SECURE ANT NET BASED ROUTING IN MOBILE AD HOC NETWORKS

A Dissertation Report

Submitted By

Mandeep Singh

To

Department of Computer Science and Engineering

In the partial fulfillment of the requirement for the

for the Award of the degree of

Master of Technology in

Computer Science and Engineering

Under the guidance of

Mr.Amritpal Singh

Asst. Professor, LPU.

(May 2015)

CERTIFICATE

This is to certify that Mandeep Singh has completed M.Tech dissertation titled Secure ant net based routing in mobile ad hoc networks 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 has ever been submitted for any other degree or diploma.

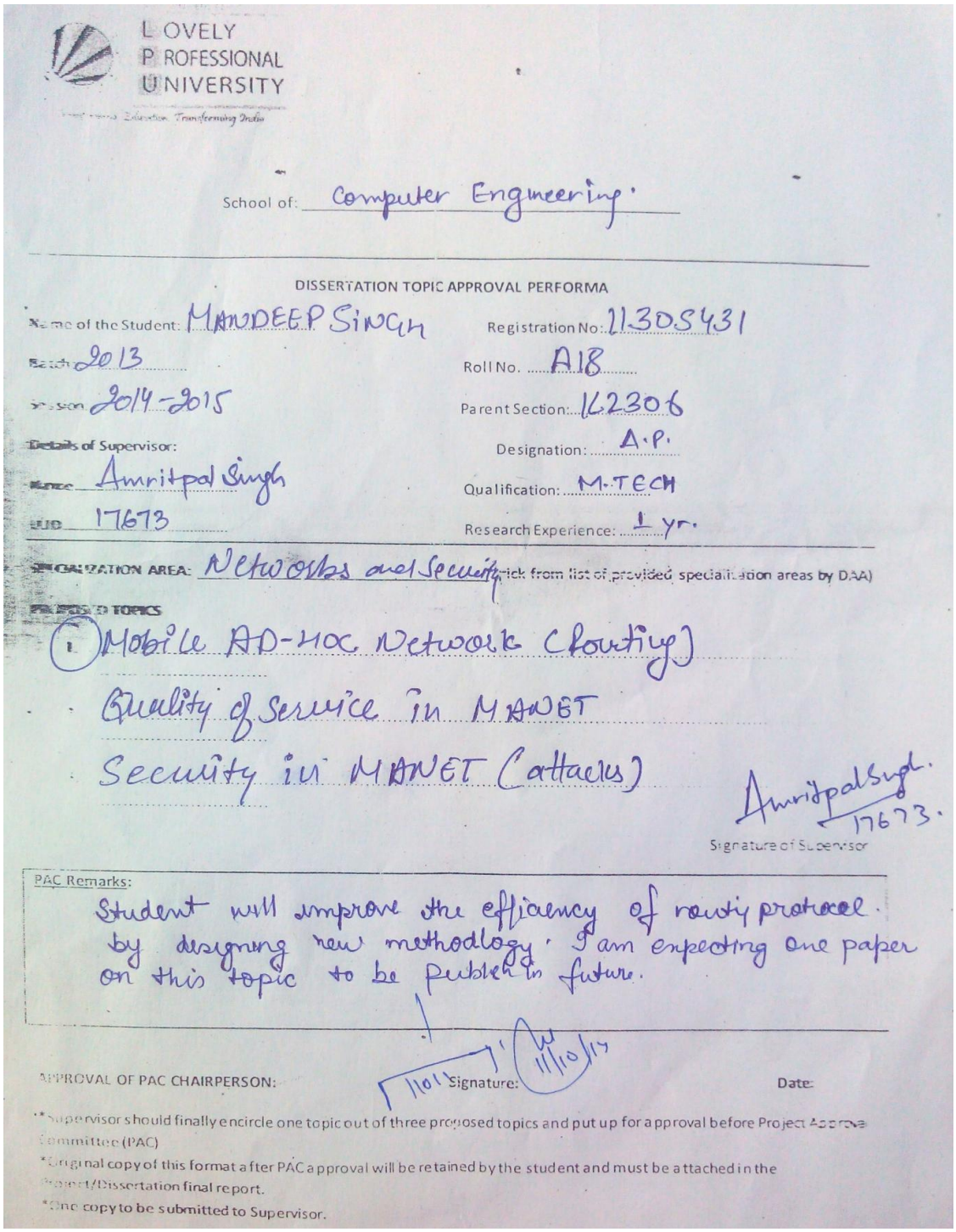
The dissertation is fit for the submission and the fulfillment of the conditions for the award of M.Tech Computer Science & Engg.

Date: _____ Signature of Advisor

Name

UID:

PAC APPROVAL



LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

School of: Computer Engineering.

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: MANDEEP SINGH Registration No: 11305431

Batch: 2013 Roll No. A18

Session: 2014-2015 Parent Section: K2306

Details of Supervisor:

Name: Amritpal Singh Designation: A.P.

UID: 17673 Qualification: M.TECH

Research Experience: 1 yr.

SPECIALIZATION AREA: Networks and Security (Tick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Mobile AD-HOC Network (Routing)
2. Quality of Service in MANET
3. Security in MANET (attacks)

Amritpal Singh. 17673.

Signature of Supervisor

PAC Remarks:

Student will improve the efficiency of routing protocol. by designing new methodology. I am expecting one paper on this topic to be publish in future.

APPROVAL OF PAC CHAIRPERSON: Signature: 11/10/14 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

Mobile Ad hoc network contains wireless nodes those can communicate with the distant nodes by forwarding the packets over the network. Routing over MANETs suffers from various issues such as limited resources and dynamic network environment. Lot of research has been done to improve the performance of the MANETs and researchers introduced the concept of ant net algorithm/swarm intelligence based routing algorithms over MANETs, in order to enhance the network performance but due to unavailability of the mentoring authority in the network, any node can transmit and receive the data over network that's why ant net based routing over the ad hoc network is also unsecure and there are lot of security threats exists for ant net based routing because if a security threat exists for MANET's routing protocol that can also affect the ant net routing algorithm and can degrade the network performance. So there is a need to explore the security threats against the ant net based routing over MANETs. In this research work, we will explore the blackhole attack on ant based trusted AODV.

ACKNOWLEDGEMENT

I would like to place on record my deep sense of gratitude of Assistant Professor Amritpal Singh, School of Computer Science, Lovely Professional University, Phagwara, India for his generous guidance, help and useful suggestions.

I wish to extend my thanks to Head of Department Mr. Dalwinder Singh, School of Computer Science for his constructive suggestions to improve the quality of this research work.

And last but not the least, I find no words to acknowledge the financial assistance & moral support rendered by my parents in making my efforts, a success. All this has become reality because of their blessings and above all, by the grace of Almighty God.

Mandeep Singh

DECLARATION

I hereby declare that the dissertation entitled, Secure ant net based routing in mobile ad hoc networks submitted for the M.Tech 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: 4 May, 2015

Investigator :

Mandeep Singh

Regn. No:11305431

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

Chapter 1

INTRODUCTION

1.1 Ad Hoc Network

A mobile ad hoc network (MANET) is a self-configuring network that does not have any central authority. Nodes act as transceiver which can send and receive the packets at same time. MANET supports the military applications, rescue operations, commercial applications. Limited capabilities of the MANETs can be extended by introducing the feature of Ant net based algorithms; called ad hoc ant net based MANETs. Routing protocols for this type of network contains the features of both protocols and with the features of ant net algorithms, ad hoc protocols can perform well.[3]

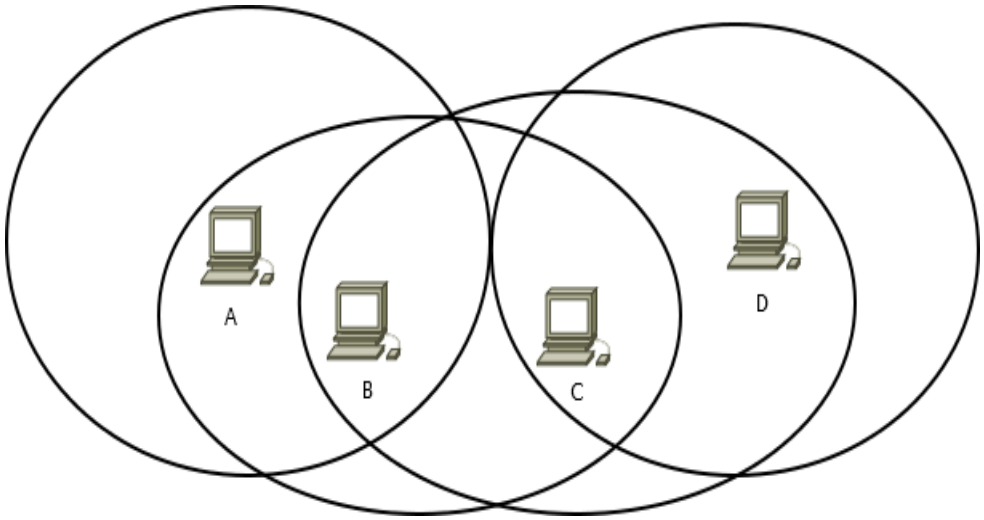


Figure 1.1 Mobile Ad hoc Network

1.2 MANET Algorithms behaviour and characteristics

Following are the operations and events for MANETs and its routing algorithm:

1.2.1 Topology Formation

It is formed by the nodes as they join the network and has dynamic nature, depends upon the node position and their mobility patterns. Topology Formation includes the Neighbor Discovery and packet forwarding algorithms.

- **Neighbour Discovery:** It depends upon the nodes and their neighborhood. When a node wants to communicates with the other, first of all that node discovers a set of nodes within the range and each node maintains this topological information, called routing information in a routing table. Nodes save the topological changes in this table in order to maintain the fresh routes.

- **Packet Forwarding Mechanisms:** MANETs use a packet forwarding mechanism which includes the flow of control packet and data packets.[5] Control packets include the routing information and data packets contain the actual data to be forwarded.

1.2.2 Topology Control

Topology control algorithms are used to maintain the topological structure of the network. Network topology suffers from various factors like mobility, routing algorithm behavior, energy efficiency etc. These are classified as centralized, localized or distributed.

1.2.3. Routing

Routing is responsible for routing over the network under the different constraints. Routing algorithm discovers the routes and also performs the route maintenance and deals with link failures. It also deals with other constraints like limited bandwidth, energy consumption, low power wireless links, error prone wireless channel and packet collision at MAC layer. Routing in these types of networks is threatening because of no centralized node to make decisions about routing. There are many protocols of routing for MANETs.

In pro-active protocols, each node needs to maintain information about topology in routing tables by periodically transferring information about routing. When a node needs a path to its destination, it plays path discovery algorithm on information it has. Examples for it are DSDV and WRP. [7]

Reactive protocol does not have information about topology. They get the route when required. So they do not transfer information periodically. AODV, DSR and TORA are this type of protocols.[7][8]

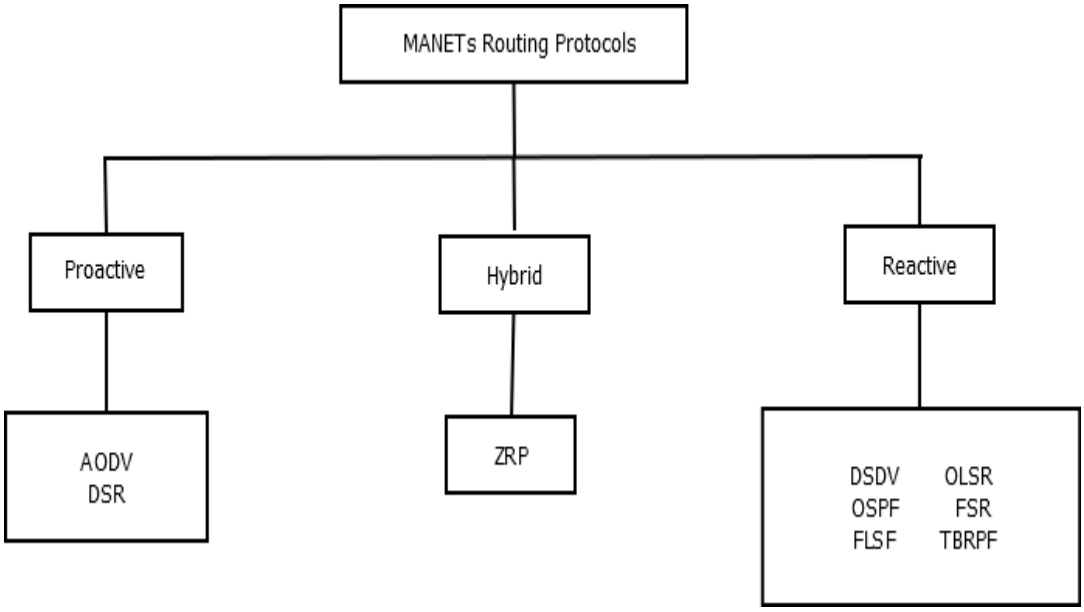


Figure 1-2: MANET Routing Protocols

Hybrid protocols are combination of both reactive and proactive protocols.

1.3 MANETs Application

MANET has spectacular properties that can change the world with its advancements. Many of the fields are still under survey. The important area in MANET is the vehicle to vehicle communication.[10 The communication within the MANET occurs as one vehicle tries to communicate to the other vehicle, thus keeping in mind the safe distance between the two vehicles. The major factor here is to avoid collision between the vehicles, so for this they are given warnings. Battlefield and war games use MANET for their functioning. Major area where MANET helps people is emergency time such as disaster recovery and relief activities where the traditional wired network doesn't exist. Other application areas are entertainment, commercials and education where MANET helps people to connect.

1.4 Ad hoc Network Security

There are lot of security threats exists for MANETs. Security goals for MANETs include the followings:

- **Authentication:** It is used to avoid the impersonation by properly identifying the nodes. It is difficult in ad hoc networks because of non-centralization property. As there is no node having overall control, so it is difficult to authenticate every node in

network. Digital signature and hash functions with cryptography are used to provide authentication.

- **Confidentiality:** It is to send information in such a form that node without authorization cannot read it. In case of MANET, every node in range can easily get the data. So it is essential to secure it and make it unreadable. Directional antennas can be used to provide confidentiality. Another way is data encryption. With confidentiality techniques, only actual receivers can access the information.

- **Integrity:** Integrity is provided to avoid any alternation in data. Hash functions and encryption are used for integrity. In case of network security, it is inherently given along with authentication.

- **Availability:** Availability is about providing services to parties who requires ti when needed. Redundancy is generally used to provide availability. Other means like protecting physically can also be used.

- **Non-repudiation:** Non-repudiation is about to avoid denying about data sent or received. Signature in message can used for this purpose. When one node puts its signature in the message with its own key, then other will authenticate it with public key. Now, sender node cannot deny about sending message.

- **Access Control:** It is about who can access services and can access which services. It is to control unauthorized usage of network resources. This property is important in network as well as individual personal computers. [3][4]

1.5 Security weaknesses in MANET

MANET is very adjusting in the nature as there is no central node to watch the incoming and outgoing nodes. This leads to the following problems:

- **Unsecure Boundaries:** As there are no specific boundaries the system faces lots of problems. In this the nodes are free to roam anywhere, they have full freedom to join and leave whenever the nodes want. When node is within radio range only then it can communicate with others. Due to the absence of boundaries attacks such as active and passive, information leakage, denial of service or replying false messages can harm system. Also there are various link attacks, first the link is invaded and then destroyed. No protection against attacks, such as firewalls or access controls is

present. Identity spoofing, tempering of data, and information leakage are the results of such attacks.

- **Compromised Nodes:** Some of the attacks act as a gateway to the system. They are performed in order to harm the system by entering it. The mobile nodes are autonomous in MANET, due to which it becomes very difficult to prevent the system from such thefts. Due to the mobility factor it becomes easy for the nodes to move anywhere, which makes it more difficult to track malicious activities. Threats from compromised nodes are dangerous than attacking threats.

- **Non-centralized Management:** Ad hoc network is self configuring network in which the nodes can move freely from one place to another without any centralized authority. Every node works as a router and can receive as well as transfer data. Because of no central authority, there are more attacks. Due to this lack of centralized system and dynamic traffic, monitoring of large ad-hoc is difficult.

- **Scalability Problem:** In earlier periods the traditional networks were based on the basis of wires. There aren't many changes that happen once the traditional system is designed. Scalability of the network is designed as soon as the system is mapped. But in MANET as the nodes are mobile, scalability changes from time to time. It almost seems impossible to find the total count of nodes in the near future. The nodes can travel freely that makes the system very flexible. Due to these feature, services and protocols provided by it have a adaptability to variations.[1][5]

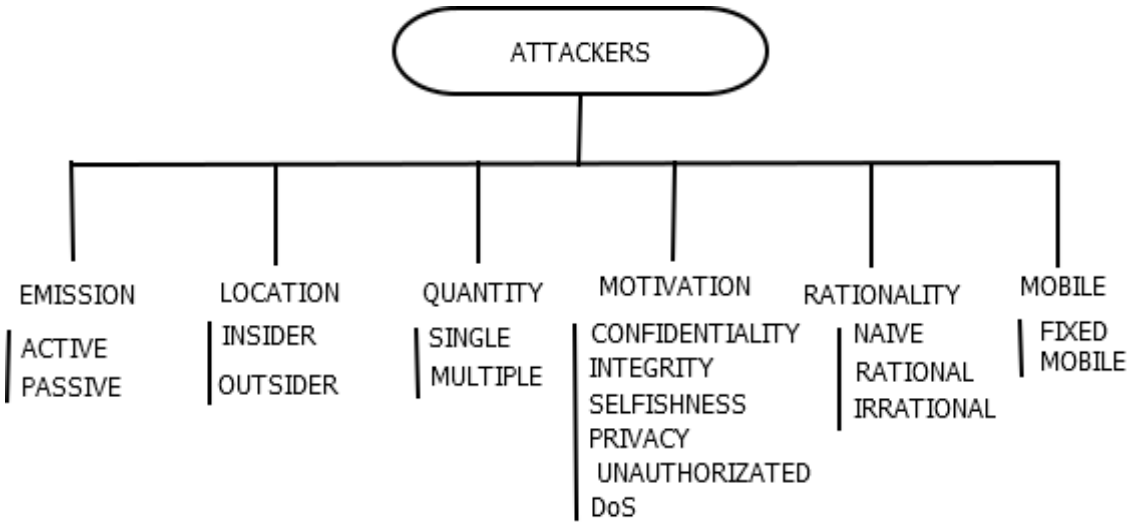


Figure 1-3: Types of attackers

1.6 Types of Attacks

The attacks are classified on the basis of their sources that are external and internal and on the behavior of their attack that is active and passive.

1.6.1 Internal and External Attacks

External attacks are the ones that need network access from the outside, they do this by transferring dummy packets to disrupt network. These attacks are similar to the others. Such attacks should be avoided by using security strategies for example firewall to deny unauthorized person.

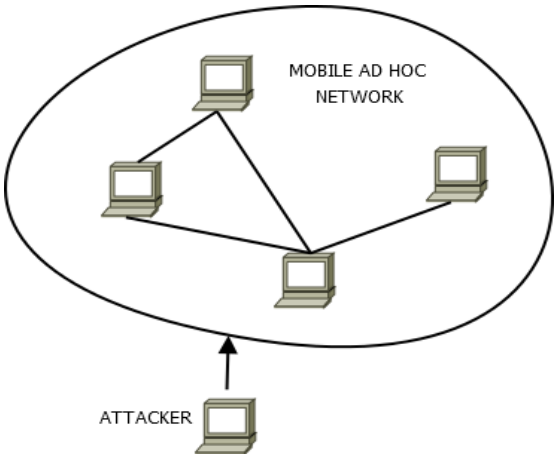


Figure 1-4: External Attackers

In case of internal attack, the outsider needs to access the network normally and wants participation in its activities. The attacker gains access with an existing node or a newly created node either by current node comprimisation in the network or by impersonating and arouse malicious activities.

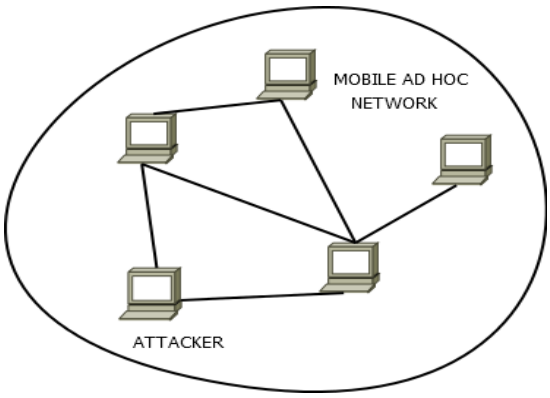


Figure 1-5: Internal Attacker

1.6.2 Active and Passive Attacks

In active attacks the hacker does analysis, watches network's performance, tries to get information and tamper it. Active attack can be external or internal. Active attack means to decay the performance; in this case it acts as the internal node. As the node becomes an active part of the system it becomes easier for it to destroy it. When the attacker gains power it can fabricate, alter and replay messages. Passive attack does not interrupt the normal network. In these kinds of attacks the attacker observes the communication in order to gain the valuable information. They want all the information related to the network, like how it works? Where does the data go and come from? Etc. This technique is quite helpful for the attacker as before it does harm the system it has a complete analysis of the communication of the network or its complete structure. [1][5]

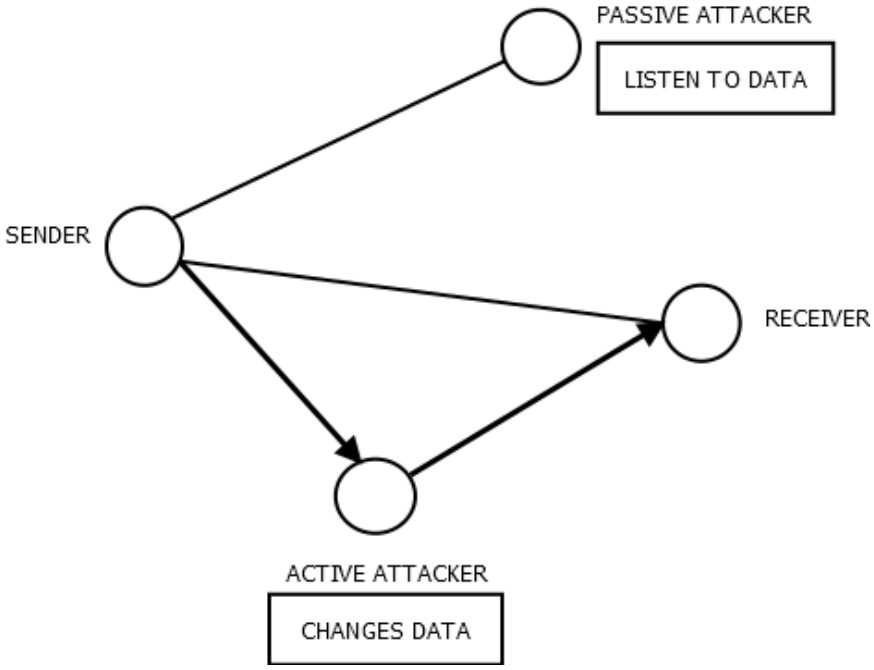


Figure 1-6: Active Attacker and Passive Attacker

1.7 Blackhole attack

In blackhole attack, in order to make itself look like having shortest path, routing protocol is used by malicious node. This attacker node advertises the availability of its route to destination without even checking its routing table. So it can reply to any route request and intercept the packets in the network. In flooding based protocols, attacker node will send reply to source node before the reception of any other nodes' reply, which lead to creation of a malicious route. Now, after the establishment of route, it depends on attacker node whether to forward all the packets to unknown or non-existed address or to drop it.

There is variation in how attacker node gets along in packet routes. Following figure shows arousal of blackhole attack. Here, node P is source node and node T is destination node. Node Q is malicious node. When P starts route discovery process, then Q advertises itself as if it active route to T. It will give response to P before anyone else. So now, P will start transferring packets to Q. Hence attack happened.

1.7.1 Black-hole attack in AODV

Internal and External are two types of attacks in Ad-hoc On-Demand Distance Vector Routing Protocol.

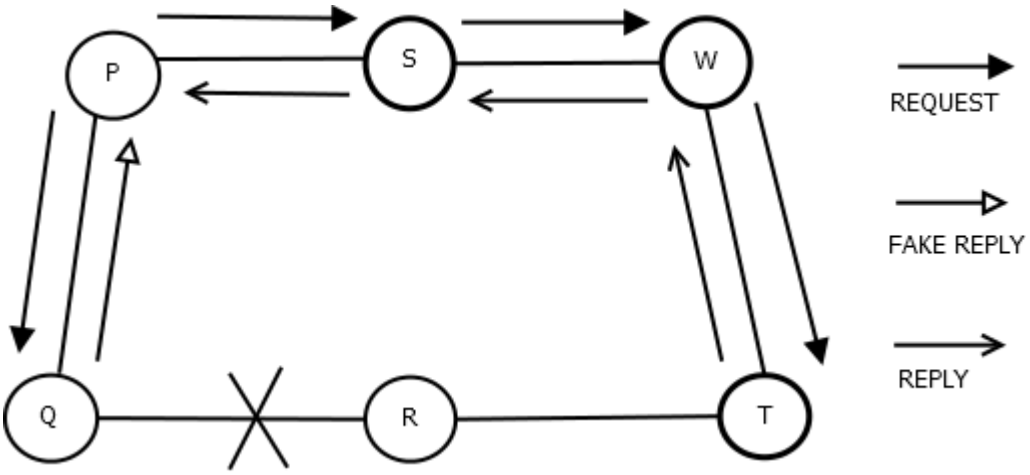


Figure 1-7: Blackhole Attack

1.7.1.1 Internal Blackhole attack

In this case, there is an internal malicious node that gets along between paths of particular destination and source. Whenever it gets a opportunity, it makes it an active route member. Now, conduction of attack is easily possible. These attacks are more difficult to prevent because it is not easy to detect these malicious nodes as they are internal.

1.7.1.2 External Blackhole attack

This attack physically stays out of network and causes congestion or do access denial to network or may be cause entire network disruption. This type can become internal type

once it controls malicious node which is internal and utilize it for attacking other nodes. It is shown in following steps:

1. Active route is detected by malicious route and destination address is noted.
2. Now it sends RREP to source. This RREP has destination field pointing to an unknown address. Sequence number is given a high value and hop count a lowest value.
3. This RREP can be sent to source node directly or to nearest node which is part of active route.
4. Then that nearest node will traverse that RREP back to source node via inverse route.
5. Source node will update its routing table as it has new information.
6. Now, malicious node is also selected in new route for transferring data.
7. Now, malicious node will receive all data and can drop it.

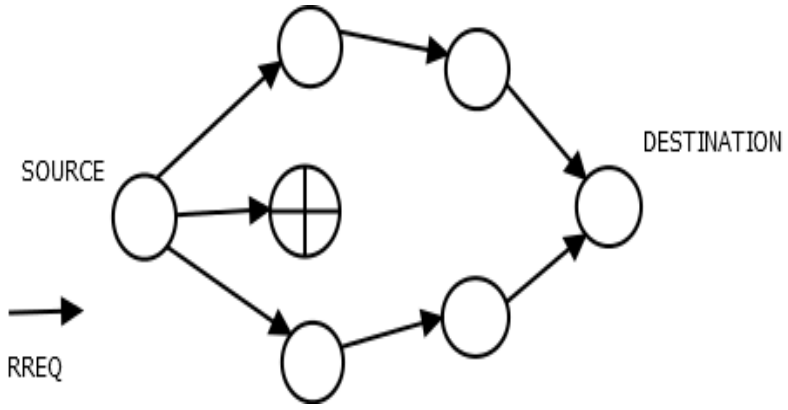


Figure 1-8: RREQ Flooding

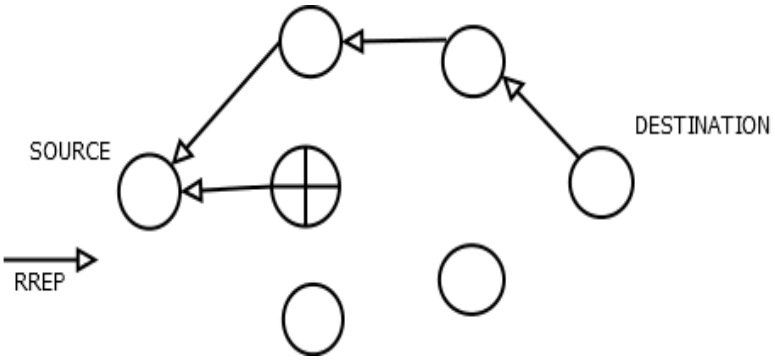


Figure 1-9: RREP Replying

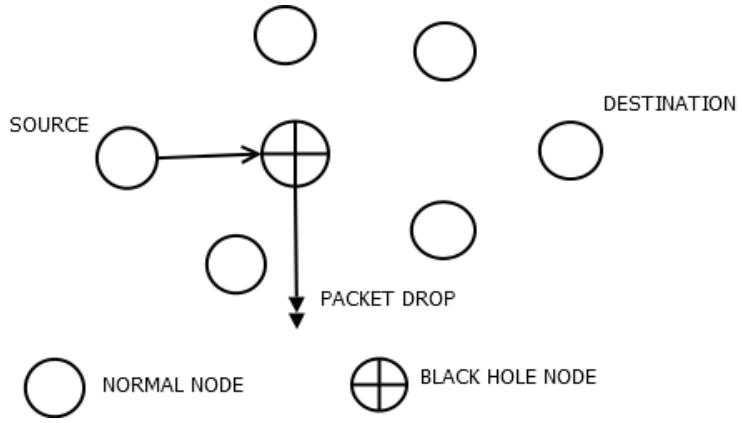


Figure 1-10: Blackhole Attack

1.7.2 Other types of attacks.

1.7.2.1 Rushing attack

This attack works well in case of on demand routing protocols. When attacker node receives a request for route from source. It broadcasts quickly through entire network before original request reaches other nodes. In following figure, node A represents the attacking node. Source node is S and destination node is D. Node A floods quickly the RREQ it received before any other node receive original RREQ. Now, other nodes simply discard the original RREQ and S does not discover a route without attacker node.

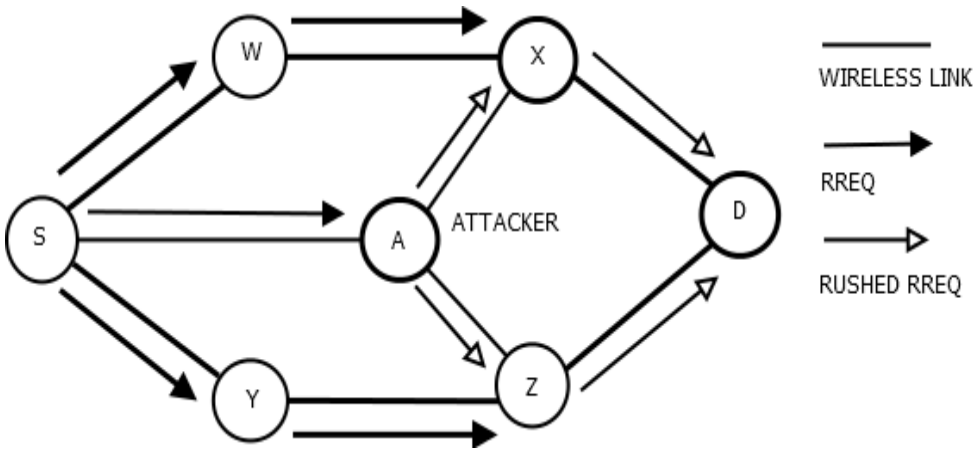


Figure 1-11: Rushing Attack

1.7.2.2 Wormhole attack

Wormhole attack involves two or more malicious nodes. In this attack, one bad node receives packet at one place and it further tunnels that packet to other bad node. This tunnel between two nodes is called wormhole. Wormholes are used to let these bad nodes be more seductive which leads to more data through these nodes. In following figure Y and X are bad nodes forming tunnel.

The neighbouring nodes of source S , 1 and 2, send the RREQ to their neighbours , X and 5. Now X, on receiving RREQ, immediately sends it to Y, which forwards it to 8 and further D. This route is established quickly due to high speed. Later, when other RREQ comes to D it ignores it.

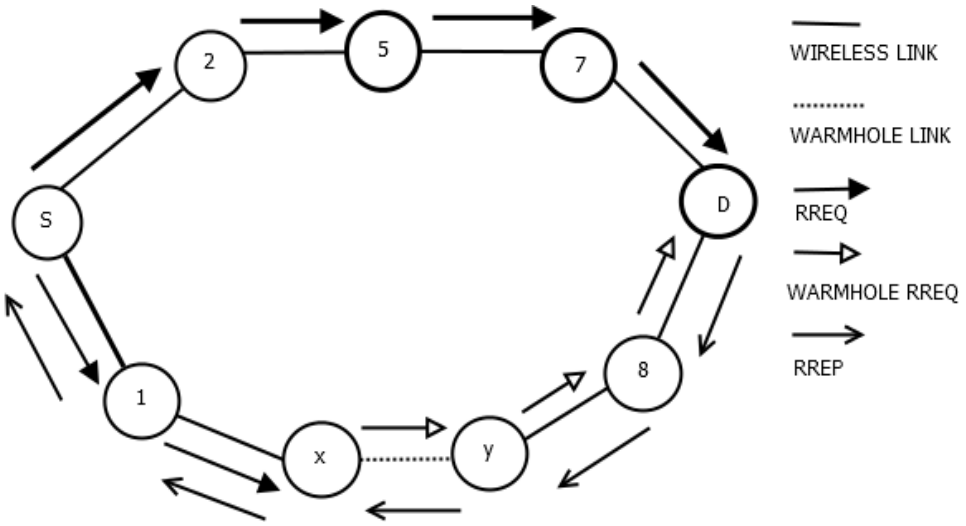


Figure 1-12: Wormhole Attack

1.7.2.3 Sinkhole attack

In sinkhole attack, a malicious node shows wrong or faulty routing information. It uses information like hop count or sequence number , which makes it appear as the best path to destination and it receives all the traffic. Once it gets traffic, it can modify the data or drop it.

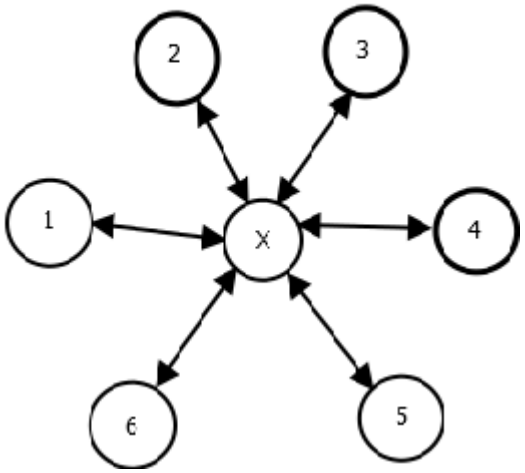


Figure 1-13: Sinkhole Attack

1.7.2.4 Replay attacks

Because of mobile nodes, topology changes frequently in MANETs. In replay attack, a malicious node saves control messages and keeps sending them again and again. This leads to other nodes having stale entries. It, obviously, can be used later to disrupt the routing in MANETs.

1.7.2.5 Link withholding & link spoofing attacks

In first one, link withholding attack, information about the links to specific nodes is not broadcasted by attacker node. It leads to loss of links between many nodes. In link spoofing attacks, fake information about routing is advertised. It causes in wrong route establishment and attacker can manipulate the traffic.

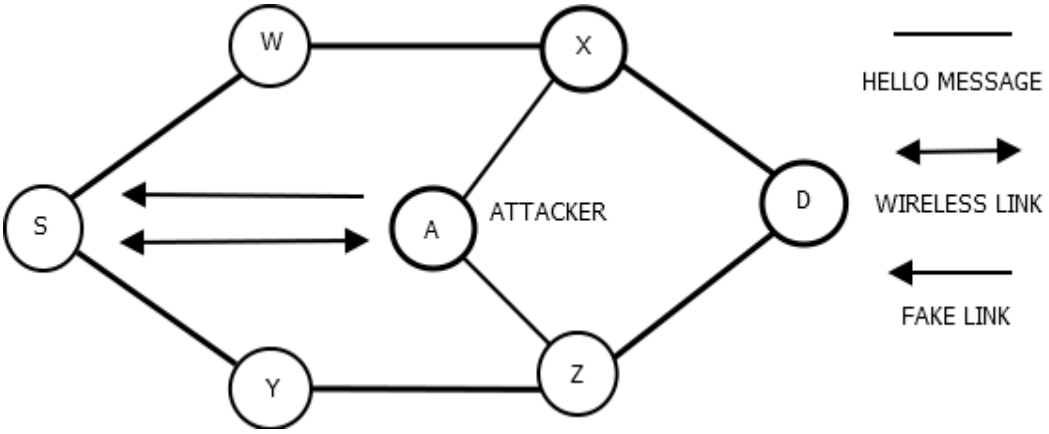


Figure 1-14: Link Spoofing

1.7.2.6 Resource consumption attack

In this case, malicious node tries to consume all battery or other resources by very high route discovery or by sending packets, which are not necessary, to the target. It can also be called “sleep deprivation attack”.

1.7.2.7 Sybil attack

Fake identities are generated for a number of node which are additional. So, there are a large number of malicious nodes now. These additional identities are called Sybil nodes. This node can also steal a legitimate node’s identity. Adverse effects due to this are:

- It makes difficult to find out a misbehaving one.
- Due to additional nodes, it also leads to unfair allocation of resources.
- In some applications, nodes can be used in voting. Due to these duplications, result of voting can be very different.
- Due to duplications, nodes can appear at many places. It affects adversely on routing operations.

1.8 Ad-Hoc on Demand Distance Vector Protocol (AODV)

It is reactive type protocol. Suppose a node does not have any route to another one, then AODV gives information about topology of network to the nodes. Control messages are used to get path to another node. Its types are as following:

Route Request Message (RREQ)

When a node needs to exchange some data with another one, then it sends RREQ , which is flooded in network. TTL value is included in each message, which tells about how many hops the message needs to be transferred.

Route Reply Message (RREP)

During routing, when a node is the destination node or there is a node which has route to destination node creates RREP. It goes back to source.

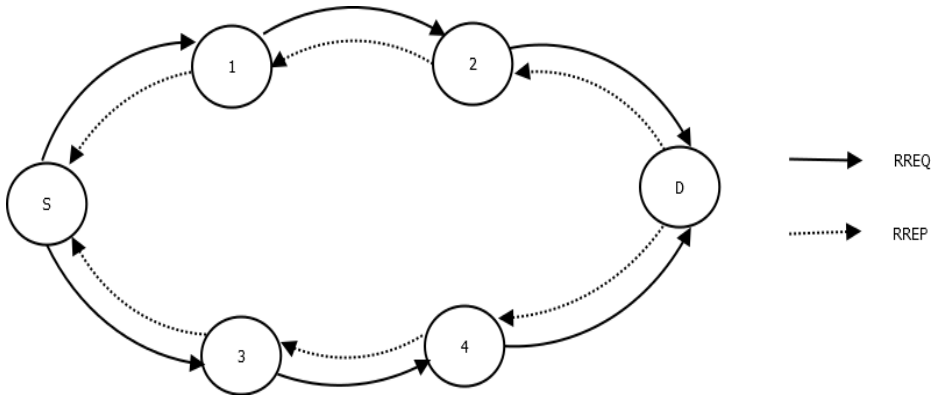


Figure 1-15: RREQ and RREP Messages

Route Error Message (RERR)

When a route is active, all nodes continuously check out the status of link to nodes in neighbor. If there is any problem or breakage in link, then RERR is created so that other nodes can be notified about link breakage.

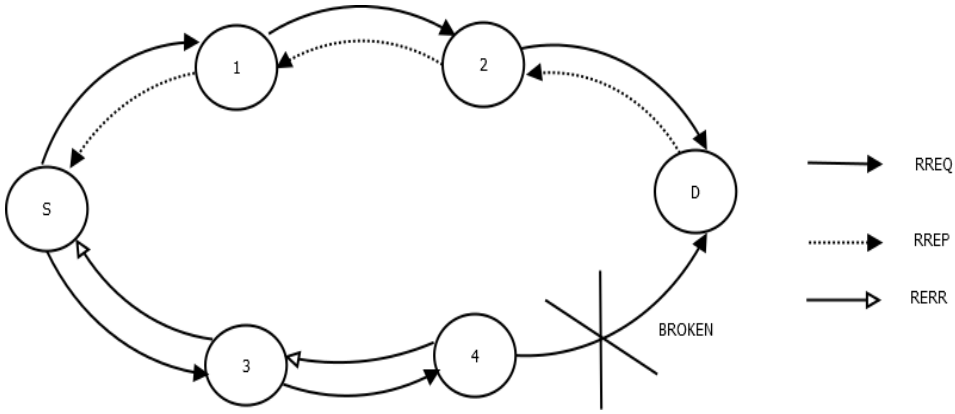


Figure 1-16: RERR Message

Route Discovery Mechanism in AODV

If there is need to start communication, then source node will flood RREQ to its neighbors. Then these neighbors will further broadcast these messages to their neighbours. This course continuous until it reaches destination node or other node having route to destination node. Then RREP is formed by this node and sent back to source node.[12] Once RREP is received by originator , path is developed from source to destination. Now both nodes exchange information with each other. If there is any link breakage in the path, then RERR is sent back to source and again whole course for finding path is initiated.[6][8][9]

1.9 Ant Colony Optimization

Ant colony optimization comes under the category of swarm intelligence technique. ACO utilizes the concept of nature of ants to find path from their nest to their food.

An Ant can find food using shortest route from the nest to its meal. It moves on basis of a material, known as pheromone left on the ground. After reaching to a point having two or more branches going out, next path selection depends upon the value of pheromone. An ant selects a path and refresh that branch's pheromone value thus increase the chances of current path.

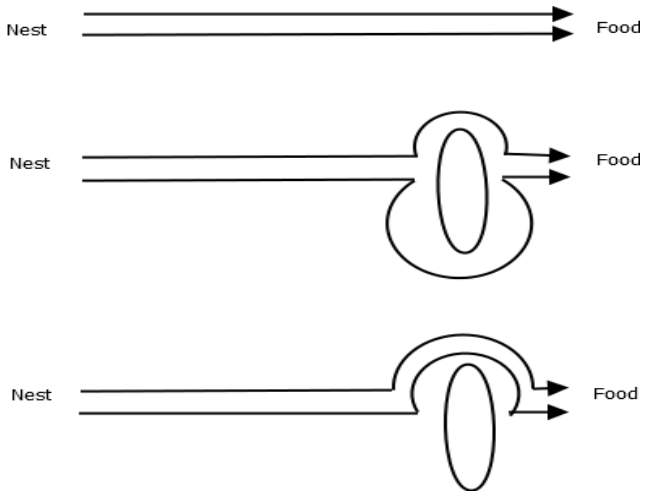


Figure 1-17: Ant Colony Optimization

Pheromone on the shortest route to the meal increases more rapidly than that on other ones but if it is not used for some time then it decreases over time and at that time that path becomes outdated. Individual ant cannot find out the shortest path without ant colony. Ant colony is self-configured and has a very dynamic nature. These characteristics of ant colony are used to improve the capabilities of ad hoc networks. [9]. Given below shows the various ACO algorithms developed for MANETs.

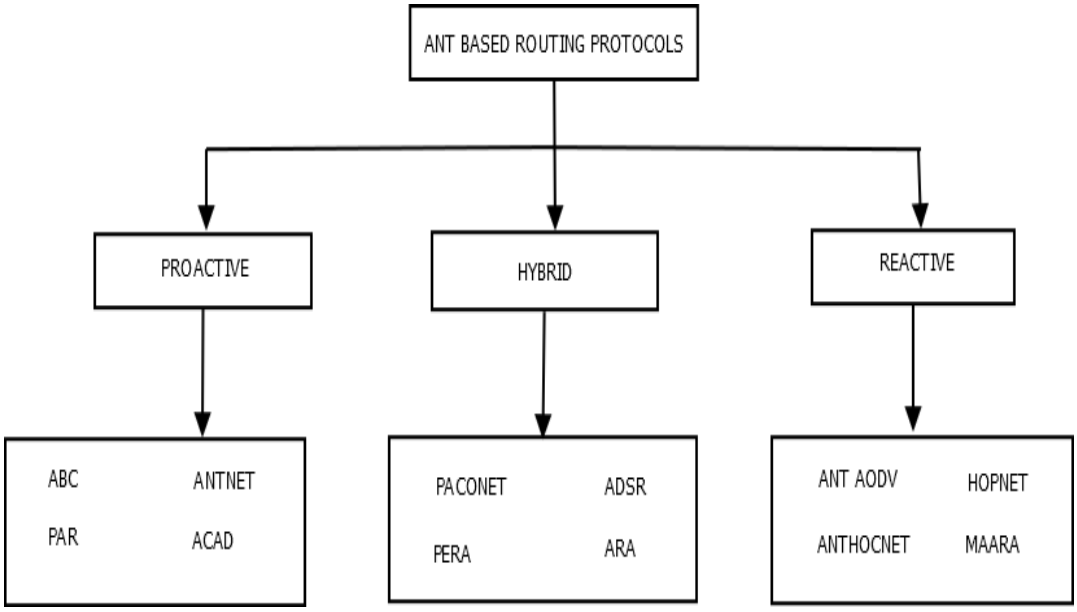


Figure 1-18: Ant based routing protocol

1.10 Various ACO routing algorithms

MANETs support various types of routing protocols and ACO algorithms are designed as per categories of these protocols.

1.10.1. Table driven/proactive ant based routing protocols

1.10.1.1 Ant based control (ABC):

This is proactive type of protocol. This is applicable for mobile ad hoc networks because of non-centralization, good balancing of loads over paths and adjustable to changing topology. In ABC, every source sends exploratory ants for updates. These ants travel to different destinations. Then, every node has data with rows containing neighbors and columns containing destinations possible. Each cell gives pheromone value for a selective neighbor and selective destination. Ants take the link having highest pheromone value for a selective or required destination.

1.10.1.2 Ant based network

Proactive protocol for routing using ant technique is called Ant net in which communication is done using mobile agents and routing information is dynamically updated that contains the data about time, path length and pheromone. On the basis of

pheromone's value, shortest path is selected. [4][16] Same path is used by forward and backward ants.

1.10.1.3 Probabilistic ant routing (PAR)

This algorithm adopts forward and backward ants to explore the network to assemble the information about traffic in network. They use priority queues. FANT is probabilistic and when it reaches at the destination, then it is de-allocated and BANT acquires stack enclosed in FANT. BANT, unlike FANT, is deterministic. It is emitted in high priority queue. Now, BANTs reiterate the FANT's route and use this data for routing table updates and other information repeatedly.

1.10.1.4 Automatic clustering inspired by ant dynamics (ACAD)

It is a searching algorithm which identifies separated clusters having different shapes such as convex and/or non-convex. Ants follow a route and mark a chemical material on the selected path (pheromone) for remaining ants and that pheromone decreases with time. Depends up on matrix formed by the different pheromone values and its freshness, nest hope is selected. [16]

1.10.2 On demand/reactive ant based routing protocols

1.10.2.1 Ant-colony-based routing algorithm (ARA)

This protocol uses ants as agents for network which react as per demand and network flooding approach is similar to AODV. Following are operations of ARA:

Route discovery phase: FANT creates the path of pheromone to source and BANT creates the trace to destination. Sender broadcasts the FANTs to neighbors. Paths can be duplicated so to prevent it, sequence numbers are utilized. When a node receives a FANT, it makes a routing table entry(next hop, destination address, pheromone). That table entry's address is filled with FANT's source address, next hop with previous node's address and pheromone value with hops required to reach at destination. After that, node transmits it to neighbors. Finally, it reaches destination that takes out all data and deletes FANT. When the FANT reaches destination, destination node extracts the information and then destroys the FANT. Then BANT is made and transmitted it to source. Hence, a route is set and data is exchanged.

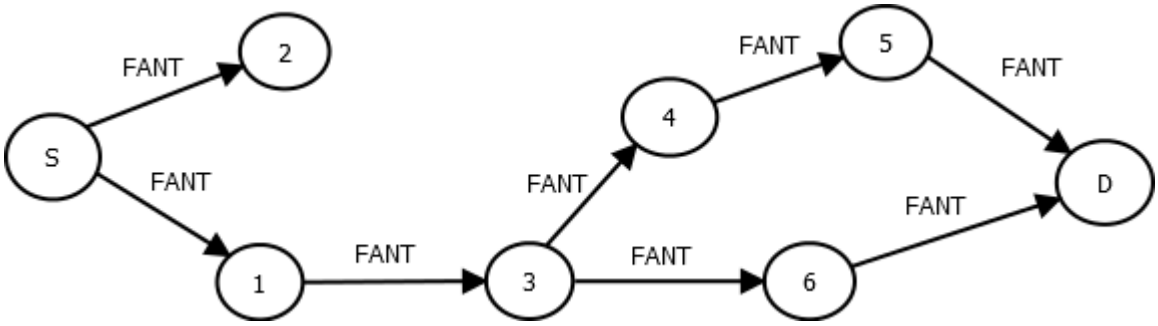


Figure 1-19: Propagation of FANT

Route maintenance: Once a pheromone route is set for two nodes, further data transmission improves the pheromone value. These values vary continuously. When one transmits the data to other node, it enhances the value. Value increases even when data is sent in reverse also.

Route failure handling: When there is an acknowledgement found missing, then pheromone is set to zero, which deletes the link. Then an alternative route is found and data is transferred through it. There is no mechanism to update according to changing topology. The link gets deleted as the acknowledgement is missing, leading to the value of zero for pheromone.

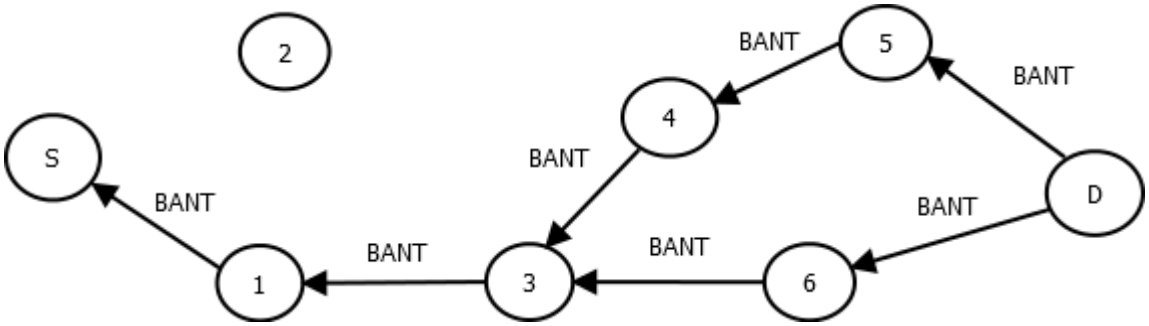


Figure 1-20: Propagation of BANT

1.10.2.2 Probabilistic emergent routing algorithm (PERA)

Probabilistic emergent routing algorithm (PERA) is suggested in which neighboring node's probability distribution is saved in routing tables. A probability distribution show the packet forwarding, if there is no path then node creates a path itself and stacks is used

for path traversal. Use of forward and backward ants at each node introduced unnecessary control overhead over the entire network.

1.10.2.3 Ant dynamic source routing (ADSR)

ADSR provides the QoS provision by maintaining different QoS parameters such as delay, jitter and energy etc. Ant DSR uses FANT and BANT packets for request and reply for route and for path discovery process. It supports route discovery and route maintenance phase. During route discovery, route cache is built up and when packet reaches at its destination, route cache is expired. For route maintenance, error packets and acknowledgements are used to find out correct links over the network.

1.10.2.4 Improvised ant colony optimization algorithm MANETs (PACONET)

It uses mobile agents as BANT and FANT. FANT is sent in a controlled broadcast way for route discovery. When every value is checked then after comparison, then only next node is selected. It makes sure that path which is selected is best one.[16]

1.10.3 Hybrid ant based routing protocols

1.10.3.1 Ant-Hoc Net Routing Algorithm

Ant-Hoc Net is hybrid algorithm that utilizes proactive as well as reactive methods. Reactive method maintains information about other nodes that are convoluted in conversation. Proactive method maintains information about existing paths during communication. Routing information is stored in pheromone tables. If there is any failure in link, then it is settled with particular reactive method like warning messages and repairing routes locally.[4]

1.10.3.2 Hop Net

In this algorithm, network is split into areas called zones. All nodes in a zone are each other's local neighbors. Two types of routing tables are used:

Inter Routing Table, which contains route ahead of its zone.

Intra Routing Table, which contains information about nodes within the zone. This table is managed proactively. Due to which, within a zone, a node can get a route promptly. When there is need for connection with node outside zone, then reactive methods are used for path discovery. First of all, it check intra RT, if it does not get required node then it goes for inter RT.[7]

Table 1.1: ACO algorithms characteristics

Algorithm	Routing approach	Ant type	Problem	Energy aware	Path type
ABC	Proactive	Exploratory ants	Congestion	-	Single Path
Ant net	Proactive	FANTs& BANTs	Delay	-	Single Path
ARA	Reactive	FANTs& BANTs	Cache pollution	-	Multipath
Ant AODV	Hybrid	FANTs& BANTs	Route Error	-	Single Path
AntHocNet	Hybrid	FANTs& BANTs	Overhead	-	Multipath
HOPNET	Hybrid	FANTs& BANTs	Scalability	-	Multipath

Chapter 2

LITERATURE REVIEW

Researcher have developed a new concept of routing by combining the concept of ad hoc network routing with the ant net algorithm, called ad hoc ant net based routing/swarm intelligence but combination of these two routing technologies still suffer from the security threats because if a security threat exists against the ad hoc routing protocol, there may be a probability that same threat can degrade the performance of the ad ant net routing protocol also. So researchers further introduced some methods to detect/ prevent/ secure the ad hoc ant net routing. Now will discuss the efforts made by them to secure the network.

Vivekanand Jha et.al (2011) did a survey of the different nature inspired routing algorithms developed for the MANETs those work in high mobile environment and having changing topology with restrictions on bandwidth and energy. These all are included in Swarm Intelligence. Swarm intelligence has many properties which are needed to deal with problems of this type of networks. We reviewed the major routing protocols inspired by collective behaviours observed in nature's self-organizing systems of ant and bee colonies, termite hills and bird flocks. [6]

U.Venkanna and R.Leela Velusami(2011) initially discusses the blackhole attack and other security attacks in mobile ad hoc networks. Trust management is one of the countermeasures. Trust is classified into identity trust and behaviour trust. Identity trust can be achieved by digital signature, encryption techniques and other mechanisms for authentication. Behaviour trust is used to differ between malicious and authorized node. Behaviour trust further leads to two types, direct trust and indirect trust. Direct trust is done by itself node. Indirect trust utilizes the advice from other nodes or third party advice. Trust management's main function is to see neighbouring nodes' behaviour and give a trust value to them. Finally, existing solutions based on trust management like watchdog and path rater, CONFIDENT (cooperation of nodes fairness in dynamic ad hoc network), CORE (collaborative reputation), SMRTI (security MANET routing with trust intrigue), PFR (packet forwarding routing), REP (recommendation exchange protocol) are discussed.[24]

Anuj K Gupta et.al (2012) discussed ant based routing protocols. It comes under the category of Swarm Intelligence. These protocols use behaviour of ants to find path from their nest to food. Ants track a substance (pheromone) on the ground left by other ants to find shortest route. Comparison between ant based protocols and other protocols has done, which shows that ant based protocols outperform other MANET protocols in many ways.[15]

Suparna Biswas et.al (2012) presented a secure check pointing way by electing gateway nodes and cluster head using model based on trust factor and ACO. They used ACO to check about availability and selfishness of nodes. MANET has various applications in different areas such as military, battlefields, disaster management, m-commerce application, controlling of mining activities, controlling of air traffic, etc. An efficient fault tolerant algorithm recovers the application so that the system should be available to the users. Proposed solution is based on ant colony that utilises trust model so that checkpoint routing goes through only nodes which are trusted. It does not use any cryptography methods. [3]

Jitender Kaushal(2012) gives a review on advancements occurred in ant colony optimization domain. Ant's behaviour is utilized for solution to continuous and discrete optimization problems and difficulties in routing and load balancing. Paper also provides classification based on evolution took place. Finally, application based on travelling salesman, assignment problem, scheduling problems, routing problems are briefly discussed.[27]

Arafat S.M et.al proposed a secured link quality, delay and energy conscious routing approach based on ACO. Route information is built up on the basis of link quality, delay and residual energy of the nearby nodes. It selects the efficient node based on the ANS mechanism and sends the data packets through that node. Ad hoc security algorithms incorporated for making the transmission more secured. [8]

P.Subathral, S.Sivagurunathan and G.S.R. Emil Selvan(2012) explained their research with security issues in mobile ad hoc network. It proposes security mechanism with antTree clustering. Cluster is a group of nodes with similar movements. For clustering, control information is needed to be flooded, which increases the overhead. To avoid it, a subset of nodes is selected for rebroadcasting. A new metric based on signal strength is introduced to predict distance between two nodes. To protect data and

information about routing, threshold cryptography is used. In this procedure, key is divided into n pieces so that it can be reconstructed using t pieces. If there are t-1 pieces, then key cannot be revealed.[23]

Chen Dajun, Wang Chao and Lin Qiang(2013) discussed wireless mesh network routing using ant based trusted algorithm. It discusses the adverse impact on performance of network due to use of tradition security methods like cryptography as they increases overhead. Now with trust mechanism, it takes into account factors like time delay, bandwidth, and packet loss. Using these factors, forged information produced by malicious nodes can be identified. Because of ant colony algorithm, right route can be found in less time and end-to-end delay. Due to ant colony optimization based routing, it also reduces overhead effectively.[30]

Rajkumar P et.al (2013) did survey of various security attacks on MANETs. Due to features like open architecture, changing topology, shared medium, etc., MANETs has some weaknesses in terms of security and attacker can utilise these weaknesses to get into network and perform attacks. There are many types of attacks possible in ad hoc network. Firstly, various attacks are discussed. After that, different detection techniques are discussed to minimise their effect.[10]

Amara Korba Abdelaziz et.al (2013) discussed the vulnerability of MANET to security threats. It includes all types of threats belonging to malicious nodes as well as selfishness of node. There are many techniques developed in recent years to counter these attacks. Some of them are cryptography based solutions and trust based solutions, etc. [31]

Qinghua Shi et.al (2013) proposed a secure QoS algorithm that uses ant colony optimization algorithm along with credit evaluation mechanism. Acceding to proposed method, nodes are introduced as the control factor in ant colony algorithm. This method discards all the nodes those cannot fulfil the QoS requirements and selected nodes are further optimized and finally an optimal route is selected by the ACO algorithm. Creditworthiness for the nodes is calculated on the basis of packet loss rate, energy and time delay of link, as ant colony optimization control factor etc. Node with high creditworthiness is select as the next hop, thus this algorithm can avoid some attack and the optimal route has higher reliability. Finally, the security of the algorithm is analysed from a variety of network attack. [2]

Nabil Ali et.al (2013) presented a secure routing protocol for sensor networks which uses ant colonization algorithm. Neighbour discovery is done using hello packets. It utilises forward ants to gather and addition of reputation values in the path. Then, destination node utilises backward ants to carry data and instructions of destination for security of route purpose. Proposed scheme takes two paths for data forwarding to resolve node failure. Simulation results show that as compared to iACO and LEACH protocols, the proposed scheme gives better performance in case of overheads and forwarding efficiency and can maintain better data delivery rate if there is malicious node present. [5]

S. Balaji, S. Sureshkumar and G.Saravanan(2013) this paper gives cluster based ant colony optimization routing in case of VANETs. VANETs are part of MANETs. They include communication of vehicles. Nodes of VANETs are very high speed. So it is difficult to perform routing operation in that much highly dynamic nature of network. So, using clustering followed by ant colony optimization based routing, called ACO-DYMO routing, and gives a good performance. Results show that using ACO procedure in cluster environment is more suitable.[28]

B.Nancharaiah B.Chandra Mohan(2013) proposes a hybrid algorithm of particle swarm optimization and ant colony optimization. This approach is designed to reduce the end-to-end delay and communication cost metrics. ACO utilizes mobile ant agent to find best and feasible path from one node to other link which takes place as input to PSO. PSO gives best answer for velocity and position of particle with minimum cost and end-to-end delay. Simulator results of proposed solution shows that this new algorithm can get along with large networks.[25]

Sudarshan D Shirkande , Rambabu A Vatti (2013) surveys on various algorithm based on ant colony optimization routing technique in wireless sensor network (WSN) and mobile ad hoc network (MANET). WSN and MANET have applications in surveillance, health care, disaster management, etc. Normal routing does not perform well in ad hoc network due to dynamic nodes and link asymmetry. To deal with it, ACO, a part of swarm intelligence is introduced. This paper makes comparisons of algorithms based on ACO in case of pheromone function to select next node, energy awareness, simulation used, etc.[26]

Kashif Saleem et.al (2014) presented the Biological inspired Self-Organized Secure Autonomous Routing Protocol (BIOSARP). Its routing decisions depend on improved ant

colony optimization (IACO) that calculates the optimal routing based on the link packet reception rate (PRR), remaining battery power and delay, which are acquired from neighboring nodes in the boot process and saved in a neighbour table for onward data forwarding. The storing process under BIOSARP helped to reduce the huge processing delay and traffic overhead. Extensive simulations were performed to analyse and compare the performance of BIOSARP. Simulation results show the efficiency the proposed scheme as compared to other methods i.e. E&D ANTS, SRTLD, and IEEABR etc. [1]

H. Simaremare et.al (2014) proposed a secure protocol by using an ant algorithm. Ant agent put a positive pheromone when the node is trusted. Path communication is chosen based on pheromone value. They evaluated the performance of proposed protocol with/without using ant algorithm under DOS/DDOS attack. Simulation results show the performance of proposed protocol increases while using ant algorithm in term of packet delivery ratio and throughput but it could not manage the end-to-end delay. [4]

Abhishek Gupta et al. (2014) developed an ACO based IDS system which can scan a specific port to identify the attack over UDP protocol. Proposed method observes the behavior of the protocols and monitors the network flow to identify the protocol misbehavior. Simulation results show its performance in terms of identification of various attacks and as well as protection against fake alerts. This scheme can be further extended to secure the other protocols such as FTP, DHCP, ICMP etc. Authors had also discussed its limitation such as it can scan the specific ports only, does not support the network scalability.[17]

Mahmoud Hashem et al (2014) presented routing scheme to secure the VANETs ACO method which can estimate the more reliable and secure routes. They also developed a VANET-oriented Evolving Graph (VoEG) model to monitor the control information related to nodes. Simulation results show it can fulfill the QoS constraints by providing the most reliable and secure routes by compromising with network overhead.[18]

Wang Hao et al. (2014) proposed a trust base model to guard against the security threats, called AraTRM which provides the resistance against attacks as well as it is capable enough to maintain the reputation also. It selects the path based on trust and it can also perform under compromised network using malicious detection methods. Simulation shows its efficiency and supports the scalable networks but it does not perform well on large number of malicious nodes. [19]

Hitesh Hasija et al. (2014) proposed a method based on ACO algorithm which can produce the codes on the basis of their frequency. Key matrix can be changed on the basis of frequency. Produced code is based on the input data and its relevant parameters also. Simulation results show that it is quite complex to identify the ACO based codes as well as the input data. This scheme can be extended to support the to flexible key size with delimited input data. [20]

Abhishek Kaleroun et al. (2014) proposed a ACO based scheme by merging trust value which can be generated on the basis of PH values and can easily adopt the dynamic environment. It builds the optimized graphs using trust values which can be updated frequently and points are searched using prediction values. Trust value is regulated using feedback system. Experiments show its performance in terms of search, prediction, trust values for the user. [21]

Ayman M. Bahaa-Eldin et al. (2014) used ACO algorithm to provide the trust based routing over MANETs, known as TARA which calculates the trust values for each node on the basis of various parameters such as node's routing history and its behavior. Later on this value is used to define the next routes. ACO method is used to achieve pheromone value for routes. Simulation results show its performance on the basis of selected routes, trust estimation in mobile environment [22].

D.Sivakumar and B.Suganthi(2014) gives us a comparison of AntHocNet, AOMDV and AODV. AntHocNet is a hybrid and adaptive routing protocol as it includes benefits of proactive and reactive routing algorithms and it is based on ACO, which comes under swarm intelligence. Comparisons are made according to throughput, end-to-end delay, and delivery ratio and packet loss. Due to better adaptability of ant based practical in dynamic environment and link failure situation, AntHocNet performance better than AOMDV and AODV.[29]

.

Chapter 3

PRESENT WORK

3.1 PROBLEM FORMATION

MANET is wireless network without any rigid infrastructure and centralized authority. These networks have high mobility. Due to these features, MANET can be easily attacked. There are attacks like DOS and blackhole, which can decline the performance of network. Initially cryptographic measures were used to provide confidentiality and authentication. Due to additional information in data packet, overhead increases. To avoid this overhead, trust based model came into play. In trust based model, malicious nodes are detected using trust factor before setting the route. Then, a new ant based trusted model is proposed to enhance the performance. In ant based trusted mechanism, if node is trusted, then pheromone value is added to that node by ant agent and transmission route is selected on the basis of pheromone value. On ant based trusted AODV, DOS attack has already been evaluated. But there is need to explore other security threats and their impact over the ad hoc ant net based routing. In this research work, we can compare the impact of blackhole attack on network by comparing performances before, during and after the attack has taken place.

3.2 OBJECTIVE OF STUDY

Main objectives of this research work are:

- To analyze the normal behavior of the AODV Ant net based routing over MANETs.
- To analyze the impact of blackhole attack over ant based routing and performance of the network.
- To develop prevention mechanism in ant based routing.

We will calculate the performance routing protocol using different parameters such as throughput, packet delivery ratio etc. before and after the security threat.

First of all, normal behavior of AODV ant net based Routing will be observed. Then, blackhole attack will be applied and check out the changes one find in various parameters. Finally, a mechanism is needed so that network can be recovered from attack.

3.3 RESEARCH METHODOLOGY

In AODV, for blackhole attack, attacker node changes sequence number to high value so that it can draw all the traffic to itself. In ant based AODV, pheromone value factor is also included. So, in our proposed methodology, we will set a maximum value for sequence number as well as pheromone value. If there is any node, having values more than these values, then there will be attack alert.

```
set threshold=t; // set theshhold value
set HighPhValue=HphV; // set High PH Value

while (routing)
{

   if (detect_chnage(routingInfo-Nodes)==true && detect_chnage(routingInfo->PH_Val)
  {
    if (PH_Val> HighPhValue  && PKT->seq_no> threshhold)
      {
       Attack_alert==true;
       }
}


If (Attack_alert)
{
alert_msg(unexpected PH value. found...);
ignore_requests(routingInfo->PH_Val, seq_no);
routing_table_update();
}
```

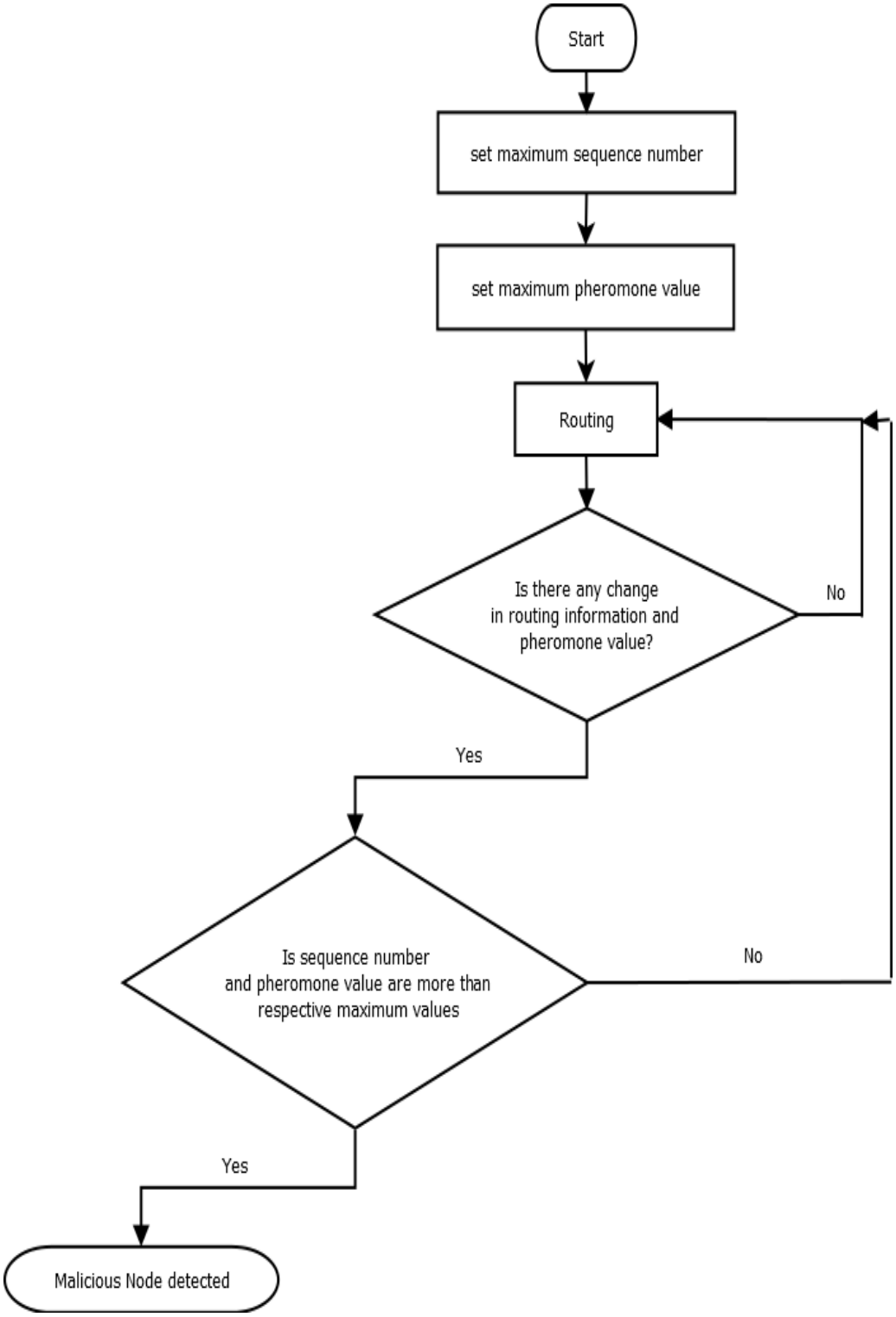


Figure 3-1: Flowchart

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Performance Metrics

Throughput, Routing load and packet delivery ratio are the performance metrics selected to evaluate the blackhole attack.

First parameter is the throughput. It is the ratio of total data, the receiver received from sender, to the total time taken. It can represented in either bits/sec or packets/sec. limited bandwidth, dynamic topology and power limitations effects the throughput in MANETs. Other factor which effects throughput adversely is unreliable communication.

Next parameter is Routing load. It implies the total number of packet sent for routing purpose per data packet.

Packet Delivery Ratio is ratio of total number packets that are delivered to destination to total number of packets sent by sender to destination. More packet delivery ratio means better protocol performance.

4.2 Simulation

We analyzed the impact of blackhole attack over ant based ad hoc network. We also proposed a prevention scheme to detect and prevent this attack. We used NS-2 for simulation purpose. Following table: shows the simulation configuration:

Table 4-1: Simulation Configuration

Simulation Parameters	Configuration
Routing Protocol	AODV Ant net based routing protocol
Wireless Terrain	1200x1200
IFQ	50
MAC Protocol	802.11.4
Transport Layer Protocol	TCP
Propagation Model	TwoRayGround
No. Of Nodes	25
Traffic Type	CBR
Interval	0.5
Packet Size	1024
Simulation Time	10
Simulation Scenario (s)	Normal, Attack, Prevention

We used AODV Ant net based routing protocol for routing, Propagation Model is TwoRayGround, MAC protocol is 802.11.4, transport layer protocol is TCP, traffic type is CBR with 0.5 sampling interval having packet size of 1024. Number of nodes are 25 and simulation time is 10.

Following figure shows the normal scenario. Normal scenario means situation before the occurring of attack. There are 25 nodes of different colours.

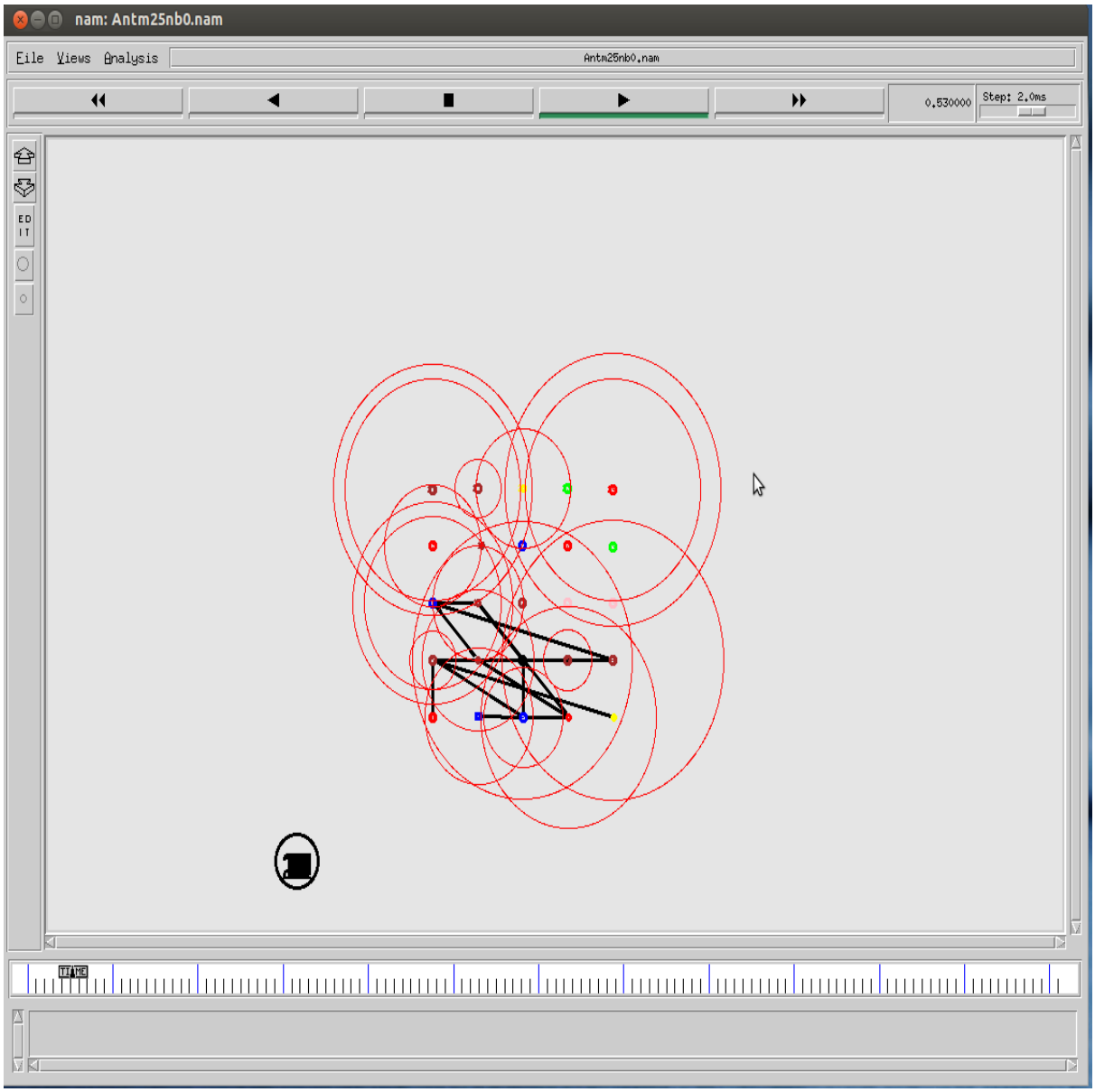


Figure 4-1: Simulation representing normal packet transfer

Following figure shows packet drop during packet transfer. Red dots near the node on the left corner of downside edge represents packet drop.

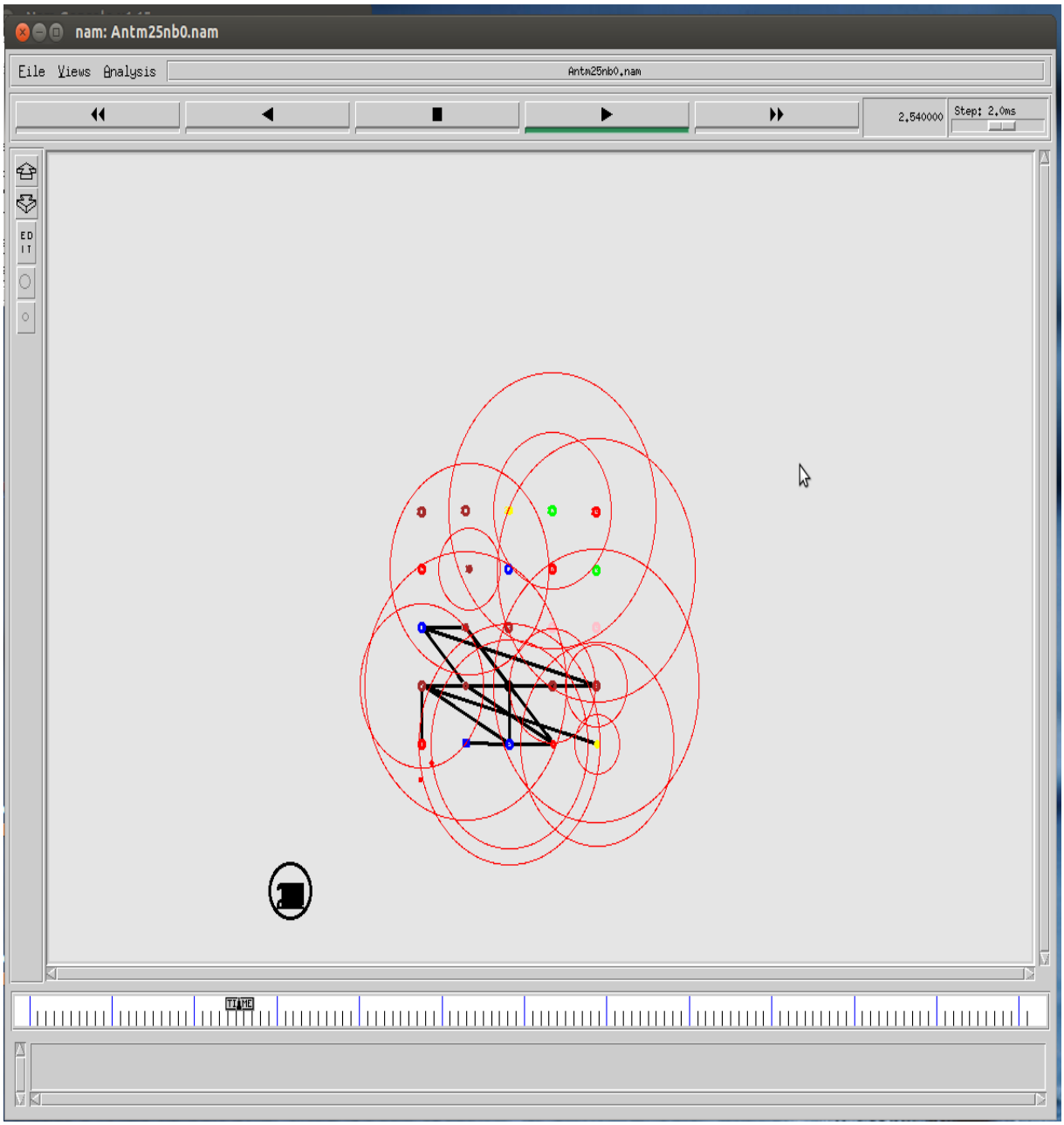


Figure 4-2: Simulation showing packet drop

4.3 Results

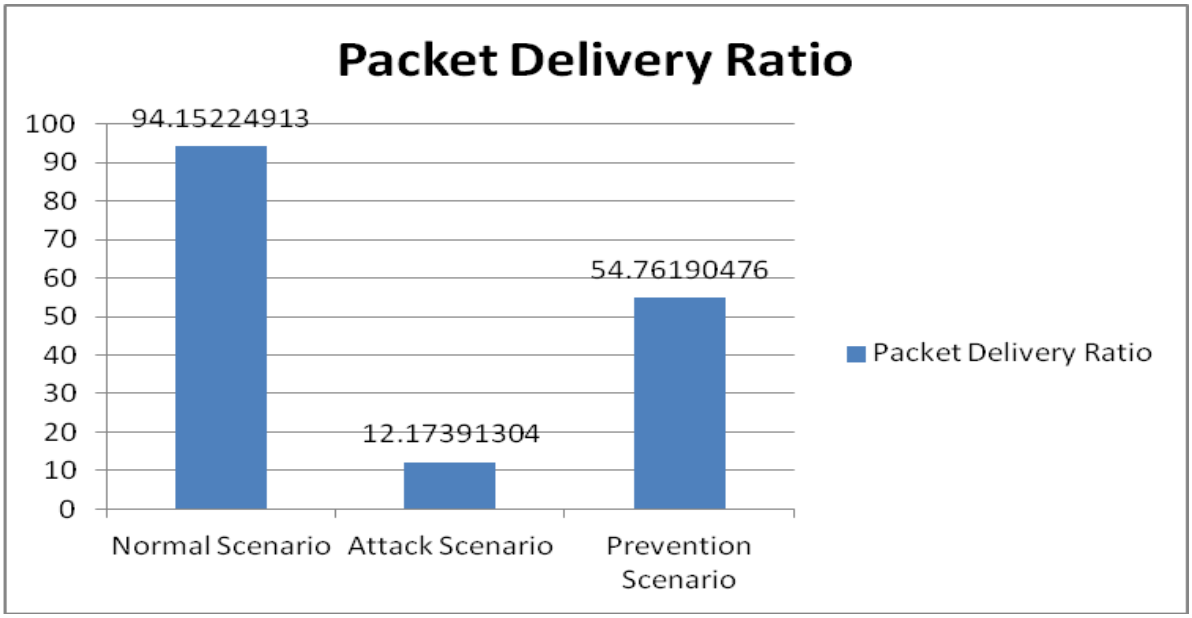


Figure 4-4: Packet Delivery Ratio for different simulation scenarios

Figure above shows the packet delivery ratio of different simulation scenarios. In normal scenario, It is 94.15, during attack its value is 12.17 and with prevention scenario, it is 54.76. Because of packet drop during attack, packet delivery ratio decreases. But with our prevention mechanism, attack is deactivated and ratio again goes up to sufficient level. As per the results, we can observe the impact of attack over PDR but our proposed scheme is capable enough to recover it again.

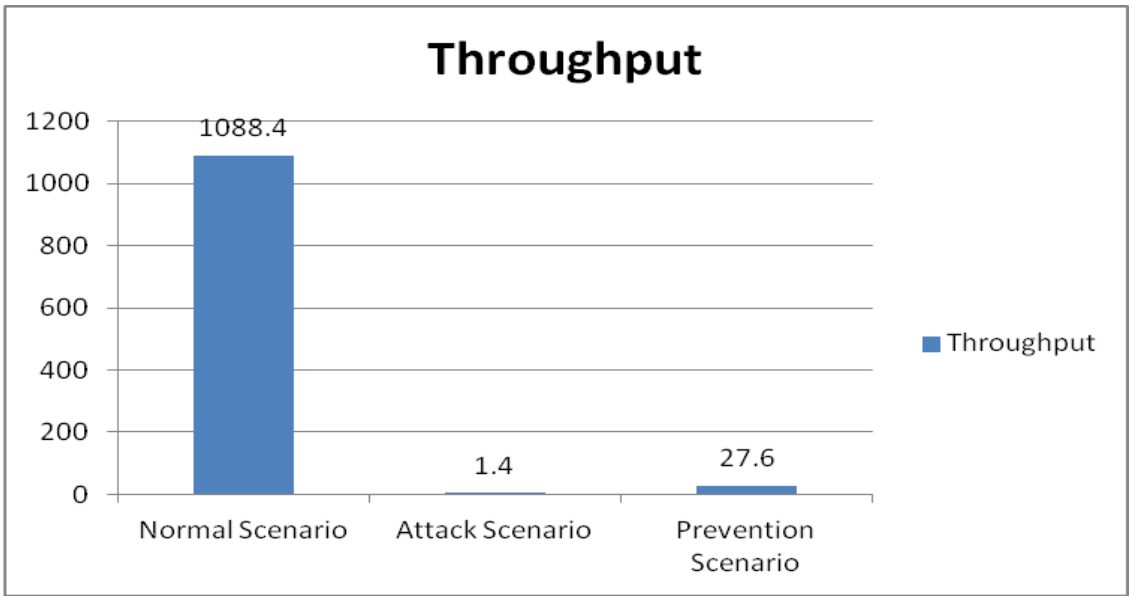


Figure 4-3: Throughput graph for different simulation scenarios

Figure above shows the Throughput of different simulation scenarios. In normal scenario, It is 1088.15, during attack its value is 1.4 and with prevention scenario, it is 27.6. Due to attack, a large number of packets are dropped which to decrease in throughput. As per the results, we can observe the impact of attack over Throughput but our proposed scheme tried to overcome from the attack and preserved the Throughput upto a certain level only.

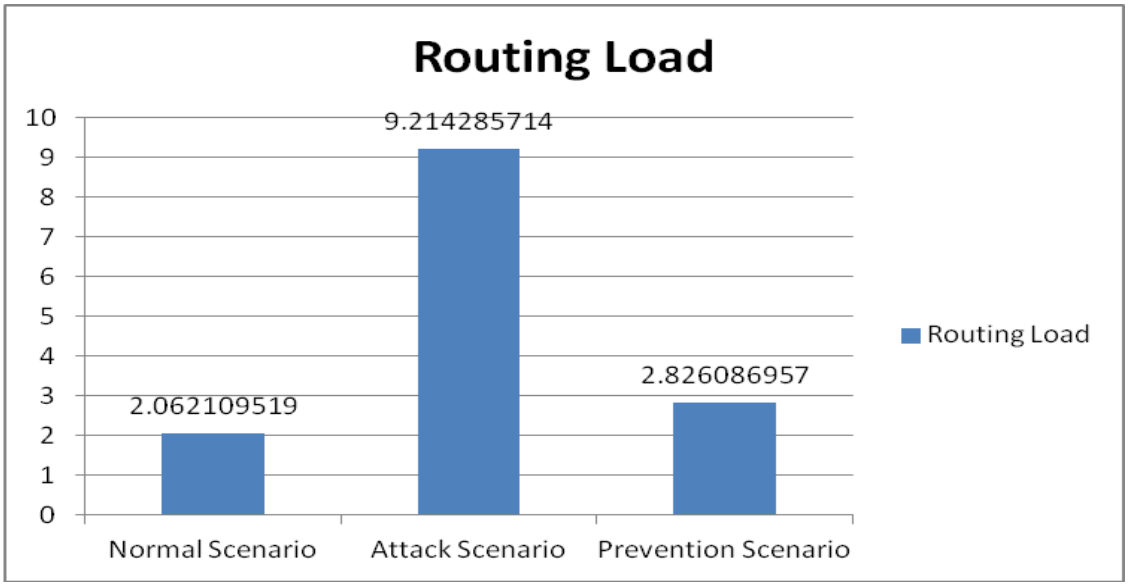


Figure 4-5: Routing Load for different simulation scenarios

Figure: above shows the Routing Load of different simulation scenarios. In normal scenario, It is 2.0, during attack its value is 9.2 and with prevention scenario, it is 2.8. As per the results, we can observe the impact of attack over Routing Load but our proposed scheme can reduce this up to a level which is slightly large then Routing Load of normal scenario.

Table 4-2: Performance Analysis Table

	Normal Scenario	Attack Scenario	Prevention Scenario
Throughput	1088.4	1.4	27.6
Packet Delivery Ratio	94.15224913	12.17391304	54.76190476
Routing Load	2.062109519	9.214285714	2.826086957

Table above shows the simulation results of different scenarios using various parameters

Now will review the performance of each scenario individually.

Network Performance in normal condition

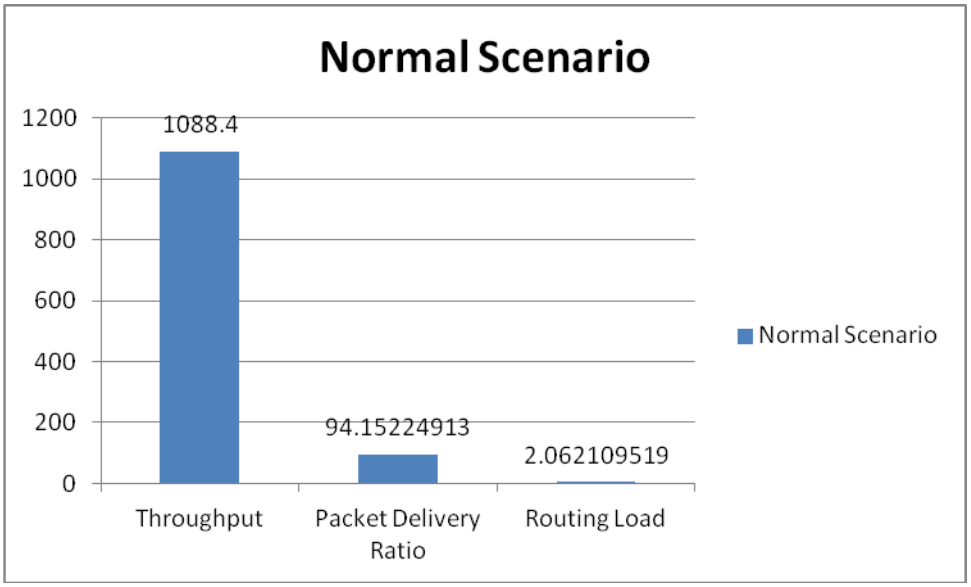


Figure 4-6: Network performance in normal condition

Figure: above shows that in case of normal scenario, Throughput is 1088.15, PDR is 94.15 and routing load is 2.06 (aprox).

Impact Analysis of Blackhole attack

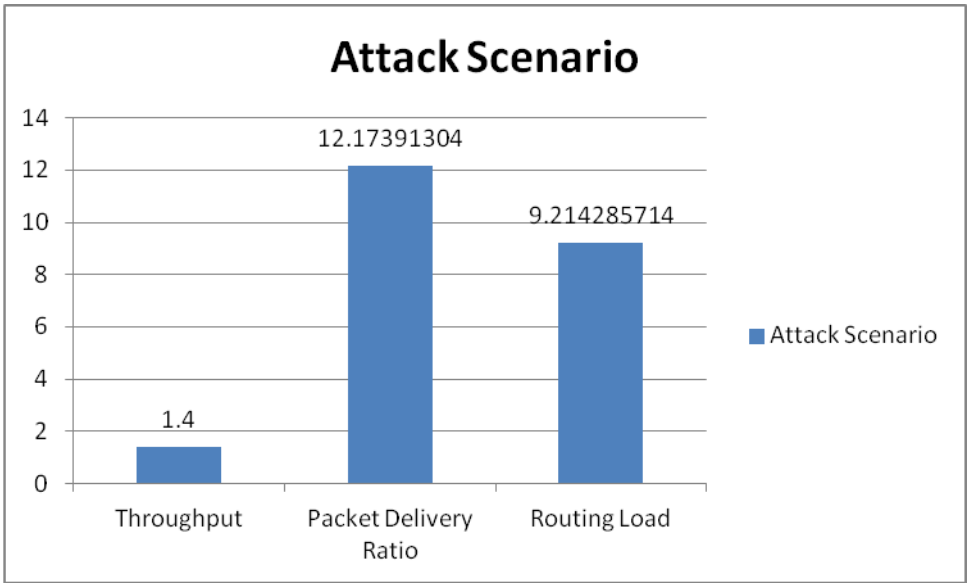


Figure 4-7: Network performance in case of attack

Figure: above shows that in case of attack scenario, Throughput is 14, PDR is 12.17 and routing load is 9.21 (approximately).

Performance of proposed Scenario

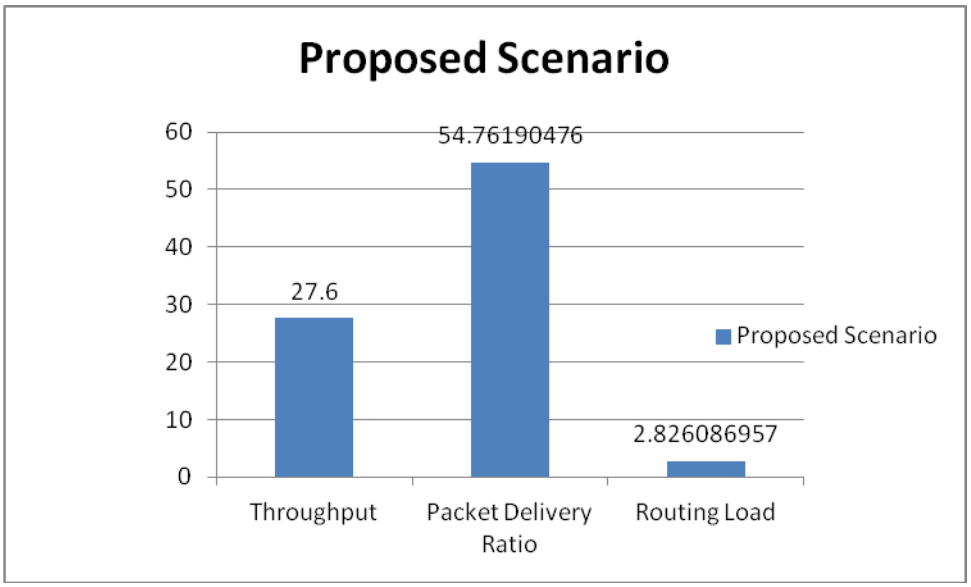


Figure 4-8: Network performance in case of prevention scenario

Figure: above shows that in case of proposed scenario, Throughput is 27.6, PDR is 54.79 and routing load is 2.82 (aprox).

Chapter 5

Conclusion and Future Scope

There are various types of security threats available those can degrade the ad hoc routing protocol's performance these days, researchers developed a new concept of routing called ad hoc ant net based routing/BeeHoc/Ant Hoc/Swarm intelligence. This new type of routing technology also suffers from the security threats which were developed for the MANET's routing protocols. Till now, authors addressed the issues related to security threats and proposed some methods to secure the network and as per their simulation results. Still, many security threats like blackhole attack are not explored for ant based routing. Security threats over this type of routing can easily degrade the network performance.

In this research work, we analyzed the impact of blackhole attack over AODV antnet based ad hoc network. We used different simulation scenarios with various performance parameters i.e. Throughput, routing load and packet delivery ratio etc. which are mostly effected by the routing layer based attacks.

Simulation results show that in normal scenario, Throughput is 1088.15, during attack its value is 1.4 and with prevention scenario, it is 27.6. As per the results, we can observe the impact of attack over Throughput but our proposed scheme tried to overcome from the attack and preserved the Throughput up to a certain level only.

In normal scenario, PDR is 94.15, during attack its value is 12.17 and with prevention scenario, it is 54.76. As per the results, we can observe the impact of attack over PDR but our proposed scheme is capable enough to recover it again.

In case of normal scenario, routing load is 2.0, during attack its value is 9.2 that is highest among all and with prevention scenario, it is 2.8. As per the results, we can observe the impact of attack over Routing Load but our proposed scheme can reduce this up to a level which is slightly large then Routing Load of normal scenario.

As per the result analysis, finally we can conclude that our proposed scheme can detect and prevent the blackhole attack successfully and future scope is that the proposed work can be extended to develop swam based intrusion detection system which would be used to protect the network from different type of attacks.

REFERENCES

[1] Kashif Saleem, Norsheila Fisal, Member, IEEE, and Jalal Al-Muhtadi, "Empirical Studies of Bio-Inspired Self-Organized Secure Autonomous Routing Protocol", IEEE SENSORS JOURNAL, VOL. 14, NO. 7, JULY 2014, pp 2232-2239.

[2] Qinghua Shi, Zhong Li, "A Secure QoS Routing Algorithm Based on ACO for Wireless Sensor Network", IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, IEEE-2013, pp 1241-1245.

[3] Suparna Biswas, Priyanka Dey, Sarmistha Neogy, "Trusted Checkpointing Based on Ant Colony Optimization in MANET", Third International Conference on Emerging Applications of Information Technology (EAIT), 2013, pp 433-438.

[4] Simaremare, H. ; Univ. of Haute Alsace, Colmar, France ; Abouaissa, A. ; Sari, R.F. ; Lorenz, P., "Performance analysis of optimized trust AODV using ant algorithm", ICC, IEEE-2014, pp 1843 – 1848.

[5] Nabil Ali Alrajeh, Mohamad Souheil Alabed, and Mohamed Shaaban Elwahiby, "Secure Ant-Based Routing Protocol for Wireless Sensor Network", International Journal of Distributed Sensor Networks Volume 2013, Article ID 326295,pp 1-9.

[6] Vivekanand Jha, Kritika Khetarpal , Meghna Sharma, "A Survey of Nature Inspired Routing Algorithms for MANETs", IEEE,2011 pp 16-24.

[7] W. Zhang*a, P. Passow*b, E. Jovanovc, R. Stolla and K. Thurow, "A Secure And Scalable Telemonitoring System Using Ultra-Low-Energy Wireless Sensor Interface For Long-Term Monitoring In Life Science Applications", CASE-2013, pp 617-622.

[8] Arafat S.M. Qaed, T. Devi, "Secured Link Quality, Delay and Energy Aware Routing Protocol (SLQDEARP) For Mobile Ad Hoc Networks", IEEE International Conference on Intelligent Interactive Systems and Assistive Technologies, IEEE-2013, pp 15-20.

[9] M.M.Goswami, R.V. Dharaskar, V.M.Thakare, "Fuzzy Ant Colony Based Routing Protocol For Mobile Ad Hoc Network", International Conference on Computer Engineering and Technology, IEEE-2009, pp 438-444.

[10] J. Wang, E. Osagie, P. Thulasiraman, R.K. Thulasiraman et al.,” HOPNET:A Hybrid Ant Colony Optimization routing Algorithm for Mobile Ad-Hoc Network, Ad Hoc Network.”, 2008

[11] .Erdal Çayırcı et al., “Security in Wireless Ad Hoc and Sensor Networks”, A John Wiley and Sons, Ltd, Publication, 2009.

[12] C Siva Ram Murthy” Wireless Ad hoc Network-Architectures and Protocols” Pearson-2012.

[13] Chen X. et al., “Sensor Network Security: A Survey”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 2, SECOND QUARTER 2009.

[14] Tamilarasan S., “Securing and Preventing AODV Routing Protocol from Black Hole Attack using Counter Algorithm”, IJERT-2012, Vol. 1 (5), pp 1-6.

[15] Azzedine Boukerche,” ALGORITHMS AND PROTOCOLS FOR WIRELESS AND MOBILE AD HOC NETWORKS”, John Wiley & Sons, Inc., Hoboken, New Jersey, 2009, ISBN 978-0-470-38358-2.

[16] Gurpreet Singh, Neeraj Kumar, Anil Kumar Verma, "Ant colony algorithms in MANETs: A review", Elsevier, pp-1964-1972.

[17] Abhishek Gupta, Om Jee Pandey, Mahendra, "Intelligent perpetual echo attack detection on User Datagram Protocol port 7 using Ant Colony Optimization ", ICESC, IEEE-2014, pp -419 - 424

[18] Mahmoud Hashem Eiza, Thomas Owens, and Qiang Ni, "Secure and Robust Multi-Constrained QoS aware Routing Algorithm for VANETs", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, TDSCSI-2014, pp1-14

[19] Wang Hao, Zhang Yuqing, "AraTRM: Attack Resistible Ant-based Trust and Reputation Model”,IEEE-2014, pp-652-657

[20] Hitesh Hasija, Rahul Katarya "Secure Code Assignment to Alphabets Using Modified Ant Colony optimization along with Compression", IEEE-2014, pp-175-181

[21] Abhishek Kaleroun, Dr. Shalini Batra, "Collaborating Trust and Item-prediction with Ant Colony for Recommendation", IC3-2014, IEEE, pp-334 – 339

[22] Ayman M. Bahaa-Eldin, "TARA: Trusted Ant Colony Multi Agent Based Routing Algorithm for Mobile Ad-Hoc Networks Ayman M. Bahaa-Eldin", Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations Intelligent Systems Reference Library Vol. 70, Springer, 2014, pp 151-184

[23] P.Subathral, S.Sivagurunathan and G.S.R. Emil Selvan," Securing mobile ad hoc network through AntTree clustering and threshold cryptography", 2012,IEEE,pp-336-340

[24] U.Venkanna and R.Leela Velusami," Blackhole attack and their countermeasures based on trust management in MANET: A Survey ", Proc. of1nt. Con/, on Advances in Recent Technologies in Communication and Computing 2011.

[25] B.Nancharaiah B.Chandra Mohan, "MANET link performance using ant colony optimization and Particle swarm intelligence algorithm", International conference on Communication and Signal Processing, April 3-5, IEEE-2013.

[26] Sudarshan D Shirkande , Rambabu A Vatti, "ACO based routing algorithms for ad hoc network (WSN, MANET): A Survey ", 2013 International Conference on Communication Systems and Network Technologies, IEEE-2013.

[27] Jitender Kaushal, "Advancement and applications of ant colony optimization: A critical review", International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012 1 ISSN 2229-5518.

[28] S. Balaji, S. Sureshkumar and G.Saravanan," Cluster based ant colony optimization routing for vehicular ad hoc network", International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 26 ISSN 2229-5518.

[29] D.Sivakumar and B.Suganthi," Performance comparison and classification of ad hoc routing protocols ", International Journal of Scientific & Engineering Research, Volume 5, Issue 4, April-2014 218 ISSN 2229-5518.

[30] Chen Dajun, Wang Chao and Lin Qiang, "Ant based trusted routing algorithm for wireless mesh network". International Journal of Scientific & Engineering Research, Volume 3, Issue 4,2014 218 ISSN 34445-7865.

[31] Amara Korba Abdelaziz," Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks", IEEE-2013

Mandeep Singh (2015), " Survey of Ant net based routing over mobile ad hoc network" in International Journal for Research in Applied Science and Engineering Technology, Volume 3, Issue III, March 2015.