



Mitigation of DDOS Attack In AODV Routing Protocol Using Token Based Identity

A Dissertation submitted

By

Satveer Kaur
(11301401)

To

Department of Computer Science & Engineering

In partial fulfilment of the Requirement for the
Award of the Degree of

Master of Technology in Information technology
Under the guidance of

Mr. Hitesh Sharma
(Assistant Professor, Lovely Professional University)

(May 2015)

PAC APPROVAL



School of: Computer Science & Engineering.

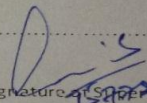
DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Satveer kaur Registration No: 11301401
Batch: 2013 Roll No: RK2308A03
Session: 2013-15 Parent Section: K2308
Details of Supervisor: Designation: Asstt-1 Professor
Name: Hitesh Sharma Qualification: M.Tech - CSE
U.I.D: 15978 Research Experience: 2

SPECIALIZATION AREA: Network Security (pick from list of provided specialisation areas by DAA)

PROPOSED TOPICS

1. Mitigation of DDOS Attack in AODV Protocol using token based system.
2. Removal of Service Attacks in Wireless network.
3. _____


Signature of Supervisor

PAC Remarks:

Topic one is approved. Student need to publish a Research paper on this topic

APPROVAL OF PAC CHAIRPERSON:


Signature:

Date:

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

ABSTRACT

In present scenario, mobile ad hoc network become the projecting mode of communication for all mobile devices. As ad hoc networks are infrastructure less networks and the nodes in the mobile ad hoc networks are connected by a wireless links. As nodes are connected by wireless links, it becomes very easy for attacker to attack on the unplanned networks. Therefore security is the major issue in ad hoc networks as compared to wired networks. DDOS attack is one of the major attack in such networks. In this attack the invader practises several machines to create a DOS attack in contrast to one or more goals. It is flung indirectly over many cooperated computer systems by sending a huge useless traffic, to create congestion and delay in the services. In our research we are discussing the various attacks which are possible in MANET. And also we proposing a new token based identity to mitigate the influence of DDOS attack in AODV routing protocol in MANET. This method will help us to reduce the packet loss, decrease the end to end delay and also increase throughput.

Hence this technique will enhance the performance of AODV protocol against DDOS attack.

ACKNOWLEDGEMENT

I would like to take this opportunity to express my deep sense of gratitude to all who helped me directly or indirectly during thesis work. I also would like to thank my supervisor **Mr. Hitesh Sharma** for being great mentor and best adviser I could ever have. His advice, encouragement and critics are sources of innovative ideas, inspiration and cause behind the successful completion of this dissertation. I am highly obliged to all faculty members of computer science and engineering department for their support and encouragement. I would like to express my sincere appreciation and gratitude towards my friends for their encouragement, consistent support and priceless suggestions at the time I needed the most. I am grateful to my family for their love, support and prayers. I would like to thank to the **Project Approval Committee members** for their treasured comments and discussions. I would also thank to **Lovely Professional University** for the support on academic studies and letting me involve in this study.

Satveer kaur

Regd no. 11301401

DECLARATION

I, SATVEER KAUR hereby declare that the dissertation proposal entitled '**Mitigation of DDOS attack in AODV routing protocol using token based identity**', submitted for the M.Tech (Information Technology) degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

Investigator:-Satveer kaur

CERTIFICATE

This is to certify that **Satveer kaur** has completed M.Tech(IT) dissertation proposal titled **“Mitigation of DDOS attack in AODV routing protocol using token based identity”** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma. The dissertation proposal is fit for the submission and the partial fulfilment of the conditions for the award of M.Tech(IT).

Date:

Signature of Guide

TABLE OF CONTENTS

INTRODUCTION	1
1.1 Introduction to mobile ad hoc networks	1
1.1.1 Infrastructured.....	1
1.1.2 Infrastructureless.....	2
1.2 Background and motivation.....	3
1.3 MANET Characteristics	3
1.4 MANET Applications.....	4
1.5 MANET Challenges	5
1.6 Routing in ad hoc networks	6
1.6.1 Routing protocols in MANET	7
1.7 Threats and attacks.....	16
1.7.1 Wireless network attacks	16
1.7.2 Attacks on Routing protocols	17
1.8 Security models and attributes.....	20
1.9 Security of ad hoc network.....	20
1.10 MANET Security	21
CHAPTER 2	23
LITERATURE REVIEW	23
CHAPTER 3	28
PRESENT WORK.....	28
3.1 Problem formulation	28
3.1.1 Problem definition	30
3.2 objectives	30
3.3 Research methodology.....	31
CHAPTER 4	38

RESULTS AND DISCUSSION.....	38
4.1 Simulation Parameters	38
4.2 Performance measurements	39
4.3 Simulation process in NS2	39
4.3.1 Network animator (.NAM).....	40
4.3.2 Trace Analyzer (.TR).....	41
4.4 Simulation results	41
CHAPTER 5	47
CONCLUSION AND FUTURE SCOPE.....	47
5.1 Conclusion	47
5.2 Future Scope	47
CHAPTER 6	48
REFERENCES	48
CHAPTER 7	50
APPENDIX.....	50
7.1 List of abbreviations	50

LIST OF FIGURES

Figure 1 Infrastructure based technologies.....	2
Figure 2 Typical MANET	2
Figure 3 Ad hoc routing protocols.....	8
Figure 4 Route request.....	12
Figure 5 Route request cont.....	13
Figure 6 Route request Rebroadcast.....	13
Figure 7 Route Reply	14
Figure 8 Route reply cont..	14
Figure 9 Data delivery	15
Figure 10 Route error message	15
Figure 11 Route error message cont.	16
Figure 12 Flow chart for token based process.....	32
Figure 13 Presentation of proposed technique in network animator .	46
Figure 14 Presentation of DSR under DDOS attack in network animator	46

LIST OF TABLES AND GRAPHS

Table 1 Parameter values used for AODV simulation results.	38
Table 2 Result table	41
Graph 1 end to end delay comparison.....	42
Graph 2 Packet delivery fraction comparison	42
Graph 3 Average throughput comparison	43
Graph 4 Throughput comparison.....	44
Graph 5 Average end to end delay comparison	44
Graph 6 Packet delivery fraction comparison	45

CHAPTER 1

INTRODUCTION

1.1 Introduction to mobile ad hoc networks

Web and correspondence engineering and administrations have been increased praiseworthy as of late. Portability is all that much imperative, as individuals need to use it at whatever time and anyplace. In the ranges where there is less or no base is accessible or the current foundation is exorbitant and not secure to utilize. Portable Ad hoc Networks are getting to be exceptionally helpful. They are going to turn into a critical part of cutting edge versatile administrations. “MANET is a gathering of remote hubs that can dynamically create a system to exchange information without using any current fixed network structure”. The term MANET implies a multi hop parcel based remote system made out of a set of versatile hubs that can impart and move in the meantime, without utilizing any sort of wired framework. MANET is really self-arranging and planning toward oneself system that can be shaped without the need of any centralized administration. The unique features of MANET bring this engineering great opportunity together with several difficulties. The military strategic and other security complex operations are the core applications of mobile ad hoc networks, even though ad hoc networks are approved for profitable uses due to their significance of belongings. Still, there are amount of problems. Usually there are two separate methodologies for empowering remote versatile hubs to speak with one another:-

1.1.1 Infrastructured

Mobile ad hoc systems are focused around the cell idea and subject to great framework support.in this kind of situation cell phones correspond with access focuses for instance base stations joined with an altered system infrastructure. Best samples of this Kind of remote systems are GSM, WLAN, and so forth.

1.1.2 Infrastructureless

In infrastructure less approach, the mobile wireless network basically known as a mobile ad hoc network. A versatile ad hoc system is an accumulation of remote hubs that can progressively make a system to exchange data without utilizing any current system foundation. It has numerous imperative applications, because in many situations information exchange between mobile nodes cannot belief on any immovable network infrastructure. Wireless mobile ad hoc networks are self-governing, widespread area of exploration and uses, as a replacement for being only a part of the cellular system.

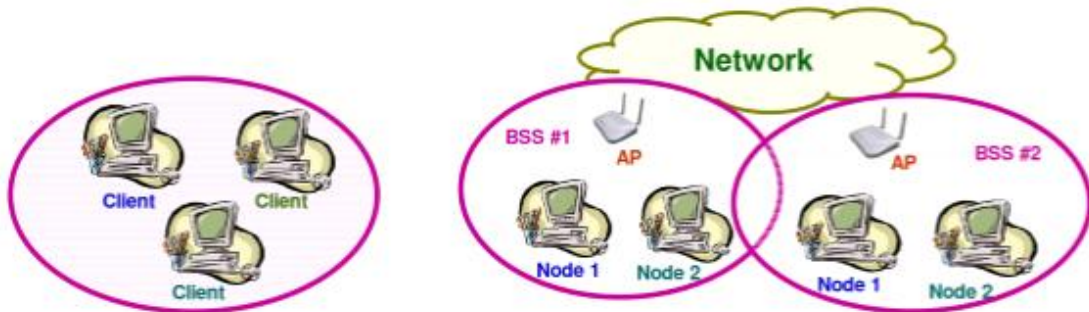


Figure 1 Infrastructure based technologies

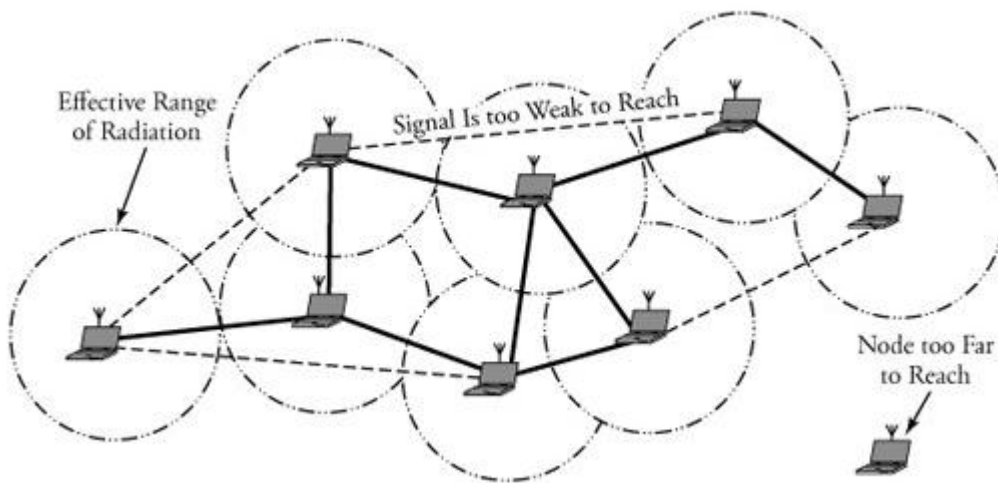


Figure 2 Typical MANET

1.2 Background and motivation

Now -a-days, Mobile ad hoc network (MANET) is one of the recent active fields and has received marvelous attention because of their self-configuration and self-maintenance skills. However primary study struggle supposed a friendly and cooperative environment and focused on problems such as wireless channel access and multiparty routing, safekeeping has become a key alarm in order to provide protected communication between nodes in a potentially hostile environment. Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks. Though portable ad hoc networks have several advantages over the traditional bound networks, on the other sides they have a distinctive set of challenges. Firstly, MANET faces challenges in safe communication. For example the resource restrictions on nodes in ad hoc networks limit the cryptographic measures that are used for secure messages. Thus it is susceptible to link attacks ranging from passive eavesdropping to active masquerade, message replay and message alteration. Furthermore, mobile nodes without acceptable protection are easy to negotiation. An attacker can snoop, alter and crack to masquerade all the traffic on the wireless communication channel as one of the legitimate node in the network. Furthermore, fixed structure may not be adequate for the dynamically changing topology in terms of security solution. Various attacks like DOS (Denial of Service) can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information. Lastly, absence of cooperation and reserved capability is common in wireless MANET which makes anomalies hard to distinguish from regularity. In broad, the wireless MANET is mainly vulnerable due to its fundamental characteristics of exposed medium, vigorous topology, and absence of essential experts, distribution cooperation and constrained capability.

1.3 MANET Characteristics

MANET provides different characteristics at different times. Here we can discuss some of the important characteristics of MANETs.

Distributed operation:-There is no background network for the chief control of the network processes, the regulation of the network is disseminated between the nodes. The nodes involved in a MANET should collaborate with each other and interconnect between themselves and each node behave as a relay as desirable, to show specific functions such as transmitting and safety.

Multi hop Routing:-When a node attempts to direct information to additional nodes which is unavailable of its communication range, the packet should be promoted through one or more middle nodes.

Dynamic Topology:-Nodes are able to move randomly with different hustles. Thus, the network topology can modify arbitrarily and at random time. The nodes in the MANET dynamically start routing between themselves as they travel around, inaugurating their own network.

Light weight terminals:-In extreme cases, the nodes at MANET are portable with fewer CPU proficiency, little power storage and lesser memory size.

Shared Physical Medium:-The wireless communication intermediate is available to every entity with the suitable equipment and satisfactory properties. Therefore, access to the station cannot be limited.

1.4 MANET Applications

Ad hoc networking system administration can be connected at any place where there is practically zero correspondence framework or the current base is lavish or badly designed to utilize. . Ad hoc network permits the devices to keep up associations with the system and effectively adding and clearing devices to the system and from the system. The set of uses for MANET is countless, extending from huge measure, movable and very dynamic systems. Static systems that are obliged by force sources. Primary applications of MANET are:-

Military battlefield:-Equipment's of military now contains computer equipments. Ad hoc networking permit the military to take benefit of everyday network technology to retain an information network among the militaries, automobiles, and military information control centre.

Commercial sector:- Mobile ad hoc network system can be reused in crisis forms for disaster recovery endeavors, e.g. in flame or shock. Crisis spare operations must occur where harmed interchanges framework and quick arrangement of a correspondence system is required. Data is spread starting with one save colleague then onto the next over a little handheld gadget.

Local level: - Ad hoc networks are transitory interactive media network using record book systems to spread and offer data among applicants i.e. at a classroom. Another fit local level application might be in household networks where devices can interconnect straight to chat.

Personal area network: - Short-range mobile ad hoc networks can cut the connectivity among various mobile devices. Guaranteed cables are changed with uncontrolled connections.

1.5 MANET Challenges

Regardless of providing striking applications, MANET has many tests that must be considered before organizing any application commercially widely. These challenges are described as below:

Routing: As due to dynamic topology of network, routing of packets between any two nodes is a challenging task. Most of protocols uses or base upon on demand routing instead of table based routing. Most of the protocols should be based on volatile routing instead of active routing. As multicast routing is another challenging task for routing. In multicast tree is remain dynamic always as due to change in nodes movement. Routes between nodes has multiple stages, which is more difficult than single hop message.

Security and Reliability: Ad hoc has a few issues as because of its security reasons. Disseminated operation is a key peculiarity which obliges diverse sorts of keys concerning verification and administration. Remote connection additionally has some dependability security issues. A portion of the issues are constrained remote transmission go in system, nature of telecast remote medium (e.g. shrouded terminal issue), and lapses in information transmission.

Quality of service: As frequently changing of system topology brings about different testing issues as one of them is giving nature of administration. Correspondence quality device

makes hard to give any certification on the tool on which administration is given. Hence there is a need of giving nature of administration on the conventional asset reservation to give mixed media administrations.

Power consumption: Consumption of power should be less for light weight mobile devices, so that they can offer their communication associated functionality anytime without any matter.

Limited Bandwidth:-Wireless connection last to have meaningfully minor volume than infrastructure networks. Also the recognized throughput of wireless communication after accounting for the result of multiple entrance, disappearing, sound, and snooping conditions is often much fewer than a radio's supreme broadcast speed.

Packet loss:-Ad hoc wireless networks practices a much upper packet loss due to issues such as enlarged crashes due to the incidence of unseen terminals, presence of snooping, uni-directional contacts, normal path breaks due to movement of nodes.

Hidden Terminal problem:-The hidden terminal problem denotes to the crash of packets at an end node due to the immediate broadcast of those nodes that are not inside the straight transmission range of the dispatcher, but are in the broadcast range of the end user.

1.6 Routing in ad hoc networks

The lack of a backbone infrastructure is based on the fact that mobile Ad Hoc networks change their topology frequently and without prior notice makes packet routing in ad-hoc networks a very tough task to do. The techniques for routing can be of two types i.e. topology-based and position-based. In topology-based routing protocols make use of the information about the links that are in the network to perform packet forwarding process. These are further of three types **proactive, reactive and hybrid** approaches and further there will be description of all of these in detail.

1.6.1 Routing protocols in MANET

In portable specially appointed systems the present all the hubs are versatile hubs and all can be associated to one another rapidly in irregular manner. But the scope of the each one host's remote transmission is restricted, hence to correspond with hosts which are outside its range, the host will needs to enlist its close-by hosts in sending parcels to the end of the line. So all hubs of these systems act as switches and participate in disclosure and upkeep of courses to different hubs in the system. Ad hoc Networks are extremely valuable in disaster hunt and emergency operations, gatherings or traditions in which persons wish to impart data. MANETs are a sort of remote specially appointed systems that normally have a routable systems administration environment on top of a Link Layer impromptu system. For MANETs, different directing conventions are accessible. Each has it attributes and some of them have inferred qualities. Depending upon the nature of application, appropriate routing protocols are implemented. it is shown in figure 3

Ad-hoc routing protocols:- Mobile Ad-hoc routing protocols are basically divided into two phases:- proactive routing protocols also called table driven protocols and second is reactive routing protocols also called on demand protocols. The main thing that is very common for both types of routing protocols is that all nodes which are participants in routing play an equal role.

Table Driven Routing Protocols (Proactive):- In such type of protocols each node preserves routes to every other node in the network. Routing information is spread through the network periodically in order to maintain routing table correctness. Thus, if a route has already be present before traffic reaches, transmission happens as soon as possible. Otherwise, traffic packets should hold in line till the node obtains routing information matching to its destination. However, for extremely self-motivated network topology, the proactive schemes need a significant quantity of possessions to keep routing information up-to-date and trustworthy.

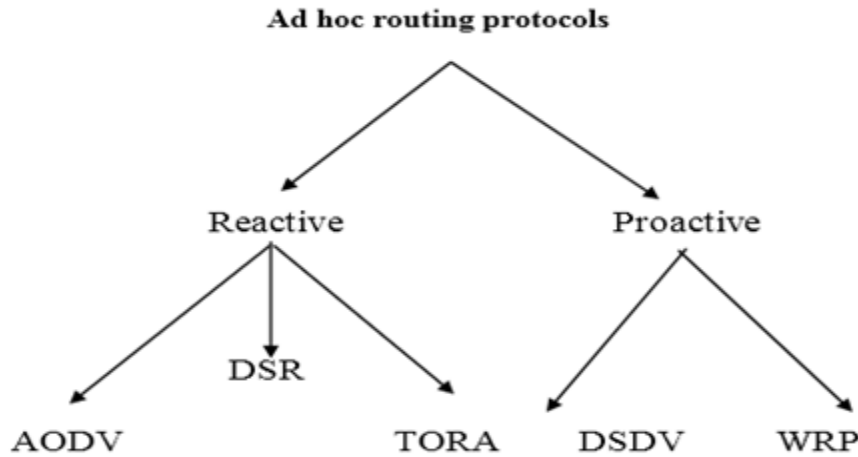


Figure 3 Ad hoc routing protocols

On-Demand Routing Protocols (Reactive):- In these protocols a node starts a route discovery once a route has been recognized, it is reserved by a route maintenance method till any of the destination becomes faraway. In reactive protocols, nodes maintain the routes to dynamic endpoints. A route exploration is mandatory for every strange endpoint. Consequently, the message overhead is concentrated at cost of delay due to route research.

Hybrid Routing Protocols:-It is combination of both above protocols, and contains the features of both protocols. Here we will describe some routing protocols with their functions.

1.6.1.1 DSR (Dynamic source routing protocol):- The Dynamic Source Routing protocol (DSR) is a protocol considered for use in wireless mobile ad hoc networks. This protocol permit the network to be independent without any necessity for present network infrastructure. Dynamic source routing protocol has been executed by various groups. DSR can work with Mobile IP, and nodes using Mobile IP and DSR have effortlessly drifted between WLANs, mobile data services, and DSR mobile ad hoc networks. The protocol is made up of the two main appliances "Route Discovery" and "Route Maintenance", which work in organized way to permit nodes to discover and maintain routes to random endpoints in the ad hoc network. All phases of the protocol function totally on demand. The protocol lets several routes to any destination and agrees each sender to select and control the routes used in routing

its packets. The DSR protocol is planned primarily for MANET for two hundred nodes, and is considered to work well with very great rates of mobility.

1.6.1.2 DSDV (destination sequenced distance vector):- Destination Sequenced Distance Vector Routing protocol (DSDV) is a table driven routing protocol for ad hoc mobile networks based on the Bellman Ford algorithm. The main benefit of DSDV over old-style distance vector protocols is that it promises loop independence by using the order numbers. DSDV is a node by node distance vector routing protocol. It is proactive protocol and each node has to occasionally announce routing updates. Every record in the routing table comprises order number. The number is maintained by the destination. Routing information is divided between nodes by sending incremental updates more frequently. Destination sequenced distance vector protocol is very suitable for creating ad hoc networks with less number of nodes. Since no specification of this algorithm is present .DSDV needs a regular inform of its routing tables, which expenditures battery power and less quantity of bandwidth even when the network is not in use. Every time the topology of the network alters, a new sequence number is compulsory. Each DSDV node keeps a routing table listing the “next hop” for every accessible destination. DSDV labels every route with a sequence number and considers a route Route1 more advantageous than Route2 if Route1 has a bigger sequence number, or if the two routes have the same sequence numbers but R has a lesser metric. Each node in the network publicizes a monotonically growing even sequence number for themselves. When a node B agrees that its way to a destination D has cracked, it publicizes the route to D with an endless metric and a sequence number one more than its order number for the route that has broken. This effects any node ‘A’ directing packets through ‘B’ to include the infinite-metric route into its routing table till node ‘A’ receives a route to ‘D’ with an advanced sequence number.

1.6.1.3 TORA (Temporally-Ordered Routing Algorithm):- TORA is a distributed routing protocol centered on a “link reverse” process. It is expected to find out routes on request, offer various paths to an endpoint, found routes quickly, and reduce message overhead by restricting algorithmic response to topological variations when possible. Shortest-path routing is considered of minor reputation, and longer paths are regularly used to evade the overhead of fresher routes. It performs three basic tasks. These three tasks are route creation, maintenance and route erasure. TORA builds a directed acyclic graph that is called DAG.

There are three messages used in TORA. These are query, update and clear message. Query is a message for creation of route. It is used when new route is required. Update message is for the preservation of route. Links are generated between nodes based on height and it ensures loop free routing. Packet movement is from source node with highest height to the destination with lowest height. TORA offers better results in dense networks and numerous paths offer quick services.

1.6.1.4 WRP (Wireless routing protocol):- In this protocol four tables are maintaining by each node in the network. These are distance table, routing table, link cost table and message retransmission list. Distance table contains the neighbor information of a node. Routing table contain up to date information of the network for all destination with short distances. Link cost table keeps information about the cost of transmitting messages through each link. Message retransmission list retains the each updated message that needs to be retransmit. This procedure also benefits in loop stoppage and offer faster route convergence when route failure arises.

1.6.1.5 AODV (Ad hoc on demand distance vector):- This routing protocol is used by portable hops in an ad hoc network. It practices destination sequence numbers to assure loop at all times escaping from problems related with classical distance vector protocols. The Ad Hoc On-demand Distance Vector routing protocol is an enhancement of the Destination Sequenced Distance Vector routing protocol (DSDV). It creates the routes on an on request basis, as contrasting to sustain a complete list of routes for each endpoint. Hence, the writings on AODV, categorizes it as a clean on-demand routing protocol. The use of the AODV protocol for mobile ad hoc networking applications delivered enhanced results for huge situations. AODV is basically a mixture of both DSR and DSDV. It fetches the simple appliance of Route Detection and Route Repairs from DSR, and use of end to end routing, and episodic beacons from DSDV. When an AODV router receives a request to send a message, it checks its routing table to realize if a route be present in the table. Each routing table record comprises of the following field:-

- Destination address
- Next hop address
- Destination sequence number

- Hop count

AODV nodes practice these messages to communicate with each other. Route Request message, Route Reply message are used for route finding. Route Error messages and HELLO memos are used for the route maintenances. AODV is an on-demand routing protocol, which starts a route detection process only when preferred by a source node. When a source node A wants to send data packets to a destination node D but cannot discover a route in its routing table, it broadcasts a Route Request (RREQ) message to its neighbors, with the previous identified sequence number for that destination. Its neighbors then broadcast again the RREQ memo to their neighbors if they do not have a route to the destination node. This procedure lasts till the RREQ message reaches the destination node or an intermediary node that has a fresh enough route. Each node has its private sequence number and RREQ ID. AODV practices sequence numbers to declare that all routes are loop-free and have the most current routing evidence. RREQ ID in combination with source IP address exclusively identifies an exact RREQ message. The destination node or an intermediary node only accepts the first copy of a RREQ message, and leave the repeated copies of the same RREQ message. Each node that forward the ROUTE REQUEST creates a back route for itself back to node A. After accepting a RREQ message, the destination updates its reverse route to the source node using the neighbor from which it collects the RREQ message. The opposite route will be used to refer the conforming Route Reply (RREP) message to the source node. When the ROUTE REQUEST ranges a node with a way to D, that node creates a ROUTE REPLY that comprises the number of hops necessary to reach D and the sequence number for D most freshly seen by the node creating the REPLY. Temporarily, it updates the sequence number of the source node in its routing table to the extreme of the one in its routing table and the one in the RREQ note. When the sender or a halfway node collects a RREP note, it informs its onward route to the endpoint node using the neighbor from which it receives the RREP message. It also updates the sequence number of the destination node in its routing table to the maximum of the one in its routing table and the one in the RREP message. A Route Reply Acknowledgement message is used to grant receipt of a RREP message. The state created in each node along the path from A to D is hop-by-hop state; that is, every node recalls only the next hop and not the complete route. To reserve routes, AODV generally needs that each node occasionally transfer a HELLO note. Unable to take three HELLO memos from a neighbor is taken as a signal that the bond

to the neighbor is despondent. Route preservation is finished with Route Error memos. If a node notices a link halt in a dynamic route, it refers out a RERR memo to its upstream node that use it as the next hop in the cracked route. Once a node gains a RERR note from its neighbor, it uphold the RERR note to its upstream nodes. AODV is a protocol without any fixed state, the sender node or a middle node changes its routing table if it gets a RREP message, irrespective of whether it has sent or promoted a RREQ message earlier. If it cannot catch the following hop in the reverse routing table, it simply drops the RREP message. Then, it unicasts the RREP message to the next hop in the reverse route. In overall, a node may update the sequence numbers in its routing table when it obtains RREQ, RREP, Route error, or RREP-ACK memos from its neighbors. The whole process is shown through figure 4 to 11.

AODV ROUTE DISCOVERY:-

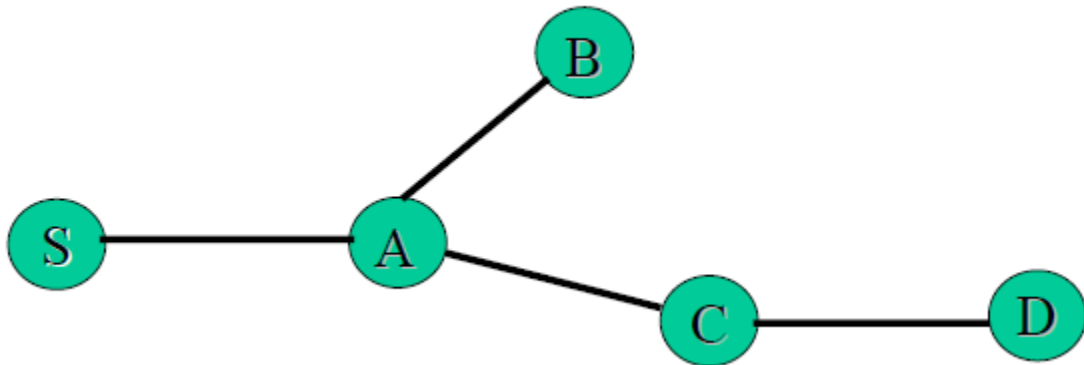


Figure 4 Route request.

- 1. Node S requires a route to node D.**
- 2. Creates a Route Request (RREQ)**

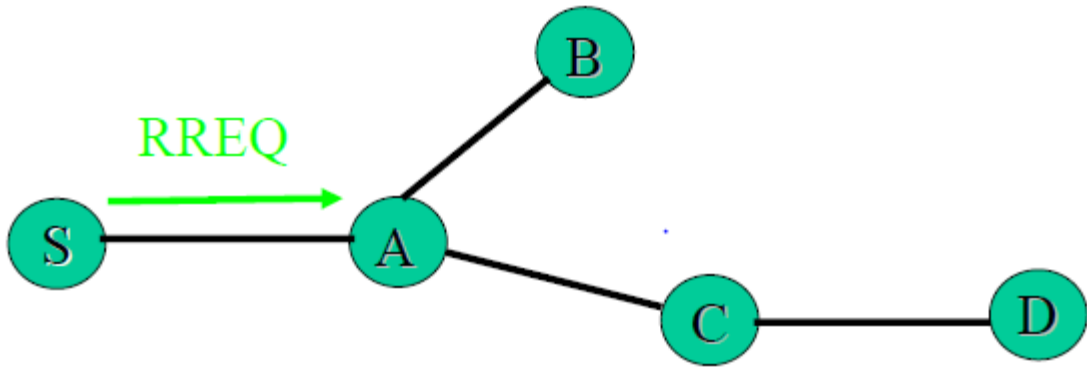


Figure 5 Route request cont.

3. Node S broadcasts RREQ to its neighbors.

4. Node A gets RREQ and makes a reverse route entry to S.

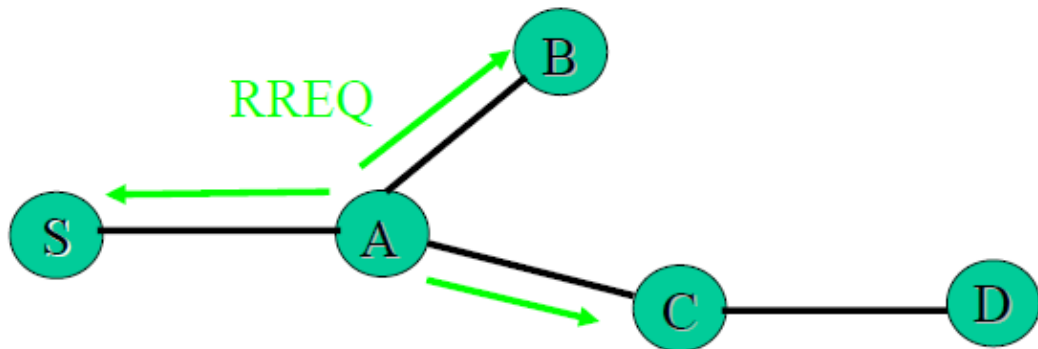


Figure 6 Route request Rebroadcast

5. But node A has no address of D so it rebroadcast RREQ.

6. Node C gets RREQ and it has entry of D in its table so it send route reply.

AODV Route Reply:-

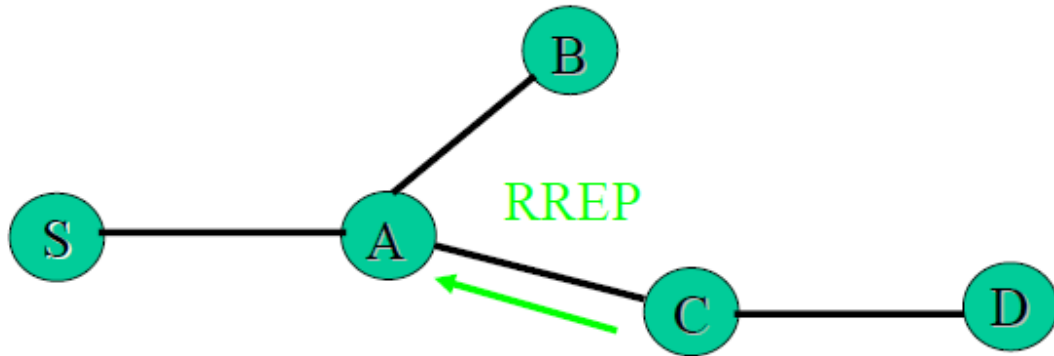


Figure 7 Route Reply

7. Thus node C unicast route reply back to node A.

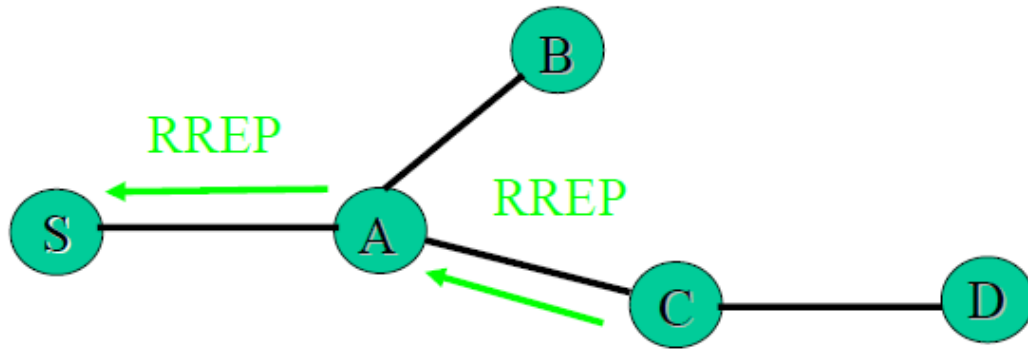


Figure 8 Route reply cont.

8. Then A also unicast RREP to S.

AODV data delivery

Thus after the route is fixed between sender and receiver the data is transmitted through the fixed path.

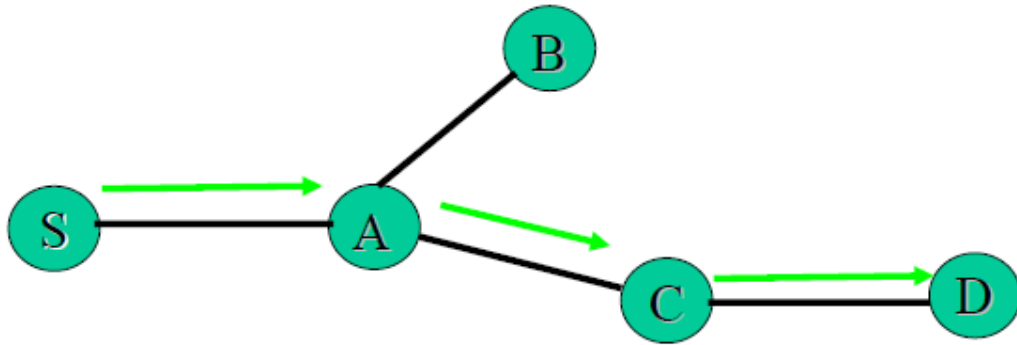


Figure 9 Data delivery

9. Thus S can send data to D through above path.

AODV Route maintenance

When the communication is going on between sender and receiver sometimes connection can be lost between intermediate devices and link is lost thus route error message is generated by the error prone node to the sender side.

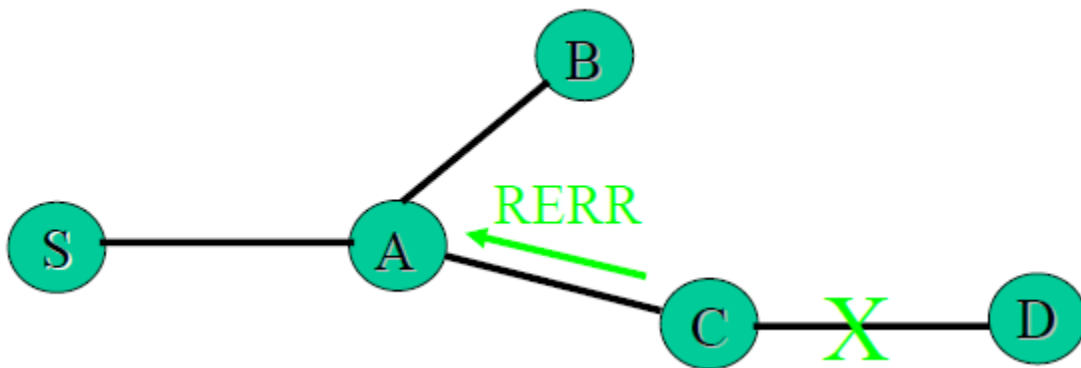


Figure 10 Route error message

10. Link between C and D is lost .

11. So C send RERR message to A.

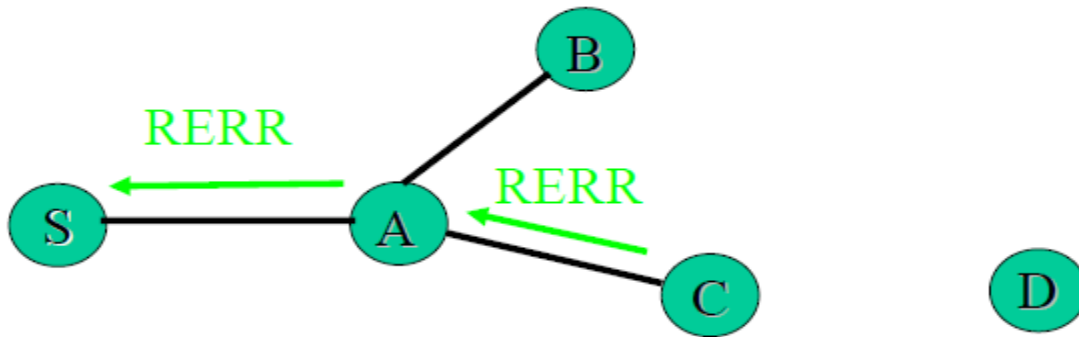


Figure 11 Route error message cont.

11. Node A further send the RERR message to its upstream node S.

Thus AODV protocol works in the above way.

1.7 Threats and attacks

The amount of dissimilar threats and attacks can be considered into a number of different zones that they target. The first is to think about the level of the attack which can be perceptual where the human perception is targeted using the media as a bearer. It may be distributing wrong information or impartial statement of social behavior to be capable to adjust decision processes. Secondly the assaults can aim the information itself where interruption and snooping comes obviously in mind. Of the more dynamic nature of these attacks might be the formation of incorrect messages inserted into networks. Also the denial or deprivation of network facilities is a procedure of active attack on the information level. In this class application level attacks such as Trojan horses or bugs and the similar are also comprised. The physical attacks are the third session. The quiet nature of this class can be radiation interruption or inductive monitoring. The extra hands on attacks contain theft of implements, cryptographic and different storage media. Surplus types of attacks are social engineering or as harsh as damage using explosives or other bodily power.

1.7.1 Wireless network attacks

In contrast to network tools in supported networks where the devices regularly are reserved behind protected entries the Ad Hoc network tools are generally approved around as small battery-powered policies or sited inside mobile elements like cars. This makes them even more

striking for attackers as they are often easier to get to and also easier to carry away from the misconduct part. Alternative point is that it can be pretty solid to interrupt wired media without getting observation of both as the media also might be hard to acquire to and to interrupt the cables regularly will need cutting the cables for a while. In the wireless intermediate it is as informal as just placing up an antenna, typically small enough not to be discerned.

Also, subsequently many users of the Ad Hoc networks will be consuming it in public places the risk of accidentally revealing mysteries are large. This can be in the formula of an exchange being held so that somebody can hear stealthy information or shoulder surfing, that is, somebody analysis the computer display or keyboard from behindhand while entering passwords or the like. The human nature of evil memory can also be of certain help for the attacker. It is not infrequent that persons write down PINs and user details on post-it records and in the future time throw them away in trash cans. The recovery of this kind of information can help assailants to estimate the accurate passwords to system assets.

1.7.2 Attacks on Routing protocols

There are many types of attack possible on routing protocols. Here we will discuss some specific attacks on protocols. We can divide these attacks in two categories:-

- Active attacks
- Passive attacks

Passive attack never destroy the working of the protocol, but it just tries to get treasured information by hearing the traffic. On the other side an active attack inserts wrong packets and tries to destroy the operation of the protocol in direction to boundary the availability, to get authentication, or to fetch packets destined to other nodes. The routing protocols in MANETs are very doubtful because attackers can definitely get information about network topology. Some major attacks are:-

1.7.2.1 DDOS:-A distributed denial of service attack is a done by various attackers to flooding the victim network with a huge number of packets. This effects the network of assets

such as bandwidth and computing power. The victim is incapable to offer services to its actual users and network performance is cut down. A DDOS attack is made up of four elements:-

- Victim
- Master
- Daemon
- Attacker

"Attacker" here means the target have that has been picked for assault. "Daemon" alludes to the operators programs that really direct the assault on the target exploited person. Assault daemons are generally sent in host machines. These daemons influence both the target and the host machines. "Expert" is an expert project to arrange the assault. "Real attacker" alludes to the genius behind the attack.by utilizing the control expert system, true assailant can stay in the background of assault.

1.7.2.2 Impersonation:-When there is no proper certification mechanism then a mischievous node can observe the network traffic by being real node. It can also send wrong routing packets, and get access to some important information.

1.7.2.3 Eavesdropping:-This is a no an active attack. The node simply get the important information. This information can be used by the attacker node the undisclosed information can get by listener.

1.7.2.4 Routing attacks:-The attacker node make routing facilities as a main goal because it is a key service in MANETs. There are basically two type of ways to implement this routing attack. One is attack on routing protocol and the one is attack on forwarding of packet. The first is aimed to be delaying the transmission of routing information of a node. The second is directed at troubling the packet delivery against a fixed path.

1.7.2.5 Blackhole attack:-In this assault, an aggressor introduces a metric to all its endpoints creating all hubs around it to track packets to it. A spiteful hub sends fake directing

data, verifying that it has a veritable course and reasons other great hubs to course information parcels through the malevolent one. A malignant hub drops all bundles that it gets rather than ordinarily sending those parcels. An aggressor listen the solicitations in a flooding based convention.

1.7.2.6 Wormhole attack:-In such type of attack an attacker gets packets at one location in the network, directs them to alternative point in the network, and then repeat packets into the network from that point. Routing can be destroyed when routing control communication is tunneled. This tunnel among two conspiring attacks is identified as a wormhole.

1.7.2.7 Replay attack:-An assailant that performs a replay assault are retransmitted the legitimate information over and over to embed the system directing activity that has been caught long ago.

1.7.2.8 Gray hole attack:-It leads to releasing of messages. Gray hole attack has two parts. In the first level the node announce itself as having a legal path to endpoint whereas in second phase, nodes drops captured packets with a certain possibility.

1.7.2.9 Rushing attack:-In reactive routing protocols almost all nodes contains a sequence number for duplicate suppression. An attacker can distribute large number of duplicate route requests with increasing sequence number and shows it as it is from another nodes. But when the actual request is sent out many nodes reject it by thinking it as duplicate one.

1.7.2.10 Resource consumption:-By inserting additional record packets into the Ad Hoc network restricted assets such as bandwidth and battery power are spent for no motive. And more resources can also be used up by inserting more control packets and these might lead to extra computation.

1.7.2.11 Dropping routing traffic:-It is necessary in the Ad Hoc network that complete nodes join in the routing process. However, a node can act greedily and process only routing

information that are connected to itself in order to preserve energy. This behavior can create network in security.

1.7.2.12 Location disclosure:-A location disclosure attack can disclose information correlated to the location of a node or the topology and configuration of the network. The information gained might disclose which other nodes are adjacent to the target of a joining node. The attack can be fulfilled by using a command like traceroute.

Above all are the major attacks possible in mobile ad hoc networks. All attacks have different impact on the network and on different routing protocols. From all of these DDOS attack is one of the major attack. Most commonly it is performed in the AODV routing protocol as it is on demand routing protocol. There are various techniques used to mitigate the impact of DDOS attack. Thus attacks makes the performance of the protocols very low.

1.8 Security models and attributes

The area of security is huge and some ideal to use for criticizing the problem is desirable. The succeeding attributes requires to be considered for categorizing the different security requirements of the requests of Ad Hoc network. The various security requirements are considered as:-

- ✓ **Integrity**
- ✓ **Availability**
- ✓ **Authentication**
- ✓ **Confidentiality**
- ✓ **Non-repudiation**

1.9 Security of ad hoc network

As of dynamic topological variations, ad-hoc networks are weak at the physical link, as they can certainly be operated. An invader can effortlessly attack ad-hoc networks by loading

accessible network assets, such as wireless acquaintances and battery levels of other operators, and then bother all consumers. Assailants can also disrupt the normal procedure of routing protocols by adjusting packets. The invader may insert false information into routing packets, producing wrong routing table updates and thus provides wrong routing. Some other safety weaknesses of ad-hoc systems are:-

Less power supply:-As nodes generally use battery as power source, an invader can use batteries by producing extra broadcasts or extreme calculations to be passed out by nodes.

Key management as a challenge:-Vigorous topology and movement of nodes in an Ad Hoc network mark key organization tough if the cryptography is used in the routing protocol.

Less computational capabilities:-Usually, nodes in ad-hoc networks are integrated, self-governing, and partial in computational skill and so may become a foundation of weakness when they grip public-key cryptography throughout regular process.

1.10 MANET Security

The facility of safety services in the MANETs background faces a set of encounters particular to this new technology. The uncertainty of the wireless links, power constraints, fairly poor physical safety of nodes in an aggressive environment, and the weakness of statically arranged security structures are positively such experiments. However, the only most chief feature that distinguishes MANETs is the lack of a static infrastructure. No portion of the network is devoted to support separately any specific network functionality, with routing being the most noticeable example. Extra examples of functions that cannot trust on a overriding service, which are also of great significance to this work, are identification services, certification authorities, and other administrative facilities. Even if such facilities were invented, their approachability would not be confident, also due to the vigorously moving topology that can easily end in a divided network or due to jammed links close to the node performing as a server.

Moreover, performance topics such as delay restraints on getting responses from the expected infrastructure would pose an extra test. The deficiency of infrastructure and the consequential absence of approval facilities delay the usual practice of beginning a line of security, splitting nodes into reliable and non reliable. Such a difference would have been built on a security plan, the ownership of the necessary authorizations and the capability for nodes to validate them. Furthermore, in MANETs easily travelling nodes form temporary associations with their neighbors, enter and leave MANETs sub-domains individually and without warning. Thus it may be hard in most cases to have a rich picture of the Ad Hoc network connection. Accordingly, particularly in the case of a large-size network, no method of recognized trust associations among the most of nodes could be expected.

In such an environment, there is no assurance that a track between two nodes would be free of mischievous nodes, which would not meet the terms with the active protocol and effort to damage the network operation. The appliances currently combined in MANETs routing protocols cannot manage with interruptions due to nasty behavior. For example, any node could privilege that is one step away from the wanted endpoint, affecting all routes to the endpoint to pass through themself. Else, a malevolent node could fraudulent any in transit route request packet and cause information to be misrouted.

The occurrence of even a slight number of oppositional nodes could result in constantly negotiated routes, and, as a result, the web nodes would have to trust on rounds of time-out and new route findings to interconnect. This would suffer random interruptions before the setting up of a non-corrupted track, while consecutive transmissions of route requests would enforce unnecessary transmission below. In specific, deliberately artificial routing memos would result in a denial-of-service practiced by the end nodes. The suggested scheme have conflicts such types of misconduct and protections the acquirement of topological information.

CHAPTER 2

LITERATURE REVIEW

Prajeet Sharma have [1] defined in (2012) involves security of wireless mobile ad hoc networks from DDOS attack by using intrusion detection system in AODV protocol. In this paper different types of attacks on ad-hoc networks are defined. DDOS attack is the core difficulty in all ad hoc scenarios. There was a IDS which uses two intrusion detection parameters i.e. packet reception rate and arrival time, but this was not sufficient for intrusion detection. So in this paper more parameters are used to work IDS more accurately.

M. Mohanapriya (2014), defines [2] that there is a modified dynamic source routing (DSR) presented to prevent and identify selective black hole attack. Selective black hole attack is special kind of attack where the malicious nodes drop the data packet selectively. There is an intrusion detection system proposed in this paper, where IDS nodes are set in random manner only when necessary. To detect the anomalous change in the number of data packets being dispatched by a node, thus when any irregularity is noticed the neighboring IDS node broadcast the block message to inform all nodes on the network to helpfully separate the mischievous node from the network. In this paper. Glomosim (global mobile information system simulator) is used to show simulation results. The MDSR (modified dynamic source routing) is also compared with an existing technique i.e. detection of black hole attack through IDS. Thus the performance is measured and it has provided better results than the existing system. Packet drop ratio, overhead and end to end delay is measured to check the results of this technique. Packet drop ratio is almost reduced up to 64%, while it is very high in DSR when it is under attack.

Kavita pandey describes [3] about the performance of proactive, reactive and hybrid protocols in MANET in 2011. As a proactive routing protocols the performance of DSDV and as a reactive routing protocols performance of AODV and DSR and as a hybrid routing protocol

performance of ZRP routing protocol has been compared. Network simulator2 is used for simulation experiments. It is an object oriented simulator. Then the performance results are shown on the basis of amount, ordinary delay, no. of packets dropped and routing overhead. In the case of throughput results, the throughput of AODV protocol is superior as compared to other protocols. In other protocols, as the number of nodes increase throughput also increases. In the case of average delay, As AODV is a table based protocol, routes are created on request, and therefore it practices higher delay. In the case of released packets, in DSDV protocol the number of packets released are greater as related to others.

Thus this paper shows results that the consistency of AODV and DSR protocol is blameless than others.

This paper by **Mohit kumar** in (2012) involves [4] various attacks which are possible in MANET due to fabrication and worm hole attack in AODV, and how to secure AODV against wormhole attack using token based approach. Four types of attacks i.e. gray hole, black hole, worm hole and byzantine attack are defined in this paper. Worm hole attack is a severe attack that disrupts the normal flow of the packet in the network. To use the token based approach against worm hole attack double encryption technique is used. In this proposed technique, session key and generated time created using double encryption and stored in the token. The token can be encrypted by the private key of sender, so we can also call it token as a digital signature certificate. Thus token based approach is used to provide security against worm hole attack in AODV protocol by using double encryption technique.

Geetika and Naveen kumari (2013) have defined [5] in there paper various algorithms for the detection and prevention of DDOS attack in MANET. There are several attacks like impersonation, eavesdropping, message redirection, traffic analysis are possible in MANET. In some specific scenarios, MANET is dispersed above large area, so some nodes are hard to monitor, so physical attack can be there. There is no central authority in MANET. Two methods are defined for attack detection:-Profile based and Specification based. Bottom-up detection and prevention technique is divided into three phases: Quality reduction based attacks, Detection of TCP sync flood attack, for normal half open connection there is window based control. New cracking algorithm is a technique in which a status table is maintained. IP

address of current user is kept there, if the particular IP address logon for four times, it is normal case. But attempt to fifth time is an attacker. IP trace algorithm has the capability to discover the source of an IP packet without trusting on the source IP field of the packet. It can trace the foundation of attack. Thus this paper have concluded MANET security as complex and challenging task.

Zhang Chao-yang in 2011 clarifies DDOS [6] attack prevention principles and gives an investigation of existing attack avoidance procedure. It characterizes data transmission and connectivity attacks. Bandwidth attack effects the system activity, so all accessible assets are exhausted. Connectivity attack is with many of connection requests that effect the server operating systems, as a result server cannot deal with client's appeals. This paper defines the four terms:-Attack principle defines about three way handshake convention to create a connection. Components of attack are attacker, console and agent. Attacker's computer is the main console to attack. Which can be anywhere in the network. Console is some host that attacker attack and control unlawfully and these hosts also control a large number of delegation host. Agent is host that attacker control illegally. Attack performance includes the development high flow impractical data, so it gives rise to blocking in network, so host cannot communicate with outside domain correctly. Defence Program has been used to defend DDOS attack. First, is by using a router. In this technique unicast reverse path forwarding function is used for routing security. Here router checks the table when it receives a packet. If the source IP address is included in the table only then it forwards next, otherwise discard it. Second, is use TCP blocking to limit synchronization attack, In this technique on established connection are taken care, half-open connection are timed out after a time period. Third is increase the trusted platform module and certification system defence. All these techniques provide prevention from DDOS attack.

Anit kumar Investigates in 2011 of the execution [7] of AODV and DSR protocol for the packet delivery rate is performed. This paper is very helpful to know about the real world problems in the MANET security. Several benefits of MANET are defined in this paper. These are: Dynamic network topology, limited bandwidth, distributed operations and security.

Routing protocols i.e. reactive, proactive and hybrid protocols are defined in brief. The simulation is performed using network simulator 2. The traffic sources are UDP. This paper also guides us to do more research in end to end delay and throughput analysis for the selection of particular protocol

B.B.Gupta in (2010) includes the [8] prevention mechanism for DDOS attack in his paper. It have defined several resources that can be targeted by the attacker. These are network bandwidth resources, system memory resources, system CPU resources. In this paper writer defines that there are various tools available in market for DDOS attack, so DDOS attack is very easy and common in networks. These tools are: Trinoo,TFN,TFN2K,stacheldraht,shaft,Mstream,Knight,trinity. There are two types of techniques used for prevention. First are the general techniques:-Disable unused services, Install latest security patches, Disabling IP broadcast, Firewalls, Global infrastructure, IP hopping. Secondly, there are filtering techniques:-Ingress and Egress. Router based packet filtering, History based IP filtering, Capability based filtering and Secure overlay service. All these techniques provide a secure intrusion detection system over DDOS attack. But still some vulnerabilities are there and possibility of attack is there.

Nisarg gandhewar presents [9]the recreation results taken as end to end delay, packet conveyance ratio, packet misfortune for AODV when the quantity of hubs shift in the network. This paper also defines the overview of occupied features and benefits of AODV protocol. It defines four types of switch messages in AODV i.e. route request, route reply, route error message, hello message. Route discovery and route maintenance is also described .As per the performance, average end to end delay time taken by the data packets to broadcast from source to destination across MANET. Thus the performance of AODV protocol is evaluated in this paper to show the benefits and performance of AODV protocol.

One more study by pankaj rohal shows [10]the analysis of end to end delay, throughput and packet delivery fraction in AODV routing protocol. From this paper we come to know that when the connectivity is good then throughput will increase automatically, so in this paper also authors have shown that AODV is better in performance as that of DSR and DSDV. On the

other side in end to end delay AODV is having slightly high delay because it is high in throughput But DSR have less delay. But in packet delivery fraction also AODV is better than both the protocols. Thus this paper simply shows the performance of three topology based protocols and concluded that reactive routing protocols are better as that of proactive.

In 2008 a research in [11] wireless sensor networks shows the influence of random based mobility models and group based mobility models on the performance of AODV protocol. The results in this research have shown that Group models are better as that of random ones. This paper poses various features of wireless sensor networks. The end to end delay packet delivery fraction and throughput and latency of AODV is measured. The scenarios have been taken in the case of varying of speed in nodes. After all this technique also shows the better performance of AODV and shows that group based mobility models are better as that of random based.

Chander Diwaker in 2013 have [12] presented a survey on the importance of MANET and also shows the MANET as most weak to cyber attacks. This paper shows the black hole attack and different prevention and detection measurements. Two types of black hole attack is discussed that is internal black hole attack and external black hole attack. Internal black hole attack here means that it is from the attacker node that is present in the internal network and cause damage to other network. On the other side external black hole attack means it is from the outside network and the attacker node is not present in the network. Researchers have also shown the techniques like distributed cooperative technique, data routing information technique and cross check technique and also tried to give light on neighbor based route recovery scheme.

CHAPTER 3

PRESENT WORK

3.1 Problem formulation

In problem foundation we are going to discuss the problem definition why mentioned problem statement was chosen. Various techniques are used till now to mitigate the effect of DDOS attack in AODV routing protocol in MANETs and different techniques have different results. Here we are discussing some of the techniques that lead us to work on the proposed system. Different techniques we studied and that give us way to reach to our technique are as follows:

The technique for packet dropping was proposed by some authors. In such type of technique the authors proposed a procedure for discovery of mischievous nodes and security against DOS attack in AODV protocol. This method preserves record of all nodes existing in the network. Recognition and avoidance from denial of service attack in AODV routing protocol is fulfilled by their following algorithm:-

- Set a threshold rate for Packet Drops
- Detect the Sequence Numbers
- compute the Packet Drops
- If Packet Drops > thresh hold value then
- Raise Alarm
- Remove the paths of the nodes on the base of packet dropped by them
- Keep a log file to prove that identified nodes are answerable for maximum packet drop, later detached. After discovery of mischievous node, it is isolated from network.

The gain of this method is that indicates to less conversation and fewer communication smashing in ad-hoc routing and restriction is it has incomplete applicability. One more technique was used by some authors is intrusion detection technique. This technique was used

for the mitigation of DDOS attack in MANET. In this case one node is set as an IDS node and this node look up for all the wireless nodes. If any unusual behavior comes to the network then this IDS node first of all checks the signs of the attack and then look for the assailant node and remove that node from the network. The authors have proposed an algorithm for it and give some improved results. In the simulation numerous presentation tables are compared with the existing ones. Throughput was increased in the IDS case and delay was also low. But still there are various situations when DDOS attacks goes undetected. Thus this technique was not so successful. There was one more method used in 2012 by authors to secure the AODV against the wormhole attacks. In this technique the researcher have used token system by using double encryption technique. Thus we have assumed the idea to mitigate the DDOS attack in AODV by using token and encryption with ECDSA. In the above technique still there were various shortages. So after reviewing all techniques we have come to know about the shortages and here we will discuss how to provide more security in MANETs:-

The necessity of today is to offer secure and trustworthy communication of MANETs.

- Key management and verification are the essential aspects of providing security in MANETs so these should not be fragile.
- Security parameters for a small network is not a big issue but when number of mobile nodes is huge and flexible then security must be provided at a large extent.
- It is easy to achieve the security of a fixed network but for a moveable and dynamically changing network it is challenging.
- Detection of the malicious node.
- Proper Route Discovery.
- Maximum throughput and less delay.

Thus there are various techniques performed by several researchers to mitigate the DDOS attack and to improve the performance of protocols. All techniques have produced different results. But still there are some limitations so we have produced a new technique to improve the results. This technique is defined in the next sections.

3.1.1 Problem definition

So first of all let's consider problem statement i.e. "Mitigation of DDOS attack in AODV routing protocol using token based identity". This problem definition clearly shows that main aim of this project is to reduce the DDOS effect in AODV routing protocol and improve the results of AODV protocol on the basis of end to end delay, packet delivery fraction and throughput. Thus further in this section we will describe how this problem definition is processed and how the results provided by this technique are better even in the case of DDOS attack. The results will be discussed in the next sections and the simulation results will be discussed through the network simulator 2.

3.2 objectives

The ad hoc routing protocols are proficient routing protocols. Between the mobile nodes, the MANET is used to route its packets. The important objectives of this dissertation are:

- 1) Study of MANET routing protocols.
- 2) Implementation of AODV routing protocol in NS2 to improve the efficiency of data transmission and security for DDOS attack in the MANET.
- 3) Performance analysis on the basis of Packet delivery fraction, throughput and end to end delay.
- 4) Performance of DSR protocol in case of DDOS attack and the performance of AODV in case of DDOS attack and improvement using proposed technique.

3.3 Research methodology

To moderate the DDOS attack in AODV convention and to improve the AODV results we are utilizing a token based personality framework for every hub in the network. Thus each hub in the network will have an identity. These character tokens will be encrypted by utilizing elliptic curve digital signature algorithm. Thus the accompanying steps will be taken:-

- ❖ Start for route request.

- ❖ The node will send information with the token to the next node.

- ❖ If the next hop decrypts the information then it acknowledge previous node to continue route request.

- ❖ If next node does not decrypt the information then it will acknowledge the previous node to change the path and locate the node as a DDOS attacker node.

- ❖ Repeat step three until the destination is reached.

- ❖ Stop and scan for next.

Further the research methodology flow chart is described in figure. Here in this technique the ECDSA is used for the token encryption and decryption. So here we will give little information about ECDSA also in this section. To show the results from this technique we will be using NS2. Thus we will also discuss before results that how Ns2 works and how the simulation is performed in it. Thus first of all let us discuss the flow chart of our technique:-

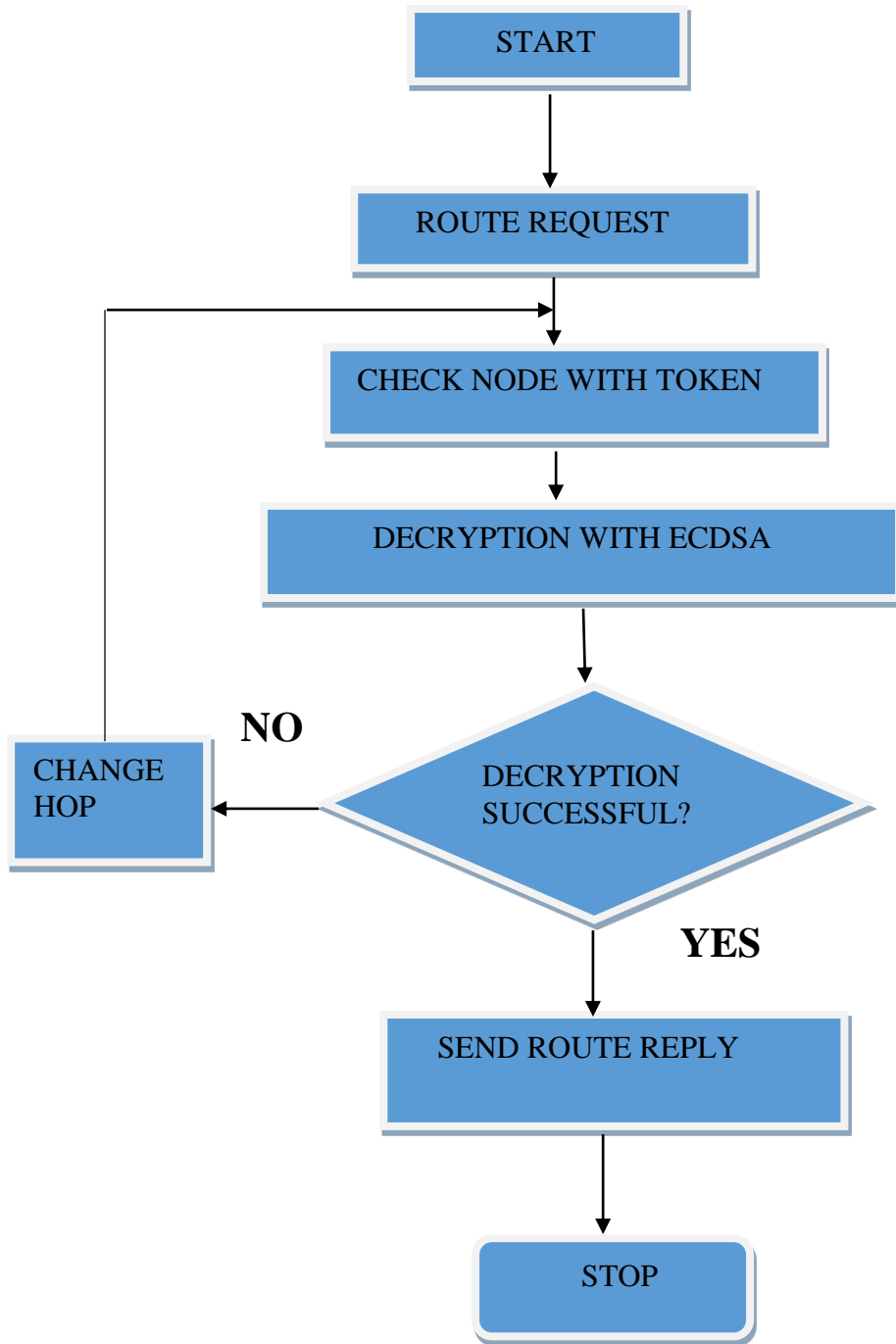


Figure 12 Flow chart for token based process

ECDSA (Elliptic Curve Digital Signature Algorithm)

ECDSA algorithm we will be using for token encryption purpose in our technique. Here we will discuss some concepts of ECDSA:

Private Key:-A secret number that is only known to the person that produced it. A private key is basically a randomly created number. This key cannot be shared with another users.

Public Key:-A number that relates to a private key, but does not essential to be kept undisclosed. A public key can be designed from a private key, but a private key can never designed from public key. A public key can be used to define if a signature is produced with the proper key without requiring the private key to be told.

Thus, the ECDSA offers remarkable advantages over other cryptographic system. The advantages are as follows:-

- It provides superior security for an agreed key size.
- It offers effective and solid implementations for cryptographic operations demanding minor chips.
- Due to slighter chips less heat generation and less power ingesting.
- It is mostly appropriate for technologies having little bandwidth, less computing power and less memory.
- It is very easy for hardware implementations.

Thus by understanding the above all advantages we will be using this algorithm in our token decryption techniques so that improved and solid results could be achieved.

Network Simulator 2

Network simulator is an open source network simulation tool. It is an object oriented, separate event determined simulator inscribed in C++ and Otcl. The main use of network simulator is

in network researches to simulate numerous types of wired or wireless limited and wide area networks, to implement network protocols like as TCP and UDP, traffic flow source behavior like as FTP, Telnet, Web, CBR and VBR, router queue management technique and many more. Ns2 is printed in C++ and Otcl to detach the control and data track actions. The emulator provisions a class hierarchy in C++ and an equivalent hierarchy within the Otcl explainer. The motive why ns2 uses two languages is that dissimilar tasks have different necessities. For example simulation of protocols needs effectual manipulation of bytes and packet headers creating the run-time quickness very significant. On the other hand, in network lessons where the goal is to differ some parameters and to rapidly observe a number of scenarios the time to modification the model and run it another time is more important.

In ns2, C++ is used for comprehensive protocol implementation and in over-all for such cases where every packet of a stream has to be treated. For example, if you need to implement a new queuing self-control, now C++ is the language of fine quality. Otcl, on the other hand, is appropriate for conformation and setup. Otcl runs fairly slowly, but it can be reformed very speedily making the structure of simulations at ease. In ns2, the assembled C++ objects can be made accessible to the Otcl interpreter. In this way, the ready-made C++ substances can be organized from the OTcl level.

Otcl Basics

It is very important to understand that how Otcl works and how the variables are assigned values and how all process take place on Otcl.

Assign values to variables:-In Otcl values are assigned to variables and then these values can be used further in commands. As we can show below how to assign values to variables:-

set b 10

set d [expr \$b/10]

In the first line, the variable b is allocated the value “10”. In the second line, the outcome of the command [expr \$b/10], which equals 1, is then used as an argument to one more command,

which in turn allocates a value to the variable d. The “\$” sign is used to get a value enclosed in a variable and square brackets are a sign of a command exchange.

Creating the topology:-To run a simulation environment, a network topology should be created firstly. In ns2, the topology involves an assembly of nodes and links. Beforehand the topology can be set up, a new simulator object should be generated at the commencement of the script with the command:

```
set ns [new Simulator]
```

The simulator object has associate functions that permit generating the nodes and the links, joining agents etc. All these elementary functions can be originate from the class Simulator. When expending functions fitting to this class, the command originates with “\$ns”, as ns was defined to be a holder to the Simulator object.

Node

Different node objects can be generated with the command:

```
set n0 [$ns node]
```

```
set n1 [$ns node]
```

```
set n2 [$ns node]
```

```
set n3 [$ns node]
```

```
set n4[$ns node]
```

The member function of the Simulator class, called “node” creates five nodes and allocates them to the handles n0, n1, n2, n3 and n4. These holders can later be recycled when denoting to the nodes. If the node is not a router on the other hand it is an end system, traffic agents i.e. TCP, UDP and traffic sources i.e. FTP, CBR must be set up, i.e. bases need to be committed to the agents and the agents to the nodes, correspondingly.

Tracing and monitoring

To calculate the result from the simulations, the data needs to be collected in some way. NS2 supports two main observing proficiencies: traces and monitors. The traces allow recording of

packets every time an event such as packet drop or entrance happens in a queue or a link. The monitors offer a means for gathering amounts, such as amount of packet drops or number of arrived packets in the line. The monitor can be used to assemble these amounts for all packets. All events from the simulation can be documented to a file with the following commands:

```
set trace_all [open all.dat w]
```

```
$ns trace-all $trace_all
```

```
$ns flush-trace
```

```
close $trace_all
```

First of all, the output file is opened and a handle is attached to it. Then the events are documented to the file stated by the handle. Lastly, at the completion of the simulation the trace buffer has to be flushed and the file needs to be closed. This is generally done with a distinct finish procedure. If links are molded after these commands, extra objects for tracing will be inserted into them.

Next we will discuss how simulation is performed in NS2 and how results can be displayed by using this simulator.

Controlling the simulation

After the simulation topology is generated, agents are organized. The start time and stop of the simulation and other all events have to be arranged. The simulation can be started and stopped by using commands.

```
$ns at $simtime "finish"
```

```
$ns run
```

Above first command can be used to finish the simulation process and the second command is used to run the process. It can start NAM i.e. network animator for graphical results only when desired and post process information and plot all the information. The finish procedure has to contain at least the following elements:

```
proc finish {} {
```

```
global ns trace_all
```

```
$ns flush-trace
```

```
close $trace_all
```

```
exit 0
```

Thus above all command and processes are used in NS2 to show the results. After tcl file is compiled it gives two files that is trace file and network animator file. Thus after that we can see results in trace files and can plot the scenarios in nam files and can visualize the graphs through trace files.

In the next chapter we will argue the results and will show the all results in graphical representation by using NS2.

CHAPTER 4**RESULTS AND DISCUSSION**

The proposed token based system is implemented in NS2. Let's discuss the result step by step. First of all we will discuss the parameters that we have choose for simulation of AODV routing protocol. Here we will discuss the parameters that we have used for our implementation.

4.1 Simulation Parameters

SIMULATOR	NS2.34
PROTOCOL	AODV, DSR
SIMULATOR AREA	1000M X 1000M
SIMULATION TIME	50 SECONDS
NUMBER OF NODES	50
PAUSE TIME	50SECONDS
MAXIMUM SPEED	DEFAULT
PACKET RATE	512KBPS
TRAFFIC TYPE	CBR

Table 1 Parameter values used for AODV simulation results.

4.2 Performance measurements

In this technique we have measure three parameters in AODV routing protocol. These parameters are as follows:-

End to end delay:-End to end delay is defined as the average time used by data packets to reach from source to recipient through MANET in AODV routing protocol. This delay defines all the delays due to buffering throughout route detection latency and delay in queue and time consumed in retransmission. As lower the end to end delay is the performance of protocol will be better.

Packet delivery fraction (PDF):- PDF is the ratio of count of packets received by the receiver to the count of packets send by the sender node. Thus it defines the level of data delivery to the destination node. The higher value of PDF means the better performance of that protocol.

Throughput:-Throughput is the average rate of positive message transfer over a communication channel. This data may be transported over a physical link or pass over a certain network node. The throughput is generally measured in bits per second and occasionally in data packets per second or data packets per time period.

Thus above all measurements are very important to recognize while calculating the performance of any protocol. So we will discuss in this section the above four components results of our technique also.

4.3 Simulation process in NS2

The simulation setting and parameters used for the accomplishment of the detailed investigation and study of DDOS attacks in MANET protocol AODV is labeled in this section. This aspect represents that in what way the actual performance parameters have been investigated to simulate the protocols.

Given steps have been used for the simulation in network simulator.

- **Inputs given to the network simulator:-**
 - Scenario file showing movement of nodes.
 - Simulation TCL file
- **Outputs File from network simulator:-**
 - Trace file (.TR)
 - Network Animator file (.NAM)
- **Output from Trace Analyzer:-**
 - .xgr file

Now let's introduce that what the network animator and trace file is. We will discuss the working of both files in this section:-

4.3.1 Network animator (.NAM)

NAM here stands for Network Animator. It contains the data for network topology and shows the graphical representation of the hops. It initiates with the scheduled command 'nam <nam-file>' here '<nam-file>' is the name of network animator trace file i.e.tr file. At LINUX workstation, the command to run NAM is ./nam.

After running the .tcl files trace files are produced. Trace file contains the following information:

- Send/Receive Packet
- Time
- Traffic Pattern
- Size of Packet
- Source Node
- Destination Node etc.

4.3.2 Trace Analyzer (.TR)

Awk scripts means .awk files trace analyzer is used to assess trace outputs from simulation. When files are evaluated via this trace analyzer then an output file i.e. .xgr file is created which lead to the formation of graphs called xgraphs.

Thus above all is the simulation process in the network simulator 2 that how the files are created and processed in this simulation environment. Thus in the next section we will discuss the simulation results of our proposed technique and then comparison will be there in further sections.

4.4 Simulation results

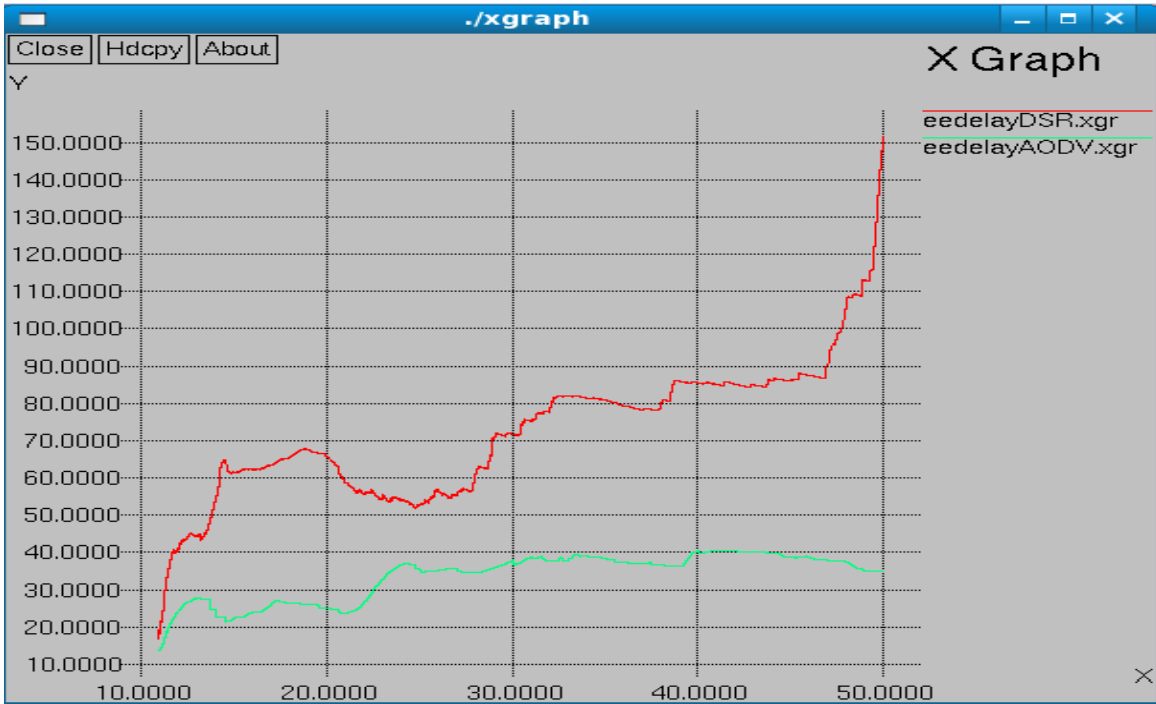
In this unit we will argue the results that have been produced from our technique and we will discuss all the results parameters.

PROTOCOL NAME	AVERAGE THROUGHPUT	AVERAGE PACKET DELIVERY FRACTION	AVERAGE END TO END DELAY
DSR IN CASE OF DDOS ATTACK	211.25kbps	75%	151.59ms
AODV IN CASE OF DDOS AND TOKEN BASED SECURITY	222.61kbps	89%	34ms

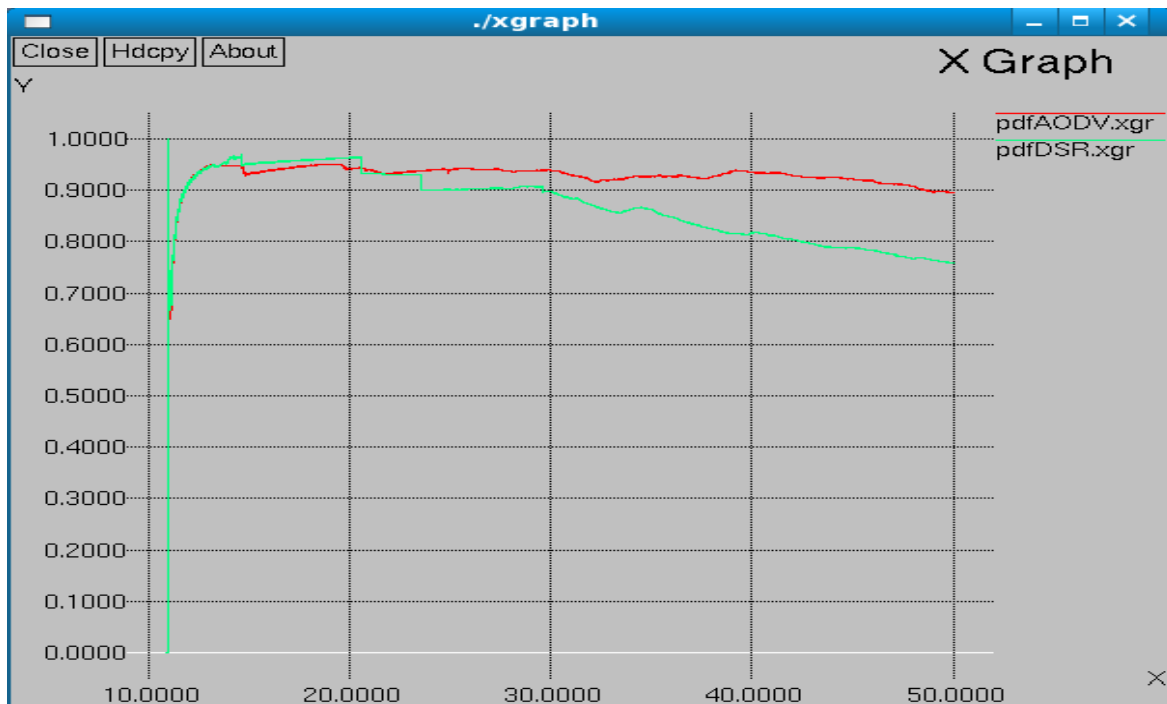
Table 2 Result table

Above table shows the simulation results of the proposed technique. Thus next we are presenting the graphs that shows the visualization of the average of end to end delay, packet delivery fraction and average throughput.

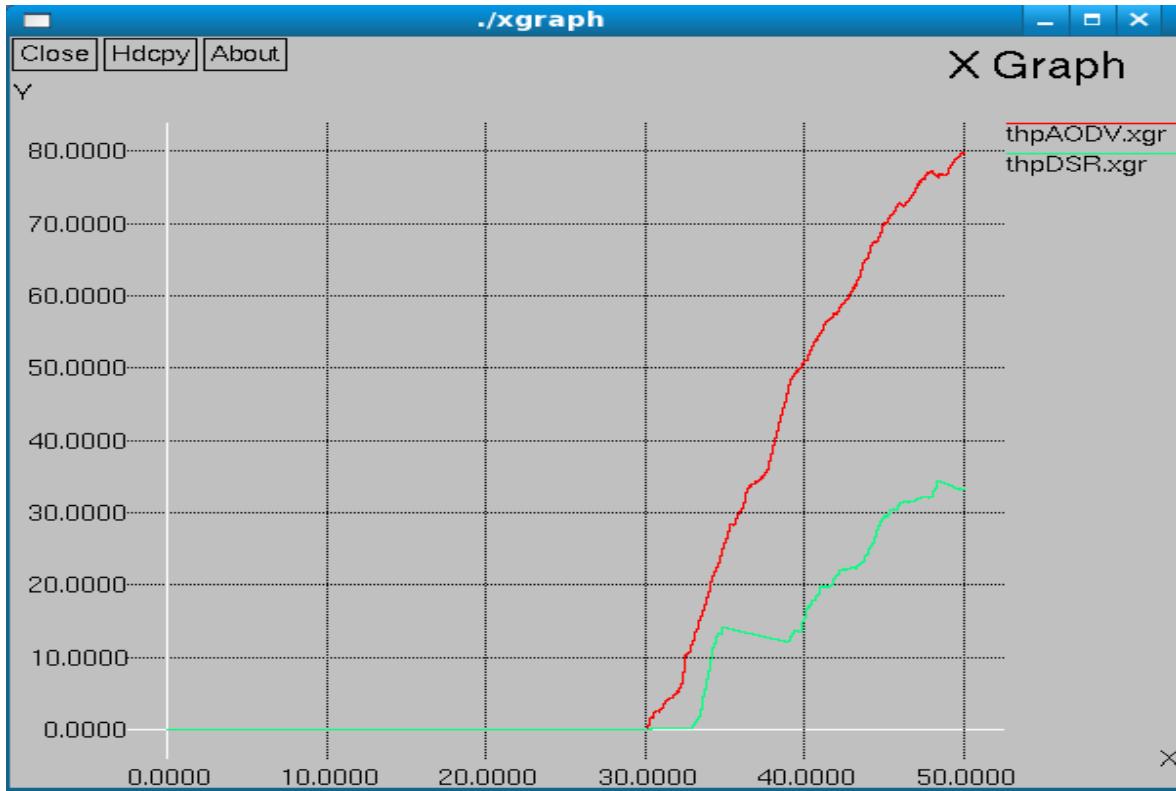
Comparison Graphs



Graph 1 end to end delay comparison



Graph 2 Packet delivery fraction comparison



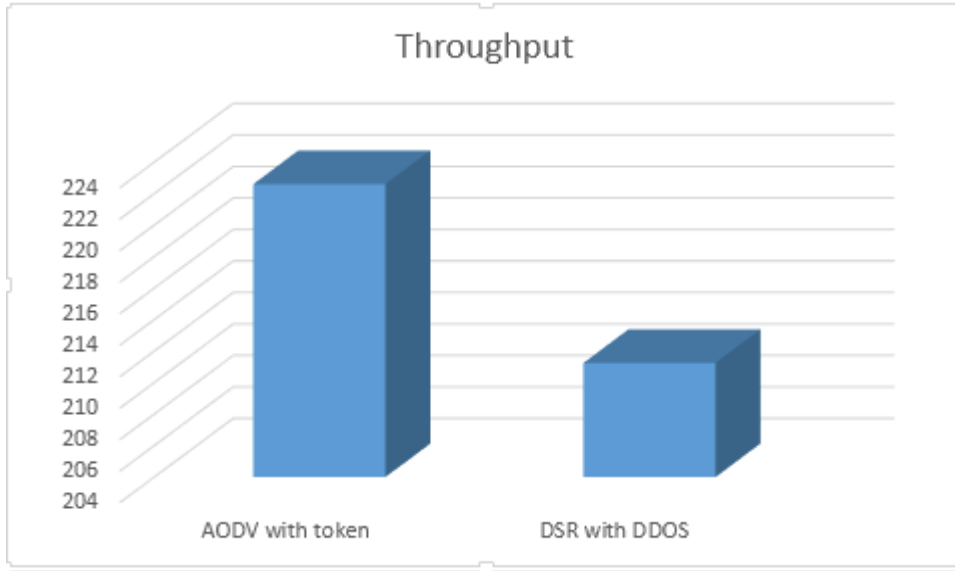
Graph 3 Average throughput comparison

The above three graph shows the simulation results through the NS2 xgraphs.

Discussion for results

Throughput

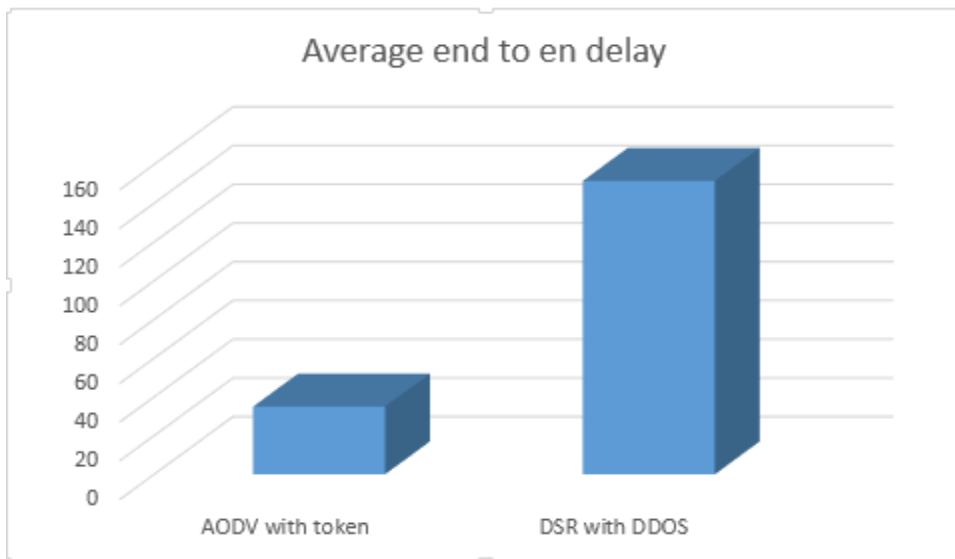
The regular rate of successful message conveyance over a communication station is called throughput. This data may be transported over a physical or logical link, or goes through a definite network node. The throughput is generally calculated in bits per second and occasionally in data packets per second. The system throughput is the totality of the data rates that are delivered to all terminals in a network. Thus in the proposed scheme in case of AODV the throughput is higher as that of DSR in case of DDOS attack. As we can see in the given bar graph that the throughput value in DSR is 211.25 kbps while in case of AODV it is 222.61 kbps. Thus throughput is improved by 11.36 kbps in the situation of DDOS attack by using token based identity in AODV. The bar graph displaying the outputs is given below:-



Graph 4 Throughput comparison

Average end to end delay

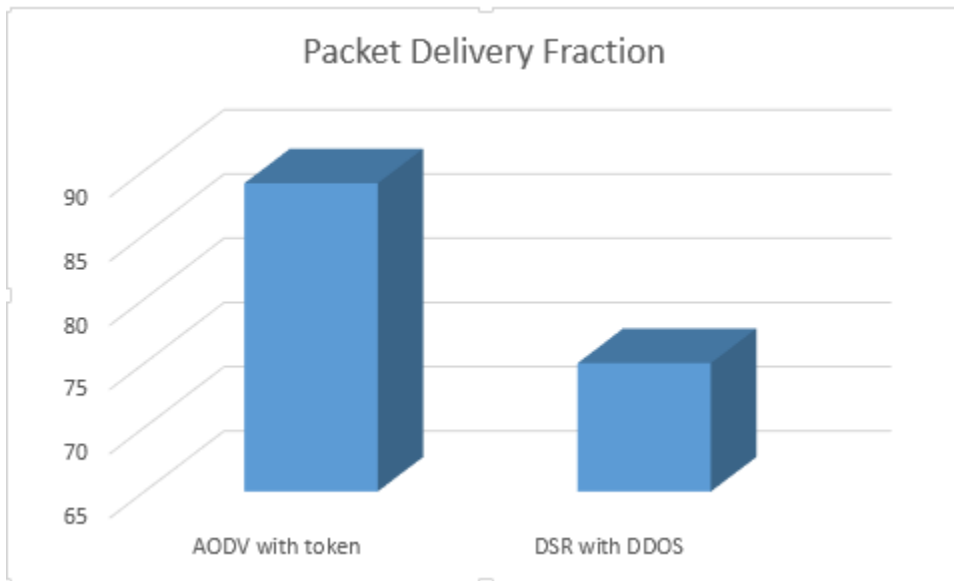
Average end to end delay includes all probable delays produced by buffering through route discovery, time spend in queue, retransmission delays, and propagation and transmission times. The average end-to-end delay is very less in the case of proposed scheme while it is very high when there is DDOS attack in DSR. Thus the end to end delay is minimized by 116.6 ms in the proposed technique. The related values are shown in the graph below:-



Graph 5 Average end to end delay comparison

Packet delivery fraction

The ratio of the packets sent to the destinations successfully generated by the CBR sources is called packet delivery fraction. The packet delivery fraction in case of AODV is higher as that of DSR. There is difference of 14% in packet delivery fraction. The comparison is shown below.



Graph 6 Packet delivery fraction comparison

Mobility and routing of nodes in network animator

Here in this section we will show the graphical representation of nodes in network animator. The Establishment of 50 mobile nodes as it is shown in the NAM console which is a built in program in NS-2-allinone at the end of the simulation process. Here is the Scenario of Mobility and routing of nodes given. The operations occurring here are as follow:-

- Packet Forwarding
- Packet Dropping
- Movement of Nodes.
- DDOS attack

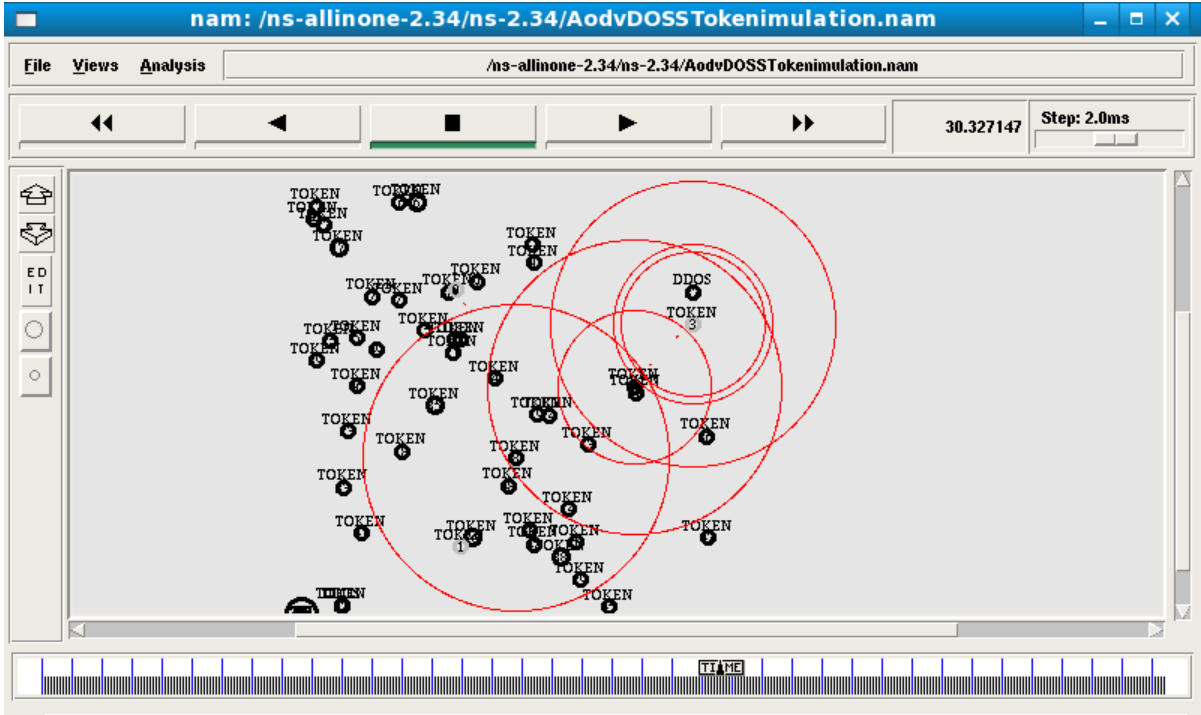


Figure 13 Presentation of proposed technique in network animator

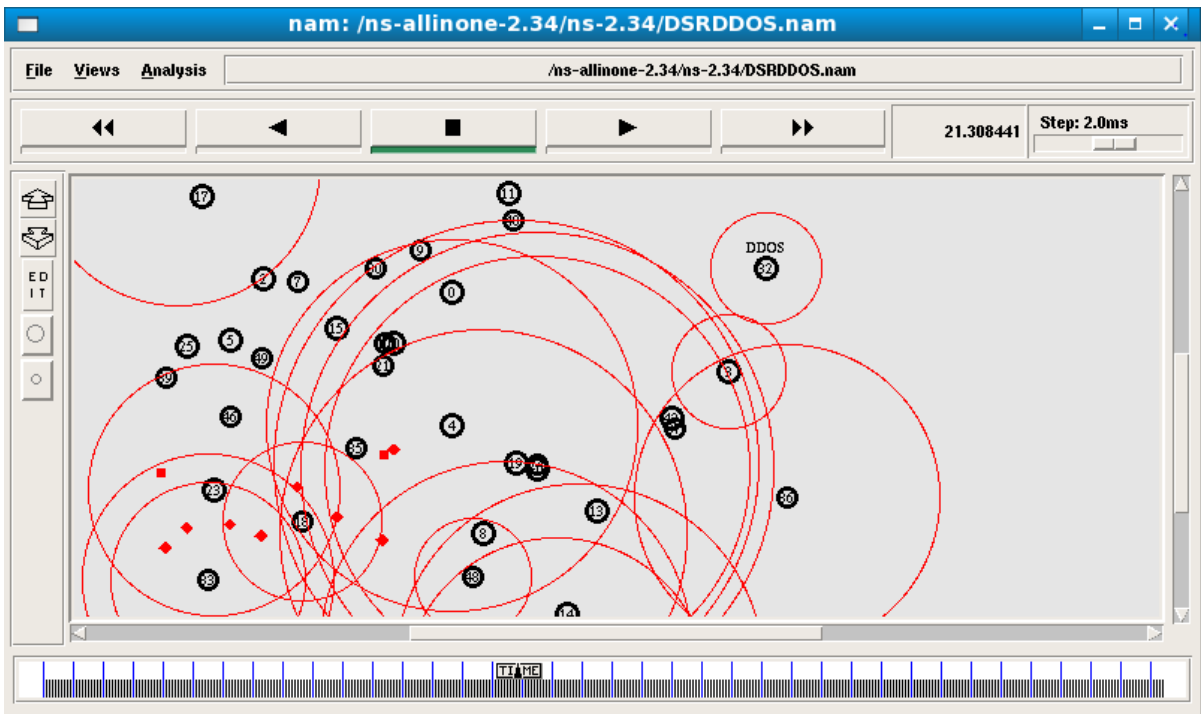


Figure 14 Presentation of DSR under DDOS attack in network animator

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

Attaining a secure routing protocol and mitigation of attacks in it is a significant task that is being challenged by the distinctive features of an ad hoc wireless network. Traditional routing protocols flop to provide security, and rely on an implicit trust between communicating nodes. We scrutinize and classify major routing attacks and main routing protocols and present a comprehensive survey on the mechanisms and explanations considered to overthrow such attacks. The recent security mechanisms, each overthrows one or few routing attacks. Planning routing protocols strong to multiple attacks rests a puzzling task. In this current thesis work we have described the token based scheme to improve the AODV protocol and mitigate the effect of DDOS on the performance of AODV protocol and it has provided better results.

5.2 Future Scope

In future this technique can be implemented with other protocols also as DSDV, DSR and TORA also with multicast routing protocols AS the On-demand Multicast Routing Protocol (ODMRP). This technique can also be used to mitigate the other attacks is various routing protocols or in AODV.

CHAPTER 6

REFERENCES

- [1] DSDV Available: <http://research.ijcaonline.org/rtmc/number15/rtmc1093.pdf>.
- [2] DSR: http://paper.ijcsns.org/07_book/200907/20090737.pdf.
- [3] N. s. R. s. Prajeet sharma, "A secure intrusion detection system against DDOS attack in wireless mobile ad hoc networks," *International journal of computer applications*, vol. 41, pp. 6-21, 2012.
- [4] I. k. M.Mohanapriya, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," *ELSEVIER*, vol. 40, pp. 530-538, 2014.
- [5] A. s. Kavita pandey, "A comprehensive performance analysis of proactive, reactive and hybrid MANETs routing protocols," *IJCSI*, vol. 8, no. 6, pp. 432-441, NOVEMBER 2011.
- [6] N. s. Mohit kumar, "Securing AODV against wormhole attack using token based approach," *IJAIS*, vol. 4, pp. 24-27, december2012.
- [7] N. k. Geetika, "Detection and prevention algorithms of DDOS attack in MANET," *IJARCSSE*, vol. 3, no. 8, pp. 61-65, August 2013.
- [8] Z. chao-yang, "DOS attack analysis and study of new measure to prevent," in *international conference on intelligence science and information engineering*, China, 2011.
- [9] P. m. Anit kumar, "A comparative study of AODV& DSR routing protocols in mobile ad hoc networks," *IJARCSSE*, vol. 3, no. 5, pp. 658-663, 2013.
- [10] R. m. B.B.Gupta, "Distributed denial of service prevention techniques," *Internationak journal of computer and electrical engineering*, vol. 2, pp. 268-276, 2010.
- [11] R. p. Nisarg gandhewar, "Performance evaluation of AODV protocol in MANET using NS2 simulator," in *International journal of computer applications*, 2011.
- [12] R. d. d. Pankaj rohal, "Study and analysis of throughput, delay and packet delivery fraction ratio in MANET for topology based routing protocols (AODV, DSR, DSDV)," *IJARET*, vol. 1, no. 11, march2013.
- [13] C. S.H manjula, "performance of AODV protocol using group and entity mobility models in wireless sensor networks," in *IMECS*, Hong kong, 2008.
- [14] c. d. Chanchal aghi, "Black hole attack in AODV routing protocols:A survey," *IJARCSSE*, vol. 3, no. 4, April2013.

[15] otcl

Available:http://s3.amazonaws.com/zanran_storage/web.unbc.ca/ContentPages/699091205.pdf.

[16] NS2 Available: <http://www.monarch.cs.rice.edu/ftp/monarch/papers/dmaltzthesis..>

[17] NS2 Available: http://irphouse.com/ijwnc/jwncev4n1_1.pdf.

[18] NS2 Available: <http://www.iracst.org/ijcsits/papers/vol2no42012/4vol2no4.pdf>.

[19] Available: http://rimtengg.com/iscet/proceedings/pdfs/adv_nw_tech/76.pdf.

CHAPTER 7

APPENDIX

7.1 List of abbreviations

AODV-Ad hoc on-demand distance vector.

DSR- Dynamic source routing.

DSDV- Destination sequenced distance vector.

TORA- Temporarily ordered routing algorithm.

DOS-Denial of service.

DDOS-Distributed denial of service.

ODMRP- On demand multicast routing protocol.

MANET-Mobile ad hoc network.

RREQ-Route request.

RREP-Route reply.

RERR-Route error.

WRP-Wireless routing protocol.