DETECTION AND DEFENSE AGAINST JELLYFISH DELAY VARIANCE ATTACK IN MANETs

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

Master of Engineering

in

Information Security

Submitted By

SIMRANPREET KAUR

Roll No. 801333027

Under the supervision of:

Dr. Anil Kumar Verma

Associate Professor

Mrs. Rupinderdeep Kaur

Lecturer

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

May 2015

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*Detection and defense against jellyfish delay variance attack in MANETs*", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Anil Kumar Verma, Mrs. Rupinderdeep Kaur and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Simranpreet Kaur
801333027

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Mrs. Rupinderdeep Kaur
Lecturer
Computer Science and
Engineering Department

Dr. Anil Kumar Verma
Associate Professor
Computer Science and
Engineering Department

Countersigned by

Dr. Deepak Garg
Head
Computer Science and Engineering Department
Thapar University
Patiala

Dr. S. S. Bhatia
Dean (Academic Affairs)
Thapar University
Patiala

ACKNOWLEDGEMENT

No volume of words is enough to express my gratitude towards my guide, **Dr. Anil Kumar Verma**, Associate Professor, **Mrs. Rupinderdeep Kaur**, Lecturer, Computer Science and Engineering Department, Thapar University, who has been very concerned and has supervised the work presented in this thesis work. They have helped me to explore this vast field in an organised manner and provided me with all the ideas on how to work towards a research oriented venture.

I am also thankful to Dr. Deepak Garg, Head of Department, CSED and Ms. Jhilik Bhattacharya, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work. I would also like to thank the staff members and my colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis.

Most importantly, I would like to thanks my parents, friends and the almighty for showing me the right direction out of the blue, to help me to stay calm in the oddest of the times and keep moving even at times when there was no hope.

Simranpreet Kaur

801333027

ABSTRACT

Mobile ad hoc networks comprise of mobile nodes communicating in multihop fashion without any infrastructure and are suitable for situations where infrastructure does not exist. These networks are vulnerable to many types of active, passive and DoS attacks. Jellyfish attack is a type of DoS attack which obeys protocol rules and is of 3 types: jellyfish reorder attack, jellyfish delay variance attack, jellyfish periodic dropping attack. Focus of thesis work is on evaluating the performance of network under the effect of jellyfish delay variance attack on AODV in MANETs and a scheme is proposed to detect and minimize the performance degradation caused by attacker. Simulations are carried out by taking different scenarios with varying node density to evaluate the effectiveness of proposed scheme and it is observed that performance of network improves in presence of scheme.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AODV	**A**d hoc **O**n demand **D**istance **V**ector
CBIDPT	**C**luster **B**ased **I**ntrusion **D**etection and **P**revention **T**echnique
CGSR	**C**luster **G**ateway **S**witch **R**outing
DoS	**D**enial **O**f **S**ervice
DSDV	**D**estination-**S**equenced **D**istance-**V**ector
DSR	**D**ynamic **S**ource **R**outing
FSR	**F**isheye **S**ource **R**outing
GSR	**G**lobal **S**tate **R**outing
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
JF	**J**elly**F**ish
JFDV	**J**elly**F**ish **D**elay **V**ariance
MANET	**M**obile **A**dhoc **N**etwork
PRNet	**P**acket **R**adio **N**etwork
PDR	**P**acket **D**elivery **R**atio
RERR	**R**oute **ERR**or
RREP	**R**oute **REP**ly
RREQ	**R**oute **REQ**uest
RTO	**R**etransmission **T**ime**O**ut
RTT	**R**ound **T**rip **T**ime
SHARP	**S**harp **H**ybrid **A**daptive **R**outing **P**rotocol
SURAN	**SU**rvivable **RA**dio **N**etworks
SCBIDPT	**S**uper Cluster **B**ased **I**ntrusion **D**etection and **P**revention **T**echnique
TORA	**T**emporarily **O**rdered **R**outing **A**lgorithm
WRP	**W**ireless **R**outing **P**rotocol
ZRP	**Z**one **R**outing **P**rotocol

CHAPTER 1

INTRODUCTION

1.1 MOTIVATION

In the past few years, wireless technology has gained precedence in the world of data communication and this has caused a proliferation of devices complying with the standards of wireless technology. In different areas like in corporate sector various computers necessitate to be connected among themselves, this can be executed either by employing infrastructured networks using base station for controlling purpose or infrastructure less networks can be used where no central administration exists.
Mobile ad hoc networks are known for employing wireless links for communication by forming collection of mobile nodes. These networks are unalike from other networks that communicate by maintaining fixed infrastructure or base station that requires a lot of time and money [1].

In MANETs, nodes in radio transmission range can communicate directly and those lying in the exterior of direct transmission range communicate in multi hop fashion with each intermediate node relaying the packets. It is the absenteeism of infrastructure in MANETs that node themselves proceed to control and organise the network on an assumption that nodes are trustworthy and are inclined to comply with protocol notion, diagnosing presence of other nodes is salient to have communication[2]. Nodes can be laptops or mobile phones. Dynamic topology is laid by nodes where nodes can join or disjoin the network anytime. Nodes also operate as router to identify and maintain routes with other nodes. Property of being adaptable and self configurable makes them deployable in situation where no infrastructure can be maintained or infrastructure is demolished or inconvenient to use or is very expensive[3].

MANETs are applicable in various areas like military, battlefields, virtual classrooms, rescue systems or emergency situations where infrastructure is damaged [2]. Along with many applications, it is fraught with challenges like dynamic topology because nodes keep moving arbitrarily and it cannot be ascertained that node will still be present the very next minute or not and that makes routing difficult so there is always a need of coherent routing protocol that can cope up with topological changes, power

constraint.In MANETs, physical security threat is higher than wired networks. Wireless link is accessible by both legitimate and non legitimate users so these networks are prone to various kinds of attacks like active attacks, passive attacks, Denial of service (DoS) attacks like blackhole attack, jellyfish attack, greyhole attack etc. Scope of thesis is to analyse the effect on jellyfish attack on ad hoc on demand distance vector routing protocol in MANETs [4]. Aftereffect of attack is studied and suitable preventive measure is proposed keeping in consideration the false positives to revamp the performance of network that was degraded by the attack.

1.2 WIRELESS NETWORK

Wireless networks are advancing because these networks are unrestricted by wires to allow communication between devices. Prime advantage is that users can move freely and still be connected to network. Wireless networks are considerably used in areas where wires cannot be brought to use like in hilly areas.

1.2.1 PRIVATE AREA NETWORK (PAN)

These are short range networks employed to transfer information between devices without the need of wires like Bluetooth. Bluetooth can create wireless connection between devices which are close to each other [5].

1.2.2 WIRELESS LOCAL AREA NETWORK (WLAN)

Popularly known as IEEE 802.11 and is used in public areas, universities, educational campuses etc. It is prominently used because of its simplicity in terms of use and installation.

1.2.3 WIRELESS WIDE AREA NETWORK (WWAN)

It has much wider range than WLAN, it can be formed by combination of two or more WLANs

1.3 IEEE STANDARDS FOR WIRELESS NETWORKS

There exist 3 IEEE standards for wireless networks- 802.11a, 802.11b, 802.11g [6]

Table 1.1: IEEE standards [6]

IEEE	BAND
802.11a	5 GHz
802.11b	2.4 GHz
802.11g	2.4 GHz

1. 4 MOBILE AD HOC NETWORKS (MANETs)

1.4.1 INTRODUCTION TO MANETs

Roots of MANETs can be traced back to DARPA PRNet (Packet radio network) project in 1972 incited by proficiency of packet switching and its strength in mobile domain. By the use of multi hopping, radio coverage barrier is suppressed, offering prolific user communication in broad geographic area. To diminish the momentum of security attacks in networks, DARPA in 1983 developed SURAN (Survivable Radio Networks) and this lead to Low-Cost Packet Radio methodology outlined in 1987. Expanded internet infrastructure in 1990's prompted more usage of packet radio networks [7].

MANETs conduct communication using mobile nodes connected via wireless links, central feature of MANETs is absenteeism of infrastructure. Direct communication is offered to nodes residing in radio transmission and Multi hop communication is offered to those lying in the exterior of direct transmission range. Nodes proceed to represent themselves as routers for relaying packets.

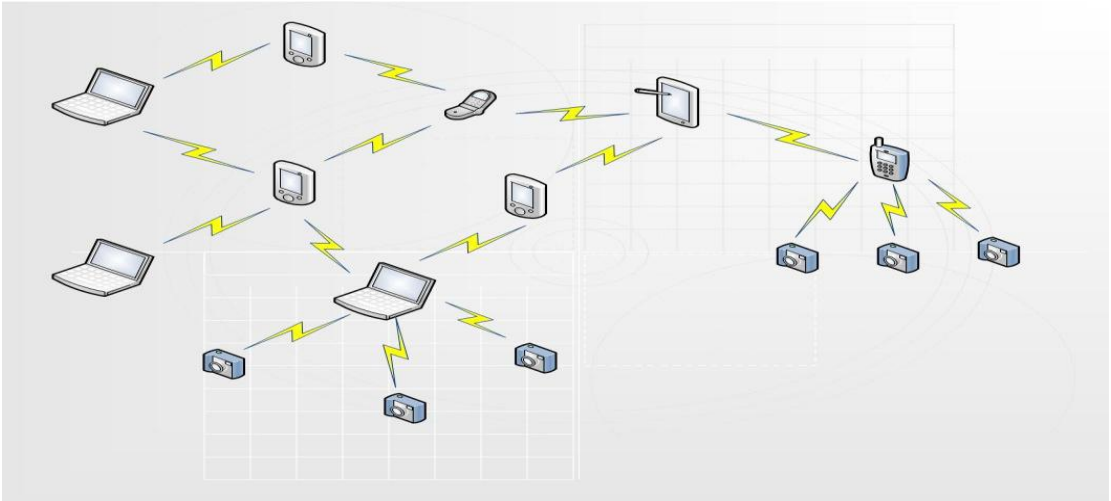


Figure 1.1: MANETs Example

Figure 1.1 depicts a network topology of Computers, Phones connected via wireless links.

1.4.2 MANET CHARACTERISTICS

MANETs are known for its working without utilising infrastructure and is characterised by dynamic topology in which nodes can be the part of network and can disjoin the network at any time. These networks are self configurable and adaptable entailed by random movement of nodes and are deployable in situation where infrastructure is not present or is expensive to fix. Each node relays data packet for other nods because communication is not under observation of central administration and nodes themselves holds responsibility of controlling and organising the network. Nodes can be laptops or mobile phones and have restricted power or battery [2,3]. Physical security of MANETs is important to protect the network from being attacked and having depreciated performance as a consequence.

Characteristics of MANETs:

- Dynamic topology
- Self configurable
- No central administration
- Power constraint
- Prone to physical insecurity
- Link breakage

1.4.3 MANET APPLICATIONS

MANETs have diverse application areas. Being infrastructure- less makes them unique and useful in areas where infrastructure is damaged or is unavailable. Typical applications are [7]:

- **Rescue Systems**

Effective use of MANETs is in rescue system in order to provide relief in disaster struck areas where infrastructure is damaged by earthquake, hurricanes, fire, flood, Tsunami. Rescue team use small hand held devices to relay information.

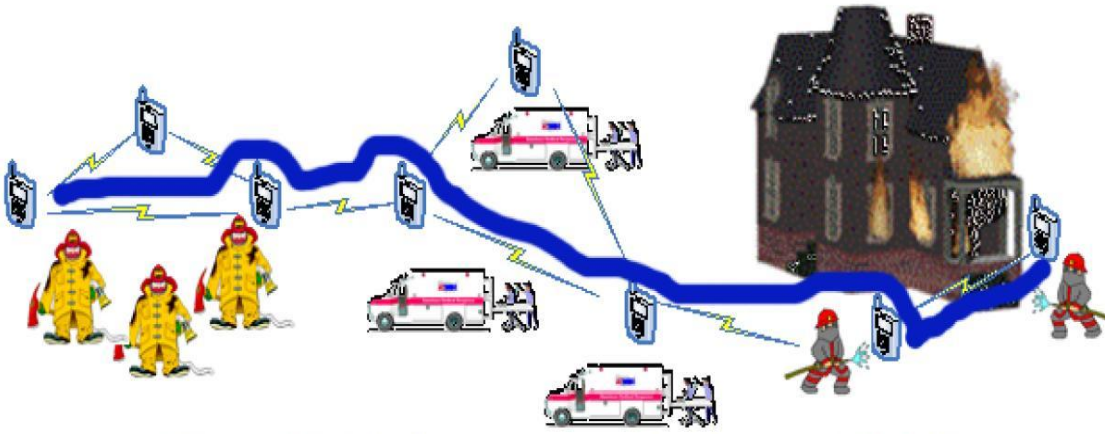


Figure 1.2: MANET as a rescue system

- **Military battlefield**

Communication among soldiers, military headquarters and vehicles used in battlefield is essential and this purpose is served by MANETs

- **Commercial use**

MANETs offer appreciable service in commercial sector, like in e-commerce to make electronic payments at any point of time and at any place [8].

- **Personal area network (PAN)**

MANETs are extensively used to maintain communication between various mobile devices like laptops, mobile phones etc; that is, to create PAN.

- **Educational and local level application**

Universities and educational campuses now a days use MANETs for conducting lectures and for setting up virtual classrooms. Local level application of MANETs can be in shopping malls, sport stadiums, fairs etc.

- **Entertainment**

MANETs have gained popularity in field of entertainment like in multi user games, entertainment parks etc.

1.4.4 MANET CHALLENGES

Besides variety of applications, specific features of MANETs impose challenges like [8]:

- **Routing**

Mobile nodes in MANETs keep moving arbitrarily thus forming dynamic topology leading to demand of efficient routing, without causing excessive level of overhead

related to traffic. Hybrid routing protocol can be of significant use because it has characteristics of proactive as well as reactive protocol.

- **Security and node cooperation**

MANETs tends to be defenceless against security attacks because of non presence of central administration and are prone to active attacks like modification, deletion of data packet and passive attacks like eavesdropping and other denial of service attacks. Communication in MANETs is solely based on mutual trust among nodes but some nodes may try to be non co-operative to routing so as to preserve their battery. Preventive measures have to be taken to get rid of selfish nodes.

- **Power consumption**

Battery constraint of mobile nodes makes them vulnerable to security attack such as denial of service attack where attacker has tendency to exhaust its energy and making it disabled to perform routing functions.

- **Device discovery**

Nodes at any time can join or disjoin the network, moved in nodes requires identification; that is, dynamic update is needed for information about the nodes in network so as to have the facility of automatic optimal route selection.

1.5 SECURITY ISSUES OF MANETs

Predisposition to security threats is more for wireless as compared to wired networks. To obtain secure communication security of network is necessity.

Wireless networks security issues are more difficult than the ones for wired networks because of rapidly changing unpredictable topology formation by mobile nodes and battery constraint and bandwidth constraint [2].

MANET often suffers from security attacks because of its features like [1] dynamically changing topology, no clear line of defence, low degree of physical security of mobile nodes, link breakage, absence of central administration, power constraint.

Mobile nodes are capable of joining or leaving the network anytime and it cannot be ascertained if node will be present the very next moment, this permits unknown nodes to participate in network and forward the packets and then they can even hinder in normal working of network by modifying or dropping the packets. Classification of adversaries-outsiders or insiders. Attackers with no knowledge of secret information

are outside attackers having no trust relationship with nodes of network and attackers with knowledge of secret information are insiders with trust relationship with network. MANETs work in absence of central administration and the nodes communicate with each other on the basis of mutual trust, this makes mobile ad hoc networks more vulnerable to the exploitation from inside the network. Non presence of predefined boundary assist them disrupting network performance.

Battery constrained mobile nodes are targeted by denial of service attack where adversary sends huge traffic to victim with objective of exhausting its battery while tackling those packets, this makes node inefficient to participate in other network activities.

Presence of selfish nodes abstaining to cooperate in routing or forwarding activities to reserve their battery is a security concern. Network collapse takes place when majority nodes obtain selfish behaviour [4].

Security parameters:

- Availability: It assures that data is successfully transmitted in timely manner from source to the destination.
- Confidentiality: It ensures that data is only read by intended destination and not by any unauthorized person and safeguards data from eavesdropping.
- Integrity: It ensures that data is not modified, deleted or altered in an unauthorized manner or malicious manner.
- Authentication: It guarantee about the identity of the node with which the communication is being carried out. It is necessary to assure about the identity of communication partner otherwise attacker may impersonate to be a legitimate entity and access the confidential information.
- Non Repudiation: It assures that the sender and receiver cannot deny that they have transmitted or received such message. This is helpful in the detection of misbehaving nodes.

Most crucial among them is authentication and once it is achieved, then confidentiality can be attained using encryption [9].

Encryption can serve as a technique for achieving security parameters. Out of public key encryption and private key encryption, regarding MANETs beneficent option is

using private key encryption because less computational power of mobile nodes cannot afford computational demands of public key encryption [4].

Being exposed to vulnerabilities, MANETs tend to be unguarded against security attacks.

1.6 SECURITY ATTACKS

Attacks can be classified as [10]:

- Active attacks
- Passive attacks

ACTIVE ATTACKS

These attacks tend to trouble normal network operations by deleting the data, modifying the data, injecting false message, impersonating benign node. Attacker can be internal or external to the network.

Classification of active attacks:

- Spoofing
- Fabrication
- Timing attack
- Dropping attack

Spoofing

Procuring the identity of benign node and availing the previously restricted services is the objective of attacker here

Fabrication

False information is injected in the legitimate packets by the malicious node. Sender of route request (RREQ) may receive multitudinous replies (RREP). Instead of modifying the existing packet attackers may forge, fabricate their own packets to create a chaotic situation in the network [10].

Fabrication attack is classified as:

- Active forge attack: It incorporate sending fake messages without receiving any message related to it.
- Forge reply attack: After being recipient to RREQ, attacker forges the route reply message.

Timing attack

Attacker's inclination is attracting other nodes by advertising itself as a node to be closer to the actual. This technique is base of Rushing attack, denial of service attacks.

Dropping attack

Selfish nodes aim at preserving their resources by dropping the packets deliberately which are not destined for them. This attack forbids end to end communication causing the data packets to be transmitted again and new routes to the destination be explored, leading to declined network performance.

In selective dropping attack, attacker's preference is to drop only some packets to defend itself from being detected [10].

PASSIVE ATTACKS

In passive attack, no obstruction on the part of attacker is there to hinder normal operations of the network making detection phase difficult. Agenda of attacker is procurement of the information being transmitted between the communicating parties.

Classification of passive attacks:

- Eavesdropping
- Traffic analysis

Eavesdropping

Attacker means to observe the private communication between two parties without them knowing and the information so accumulated can be used later on. The information may incorporate private key, public key, and location of the node or passwords.

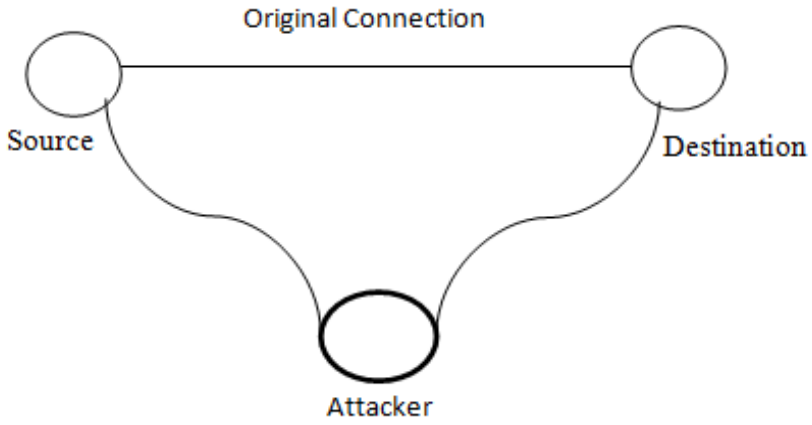


Figure 1.3: Eavesdropping attack [11]

Traffic analysis

Analysing network traffic patterns helps collecting information on network topology. Information that can be obtained from traffic analysis is [10]:

- Location of nodes and network topology
- Roles played by the nodes
- Source and destination of communication

Another classification of security attacks is on the basis of layers of protocol stack [10, 11, 12].

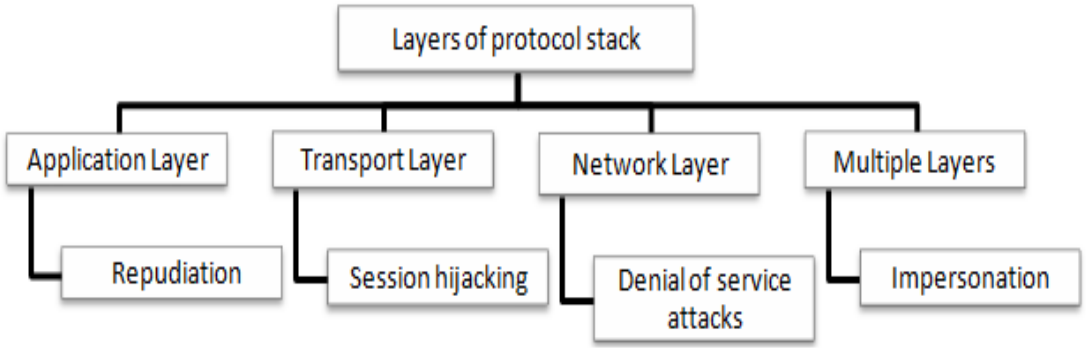


Figure 1.4: Attacks on the layers of protocol stack [12]

Application Layer Attacks

- **Repudiation attack**

It is an attack when sender or receiver has disavowed about received message. Attacker may deny about the online bank transaction or may refuse about credit card or debit card purchase which is a repudiation attack.

Transport Layer Attacks

- **Session hijacking**

In this attack, Attacker hijacks an undefended session. Attacks works by spoofing IP address of victim and launching DoS attack against it by estimating correct sequence number that was expected by target. Attacker's motive is to procure secure information like login id and password of the target [13].

Network Layer Attacks

- **Denial of service attacks**

Denial of Service attack is an attempt to circumscribe the access to a particular resource be it a node or whole network itself.

Types of Denial of Service attacks:

a. **Wormhole attack**
b. **Blackhole attack**
c. **Grayhole attack**
d. **Rushing attack**
e. **Jellyfish attack**

1.6.1 WORMHOLE ATTACK

In this two attackers are placed at powerful spots and construct tunnel between them , they attempt to create an illusion that they are immediate neighbours, one worm replays the recorded packet to peer worm and this type of attack have less chances of detection.

Example of wormhole attack

Consider A and B two nodes forming a high speed tunnel. In MANETs multi hop trend is followed if two nodes are not in direct range, but presence of A and B formulates misconception of being immediate neighbours. Packet travelling from tunnel is swift then packet following multiple hops. A replays the packets to B by availing tunnel and vice versa. A and B may either prefer dropping of packets selectively, scrutinize the traffic and interpose in network communication [14]. Figure 1.5 shows diagram of wormhole attack.

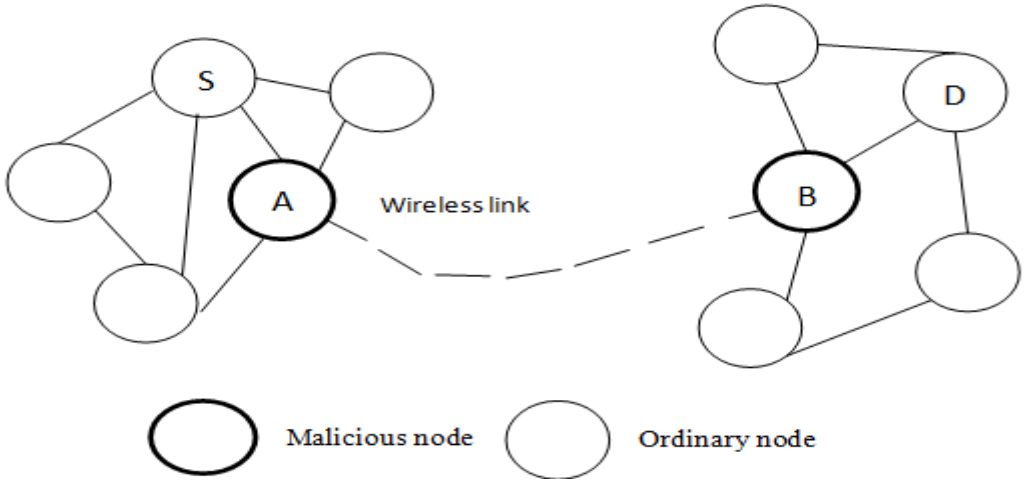


Figure 1.5: Wormhole attack [12]

1.6.2 BLACKHOLE ATTACK

Blackhole attack exploits the ad hoc on demand distance Vector (AODV) routing protocol. It is a routing protocol in MANETs. It comes to play whenever new route is to be found out. To ascertain route to the destination RREQ message is broadcasted to node's neighbours, if neighbour is itself the destination then it replies with RREP if not then it forwards the RREQ to its neighbours and so on. Each node receiving request caches route back to sender so as to send back RREP to correct sender. Monitoring link status helps nodes keep information about active paths of next hops and if link breakage is realised then RERR is sent to other nodes [15].

It is a DoS attack. Attacker node publicises itself as having shortest path to destination and if sender of RREQ receives reply from attacker before benign node could manage to reply then a deceived route is established, attacker may degrade network performance by not forwarding packets to actual destination or dropping the packets.

Example of blackhole attack

Consider source S wanting to have communication with destination D, it will broadcast RREQ and if no intermediary node has fresh route to destination then RREQ will be forward. Malicious node Z claims about possessing fresh route to destination and abstain from forwarding the packet ahead. If reply sent by Z reaches S before reply sent by neighbour of S then according to AODV rules, S ignores other reply packets and believes that Z has shortest path to D and due to this Z can disturb the traffic and consume the packets or drop them. [14]. Figure 1.6 shows blackhole attack.

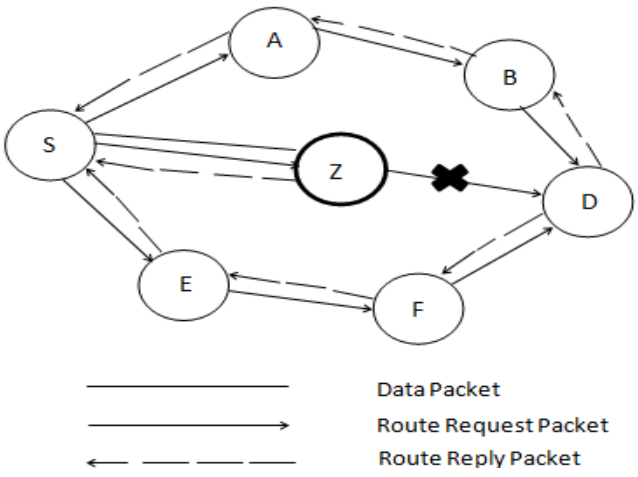


Figure 1.6: Blackhole attack [14]

1.6.3 GRAYHOLE ATTACK

It is an extension of blackhole attack and is not easy to detect. Grayhole attack is of 3 types:

- Attacker dropping certain packets only.
- Attacker acts maliciously for some time and is normal at rest of the time
- Attacker drop packets from particular nodes for some time and later on it starts behaving as other ordinary nodes.

At initial stage node Z is normal and forwards all the packets from S to D. Figure 1.7 shows ordinary behaviour of node Z.

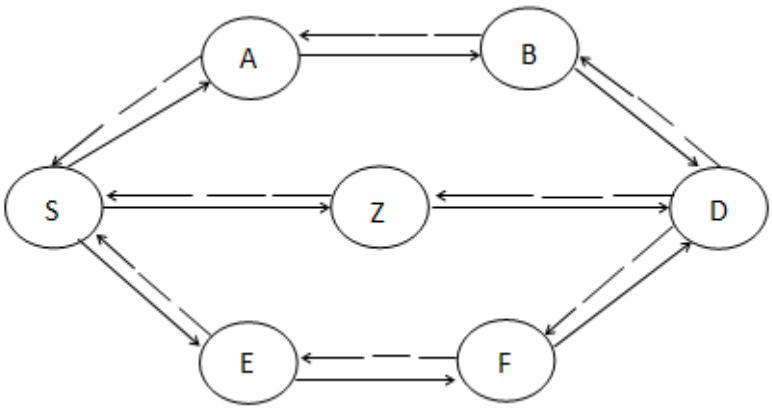


Figure 1.7: MANET using AODV Routing protocol [14]

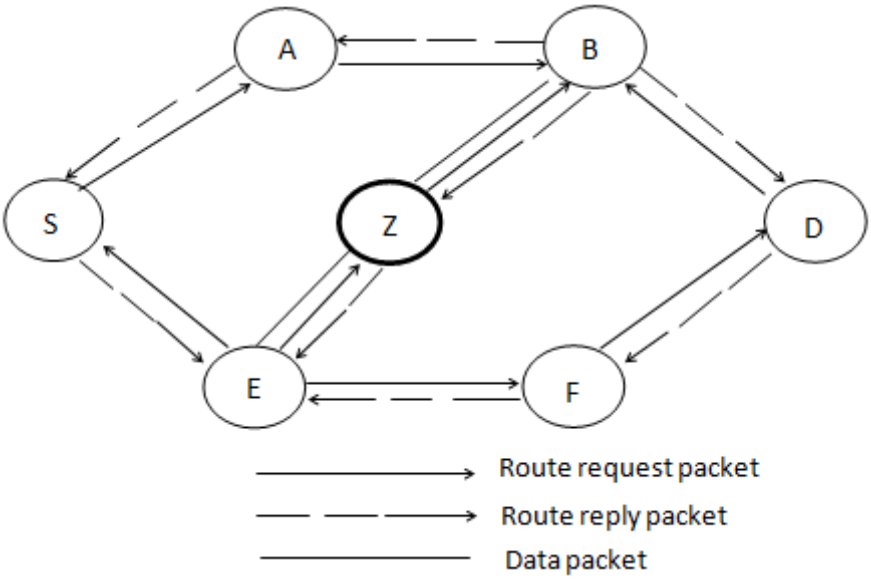


Figure 1.8: Grayhole attack [14]

After some time, Z starts dropping packets sent by S to D and after that again behaves normally. Figure 1.8 shows malicious behaviour of node Z [14].

1.6.4 RUSHING ATTACK

Consider S as source node and P as destination node. C and G are the two immediate neighbours of P. S in order to have communication with P, will broadcast RREQ. There are multiple paths to reach P. C and G will pass RREQ to P. If D acts maliciously, then S will turn out to be unsuccessful in obtaining benign path to P because if D passes RREQ swiftly taking multiple paths through C and G than other nodes then S will ignore other RREQ packets. Later on, D may not forward RREQ [16]. Figure 1.9 shows rushing attack.

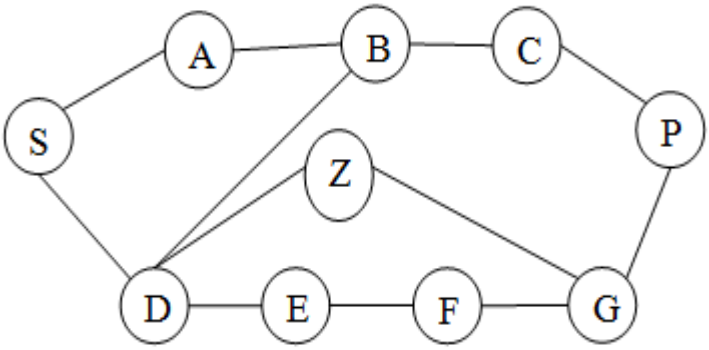


Figure 1.9 Rushing attack [16]

1.6.5 JELLYFISH ATTACK

This attack is similar to blackhole attack but here detection is more difficult because of tendency of attacker to behave in accordance with protocol rules. Attacker may reorder the sequence of packets, generate delay in packet forwarding, or drop packets.

Attack on multiple Layers

- **Impersonation attack**

Impersonation of id takes place like MAC address or IP address. Most attacks are performed after launching this attack.

1.7 THESIS OUTLINE

Thesis is outlined in form of 7 chapters. Chapter 1 presents Introduction to MANETs, its applications and challenges and most importantly security issues and attacks in MANETs like active, passive, DoS attacks. Brief explanation of attacks like blackhole, wormhole, grayhole, jellyfish is provided. Chapter 2 outline literature survey which deals with explanation of jellyfish attacks and its variants,

Countermeasure for jellyfish attack along with routing protocols in MANETs and overview of DSR, TORA, AODV protocol. Chapter 3 specifies problem statement, and objectives of thesis work. Chapter 4 lays out introduction to NS2 and its architectural components, steps followed in simulation. Chapter 5 presents implementation details and scheme proposed for detection and prevention of jellyfish attack and algorithm for the same. In chapter 6, Simulation parameters are tabulated, results are discussed and analysis is done using tables and graphs. Chapter 7 concludes the thesis.

CHAPTER 2

LITERATURE SURVEY

2.1 JELLYFISH ATTACK

Jellyfish attack affects AODV routing protocol.

Jellyfish attack is passive attack working in accordance with protocol rules and is difficult to detect. Attacker here intends to minimise goodput of traffic by reordering the packet sequence, dropping or delaying the packets. It is similar to blackhole attack with dissimilarity in terms of dropping the packets, blackhole attack drops all the packets but jellyfish (JF) attacker drops periodically [17].

Performing rushing attack may be essential before performing JF attack to gain access to routing mesh and intrude in forwarding group [1].

JF attack is of 3 types [17]:

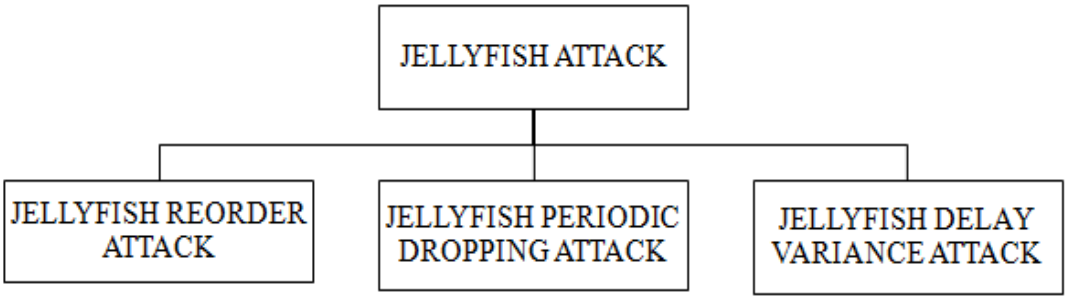


Figure 2.1: Types of jellyfish attack [17]

Jellyfish reorder attack

In this attack, packets are reordered before sending. Attacker forward packets in arbitrary order rather than following FIFO order, this results in degraded goodput, random buffer is used over FIFO buffer. Diagram of JF reorder attack is shown in figure 2.2. When reordered packets are received by destination, it sends back duplicate acknowledgement. Sender begins to retransmit packets without considering retransmission timeout (RTO), being under an impression that packets are lost, if it receives three duplicate acknowledgements. Even when packets arrive at destination, retransmission is continued because sender is still having impression that packets are lost.

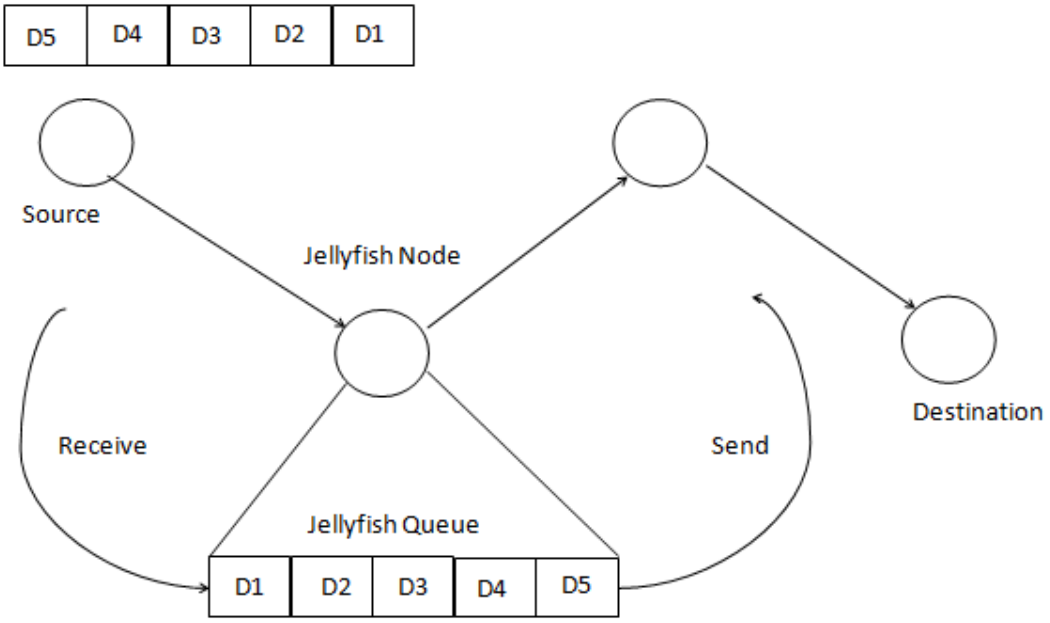


Figure 2.2 Jellyfish reorder attack [18]

Example:

Sender send packets from 1 to 6 in sequential order, attacker reorders the packets such that destination receives packet 1 in last thus making reorder length 5. If three duplicate acknowledgements are sent by destination then sender assumes that packet is lost and carries out retransmission of segment, with this throughput decreases because TCP enters congestion control state.

Jellyfish periodic dropping attack

Unlike blackhole attack where attacker drops all the packets, JF attacker follows periodic dropping. Attacker discards packets either all during adopted time interval or some packets (1 after 10 packets), this assists eventuation of congestion due to stretched RTO, depreciating throughput [19].

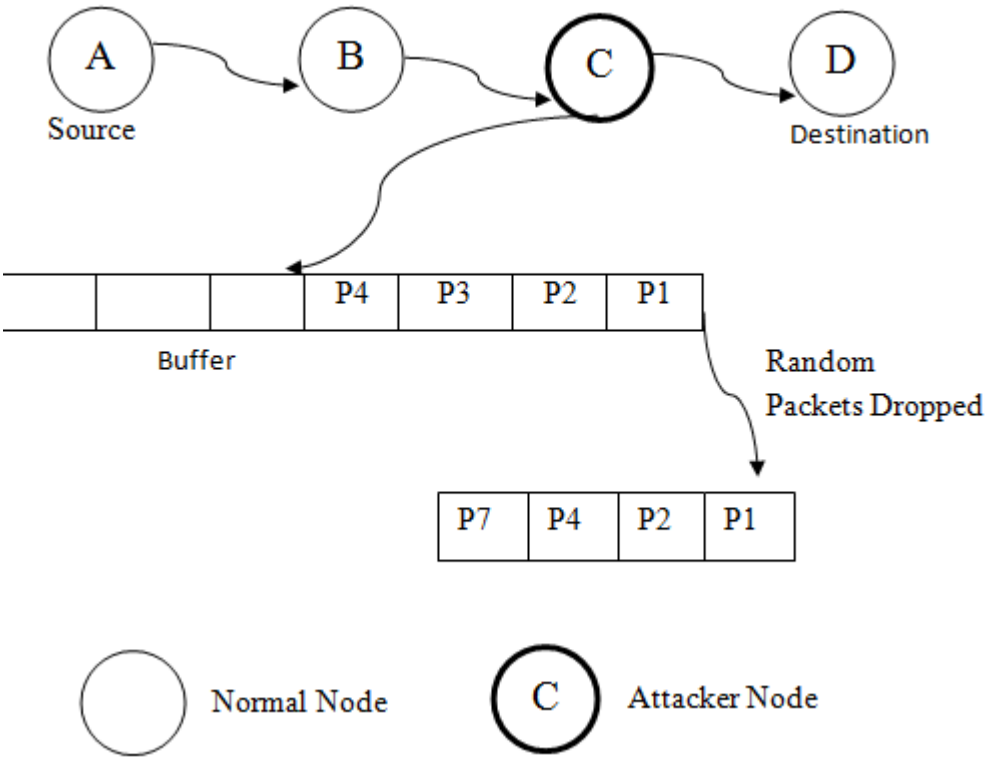


Figure 2.3: Jellyfish periodic dropping attack [19]

Jellyfish delay variance attack

This variant does not reorder the packets but delays them before forwarding after acquiring access to routing mesh. It revolves around the concept of Round Trip Time (RTT). It fluctuate due to congestion and TCP is unsuccessful in catching clarity whether RTT fluctuation is instigated by congestion, abrupt topology or due to JF attack, RTO is stretched due to increased RTT which assists sender in congestion window size elongation to send traffic in bursts inciting congestion and packet loss because insufficiency of network to handle packets more than its capacity. High RTO affects Throughput.

TCP in self clocking incites congestion heading towards packet loss; thus degraded Packet Delivery Ratio (PDR) [19].

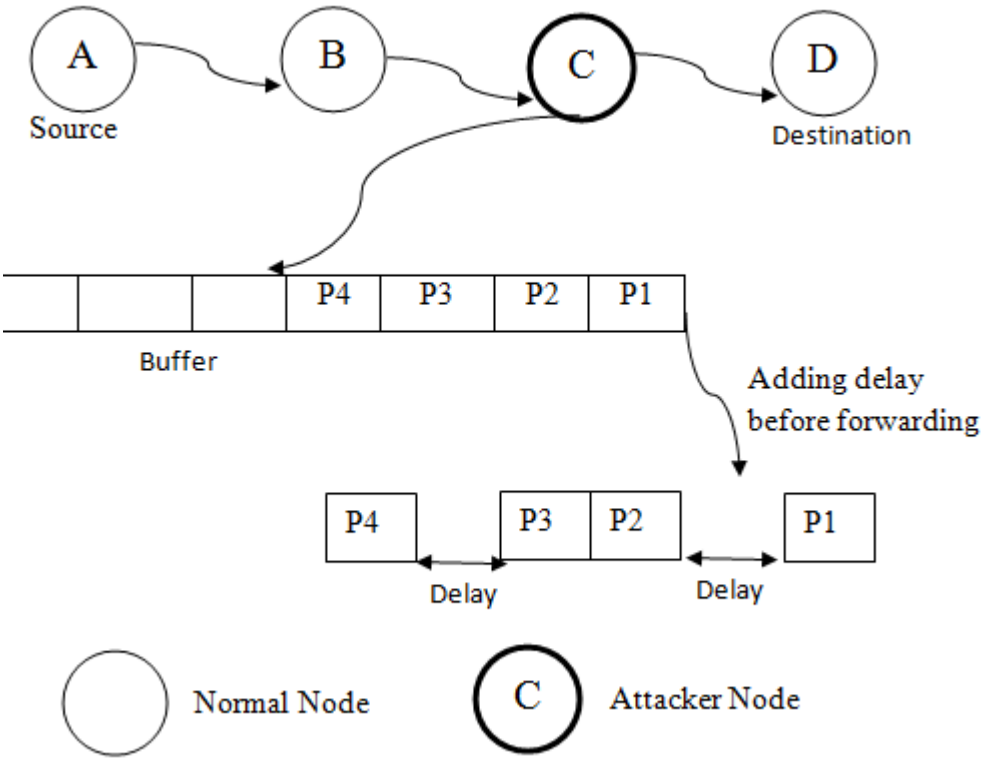


Figure 2.4: Jellyfish delay variance attack [19]

Table 2.1: Comparison of 4 variants of jellyfish attack

Attack	**Purpose**	**Cause**	**Effect**
Jellyfish Reorder Attack	Reordering of the packets is done	Due to vulnerability of TCP	Results in degraded throughput and retransmissions
Jellyfish Periodic Dropping Attack	Jellyfish Node drops the packets in periodic manner	Due to malicious period chosen by attacker node	Attacker tries to maintain synchronicity with transmission window and can cause near zero throughput
Jellyfish Delay Variance Attack	Packets are delayed in arbitrary order	Can be exploited through TCP	Increases delay Variance and leads to congestion inference.

2.2 COUNTERMEASURES OF JELLYFISH ATTACK

In *Aad et al. (2008)* [20], authors proposed attacks that are difficult to detect because of their tendency to stick with the protocol rules without violating them, named JF attack and they have presented simulation results showing the effect of JF attack on end to end goodput of network, however the simulation is done by taking lesser number of nodes.

In *Wazid et al. (2013)* [21], authors proposed efficient TCP by changing some parameters of TCP like disabling fast retransmission and enabling selective ACK if JF attack is detected. In this scheme cluster head executes the task of calculating forwarding rate based on the sending time value of packet.

In *kaur et al. (2014)* [22], authors proposed a novel method using genetic algorithm to tackle JF attack in MANETs and simulation results of the same are presented in the paper.

A novel metric for detection of JF reorder attack is proposed in *Jayasingh and Swathi(2010)* [23], the proposed scheme makes use of reorder density which is calculated using receive index and this method tends to check if acknowledgment number is also reordered, however no method to combat the attack is provided.

In *Wazid et al. (2012)* [24], authors proposed two novel schemes named Cluster Based Intrusion Detection and Prevention Technique (CBIDPT) and Super Cluster Based Intrusion Detection and Prevention Technique (SCBIDPT) for detection and prevention of JF reorder attack. Former is applicable when intermediate node acts maliciously and is this comparison of sequence number of packet in the buffer maintained by cluster head and intermediate node is done and latter is applicable when cluster head itself acts maliciously, however these schemes introduce some delay in the network.

In *patel and Chaudhari* [18], authors presented a scheme that makes use of time space key cryptography and modified SHA-1 that use hashing function for detecting and preventing JF attack, however there is overhead in transmission of dummy packets.

In *Garg and chand(2014)* [25], authors presented enhanced AODV routing protocol which detects and prevents jellyfish delay variance attack. In this scheme threshold value plays vital role in detection of delay in data packets; threshold value is calculated by taking various network parameters into consideration. Hence, this is an

efficient scheme to upgrade the performance of network which is shown by the simulation results present in paper.

In *Avani and Rajbir(2014)* [26], authors proposed a scheme that adopts non cryptographic approach as a countermeasure against jellyfish delay variance attack, this approach makes use of delay threshold for detecting malicious node and thereafter traffic is re routed through non malicious route, however there exist increased overhead owing to the innumerous attempt of re routing.

Comparison of various schemes is done in table 2.2.

Table 2.2: Comparison of schemes for detection and prevention of jellyfish attack

Scheme	**Method**	**Use**	**Attack variant detected**
CBIDPT	Comparison is done for sequence number of packet in the buffer with cluster head and intermediate node.	Intermediate node acting as jellyfish attacker is detected and prevented.	Jellyfish reorder attack
SCBIDPT	Comparison of the sequence number of packets of buffer of super cluster head is done with that of the sequence number of packets of buffer of intermediate node and cluster head	Node elected as cluster head acting as jellyfish attacker is detected and prevented.	Jellyfish reorder attack
Scheme using parameters like FD and RD	Product of frequency and reorder density for all the displacements and their summation is used for calculating the metric i.e. Σ FD*RD	Simple and efficient metric is used to detect jellyfish reorder attack	Jellyfish reorder attack
E-TCP	For each node buffer is created and number is assigned to each packet along with sending time and then cluster head compares the sending time at intermediate node and cluster head itself.	Disables fast retransmission and enables selective acknowledgement if jellyfish attacker is there.	Jellyfish delay variance attack

EAODV	Broadcasting a packet after every interval of time and noticing which node is delaying packets more than threshold	Enhancement is done in AODV protocol to detect malicious node responsible for degraded network performance and RREP from that node are rejected and that node is prevented from to be part of routing mesh	Jellyfish delay variance attack
Time space Cryptographic solution	Technique uses time-space cryptography and modified SHA-1 hash function.	It performs hashing on the key value obtained from the packet and verifies it with the hashed value that is received along with the RREQ packet and suitable mitigation is followed	Jellyfish reorder attack
Non-cryptographic approach	Delay Threshold is used to determine delay caused by nodes	Process of re-routing is initiated to route the data packet through path consisting of non-attacking nodes.	Jellyfish delay variance attack

2.3 ROUTING PROTOCOLS

Certain metrics can be used to determine the efficaciousness of routing protocols [27].

Qualitative Properties:-

- Loop-Freedom
- Demand Based Routing
- Security
- Sleep period operation

Loop-Freedom: Packets rotating for arbitrary time need loop freedom.

Demand Based Routing: Nodes need not accumulate routing information of other nodes until they are in communication; route is searched on-demand basis whenever communication is to happen.

Security: Secure network is epitome of reliable communication. Ad hoc networks are prone to attacks like impersonation, eavesdropping, modification, packet dropping,

redirection, replaying of packets, DoS attacks like grayhole, blackhole, wormhole, jellyfish attack. There is demand of secure network for efficacious communication

Sleep period operation: Power constrained for energy conservation abstain from sending or receiving, routing protocols should adjust to sleep period still not effecting adversely.

Quantitative Properties:-

- Throughput
- Route Acquisition time

Throughput: Protocol must be able to provide efficient throughput with minimum packet loss to retain efficient network performance.

Route Acquisition time: Minimum end to end delay is required while establishing routes demanded for. Routes reactive protocols are looked for only when in need, if there is extra overhead in route establishment than it effects network performance.

Classification of routing protocols is as shown in figure 2.5

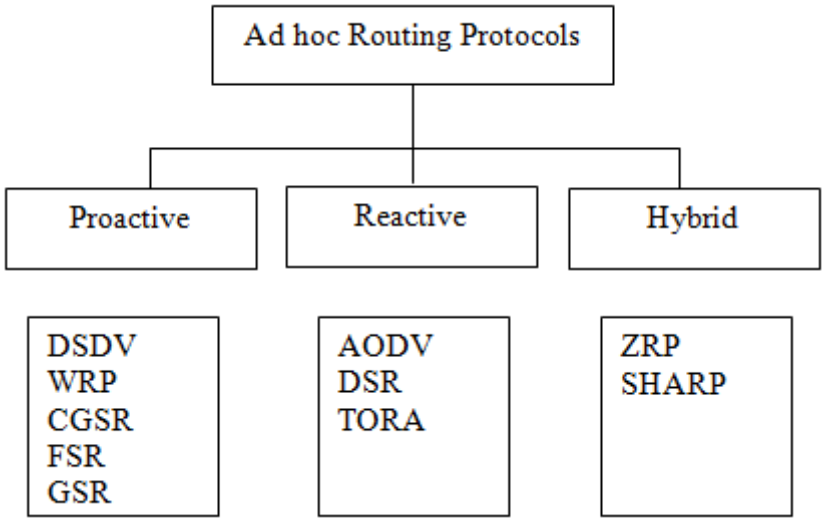


Figure 2.5: Classification of routing protocols

PROACTIVE ROUTING PROTOCOLS

In this, nodes are meant to keep information pertaining to network topology in routing tables even when not required and this is powers consuming, alteration in network topology updates routing tables periodically. These are inappropriate for large networks [28].

Example: Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV), Cluster Gateway Switch Routing Protocol (CGSR), Wireless Routing Protocol (WRP), Fisheye Source Routing (FSR), GSR Global State Routing (GSR)

REACTIVE PROTOCOLS

Routes are looked for whenever needed on demand basis. Two important parts are:

Route Discovery: Source look for already existing routes in its table for destination and if route is absent then this part is initiated

Route Maintenance: Link breakage is handled by this [28].

Example: Ad hoc on demand distance vector routing (AODV), Dynamic Source Routing (DSR), Temporarily Ordered Routing Algorithm (TORA)

HYBRID PROTOCOLS

These are mix of proactive and reactive protocols and consist of plus points of both, it incorporates route discovery of reactive protocols and table maintenance of proactive protocols [29].

Example: Zone Routing Protocol (ZRP), Sharp Hybrid Adaptive Routing Protocol (SHARP)

2.3.1 OBJECTIVES OF ROUTING PROTOCOLS

- Easy usage
- Stability
- Efficiency
- Optimal Routes

Prime intention of routing protocol is establishment of optimal route based in which is network performance merit is judged.

Every protocol accomplish task of maintaining stability of network to withstand failure but the time consumed to handle such events decides effectiveness.

2.3.2 OVERVIEW OF DSR

Dynamic Source Routing Protocol (DSR) is reactive Protocol. Sending request message is way by which sender recognise path to destination. Its twofold functions are [30]:

- Route Discovery

  Explanation is based on figure 2.6. B broadcast request with address of E, and A,D,C on receiving request packet add their own address and broadcast further. When E receives route request, it now knows path to B because of address appended by other nodes and replies back

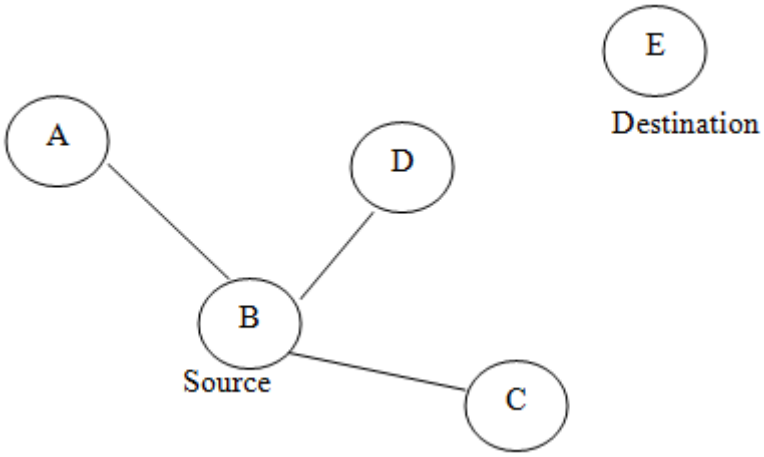


Figure 2.6: Routing Process of DSR [30]

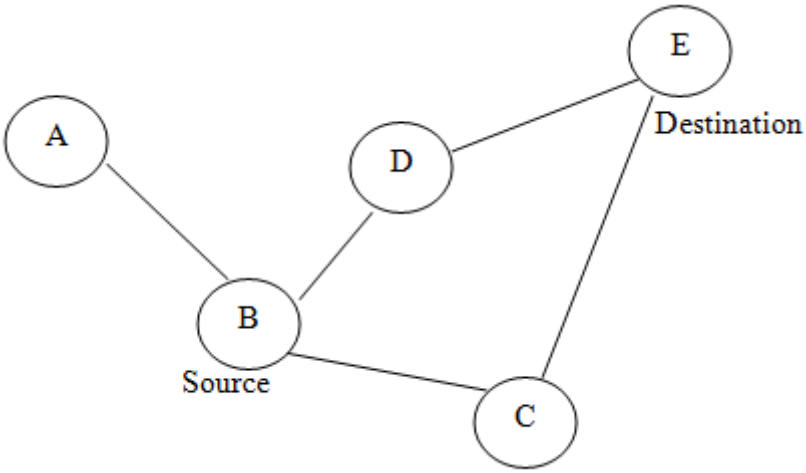


Figure 2.7: Re-broadcasting by nodes A, D, C [30]

- Route maintenance

  On link breakage source is notified about the same and another path is followed, example, if there is link breakage at D, then path B-C-E is followed.

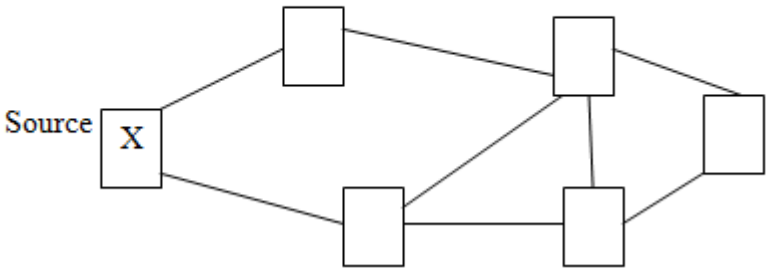
2.3.3 OVERVIEW OF TORA

Temporally-Ordered Routing Algorithm (TORA) works on "link reversal" concept. Longer routes are preferred to eradicate overhead caused in calculating new routes.

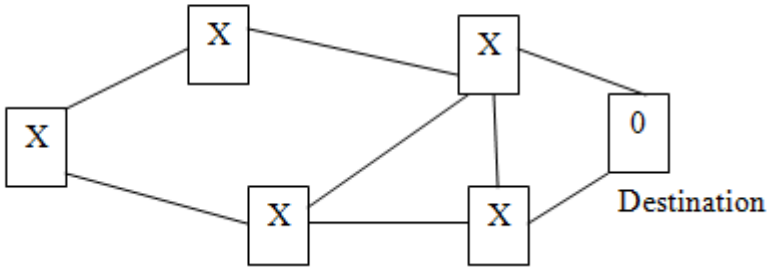
Broadcasting route query packet accompanied by address of destination is way to ascertain route to destination. Recipient of query packet if destination itself is then height specified in update packet broadcasted is 0 else height from destination is enumerated in update packet.

On packet reversal, node recipient of packet increments the enumerated height in update packet from neighbour. Step by step generation of path is as follows [31]:

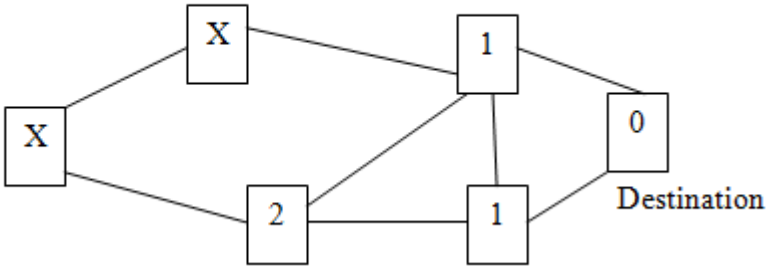
STEP 1: Source Broadcast request Query Packet



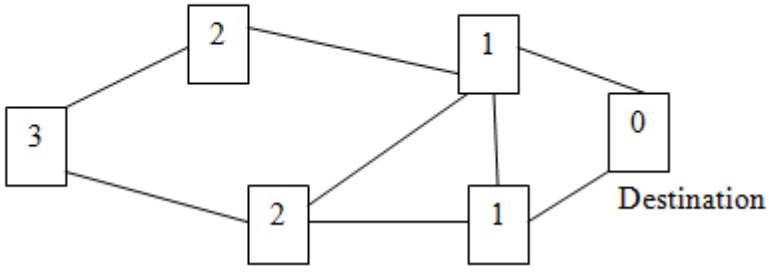
STEP 2: Update Packet from destination



STEP 3: Other nodes set height accordingly



STEP 4: Directed path Known



2.3.4 OVERVIEW OF AODV

AODV is routing protocol using dynamic routing; it need not maintain particulars of mobile nodes not in active communication. AODV is beneficial whenever a route to new destination is to be calculated. Calculation of new route is proceeds by broadcasting RREQ, if the node receiving RREQ it itself the destination then it sends back RREP and cache back the route to sender else it forwards the RREQ. When sequence number of destination is no less than that in RREQ, a valid route is known. There are extensive chances of link breakage in wireless networks, so AODV uses RERR message to notify other nodes about no more alive link. Broadcasting hello message after every interval of time helps knowing information on connectivity with nodes [15].

CHAPTER 3

PROBLEM STATEMENT

3.1 GAPS IN STUDY

Security is major aspect in MANETs, there is need to heal performance of attack affected networks. Jellyfish delay variance attack (JFDV) introduces delay in network and leads to decreased throughput; thus degraded network performance. A lot of work is done to deal with this attack but still there is scope of improvement. In thesis, work is done to study influence of JFDV attack in AODV and a suitable mechanism is proposed to ameliorate depreciated network performance. Results collected from analysis are also depicted.

3.2 AIMS AND OBJECTIVES

Objectives are as follows:

- Simulating JFDV attack in AODV in MANETs
- Using performance metrics like throughput and packet delivery ratio to check effect of attack on network
- Applying suitable mechanism to improve network performance
- Comparison of results obtained in three cases - when no attacker node present in network, Attacker node introduced in network, Application of prevention mechanism.

3.3 METHODOLOGY

- Setting up simulation environment using NS-2
- Using TCL scripts of simple AODV, AODV under attack, AODV after applying prevention scheme.
- Computation of Throughput and PDR using AWK scripts.
- Using Xgraph for graphical representation of results.

.

CHAPTER 4

NETWORK SIMULATOR

4.1 NETWORK SIMULATOR 2.34

For simulation NS-2.34 is used. It is written in C++ and OTcl and can simulate protocols like TCP, UDP, FTP, Telnet etc. To work in NS, Tcl scripts is used and simulation is carried out by specifying the particulars needed in network topology like routing protocol, Channel, number of nodes etc. Event scheduler is prime part of NS 2. A unique packet id with time is an event. Simulation time is to be kept track of. Example: Timer is necessary in TCP for tracking RTO and timer use event scheduler.

4.2 ARCHITECTURE OF NS

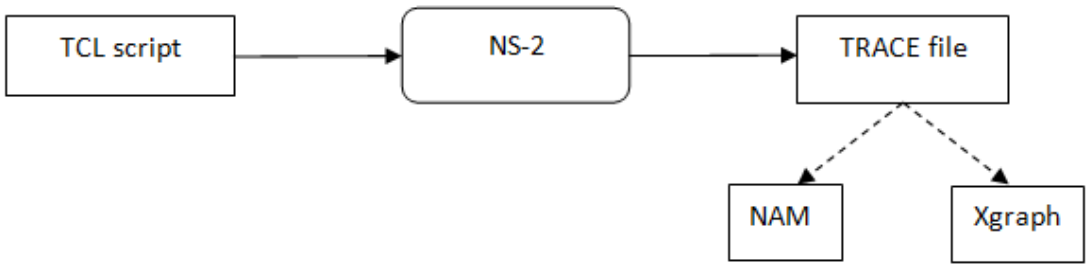


Figure 4.1: Architecture of NS 2

User writes an OTcl script specifying protocol to be used, simulation time, number of nodes etc. On culmination of simulation, two output files are generated, one is trace file (.tr) and other being nam file. NAM is network animator for visual display of simulation as shown in figure 4.2**.** Analysis of results is done using .awk file which is created using AWK script. Trace file serves as input to awk file and corresponding output is displayed and if desired xgraphs can be used to make graphical display of results so procured[32, 33]. Figure 4.1 shows 10 nodes connected wirelessly using AODV protocol.

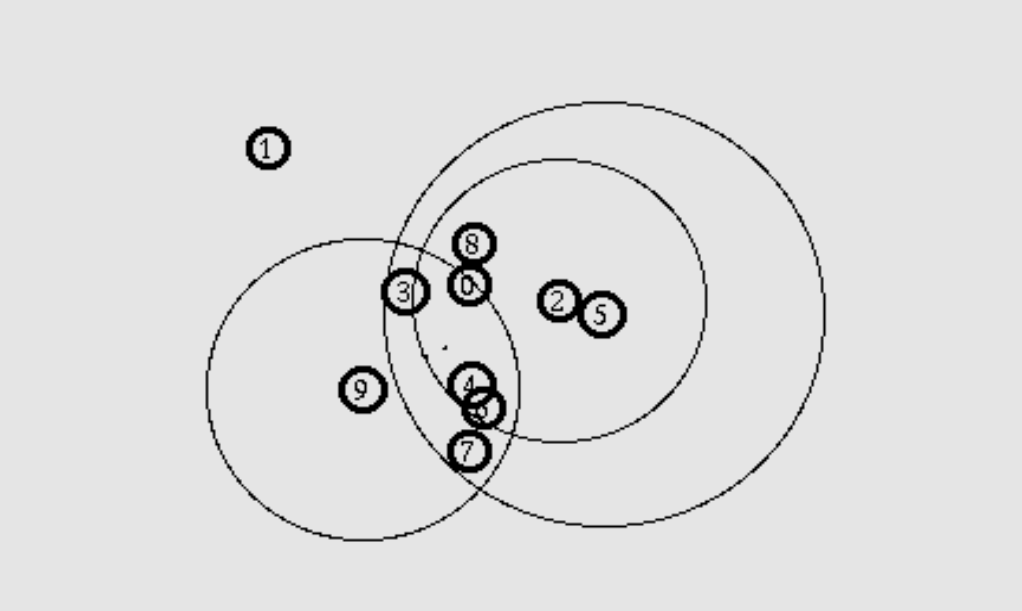


Figure 4.2: Screenshot of NAM

4.3 STEPS OF SIMULATION

First requirement is generating .tcl file where user can specify parameters to be employed in network topology like specified below, routing protocol to be used is AODV, number of nodes 20, topography selected is 750 x 750

```
# Define options
set val(chan) Channel/WirelessChannel ;#Channel Type
set val(prop) Propagation/TwoRayGround ;# radio-propagation model
set val(netif) Phy/WirelessPhy ;# network interface type
set val(mac) Mac/802_11 ;# MAC type
set val(ifq) Queue/DropTail/PriQueue ;# interface queue type
set val(ll) LL ;# link layer type
set val(ant) Antenna/OmniAntenna ;# antenna model
set val(ifqlen) 150 ;# max packet in ifq
set val(nn) 20 ;# total number of mobilenodes
set val(nnaodv) 19;# number of AODV mobilenodes
set val(rp) AODV ;# routing protocol
set val(x) 750 ;# X dimension of topography
set val(y) 750 ;# Y dimension of topography
```

Figure 4.3: Screenshot of Tcl file

Once tcl file is generated it can be run in NS by using command shown in figure 4.4

```
simrann@ubuntu:~/Desktop/awks$ ns jellyfish10.tcl
num_nodes is set 10
Creating nodes...
INITIALIZE THE LIST xListHead
Loading random connection pattern...
Starting Simulation...
SORTING LISTS ...DONE!
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 193.0
```

Figure 4.4: Command for running NS

AWK script is then used to calculate performance metrics; it takes trace file as input and syntax is as shown in figure 4.5

```
simrann@ubuntu:~/Desktop/awks$ awk -f Throughput2007.awk simran.tr
Average Throughput[kbps] = 156.53                StartTime=2.56 StopTime=113.77
Average Throughput[kbps] = 156.53                StartTime=2.56 StopTime=113.77
```

Figure 4.5: Command for running awk script

After procurement if results, xgraphs are drawn by specifying data in .xg file and command goes as shown in figure 4.6

Here throughput1.xg is file from which data is fetched.

-t = Title of graph

-x = Labelling of x co-ordinate

-y = Labelling of y co-ordinate

```
simrann@ubuntu:~/Desktop/awks$ xgraph throughput1.xg -t "Throughput vs number of
 nodes" -x "THroughput" -y "number of nodes"
```

Figure 4.6: Command for xgraph

CHAPTER 5

IMPLEMENTATION

5.1 IMPLEMENTATION

This section presents simulation and implementation of JFDV attack on AODV. To show this simulation is carried out by making one or two nodes to act as attackers and analysis is done on network performance.

Implementation is done by adding new protocol in NS-2.34 and making changes in some of the files like priqueue.cc, packet.h, ns-lib.tcl, ns-agent.tcl, makefile. In these files, patch for attack is added. Appropriate changes are made in .tcl file so that tcl file now follows new protocol. Changes in packet.h are shown in figure 5.1, protocols are numbered sequentially so PT_NTYPE must be last one.

```
If jellyfishAODV packet
{
        Set packet type PT_jellyfishAODV to 62
        Set packet type PT_NTYPE to 63
}
```

Figure 5.1: Changes from packet.h

The patch in following figure 5.2 specifies that packet is routing protocol packet.

```
Static packet class classify (packet_t type)
{
        If packet type =PT_ jellyfishAODV
        Return routing;
}
```

Figure 5.2: Packet specification

Patch added in priqueue.cc is shown in figure 5.3

```
// JellyfishAODV patch
case PT_jellyfishAODV:
```

Figure 5.3: Patch in priqueue.cc

Routing Agent is specified in ns-lib.tcl as shown below in figure 5.4 and ports are specified ns-agent.tcl as shown in figure 5.5.

```
jellyfishAODV {
        Set ragent (create jellyfishaodv-agent $node)
        }
```

Figure 5.4: Changes from ns-lib.tcl

```
Agent/jellyfishAODV set sourceport to 0
Agent/jellyfishAODV set destinationport to 0
```

Figure 5.5: Changes from ns-agent.tcl

Modifications are done in Makefile for creation of object files as shown in figure 5.6.

```
jellyfishaodv/jellyfishaodv_logs.o jellyfishaodv/jellyfishaodv.o \
jellyfishaodv/jellyfishaodv_rtable.o jellyfishaodv/jellyfishaodv_rqueue.o \
```

Figure 5.6: Changes from Makefile

In NS2.34 directory a folder for new routing protocol will be included and changes are to be made in various files of aodv directory by replacing aodv with jellyfishaodv and also names of functions and classes.

Its behaviour will be similar to existing AODV protocol until we add code for attacker in header file as shown in figure 5.7.

```
/* history management*/
nsaddr_t        malicious;
```

Figure 5.7: Attacker defined in header file

Attacker is to be initialised as shown in figure 5.8.

```
If( strncasecmp ("jellyfish", 9) == 0){
        Malicious = true;
        Return TCL_OK;
        }
```

Figure 5.8: Attacker initialization

Figure 5.9 shows code for route request, route request is to be sent without any delay.

```
If (malicious == true)
        forward((jellyfishaodv_rt_entry*) 0,p,0);
else
        forward((jellyfishaodv_rt_entry*) 0,p,DELAY);
```

Figure 5.9: Code for route request

Delay introduced by attacker is as shown in figure 5.10

```
        Forward (rt ,p , 0.8);
Else
        Forward (rt, p, NO_DELAY);
```

Figure 5.10: Delay introduced by attacker

5.2 PROPOSED SCHEME

5.2.1 OVERVIEW

JF attacker on becoming the part of routing mesh tends to delay the packets it receives before forwarding them. When ACK is delayed and sender does not receive ACK in a specified time then it assumes that packet is lost and begins to retransmit the packet, this result in increased congestion and reduced throughput.

A scheme is proposed to revamp the declined performance of network by detecting and preventing JFDV attack.

In this scheme, every node broadcasts a packet to its neighbour node after an interval of time and a timer is set to keep track of delayed packets. A counter is used to avoid false positives and each node is twice given a chance to not be marked as attacker incorrectly. Timer is set such that it takes threshold value. If node that sent broadcast packet receives back a packet from some other neighbour node then timer is checked and if timer is found to be expired then node is suspected to be a JF node and value of counter is decremented and if value of counter falls below 0 then node is considered as a JF attacker node.

Once attacker node is detected re routing is initiated to prevent the attacker node from disturbing the performance of network and in this process attacker node is precluded from the route and transmission of packets is done via route consisting of legitimate nodes.
Threshold depends on parameters like packet delivery time and processing delay and it is set at 1 s.

In proposed scheme, with packet broadcasted timestamp is saved so that timer can be set accordingly. Eradication of false positives is necessary so as to preserve benign nodes from being marked as attackers when they are not.

5.2.2 ALGORITHM

Algorithm

P: Broadcast packet

Count=2

T: Timer

```
For each node
        Create a packet P
        Broadcast the packet to its neighbour nodes
End
For each node
        If (P received) {
                If (T expired) {
                        Jellyfish attacker suspected
                        Count= Count -1
                        If (Count < 0) {
                                Node is a jellyfish node
                        }}}
End
For each node
        While (route discovery)
                If (RREP from jellyfish attacker) {
                        Reject RREP}
End
```

CHAPTER 6

SIMULATION RESULTS

6.1 SIMULATION ENVIRONMENT

This section deals with performance analysis of network under normal scenario when no attacker node is present, when attacker node exists in the network and on the other hand when proposed algorithm is applied to revamp network performance. Simulations are performed adopting NS 2.34 by taking different scenarios with varying node density and checking the effect of malicious nodes on the performance of network. Effectiveness of proposed algorithm is depicted with the help of graphs.

Simulation parameters:

Table 6.1: Simulation parameters

PARAMETER	**VALUE**
SIMULATOR	NS 2
AREA	750 x 750
ROUTING PROTOCOL	AODV
NUMBER OF NODES	10,15,20,30
MALICIOUS NODES	0,1,2
SIMULATION TIME	500 s

6.2. PERFORMANCE METRIC

JF attack effects adversely throughput of network because of congestion caused due to retransmissions and PDR decreases due to increased RTO lead by delay introduced by attacker.

Metrics used for estimating the effect of JFDV attack on network and assessing the effectiveness of proposed algorithm are:

Throughput

It is data transferred per unit time

Packet Delivery Ratio

It is calculated as packets successfully delivered to destination to the number of packets generated by sender.

6.3 RESULT INFERENCES

Manifestation of results is in the form of graphs and tables.

6.3.1 EFFECT ON THROUGHPUT

Figure 6.1 shows command used to get throughput. Here simran.tr is trace file which serves as input to awk script for calculating throughput.

```
simrann@ubuntu:~/Desktop/awks$ awk -f Throughput2007.awk simran.tr
Average Throughput[kbps] = 187.66                StartTime=2.56 StopTime=451.02
Average Throughput[kbps] = 187.66                StartTime=2.56 StopTime=451.02
simrann@ubuntu:~/Desktop/awks$
```

Figure 6.1: Command to get throughput

Table shows results of throughput obtained after simulation carried out by taking varying node density (10, 15, 20, 30) and it can be seen that throughput is depreciated when attacker node is introduced in network and on application of proposed algorithm, fine improvement is made.

Table 6.2: Comparison of Throughput when there is one attacker

Node density	**AODV**	**AODV under one attacker**	**Proposed algorithm**
10	**187.63**	**88.79**	**178.43**
15	**256.93**	**74.76**	**165.86**
20	**311.12**	**87.15**	**285.52**
30	**384.36**	**81.42**	**372.73**

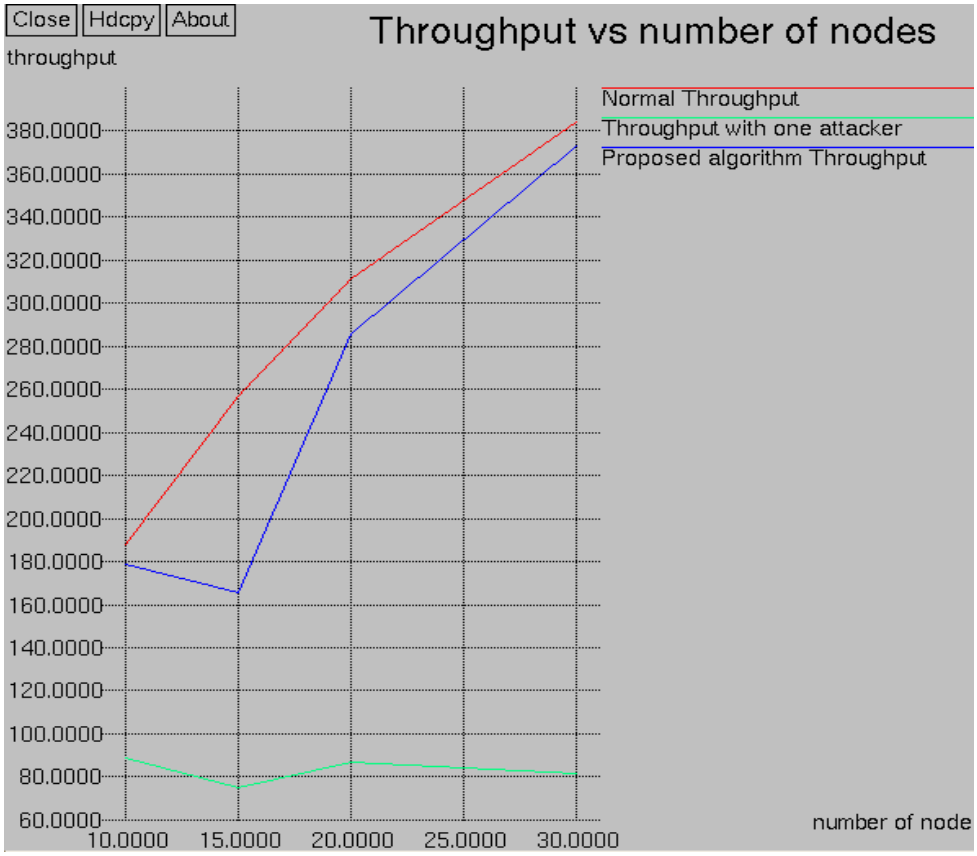


Figure 6.2: Xgraph for throughput when there is one attacker

Table below shows the results of throughput obtained when there are two attacker nodes in network. It can be seen that throughput declines further when number of attacker nodes are increased from 1 to 2, but proposed algorithm has successfully improved the throughput.

Table 6.3: Comparison of Throughput when there are two attackers

Node density	**AODV**	**AODV under two attackers**	**Proposed algorithm**
10	**187.63**	**76.08**	**172.01**
15	**256.93**	**51.38**	**160.67**
20	**311.12**	**84.96**	**252.46**
30	**384.36**	**56.25**	**358.89**

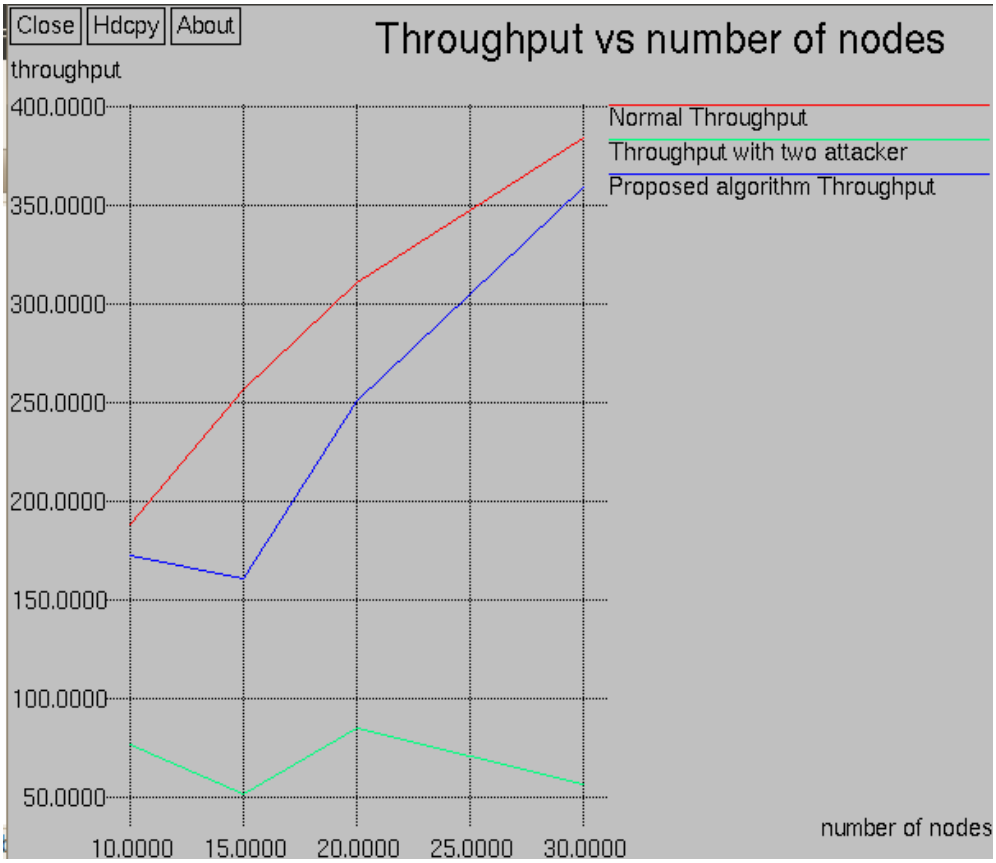


Figure 6.3: Xgraph for throughput when there are two attackers

6.3.1 EFFECT ON PDR

Figure 6.4 shows command used to get PDR.

```
simrann@ubuntu:~/Desktop/awks$ awk -f packetdeliveryratio.awk simran.tr
cbr s:14530 r:10273, r/s Ratio:0.7070, f:9252
simrann@ubuntu:~/Desktop/awks$
```

Figure 6.4: Command to get PDR

Table shows effect of attacker node in network on PDR that has declined under attack and prevention scheme proposed has improved the PDR

Table 6.4: Comparison of PDR when there is one attacker

Node density	**AODV**	**AODV under one attacker**	**Proposed algorithm**
10	**0.7070**	**0.3349**	**0.6761**
15	**0.7377**	**0.2152**	**0.4772**
20	**0.6017**	**0.1680**	**0.5498**
30	**0.7129**	**0.1511**	**0.6906**

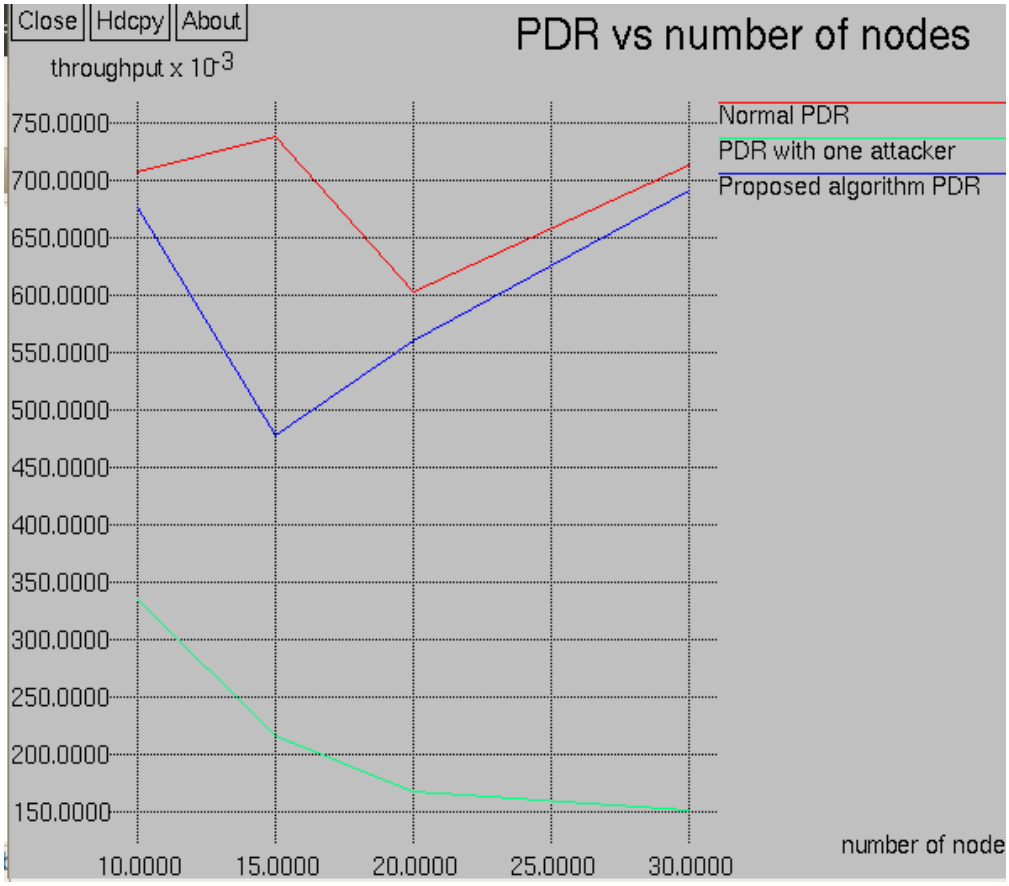


Figure 6.5: Xgraph for PDR when there is one attacker

Table shows PDR when there exist two attacker nodes, it can be observed that PDR shrinks further with two attackers in comparison to PDR under one attacker node, which means more attackers heads towards degraded performance.

Table 6.5: Comparison of PDR when there are two attackers

Node density	**AODV**	**AODV under two attackers**	**Proposed algorithm**
10	**0.7070**	**0.2870**	**0.6501**
15	**0.7377**	**0.1479**	**0.4620**
20	**0.6017**	**0.1642**	**0.5026**
30	**0.7129**	**0.1030**	**0.5661**

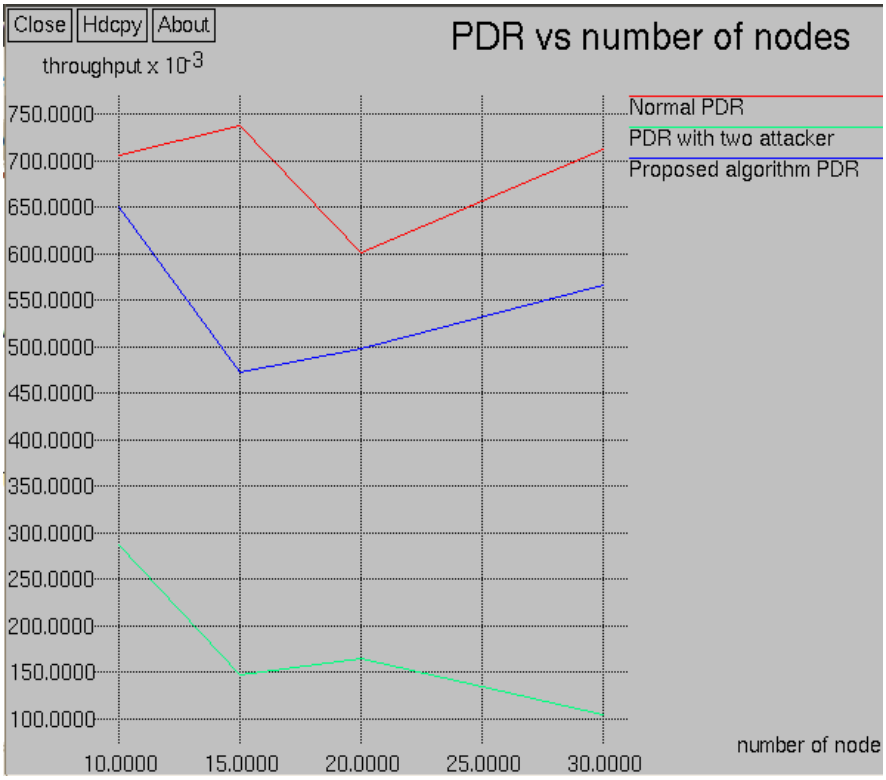


Figure 6.6: Xgraph for PDR when there are two attackers

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

In this thesis work, main focus was on evaluating the effect of JFDV attack on AODV in MANETs. On grounds of insight obtained from simulation results it is observed that presence of JF attacker node significantly degrades the performance of network in terms of throughput and PDR. A scheme is proposed to detect and prevent JF attacker node from deteriorating the network performance and effectiveness of scheme is verified with the help of graphs constructed after performing simulations and it is observed that the scheme helps in improving the performance of network. In future, a scheme can be formulated to improve the performance of network affected by other two variants of JF attack

REFERENCES

[1] Nguyen H.L and Nguyen U.T, “A study of different types of attacks on multicast in mobile ad hoc networks”, *Ad Hoc Networks*, vol. 6, no. 1, pp. 32-46, 2008.

[2] Han L., Wireless Ad hoc Network, 2004.

[3] Marti S., Giuli T.J., Lai K., and Baker M., "Mitigating routing misbehavior in mobile ad hoc networks." In *Proceedings of the 6th annual international conference on Mobile computing and networking*, ACM, pp. 255-265, 2000.

[4] Yang H., Luo H., Ye F., Lu S., and Zhang L., "Security in mobile ad hoc networks: challenges and solutions." *Wireless Communications, IEEE*, vol. 11, no. 1, pp. 38-47, 2004.

[5] Kargl, Frank, Elaine Lawrence, and Gergely V. Záruba. "Introduction to the minitrack on wireless personal area networks (WPANs)." *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*. IEEE, 2004.

[6] Forouzan, A. Behrouz. *Data Communications & Networking (sie)*. Tata McGraw-Hill Education, 2006.

[7] Chlamtac, Imrich, Marco Conti, and Jennifer J-N. Liu. "Mobile ad hoc networking: imperatives and challenges." *Ad hoc networks* 1.1, pp. 13-64, 2003

[8] Hoebeke, Jeroen, et al. "An overview of mobile ad hoc networks: Applications and challenges." *Journal-Communications Network* 3.3, pp. 60-66, 2004

[9] Redwan H., and Kim K.H., "Survey of security requirements, attacks and network integration in wireless mesh networks." In *New Technologies, Mobility and Security, 2008, NTMS'08*, IEEE, pp. 1-5, 2008.

[10] Şen S., Clark J.A., and Tapiador J.E., "Security Threats in Mobile Ad Hoc Networks." *Department of Computer Science, University of York, YO10 5DD, UK*, 2010.

[11] Sivakumar, K., and Selvaraj D.G., "Overview of Various Attacks in MANET and Countermeasures for Attacks." *International Journal of Computer Science and Management Research, ISSN*, pp. 1366-1372, 2013.

[12] Lee G., Seo J., and Kim D.K., "An approach to mitigate wormhole attack in wireless ad hoc networks." In *Information Security and Assurance, 2008. ISA 2008. International Conference on*, IEEE, pp. 220-225, 2008.

[13] Wu B., Chen J., Wu J., and Cardei M., "A survey of attacks and countermeasures in mobile ad hoc networks." In *Wireless Network Security*, Springer US, pp. 103-135, 2007

[14] Jhaveri, R. H., Patel S.J., and Jinwala D.C., "DoS attacks in mobile ad hoc networks: A survey." In *Advanced Computing & Communication Technologies (ACCT), Second International Conference on*, IEEE, pp. 535-541, 2012.

[15] RFC 3561: Ad hoc on demand Routing protocol

[16]]Hu Y.C., Perrig A. and Johnson D.B., "Rushing attacks and defense in wireless ad hoc network routing protocols." In *Proceedings of the 2nd ACM workshop on Wireless security*, ACM, pp. 30-40, 2003.

[`17] Aad I., Hubaux J.P., and Knightly E.W., "Impact of denial of service attacks on ad hoc networks." *IEEE/ACM Transactions on Networking (TON)* 16, no. 4, pp.791-802, 2008.

[18] Patel H.P. and Chaudhari M.B., "A Time Space Cryptography Hashing Solution for Prevention Jellyfish Reordering Attack in Wireless Adhoc Network". *International Conference on Computing, Communication and Networking Technologies (ICCCNT),* 2013.

[19] Laxmi, Vijay, et al. "JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET." *Journal of Information Security and Applications*, 2014.

[20] Aad, Imad, Jean-Pierre Hubaux, and Edward W. Knightly, "Denial of service resilience in ad hoc networks." *Proceedings of the 10th annual international conference on Mobile computing and networking*. ACM, 2004.

[21] Wazid, Mohammad, et al. "E-TCP for efficient performance of MANET under JF delay variance attack." *Information & Communication Technologies (ICT), 2013 IEEE Conference on*. IEEE, 2013.

[22] Kaur, Manjot, Malti Rani, and Anand Nayyar. "A novel defense mechanism via Genetic Algorithm for counterfeiting and combating Jelly Fish attack in Mobile Ad-Hoc Networks." *Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference-*. IEEE, 2014.

[23] Jayasingh, B. B., and B. Swathi, "A Novel Metric for Detection of Jellyfish Reorder Attack on Ad Hoc Network." *Bharati Vidyapeeth's Institute of Computer Applications and Management*, pp. 164, 2014.

[24] Wazid, M., A. Katal, and R. H. Goudar, "Cluster and super cluster based intrusion detection and prevention techniques for JellyFish Reorder Attack."*Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on*. IEEE, 2012.

[25] Garg, Sakshi, and Satish Chand, "Enhanced AODV protocol for defence against JellyFish Attack on MANETs." *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*. IEEE, 2014.

[26] Sharma, Avani, and Rajbir Kaur, "Non-cryptographic Detection Approach and Countermeasure for JFDV Attack." *Proceedings of the 7th International Conference on Security of Information and Networks*, ACM, 2014.

[27] RFC 2501: Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations

[28] Kaur Harvaneet, "A Survey on Manet Routing Protocols"**,** *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, 2015

[29] Kaur, Harjeet, Varsha Sahni, and Manju Bala, "A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review." *network* 10, pp. 11, 2013.

[30] Shrivastava, Amit, et al. "Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols." *Department of Computer Science Lamar University*, 2005.

[31] V. Park, S. Corson, *Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification*, Internet Draft, draft-ietf-manet-tora-spec-01.txt, August 7, 1998.

[32] "The Network Simulator ns-2: Documentation", http://www.isi.edu/nsnam/ns/ns-documentation.html *accessed on* 10/09/2014

[33] http://www.idt.mdh.se/~icc/SDE/5.0-0/doc/RefMan/xgraph.html *accesssed on 2*9/11/2014

[34] https://ajlinx.wordpress.com/2013/06/19/install-ns2-ns-allinone-2-35-on-ubuntu-12-04-for-beginners/ *accessed on* 10/09/2014

LIST OF PUBLICATIONS

- Kaur Simran, Kaur Rupinderdeep, Verma A.K, "Jellyfish Attack in MANETs: A Review" *IEEE International Conference On Electrical, Computer and Communication technologies (ICECCT)*,SVS College of Engineering, Coimbatore, Tamilnadu , India, pp. 1373-1377, 2015. [**Accepted and Presented**]
- Kaur Simran, Kaur Rupinderdeep, Verma A.K "timer based scheme for detection and prevention of jellyfish delay variance attack" *International journal of communication networks and information security (IJCNIS),* 2015. **[Communicated]**

VIDEO PRESENTATION

https://www.youtube.com/watch?v=cXfZmaTpijo