP and hybrid category of protocols like ZRP and ZLSR.

REFERENCES

[1] Kamali, Mojgan, and L Petre. "Comparing Routing Protocols" in *Engineering of Complex Computer Systems* , in *Proceedings of 20th International Conference on*, pp. 206-209, IEEE, 2015.

[2] S. S. Ali and G. M. Someswar, "Mobile adhoc network routing protocols under analytical study", in *IOSR Journal of Computer Engineering*, Vol. 10, Issue 4, 2013.

[3] Abdelshafy and A. Mohamed, "Dynamic source routing under attacks" , *7th International Workshop on Reliable Networks Design and Modeling*, pp. 174-180, IEEE, 2015.

[4] D. Tedia and U. K. Lilhore, "Various attacks including jellyfish attack along with security issues in MANET", in *International Journal for Research in Applied Science & Engineering Technology* , Vol. 4, Issue 7, 2016.

[5] M. Kaur, M. Rani and A. Nayar, "A comprehensive study of jellyfish attack in mobile adhoc networks",*in International Journal of Computer Science and Mobile Computing*, Vol. 3, Issue 4, pp. 199-203, 2014.

[6] B. Singla, A.K. Verma and L.R. Raheja, "An evaluation on selfish behaviour attack and jellyfish attacks under AODV routing protocol", *in International Journal in Foundations of Computer Science & Technology*, Vol. 7, No. 2, pp. 15-28, 2017.

[7] M.Yu and M Zhou, "A secure routing protocol against byzantine attack for MANETs in adversarial environments", in *IEEE Transactions on Vehicular Technology*, Vol. 58, No.1, pp. 449-460, 2009.

[8] S. Abbas, M. Merabati, D. Llewellyn-Jones and K. Kifayat, "Lightweight sybil attack detection in MANETs", in *IEEE System Journal*, pp. 236-248, 2013.

[9] N. Gupta and S. Narayan Singh, "Wormhole attack in MANET", in *Proceedings of 6th International Conference on Cloud Computing and Big Data Engineering*, Noida, India, pp.14-15, 2016.

[10] A. M. Halan and I. A. Ali, "TRIUMF: Trust based routing protocol with controlled degree of selfishness for securing MANET against protocol dropping attack", in *International Journal of Computer Systems*, Vol. 8, Issue 4, 2011.

[11] J. Sen, G. Chandra, Harihara S.G, H. Reddy and P. Balamuralidhar, "Mobile ad-hoc networks", in *7th International Symposium on Communication and Information Technologies*, Sydney, NSW, Australia, pp.17-19, 2007.

[12] M. Wazid, V. Kumar and R.H. Goudar, "Comparative performance analysis of routing protocols in mobile Ad Hoc networks under JellyFish Attack", in *Proceedings of 2nd IEEE International Conference on Parallel, Distributed and Grid Computing* , Solan , India, pp. 6-8, 2012.

[13] Wazid, Mohammad, Avita Katal, Roshan Singh Sachan, and R. H. Goudar. "E-TCP for efficient performance of MANET under JF delay variance attack" In *Information & Communication Technologies, 2013 IEEE Conference on*, pp. 145-150, IEEE, 2013.

[14] S. Kumar, "Detection and prevention of jellyfish Attack in AODV routing protocol in MANET", in *International Journal of Science Technology & Engineering*, Vol. 3, Issue 6, 2016.

[15] S. Garg and S. Chand, "Enhanced AODV protocol for defense against jellyfish attack on MANETs", in *IEEE International Conference on Advances in Computing*, Communications and Informatics , Greater Noida, India, pp. 24-27, 2014.

[16] Mr. H. R. Khirasariya, "Simulation study of jellyfish attack in MANET using AODV routing protocol" ,in *Journal of Information*, Knowledge and Research in Computer Engineering, Vol 2, Issue 2, 2013.

[17] A. Sharma and R. Kaur, "Non-Cryptographic Detection approach and countermeasure for JFDV attack", in *Proceedings of the 7th International Conference on Security of Information and Networks*, Glasgow, Scotland, UK, pp. 9-11, 2014.

[18] P. Dahiya and Miss Bhawana, "Design and implementation of NAODV-ETCP to handle jellyfish attack", in *International Journal & Engineering Trends and Technology*, Vol. 35, No. 7, 2016.

[19] S. Kaur and R. Singh, "Detection and prevention of JFPD attack in MANETs using NBA Technique", in *Worldwide Journal of Multidisciplinary Research and Development* , Vol. 3, Issue 6, pp. 88-91, 2017.

[20] I. Aad, J.P Habaux and E W. Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks", in *IEEE/ACM Transactions on Networking*, Vol. 16, Issue 4, pp. 791-802, 2008.

[21] H.L Nguyen and U. T Nguyen, "A Study of Different types of attacks on multicast in mobile adHoc networks", in *Proceedings of IEEE International Conference on Networking*, pp. 32-46, 2016.

[22] P. Patel , P. Manish and P. Megha , "Jellyfish Attack Detection and Prevention in MANET: A Review", in *International Journal of Advance Research in Engineering*

[23] V. Laxmi, C. Lal, M.S Gaur and D. Mehta, "Jellyfish attack: Analysis Detection and Counter Measure in TCP-based MANET", in *Journal of Information Security and Applications,* Elsevier, 2014.

[24] S. Sachdeva and P. Kaur, "Detection and Analysis of Jellyfish Attack in MANETs", in *Proceedings of IEEE International Conference on Inventive Computation Technology,* Coimbatore, India, pp. 26-27, 2016.

[25] I. Aad, J.Habaux and E.W. Knightly, "Impact of denial of service attacks on Ad Hoc networks", in *IEEE/ACM Transactions on Networking",* Vol. 16, Issue 4, pp. 791-802, 2008.

[26] A .K .Said Ali and U.V. Kulkarni, " Comparing and Analyzing Reactive Routing Protocols (AODV, DSR and TORA) in QoS of MANET", in *Proceedings of IEEE 7th International Advance Computing Conference, 2017.*

[27] Y. Bai and Y Mai, "Performance Comparison and Evaluation of the Proactive and Reactive Routing Protocols for MANETs", in *Wireless Telecommunications Symposium* ,2017.

[28] P. Nayak and P. Sinha "Analysis of Random Way Point and Random Walk Mobility Model for Reactive Routing Protocols for MANET Using NetSim Simulator" in *Proceedings of International Conference on Artificial Intelligence, Modelling and Simulation,* 2013.

[29] D. N. Patel , S. B. Patel and H.R Kothdiya, " A Survey of reactive protocols in MANET", in *Proceedings of International Conference on Information Communication and Embedded Systems,* 2014.

[30] B. Karthikeyan, N. Kanimozhi and S. H. Ganesh, "Analysis of Reactive AODV Routing Protocol for MANET", in *World Congress on Computing and Communication Technologies, 2014.*

[31] S.Jain, A. Shastri and B. K. Chaurasia , "Analysis and Feasibility of Reactive Routing Protocols with Malicious Nodes in MANETs", in *Proceedings of International Conference on Communication Systems and Network Technologies,* 2013.

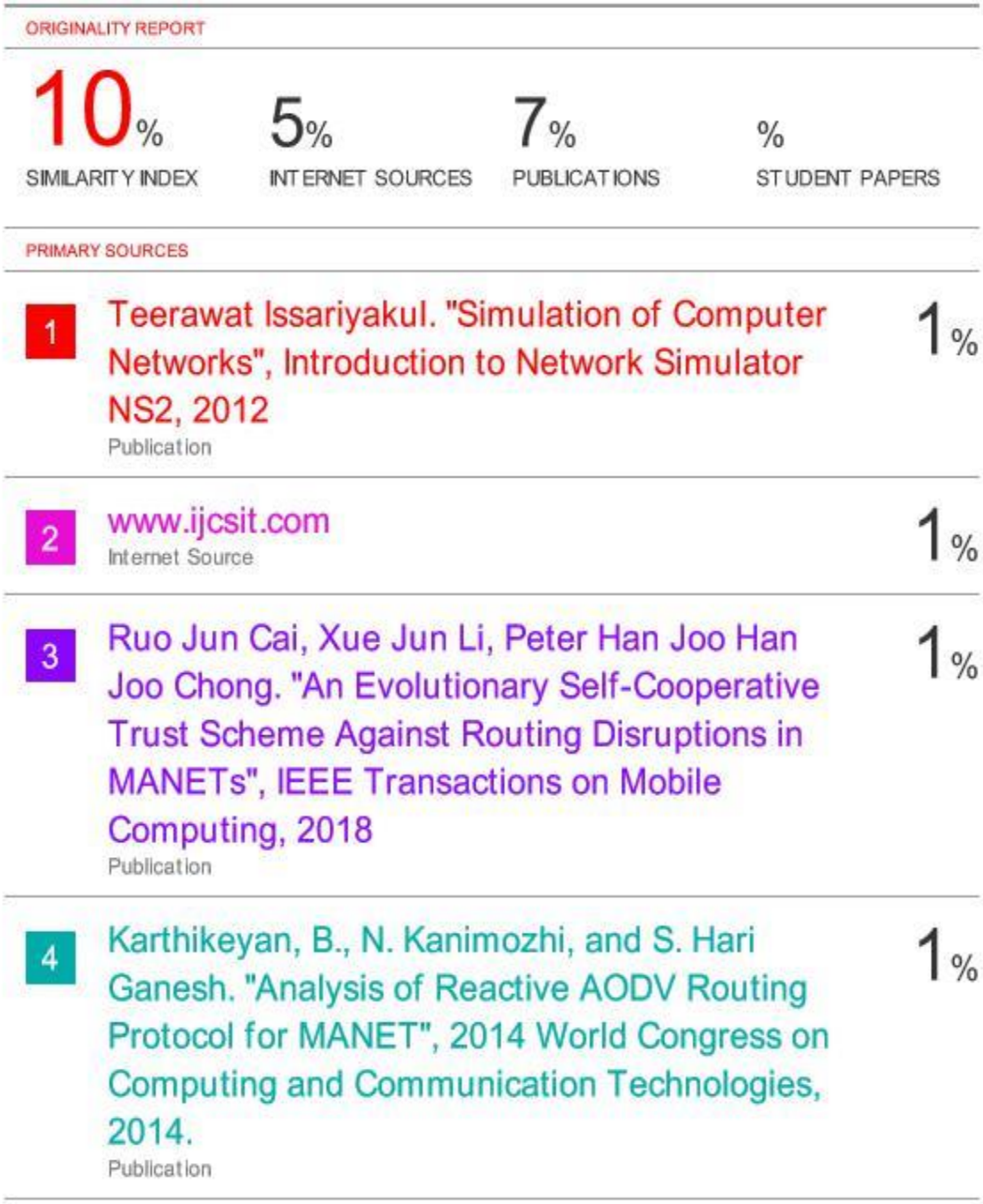
[32] R. Yercajana and A.K. Sarjr, "A Timestamp Based Multipath Source Routing Protocol for Congestion in MANET", in "*International Advance Computing Conference, Communication,* IACC, 2009.

LIST OF PUBLICATIONS

- D. Sabharwal, S. Saxena, " Performance Evaluation of AODV with Self-Cooperative Trust Scheme Using Jellyfish Delay Variance Attack" in *ICICCS*, June 14-15, 2018, Vaigai College of Engineering, Madurai, India (IEEE) (Accepted and Presented).

APPENDIX

Plagiarism Report



ORIGINALITY REPORT

10%	5%	7%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Teerawat Issariyakul. "Simulation of Computer Networks", Introduction to Network Simulator NS2, 2012 Publication	1%
2	www.ijcsit.com Internet Source	1%
3	Ruo Jun Cai, Xue Jun Li, Peter Han Joo Han Joo Chong. "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs", IEEE Transactions on Mobile Computing, 2018 Publication	1%
4	Karthikeyan, B., N. Kanimozhi, and S. Hari Ganesh. "Analysis of Reactive AODV Routing Protocol for MANET", 2014 World Congress on Computing and Communication Technologies, 2014. Publication	1%