To Isolate and Prevent Selective Packet Drop Attack in MANET

DISSERTATION-II

Submitted

By

SAGAR BABUBHAI PATOLIA

(11309057)

to

Department of Computer Science

In Partial Fulfilment of the Requirement for

Award of the Degree of

Master of Technology in Computer Science & Engineering

Under the guidance of

MR NARENDRA KUMAR BAGDE

June-2015

PAC FORM

LOVELY PROFESSIONAL UNIVERSITY

School of:Computer Science and Engineering

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the student	: Patolia Sagar Babubhai	Registration No	: 11309057
Batch	:2013-2015	Roll No	:A15
Session	:2014-2015	Parent Section	:K2307

Details of Supervisor:

Name	:Harmandeep Singh	Designation	: Assistant Professor
UID	:17700	Qualification	: M.E
		Research Exp.	:1.5 year

Specialization Area: Wireless Adhoc Networks

Proposed Topics:-

1. Proposing a method to prevent attack in MANET.
2. Proposing a enhcanced routing protocol.
3. Comparison of various routing protocols of MANET.

Harmandeep Singh 17700

Signature of supervisor

PAC Remarks: Topic No 1 is Approved Paper is expected 11570

16/9/14

APPROVAL OF PAC CHAIRMAN Signature: 1104 Date:

*Supervision should finally encircle one topic out of three proposed topics and put up for an 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

A Selective packet drop attack is notorious security problem in wireless Mobile Ad-Hoc network (MANET). A mobile Ad-Hoc network is wireless networks without any pre-existing infrastructure and centralizes control. They have self-organizing capabilities with mobile nodes. Ad-Hoc network contains multi-hop routes capabilities within short transmission range. Because of openness nature MANET is malicious by attacker. Several approaches have been proposed for finding malicious activity in MANETs. Due to nonexistence of MANETs infrastructure and well defied perimeter MANETs are susceptible to variety of attacker types. To develop a mechanism which provide strong security and understand the malicious node activity in the MANETs. A new mechanism presented is called KEAM (Key Exchange and Monitoring), which isolate malicious node on selective path in AODV routing protocol and secure the channel. This new methodology is named as "Isolate and prevent Selective Packet Drop Attack in MANETs. It is based on Diffie-Hellman Key exchange and monitor mode technique. Experimental result will be drone with use of NS-2 simulator and simulate result for Throughput, Packet loss, End-to-End Delay and compare the result with existing technique.

.

ACKNOWLEDGEMENT

I am very grateful to my guide **Mr Narendra Kumar Bagde,** Assistant Professor in Department of Computer Science & Technology, Lovely Professional University, Punjab. For his extensive patience and guidance throughout my project work. Without his help I could not have completed my work successfully .I would like to thank **Mr Dalwinder Singh**, Professor and Head, Department of Computer Science and Engineering ,Lovely Professional University, Punjab, for having provided the freedom to use all the facilities available in the department, especially the library. I would like to thank my classmates for always being there whenever I needed help or moral support. Finally, I express my immense gratitude with pleasure to the other individuals who have directly or indirectly contributed to my need at right time for the development and success of this work.

Sagar Patolia

DECLARATION

I hereby declare that the dissertation-II proposal entitled, "**To Isolate and Prevent Selective Packet Drop Attack in MANET**" 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: 27th April 2015 **Investigator**

Reg. No._____

CERTIFICATE

I hereby certify that the work which is being presented in the Dissertation-II entitled **" To Isolate and Prevent Selective Packet Drop Attack In MANET "** in partial Fulfilment of the requirement for the award of degree of **Master of Technology** and submitted in Department of Computer Science and Engineering, Lovely Professional University, Punjab is an authentic record of my own work carried out during period of Dissertation-II under the supervision of **Mr Narendra Kumar Bagde**, **Assistant Professor**, Department of Computer Science and Engineering, Lovely Professional University, Punjab.

The matter presented in this dissertation-II has not been submitted by me anywhere for the award of any other degree or to any other institute.

Date: **(Sagar Babubhai Patolia)**

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

Date: **(Narendra Kumar Bagde)**

Supervisor

Signature of Examiner

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

A network is a group of two or more computer systems which linked together communication. It is the way of exchange of information to communicate with one another. It is an association or set up of computer devices which are involved with the communication facilities [1]. When numerous devices are joined together to exchange information they establish networks and share resources. Networking is used to replicate, swapping and share information like data communication. Allocation resources can be software type or hardware types e.g. routers. There is centralized master system that handles and supports these types of system.

Various types of networks are as following:

1. Transmission media based networks like wired network and wireless network. Example of wired network is Coaxial cables and fibre-optic cables.
2. Network Size based network like MAN (Mobile Ad Hoc Network), LAN (Local Area Network) and WAN (Wide Area Network).
3. Management based networks like peer-to-peer and client/server
4. Topology based networks called connectivity like bus, star, and ring topology.

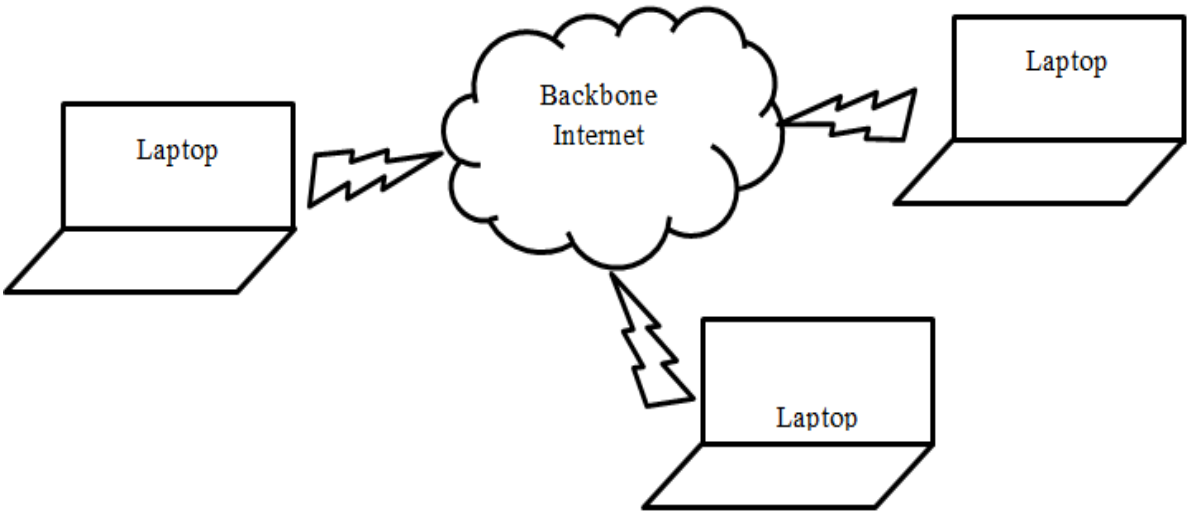


Figure 1. Diagrammatically presentation of Computer Networks

Networks can be classified as Wired and Wireless Networks. As the name only suggest one is organized with wired and another Wireless medium. Both can be differentiate by their characteristics of transmission medium, resources, hardware and software constraints. Different communication protocols being use to maintain network traffic, network size and selection topology.

1.1 Wireless Networks

Wireless communication is the level at which the transfer of user data over a distance without the use of “wired" or electrical conductor. The term “wireless” referred to tele-communication. Communication between two or more device can be with in the short range or may be thousands of kilometres range. Wireless Networks term is refers to a kind of networking that does not require cables to connect with devices during communication. Radio waves are used for transmission at physical level [2]. It is widely known as Wi-Fi or WLAN. With the help of this network, devices can be joined easily with the help of radio frequency without wires to sharing information. The IEEE specifies some standard on which all wireless networks works called 802.11. From this standard allocate dedicated ranges of frequency to numerous types of communication between multiple devices across the world without using any wire and fixed medium [3].

Convenience offered by Wireless Networks

- **Mobility:** This is one of the obvious advantages of the wireless networks. Mobile users can connect to the existing networks while roaming freely.
- **Simplicity:** We can translate simplicity into rapid development. It is easy to install a wireless infrastructure, compared to a wired network.
- **Flexibility:** Wireless network coverage area can reach where wire cannot go. It is very useful for moving vehicles or for the places where running cable is not possible.

According to wireless operation modes categories in 2 type:

1. Infrastructure
2. Ad-Hoc or Infrastructure less

Infrastructure mode is that mode in which wireless network adaptor is used to connect with the already existing networks with the help of access point. Wireless adaptor is also known as wireless clients [4].It has a central master controller. Ad-Hoc mode is connecting wireless clients directly without the desideratum of access point and wireless router. It has no central controller. So it is infrastructure less mode.

1.1.1 Infrastructure Networks:

In infrastructure predicated network, communication is takes place only between the wireless nodes and the access points. The communication is not established between the wireless nodes. Here the access point is utilized to command the medium access as well as it acts as the bridge to the wireless and wired networks.

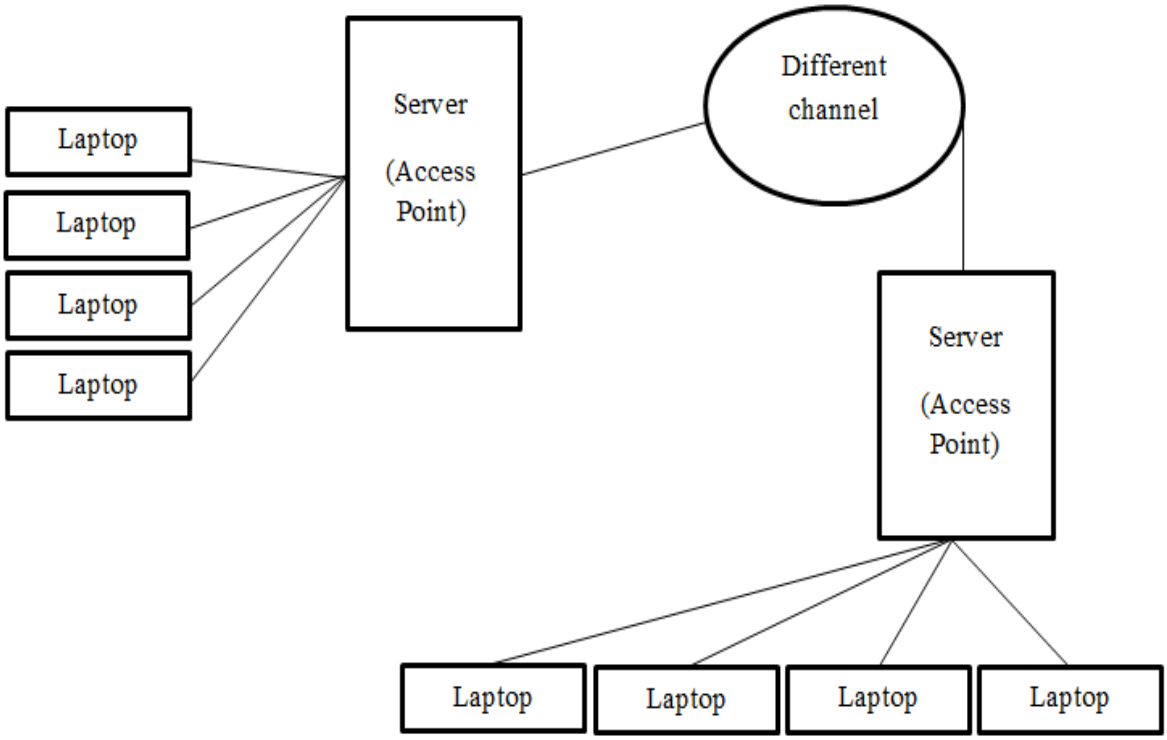


Figure 2. Infrastructure Network

In this network, fine-tuned base stations are utilized when the node goes out of the range of base station another base station come into range. The example of infrastructure deployed network is cellular networks system. It is centralized dominance device like router or Master

system [1]. The major problem which occurs in this system is that if controller fails all the system link to it will go down or crash.

1.1.2 Infrastructure less Networks :

The infrastructure less network does not require any infrastructure to for communication. In this network each host can transmit data to wireless node and it does not access point or controlling medium access. Infrastructure less networks do not have routers that are fine-tuned. In this network all the nodes need to act as routers and all nodes are capable of kineticism and can be connected dynamically in an arbitrary manner. All the contrivances in infrastructure less network are wirelessly communicated to each other. The speciality of this networks is that it has fileserver encompass core station of Wi-Max which controls pool of access point with in 6 kms rage. Utilizing Wi-Max base station and access points communicating and utilizing Wi-Fi utilizer and access points communicating [5].It is of three types:

1. Wireless Sensor Networks
2. MANET
3. Wireless Mesh Networks

❖ **Ad-Hoc Networks[2]:**

Ad wireless network is collection of many devices equipped with wireless communications and networking capabilities. Ad-hoc network is decentralized with no pre-subsisting infrastructure such as routers in wired networks or access points in wireless networks on which it is depended. In routing each node participates by forwarding data for other nodes in ad hoc network the resoluteness of which nodes forward data is made dynamically on the substratum of network connectivity. Ad-hoc networks are an incipient standard of wireless communication for mobile hosts. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. Wireless networks make utilization of radio waves or microwaves in order to establish communication between the contrivances. Each node participating in the network acts both as a host and a router and must therefore is willing to forward packets for other nodes.For this purpose a routing protocol is needed.

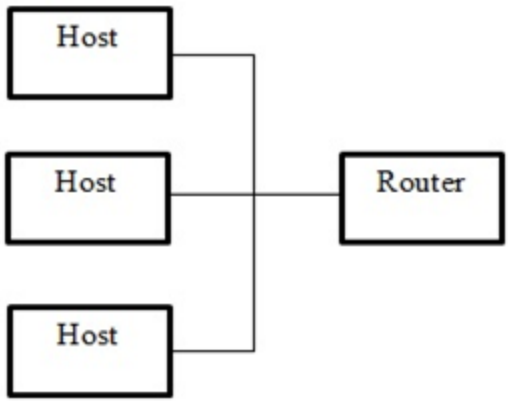


Figure 3. Block diagram of mobile node acting both as hosts and as router

Ad-hoc network is a wireless, self-organizing and rapidly deployable network in which neither a wired backbone nor a centralized control exists. The nodes are often energy constrained i.e. battery powered devices with great diversity in their capabilities.

The main characteristics of Ad-Hoc networks are as following:

1. Network topology changes regularly and suddenly.

2. There is no centralized administration is present in it.

3. Each host is act as an independent router.

4. Network interface hosts use wireless RF transceivers.

6. Number of nodes can be from 10 to 100 or at most 1000.

7. It is self-organizing in nature.

8. Multi-hopping is used.

Classification of Ad-Hoc Networks[6]

There are two types of classification available in Ad-Hoc networks which are as following:

1. Single-Hop

2. Multi-Hop

Single-hop: In this hop nodes are in direct communication and both nodes are in range of each other's. The chances of link failure are more in this hop.

Multi-hop: In this hop nodes are communicate with the help of internal nodes not directly. To reach from source to destination internal nodes participate.

1.1.2.1 Wireless Sensor Networks

Recent advances in wireless communications, digital electronics, and analog devices have enabled sensor nodes that are low-cost and low-power to communicate untethered in short distances and collaborate as a group. These sensor nodes leverage the strength of collaborative effort to provide higher quality sensing in time and space as compared to traditional stationary sensors, which are deployed in the following two ways :

• Sensors can be positioned far from the actual phenomenon, i.e., something known by sense perception. In this approach, large sensors that use some complex techniques to distinguish the targets from environmental noise are required.

• Several sensors that perform only sensing can be deployed. The positions of the sensors and communications topology are carefully engineered. They transmit time series of the sensed phenomenon to the central nodes where computations are performed and data are fused.

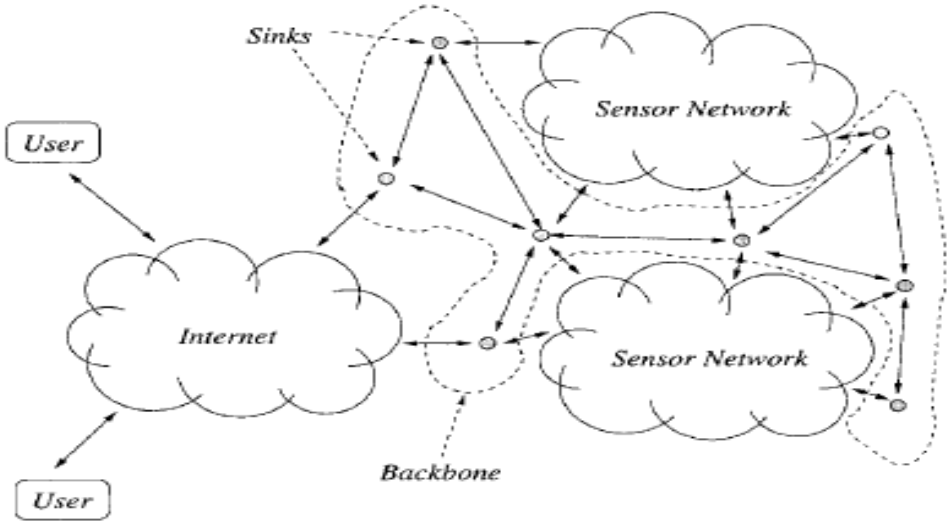


Figure 4. Internetworking between Senor Nodes and User

Sensor networks are also large collections of nodes. Individually, each node is autonomous and has short range; collectively, they are cooperative and effective over a large area. A system composed of many short-range sensors lends itself to a very different set of applications than one that uses a small number of powerful, long-range sensors. The sensor

nodes are deployed either inside the phenomenon or very close to it. They may self-organize into clusters or collaborate together to complete a task that is issued by the users. In addition, the positions of these nodes do not need to be predefined. As a result, the sensor nodes are fit for many applications, e.g., location tracking and chemical detection in areas not easily accessible. Since sensing applications generate a large quantity of data, these data may be fused or aggregated together to lower the energy consumption. The sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data. In essence, wireless sensor networks with these capabilities may provide the end users with intelligence and a better understanding of the environment. In the future, the wireless sensor networks may be an integral part of our lives, more so than the present-day personal computers.

The distributed (but wired) sensor network produces local observations using short-range sensors. While the system is temporally continuous, it is spatially sparse, and therefore cannot be used to sense phenomena at a greater resolution than several miles. This is an important and fundamental limitation: each sensor site requires a support infrastructure, including connections to the power and communications grids. The high overhead cost makes spatially dense sensing prohibitively impractical. Wireless sensor networks can address the issue of observing the environment at close range, densely in space, and frequently in time. This has the potential to reveal previously unobservable phenomena in the physical world, making sensor networks attractive to a broad spectrum of scientists

1.1.2.2 Wireless Mesh Networks

Wireless Mesh Network (WSN) is a promising wireless technology for several emerging and commercially applications, e.g., broadband home networking , community and neighbour-hood networks , coordinated network management, intelligent transportation systems. It is gaining significant attention as a possible way from Internet service providers (ISPs) and other end-users to establish robust and reliable wireless broadband service access at a reasonable cost. WMNs consist of mesh router and mesh clients as shown in fig : 5. In this architecture , while static mesh routers form the wireless backbone, mesh clients access the network through mesh routers as well as directly meshing with each other.

Different from traditional wireless networks, WMN is dynamically self-organized and self-configured. In other words, the nodes in the mesh network automatically establish and maintain network connectivity. This feature brings many advantages for the end-users, such as low up-front cost, easy network maintenance, robustness and reliable service coverage. In addition, with the use of advanced radio technologies ,e.g., multiple radio interfaces and smart antennas, network capacity in WMNs is increased significantly. Moreover, the gateway and bridge functionalities in mesh routers enable the integration of wireless mesh networks with various existing wireless networks, such as wireless sensor networks, wireless-fidelity (Wi-Fi), and WiMAX. Consequently, through an integrated wireless mesh network, the end-users can take the advantage of multiple wireless networks.

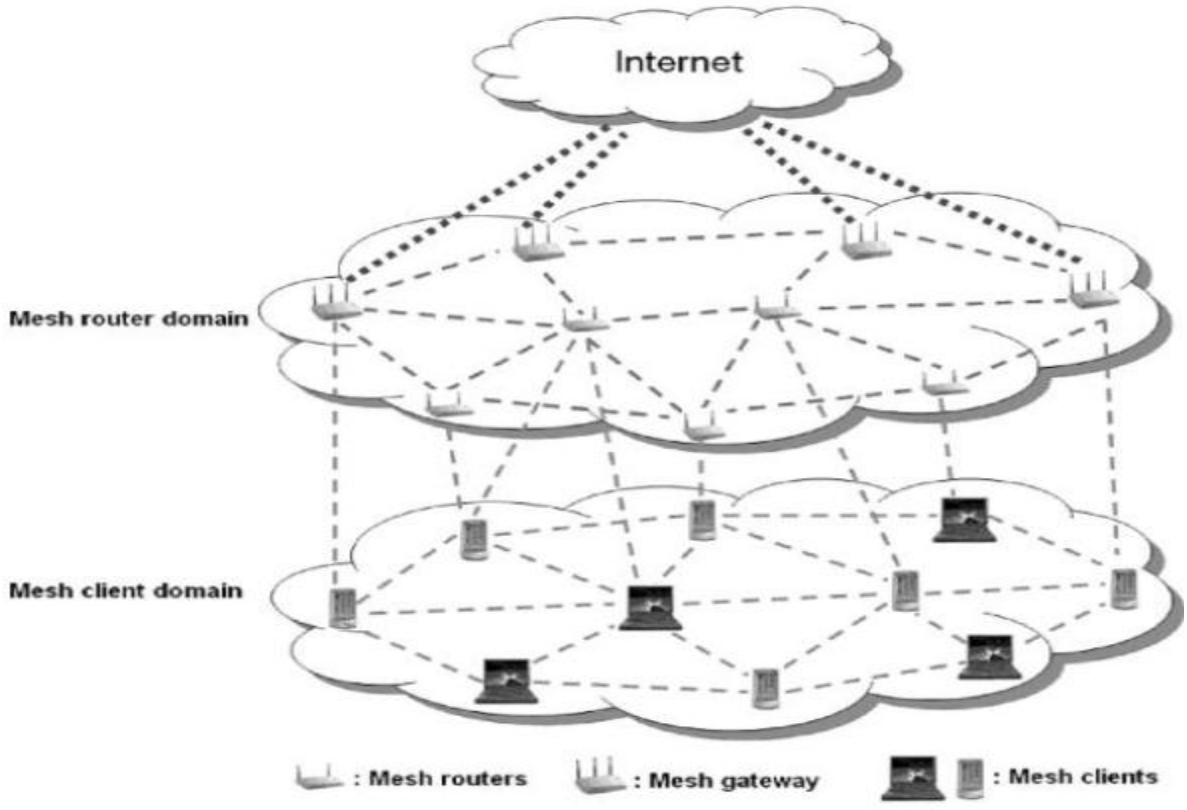


Figure 5. Wireless Mesh Network

Some of the benefits and characteristics of wireless mesh networks are highlighted as follows:

Increased Reliability : In WMNs, the wireless mesh routers provide redundant paths between the sender and the receiver of the wireless connection. This eliminates single point

failures and potential bottleneck links, resulting in significantly increased communications reliability.

Low Installation Cost: Recently, the main effort to provide wireless connection to the end-users s through the deployment of 802.11 based Wi-Fi Access points (Aps) and very expensive to deploy Aps .On the other hand, constructing a wireless mesh network decreases the infrastructures costs, since the mesh network requires only a few point of connection to the wired network. WMN can enable rapid implementation and possible modification of the network at a reasonable cost, which is extremely important in today's market place.

Large Coverage Area: Currently, the data rates of wireless local area networks (WLANs) have been increased, e.g., 54Mbps for 802.11a and 802.11g, by utilizing spectrally efficient modulation schemes. Although the data rates of WLANs are increasing, for a specific transmission power, the coverage and connectivity of a LANs decreases as the end-user becomes further from the access point.

Automatic Network Connectivity: WMNs are dynamically self-organized and self-configures. In other way, the mesh clients and routers automatically establish and maintain network connectivity, which enables seamless multi-hop interconnection service. Furthermore, the existing mesh routers reorganize the network considering the newly available routes and hence, the network can be easily expanded.

1.2 MANET

MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. It can be composed either by mobile nodes or by both fine-tuned and mobile nodes. Nodes are arbitrarily connected with each other and composing arbitrary topology. They can act as both routers and hosts. They have ability to self-configure makes this technology opportune for provisioning communication to, for example, disaster-hit areas where there is no communication infrastructure or in emergency search and rescue operations where a network connection is exigently required. In MANET routing protocols for both static and dynamic topology are utilized. To transfer the data between source and destination it follows a routing technique. A mobile host may not be communicate with the destination node directly in a single hop network design, in this view it should occur the multi hop scenario

,where the packets can be sent through several nodes which acts as the intermediate between source and destination. We can trace the location of the concrete node by the task of location vigilant routing protocols.

An ad hoc network is a wireless network describe by the nonexistence of a centralized and fine-tuned infrastructure. The absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks. Therefore, we refer to a wireless ad hoc network with mobile nodes as a Mobile Ad Hoc Network. In a MANET, mobile nodes have the capability to accept and route traffic from their intermediate nodes towards the destination, i.e., they can act as both routers and hosts. More frequent connection tearing and re-associations place an energy constraint on the mobile nodes.

1. AODV (Ad-Hoc On-Demand Distance Vector
2 DSDV (Destination Sequence Distance Vector
3 DSR (Dynamic Source Routing)
4 OLSR (Optimized Link State Routing)
5 WRP (Wireless Routing Protocol)
6 ZRP (Zone Routing Protocol)

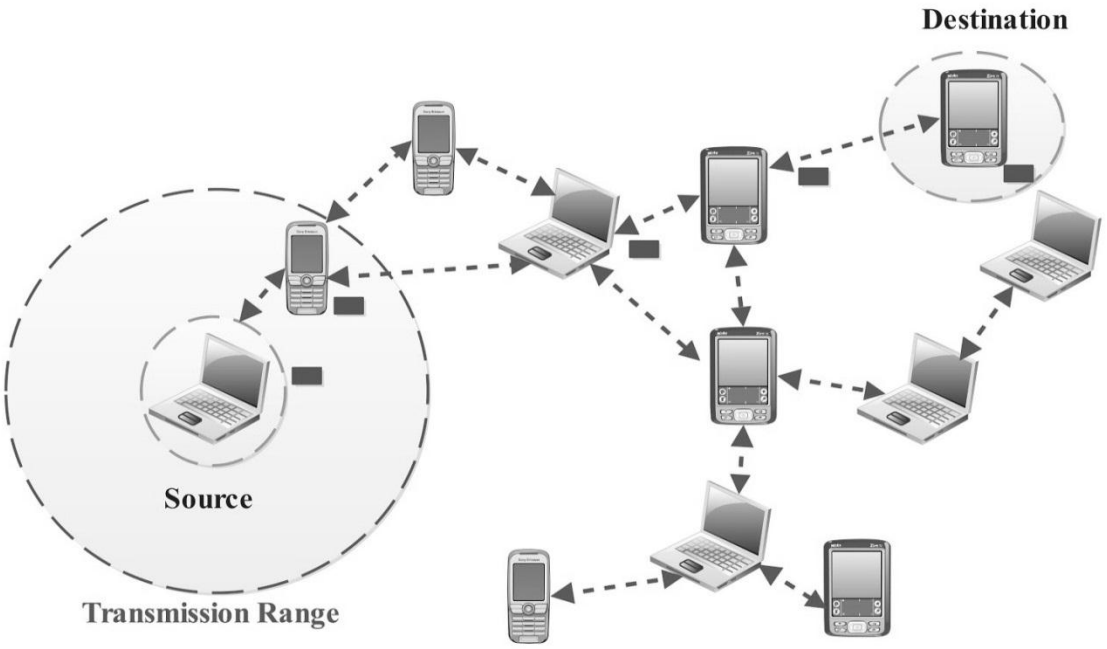


Figure 6. Diagram of MANET

In MANETs, accumulation of mobile nodes may dynamically vary the topological structure. With veneration to the more widely used mobile cellular networks .Mobile Ad Hoc Networks do not utilize any form of fine-tuned infrastructure or centralized administration. These types of networks have the salient characteristics: dynamic topologies, bandwidth constraints, variable capacity links, inhibited physical security and energy –constrained operations [7].

1.2.1 Characteristics of MANET:

There are some characteristics which define strength of MANET:

- **Dynamic Topology** : MANET is made up of mobile nodes, for this any node can be frequent change so any random or dynamic topology required to establish communication.
- **Multihop Routing** : In Ad-Hoc multi-hop routing is very important factor,, Becsause one node want to broadcast its packet information to destiantion nodebeyond its scope outside networkrange.packet should pass with number of intermediate or neighbour node.
- **Energy Constrained Operation** : Some or all MANET nodes relay on batteries so important challenges is to design the system to consume law battery power.
- **Limited Bandwidth** : Bandwidth is law compare to wired network is law due to stale routes ,various noise, distortion and fadding effect.
- **Limited Physical Security** : Bandwidth is lw compare to wired network is law due to stale routes, various noise, distoration and fadding effect.
- **Autonomous (Region or Orgiation) Node (Terminal)** : In MANET each node is act as host and router depend on the situation of communication so it is called Autonomous System (AS).

1.2.2 Types of Mobile Ad-hoc Network

Vehicular ad-hoc networks (VANET) are used for communication among vehicles and between vehicles and roadside equipment. Intelligent vehicular ad-hoc networks are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents etc. internet based Mobile Ad-hoc Networks (MANET) are ad-hoc networks that link mobile nodes and fixed internet-gateway nodes.

Table 1. Mobile Ad-hoc Network Types:

Technology	**Bitrate**	**Frequency**	**Range(meters)**	**Power consumption**
IEEE 802.11b	1,2,5.5 and 11 Mbit/s	2.4 GHz	25-100 indoor 100-500 Outdoor	30 mW
IEEE 802.11g	Up to 54 Mbit/s	2.4 GHz	25-50 indoor	79 mW
IEEE 802.11a	6,9,12,24,36,49 and 54 Mbit/s	5 GHz	10-40 indoor	40mW,250 mW
IEEE 802.15.1	1 Mbit/s	2.4 GHz	10-100 indoor	1mW
IEEE 802.15.3	110-480 Mbit/s	3-10 GHz	10-10	100mW, 250mW
IEEE 802.15.4	20, 40 or 250 Kbit/s	868 MHz, 915 MHz or 2.4 GHz	10-100	1 mW
HiperLAN2	Up to 54 Mbit/s	5 GHz	30-150	200 mW or 1W
IrDA	Uo to 4 Mbit/s	Infrared 850 nm	10	Distance Based
Home RF	1 mbit/s (v 1.0) 10 Mbits/s (v 2.0)	2.4 GHz	50	100mW
IEEE 802.16	32-134 Mbit/s	10-66 GHz	2-5 km	Complex power
IEEE 802.16a	Up to 75 Mbit/s	<11 GHz	7-10 km	Control
IEEE 802.16e (Broadband Wireless)	Up to 15 Mbit/s	<6 GHz	2-5 km	

1.2.3 Applications of Mobile Ad-hoc Network

There is no clear picture of what these networks will be used for. The suggestion varies from document sharing at conference to infrastructure enhancement and military applications. In areas where no infrastructure is available, an ad-hoc network could be used by a group of wireless mobile hosts. Other examples include business associates wishing to share files or a class of students needs to interact during a lecture. If each mobile host wishing to communicate is equipped with a wireless local area network interface, the group of mobile hosts can form an ad-hoc network. Access to internet and access to the resources in the network such as printer, will probably be supported.

Table 2. Mobile Ad-Hoc Network Application

Application	**Possible Scenaario**
Tactical networks	• Military communication • Automated battlefield
Emergency services	• Search and rescue operation • Disaster recovery • Policing and fire fighting • Supporting doctors and nurses in the hospital
Commercial and civilian environment	• E-commerce • Dynamic database access, mobile offices • Vehicular services: taxi cab network, road or accident guidance • Sports stadium, trade fair, shopping malls
Home and enterprise networking	• Home/office wireless networking • Conference, meeting rooms • Personal area networks • Network at construction site
Education	• Universities and campus setting • Virtual class rooms

	• Ad-hoc communication during meetings or lectures
Entertainment	• Multi user games • Wireless P2P networking • Outdoor internet access • Robotic pets • Theme parks
Sensor networks	• Home appliances • Body area network • Data tracking of environment conditions
Coverage extension	• Extending cellular network access • Linking up with the internet, intranet etc.

1.3 Routing Protocol in MANET

Routing protocol specifies how to communicate with the help of routers. It shares information among intermediate nodes then with the whole network. It helps to search shortest route from source to destination . There are mainly two types of routing protocol available. These are as following:

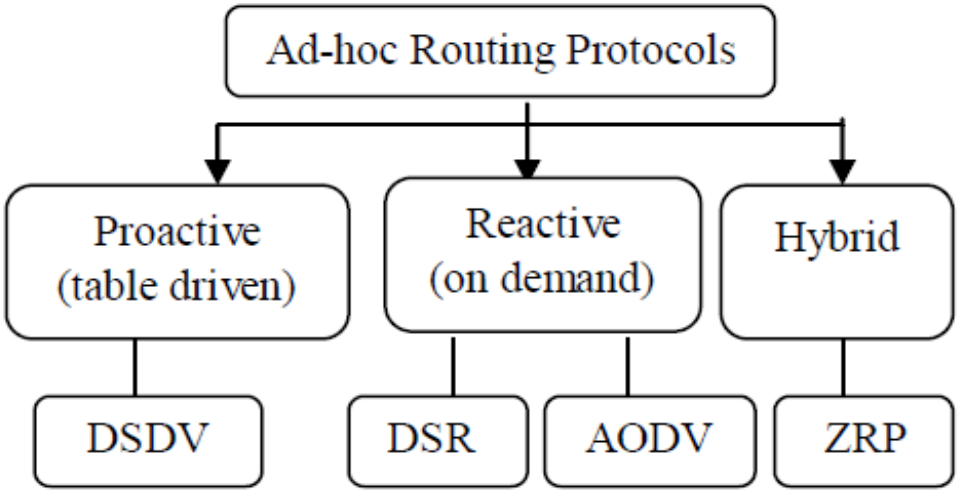


Figure 7. Ad-Hoc Routing Protocol

1.3.1 Proactive Routing Protocol

Proactive protocol contains fresh list of the route and their destination from source. In this type of protocol one node contains more than one table for each node in the network. All the nodes are update regularly. If the topology frequently changes than update information propagate to every node of the network and update table.

1.3.1.1 Destination Sequence Distance Vector (DSDV):

It is table driven routing protocol. It is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements. The sequence number is used to distinguish stale routes from new ones and to avoid the loops formation. Every node maintains a routing table that have lists of all available destinations, the assigned sequence number by the destination node and the number of hops to reach the destination . If a significant change has occurred in its table from the last update a station also transmits its routing table. If two routes have the same sequence number then the route with the shortest route is used.

The periodically stations transmit their routing tables to their immediate neighbours. DSDV does not support multi-path routing. It provides shortest path of good quality, trust worthy and cooperative.

1.3.1.2 Wireless Routing Protocol (WRP):

It is a routing protocol based on distance vector routing protocol. Each node in the network maintains a Routing table, Distance table, a Link-Cost table and a Message Retransmission list. The Message Retransmission list (MRL) contains in order to let a node know which of its neighbour has not acknowledged of update message and to retransmit update message to that neighbour. The node is required to send an idle Hello message to ensure connectivity If there is no change in routing table since last update to receive an update message the node modifies its distance table and looks for better paths using new information.

1.3.1.3 Clustered head gateway Switch Routing Protocol (CHGSRP):

It uses the basis of DSDV Routing algorithm .The node are aggregated known as clustered and a cluster-head is elected according to election algorithm. All nodes belong to its cluster that are in the communication range of the cluster–had. A gateway node is the node that is in the communication range of two or more cluster head. By using LCC when two cluster heads

come into the contact or when a node moves out of contact of all other cluster-heads only change.

1.3.1.4 Zone-Based Hierarchical Link State Routing Protocol (ZHLSRP):

Network is divided into non-overlapping zones in this protocol. ZHLS defines two level of topologies Zone level & node level. A node level topology tells how nodes are connected to each other physically of a zone. Zone level tells how zones are connected. A node LSP of a node contains its neighbour node information and is propagated with the zone where as a zone LSP contain the zone information and is propagated globally. It comes under hybrid category.

1.3.2 Reactive Routing Protocol

It is on-demand a reactive type routing protocol. It is idle approach in which all the node are not comprises the information of the all the nodes and keeps table only on demand. To find the path route discovery process is follow. Reactive routing protocols are bandwidth effective. In this, routes are built as and when they are required. This is achieved by sending route requests across the network. There are shortcomings with this protocol that it offers high latency when finding routes and other is the possibility of network clog when flooding is extreme. In this thesis, we considered AODV, DSR [6]

1.3.2.1 Ad-Hoc On-Demand Distance Vector (AODV):

AODV is an on-demand routing protocol utilized in ad hoc networks. This protocol is like any other on-demand routing protocol which facilitates a smooth adaptation to transmutations in the link conditions. In case when a link fails, messages are sent only to the affected nodes. With this information, it enables the affected nodes invalidate all the routes through the failed link. AODV has low recollection overhead, builds unicast routes from source to the destination and network utilization is less. There is least routing traffic in the network since routes are built on demand. When two nodes are in an ad hoc network wish to establish a connection between each other, it will permit them build multi-hop routes between the mobile nodes involved. It is loop free protocol which uses Destination Sequence Numbers (DSN) to avoid counting to illimitability. This one is the distinguishing feature of this protocol. Requesting nodes in a network send Destination Sequence Numbers (DSNs)

together with all routing information to the destination. It culls the optimal route predicated on the sequence number [7].

AODV defines three messages: Route Requests (RREQs), Route Errors (RERRs) and Route Replies (RREPs). These messages are used of UDP packets to discover and maintain routes across the network from source to destination. Whenever there is need to produce a new route to the destination, the node which is requesting broadcasts Route Requests. A Route is determined when this message reaches the next hop node (intermediate node with

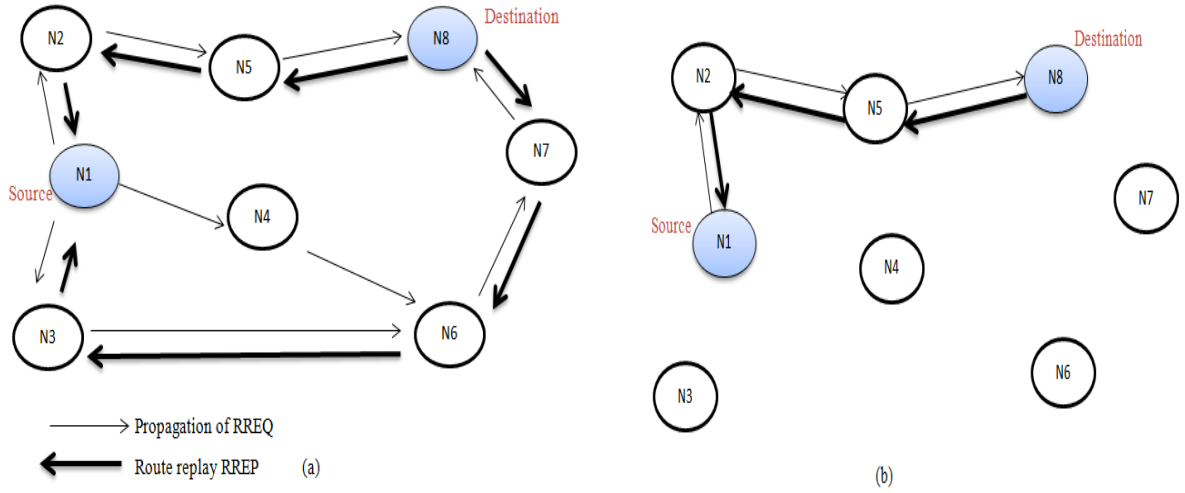


Figure 8. Propagation of RREQ (b) Reverse path with minimum Hop-Count

routing information to the destination) or the destination itself and the RREP has reached the originator of the request. Routes from the originator of the RREQ to all the nodes that receive this message are cached in these nodes. When a link failure occurs, Route Errors (RERRs) message is generated [7].

In the figure 1.5 N1 nodes broadcasts the packets to its neighbour nodes with RREQ and update its table. Then these nodes further forwards packets to its neighbour until the destination find outs and fresh route ascertain. Each node maintains its sequence number and broadcast ID. For every RREQ the node initiates broadcast ID which is incremented and together with the node's IP address, uniquely identifies an RREQ. At last that route will be the final route that has the minimum hop count from source to destination.

1.3.2.2 Dynamic Source Routing (DSR):

DSR is reactive type of protocol.The indentical features of DSR is source routing in which all mobile node maintain route cashes that preserve the source routes of which all mobile node know (aware). All caches updates for new learned routes 2 Major phase. I] Route Discovery II] Route Maintenance

In DSR when On-Demand route reqquirement comes first it willl check route caches for preevious route information to destionation. If trhe previous route link is expire then route discovery is establish and forward new RREQ. Route maintenance is accomplished when route error and acknowledgement came for fatal transmission problem.

Table 3. Comparison of Reactive Protocol

Qualitative Metrics	**AODV**	**DSR**
Loop Free	Yes	Yes
Reactive Behaviour	Yes	Yes
Security	No	No
Support for Unidirectional Links	No	No
Sleep Mode	No	No
Multicasting	Yes	No
Routing scheme	Flat	Flat
Nodes with special tasks	No	No
Routing Metric	Shortest Path	Shortest Path

1.4 Attacks on MANET [8]:

There are a variety of attacks possible in MANET. The attacks can be classified as active or passive attacks, internal or external attacks, or different attacks classified on the basis of different protocols. A passive attack does not disrupt the normal operation of the network.

The attacker only snoops the data exchanged in the network without altering it. It includes Eavesdropping, jamming and traffic analysis and monitoring. In case of active attacks, the attacker attempts to alter or destroy the data being exchanged in the network. This attack disrupts the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks .The ultimate goals of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, authentication, non-repudiation, and availability to mobile users.

There are two types of attacks are present in MANET which breach security of network:

1. Passive attack
2. Active attack

1. Passive attacks: A passive attack obtains data switched in the network without disturbing the communications operation. The passive attacks are difficult to detection [4] . This attack target confidentiality attribute of the system. It include accessing network traffic between browser and server accessing restricted information on a website. Examples of Passive Attacks are eavesdropping, snooping.

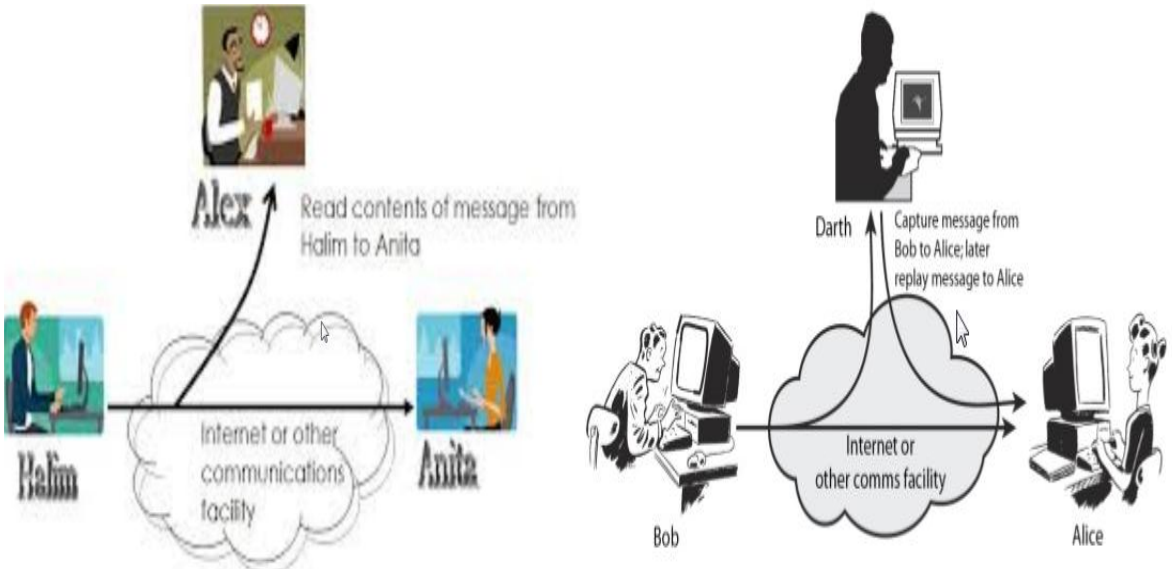


Figure 9. (a) Passive Attack, (b) Active Attack

2. Active attacks:

An active attack in which any data or info is interleaved into the network so that information and procedure may harm [4]. It involves modification, fabrication and disruption and affects the operation of the network. Example of active attacks is impersonation, spoofing [10].

Other types of attack are as follow:

1. Internal attacks:

Internal attacks are as of compromised nodes that are part of the set of connections. In an internal attack from the network the malicious node gains unauthorized access and behave as a genuine node. Traffic can be analyse between other nodes and may participate in the activities of other networks [6].

2. External attacks:

The external attack is conceded out by the nodes which do not belong to network. It may cause unavailability and congestion by sending false information for the network [12].

3. Black-hole attacks:

In blcak-hole attack malicious node use its routing protocol to know other node that it has shortest path towards destinationand attacker drop the packet to reduce the quantity of information is available to other node. This type of attack made intentionaly for deniall of service type attack. This make destination system unreachable or shutdown in network.

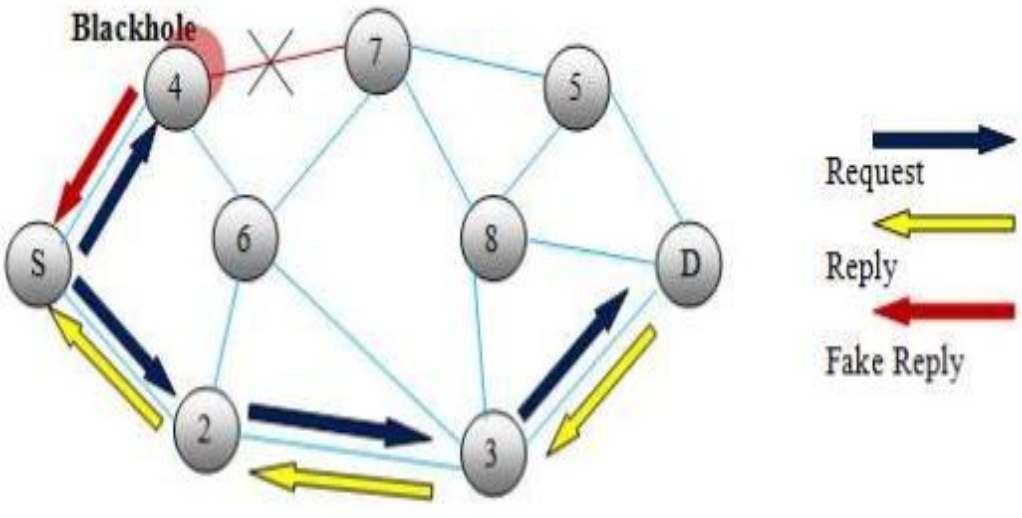


Figure 10. Black-Hole Attack

4. Worm-hole attacks:

The worm hole attack is quite tipical and merciless attacks, which can be executed in MANET. In this type of attack message is captured from the one region of network and replaying in other region. Attacker creates tunnel between two node which participate for communication. One attacker gather all message and other attacker replay to misinterprate to make destination unrechable from network.

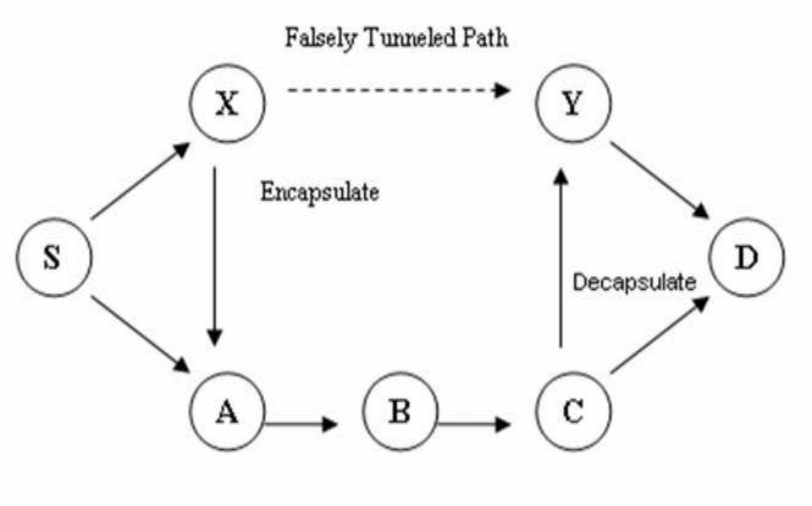


Figure 11. Worm-hole Attack

5. Gray hole Attack:

The gray hole attack is also termed as misbehaving attack. In this attack, the attacker selectively drops the packet with certain probability. Also, in this attack the intruder node behaves maliciously for the time it selectively drops the packets and then switches to its normal behavior.

6. Byzantine attack:

In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services.

7. Information Disclosure:

An attacker may leak the confidential or important information to unauthorized nodes present in the network. The secret information may the information about network topology, geographic location of nodes or optimal routes to authorized nodes in the network.

8. Resource Consummation attack:

In this attack, an attacker attempts to consume or waste away resources of other nodes present in the network. The resources can be the battery power, bandwidth, and computational power, which are only limitedly available in ad hoc wireless networks. An attacker can consume the batteries by requesting routes and unnecessary packet forwarding to the nodes.

1.5 Selective Packet Drop Attack

Selective Packet drop attack is the type of denial of service attack. Packet dropping attack is launched on the forward phase. So it is very complex and difficult to isolate. This attack is very easy to perform but very difficult to detect it. Selfish node also drop packet in their different ways. They drop packets only to save their resources not damage any other nodes. Selective forwarding attacks may damage some mission of applications. In these types of attacks, malicious nodes act as normal nodes every time but selectively drop sensitive packets, such as packet coverage the movement of the differing forces. Such selective dropping is tough to detect. Counter measures to selective forwarding attacks cannot recognize malicious nodes or need time synchronization.

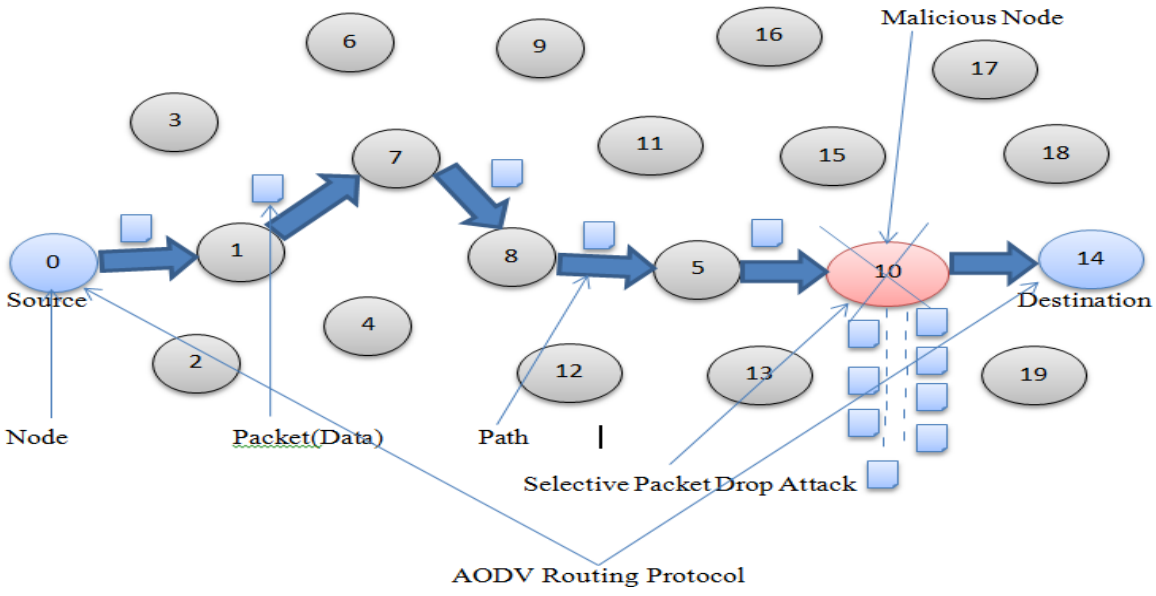


Figure 12. Selective Packet Drop Attack

Selective forwarding attacks can root serious threats on many applications. Selective forwarding attacks have some nodes which drop some or all packets. Attacker can initiate the selective forwarding attack and crash a portion of packets for which it require to store set while forward the rest. Selective forwarding attack is complex attack to detect, since packet drops in sensor networks may be caused by untrustworthy wireless communications or node failures.

Selective Packet drop is only possible when jamming attack is unsuccessful. Once the packet is expected by the compromised node, it can examine the packet headers, categorize the packet, and decide whether to forward it or not. This action is known as misbehaviour . Post-reception dropping is fewer bendy than selective jamming because the challenger is limited to dropping only the packets routed through it.

Selective policy known as the Jellyfish attack which is a compromised node that is occasionally drops a small part of consecutive packets and can be efficiently reducing the throughput of a TCP flow to near zero. This attack can be achieve even by remind random delays to TCP packets, without dropping them, while left over protocol compliant. Similar selective dropping attacks can be construct for other network functions such as the association/de-association of STAs, and topology management .

1.5.1 Migration of Selective Dropping:

Selective dropping attacks can be mitigated by employing fault-tolerant mechanisms at a variety of layers of the protocol stack. At the routing layer, multi-path routing provides tough multi-hop communication in the occurrence of association faults, by utilizing more than one path from a source to a destination. A selective dropper can always feature his losses to congestion, in order to avoid detection as a malicious node. In this case, classification mechanisms employing long-term statistics, can accurately pinpoint selective droppers.

1.5.2 Identification of Selective Droppers:

There are three methods under this technique. These methods are:

1. Reputation Based System
2. ACK based System
3. Credit Based System

In Reputation systems identify misbehaving nodes based on per-node reputation metrics, computed based on interactions of each node with its peers. These systems typically incorporate two critical operations. These operations are as follow:

(a) The collection of accurate observations of nodes' behavior
(b) The computation of the reputation metric.

In ACK-based scheme which is differ from overhearing techniques in the method of collecting first-hand behavioral observations. Downstream nodes are dependable for acknowledging the reception of messages to nodes several hops upstream. These systems are appropriate for monitoring the exact relay of unicast traffic, at the expense of communication overhead for relaying a supplementary set of ACKs. ACK-based schemes cannot be used to recognize insiders with the purpose of selectively fall broadcast packets. Such packets stay, in general, unacknowledged in wireless networks, to keep away from an ACK implosion situation. Moreover, a small set of colluding nodes can still offer real ACKs to upstream nodes while dropping packets.

In Credit-based systems alleviate selfish behavior by incentivizing nodes to forward packets. Nodes that relay traffic obtain credit in return, which can be later used up to promote their own traffic. However, in the context of WNMs, MPs do not produce any traffic of their own, but act as dedicated relays. Hence, compromised MPs have no incentive for collecting credit. Furthermore, in the case of selective dropping attacks, misbehaving nodes can at rest collect sufficient credit by forwarding packets of low importance, while dropping a few packets of "high value." In addition, the credit collected by a particular node depends.

1.6 Diffie Hellman key exchange

Diffie Hellman was the first public key algorithm ever invented, in 1976. Diffie Hellman key agreement protocol is [29]:

- Exponential key agreement
- Allows two users to exchange a secret key
- Requires no prior secrets
- Real-time over an untrusted network

Definition of Diffie Hellman : Let n be a prime number and p be an integer. The Diffie Hellman Problem (DHP) is the problem of computing the value of p^{ab}(mod n) from the known values of p^a (mod n) and p^b(mod n).The setup of Diffie Hellman algorithm

- Suppose we have two parties Master and Slave, they want to communicate to each other.
- They do not want the eavesdropper to know their message
- Alice and Bob agree upon and make public two number n and p, where n is prime number and p is a primitive root mod n. Anyone has access to these numbers.

Table 4. private computations

Master	Slave
Choose a secret number a. Compute M≡ p^a (mod n)	Choose a secret number b Compute S≡ p^b(mod n).

- Public interchange of values.
- Master leads M to Slave ==M
- S= Slave sends S to Master
- Master compute the number K≡ $S^a \equiv (P^a)^b$ (mod n).
- Bob calculate the number K≡$M^b \equiv (p^b)^a$ (mod n).

Here Master and Slave have the same key that is K=p^{ab} (mod n).

In the Diffie-Hellman algorithm if two parties, say, Master and Slave wishes to exchange data, both agree on a symmetric key. Symmetric key is used for encryption or decryption the messages. We knows that Diffie Hellman algorithm is used for only key agreement or key exchange, but it does not used for encryption or decryption. Before starting the communication, secure channel is established. Both parties select their own random number. On the basis of the selected random numbers, secure channel and shared key is established.

Figure 13, shows that Master and Slave wants to communicate with each other. To start communication both parties need to establish secure channel. To establish secure channel, two random prime number p and n are selected, both devices are agreed on these two numbers. Selected p and n are the public numbers.

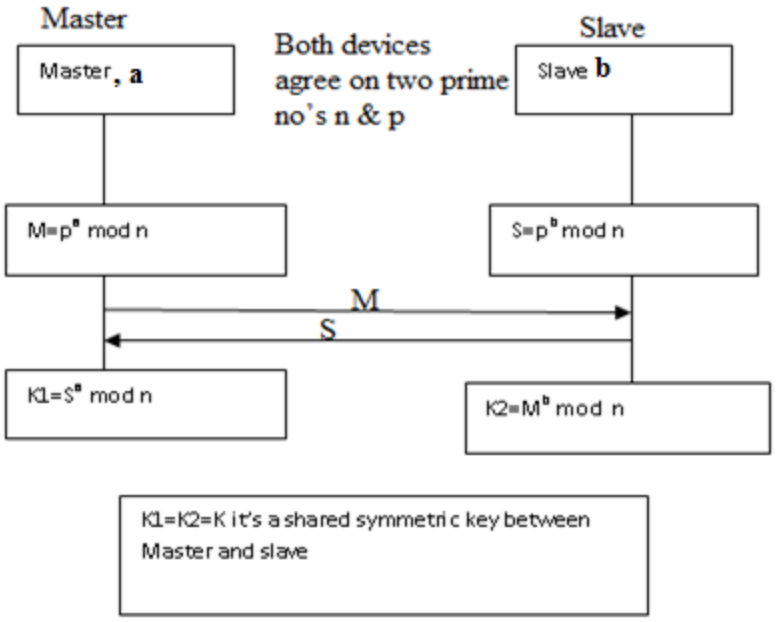


Figure 13. Diffie-Hellman Key Exchange

Both parties, say device 1 become master and device 2 become slave, both master and slave select their private numbers a' and 'b' respectively. Master and slave use their public and private number and calculated their private keys.

Master computes: Slave computes:

$M= p^a \bmod n$ **$S= p^b \bmod n$**

Now both master and slave exchange their private keys such as 'M' and 'S'. After getting 'M' and 'S', master and slave calculates the secret keys such as K1, K2.

From S, master computes: **$K1= S^a \bmod n$**

From M, slave computes: **$K2= M^b \bmod n$**

If both master and slave calculate same values of K1 and K2, then secure channel is established between them. The combination of K1 and K2 becomes the shared symmetric key between master and slave.

To encrypt the messages, they used the public key or shared key (K) of both parties. For decryption of messages private key of both parties which is randomly chosen by the users i.e. 'a' and 'b' are used.

CHAPTER 2

REVIEW OF LITERATURE

Thongchi Chuachan and Somnuk Puangpronpitag al. [13], proposed new methodology how to detect and prevent selective packet drop attack. In this paper they discuss 4 previous method to protect against 1.reputation bsed 2. Acknowledgement based 3. IDS based 4. Trusted based. The new proposed schema called challenge and response schema. It contain 2 phase I) Key distribution phase II) Challenge ad response phase . The message is encrypted using the public key and routed in two-hop neighbor, take ratio of local one compare it with neighbor node.The melocious node can be detect by setting thresold vlaue to cache and at the end this value to the nieighbours value. To simuate this result they use Commn Open Reserch Emulator (CORE).

Seung Yi and Robin Kravets et al. had discuss some previous mutual authentication schemes of mobile ad-hoc network. They proposed the symmetric key distribution schemes [9]. They explain PKI(Public key distribution) scheme which based on the symmetric key distribution scheme. In this paper author proposed a new authentication scheme named as MOCA which hybrid type of scheme and use both Public key exchange and asymmetric schemes for mutual authentication.

Pradeep kyasanur et al. proposed a protocol extension of 802.11 DCF protocol to detect the selfish behaviour of the nodes in MANET. The Selfish nodes incomes nodes which select the contentional window (CW) time such that all of its neighbour node cannot able to transmit the packet at the end at it degrade the network performance [10]. The proposed scheme has three mechanisms first one is that the receiver agrees that whether sender is diverting form protocol or not. Second is penalize ,in this schema sender is penalize if it is not able to submit the packet to the destination within the time period define in contention window to sender by receiver. Plenty means that in next time when sender sends that data they have to wait more to send data to receiver .The third mechanism is the diagnosis scheme receiver decide whether the sender is selfish or not on the basis of the total data send by the sender and number of times the sender pay plenty .if no of plenty paid by the sender is more than the

threshold value which is fixed then the sender is selfish and no more data is received form that sender.

Yixin Jiangand et al. In this they have proposed a new mutual authentication and key exchange protocol. In the proposed mechanism giving the identity anonymity and session key renewal. This protocol provides secure roaming services to the authentic user between the home and visiting agent or in short, this protocol offers secure handoff to the legitimate user [11]. The proposed protocol is based on the secrete splitting principle and self-certified scheme. The protocol works in two phases: First phase is the mutual authentication with anonymity when a legitimate user is roaming from the home agent to the visiting agent. The phase uses the temporal identity (TID) rather than the user's real identity. Second phase is the session key renewal phase which renews the shared key which is shared between the legitimate user and the serving agent.

Caimu Tang et al. discuss methodology for efficient authentication mechanisms which use by low-power devices. In this mythology only one way single packet transmit by mobile base station for mutual authentication. They used the trust delegation Mechanism by elliptic-curve-crypto system based to generated group pass code for mobile station authentication [12]. By using this authentication mechanism many active and passive attacks will be prevented including the denial of service attack. The mobile device authenticated with the visiting base station only by the exchange of one of the packet. This proposed mechanism is required less computations power and less message exchange delay as compares to other authentication schemes.

Ahmed M.Abd EL-Haleem and Ihab A.Ali et al. [14], Propose mythology to isolate packet dropping attack by using two disjoint routes protocol in MANET. In this technique two node disjoint routes are selected based in their trust value and use to routes from source to destination. They use DLL-ACK (acknowledgement) and end-to-end Tcp-Ack to identify and examining the behaviour of routing path, node. If any malicious node find in the path then path search engine tool get run and identify the malicious node and prevent it.

K.Sangeetha et al. [15], Propose technique to secure transmission in the MANET using Ad-Hoc on-Demand routing protocol (AODV). Due to lack of resource and infrastructure ad-hoc network is not able to prove logical operation. Proposed schema called Enhanced Adaptive

Acknowledgement (EAACK) which raises Integrity of IDS (Intrusion Detection System) by using digital signature. It reduces overhead which arise during routing in AODV protocol. In this paper they discuss some previous IDS based technique to identify and remove misbehaving node in network, i) watchdog II) TWOACK(two acknowledgement) III) AACK(end-to-end ACK) IV) S-ACK(secure acknowledgement) V) MRA(Misbehavior report authentication).

Bo Sun Yong et al. [16], In this paper they proposed a neighbor set based approach to detect black hole attack and **a** muting recovery protocol to mitigate the effect of black bole attacks. The demonstrated through simulation that this methods could effectively and efficiently detect black hole attack without introducing much routing control overhead to the network. The data shows when we simulate that packet throughput is being improved by at least **15%** and the false positive probability is usually less than **1.7%.** In the future, they would like to further explore whether there exists a non-cryptography based method to identify them and destination and the optimal detection and response mechanism to improve the packet throughput.

Kashyap Balakrishnan, Jing Deng, Pramod K. Varshney et al.[17] , proposed a new technique to prevent selfishness behavior of the node in MANET . They have discuss a technique called TWOACK . This technique will work with two network layer acknowledgement base schema to detect misbehaving node in network and prevent which work on top of any source routing protocol. E.g. DSR. Because before establishment of routes in network this technique will remove misbehaving node and improve network performance 20 % more. It improves packet delivery ratio and throughput.

Sushma Yalamanchi and K.V.Sambasiva Rao et al.[18], they had proposed a two phase authentication structure for wireless networks. They discus that in wired network use the authentication protocol which is having excessive computations but in wireless networks we require less computation and energy efficient authentication protocol. Because in wireless networks the hand held devices are having limited battery and constrained computational resources additionally wireless networks on suffer from packet losses and bit errors and offers low bandwidth. In the paper, they presents a two-stage authentication scheme for wireless networks that utilizes a computationally intensive but highly secure strong

authentication in Stage 1 and a lightweight symmetric key predicated protocol in Stage 2. The cost of the strong authentication adopted in Stage 1 is amortized over N sessions thus reducing the overall cost of the scheme. We adapt the Dual-signature predicated IKE authentication that we proposed in our earlier work and employ it as Stage 1 authentication. The Symmetric key protocol in Stage 2 authentication that we propose utilizes the symmetric keys that are engendered in Stage 1.

S. Sharmila and G. Umamaheswari et al.[19], discussed about the defensive mechanisms predicated on cumulative ack and energy predicated is proposed to detect selective forward attack in mobile wireless sensor networks. The scheme is evaluated in terms of packet distribution ratio and throughput. The attacker node is detected based on the ack and energy level of the node . The energy consumption of the detection scheme is less when compared with subsisting detection schemes. From the simulations, byte overhead is 0.39 percentages and detection precision is 80% are observed and thus incrementing the network throughput. These results show that the packets can be forwarded without any selective packet drop by minimizing the misbehaviour nodes in the network. The further enhancement of the proposed scheme is to amend the prosperity rate to 100% with sundry mobility and receiver sensitivity of the node.

Hui Xia, Zhiping Jia, Lei Ju ,Xin Li and Edwin H.-M. Sha et al.[20], proposed trust prediction model to evaluate the trustworthiness of nodes, which is based on the nodes' historical behaviors and fuzzy logic rules prediction method. As an application of the proposed trust model, extended from the ad-hoc on-demand multi-path distance vector routing (AOMDV) protocol, a trust-based reactive multi-path routing protocol, named as ad hoc on-demand trusted multi-path distance vector routing (AOTMDV) protocol, is proposed for MANETs. This new protocol provides a flexible and feasible approach to choose the shortest path that meets the security requirements of data packets transmission, malicious node detection in multi-agent systems and threat mitigation from those nodes. Extensive experiments have been conducted to evaluate the efficiency and effectiveness of the proposed mechanism in malicious node identification and attack resistance. Experimental results show that AOTMDV achieves a remarkable improvement in the packet delivery ratio, network throughput and malicious attack resistance.

Hung-Min Sun and Chiung-Hsun Chen and Yu-Fang Ku et al.[21], they propose an acknowledgment-based technique, called NACK, to detect and mitigate the dropping attacks. Moreover, NACK can resist the collusion attack by using the timestamp mechanism. Although NACK can resist successfully collusion attack, it only considers the case of two consecutive nodes.

Djamel Djenouri and Nadjib Badache et al.[22], propose a new solution to monitor, detect, and safely isolate such misbehaving nodes, structured around five modules: (i) The monitor, responsible for controlling the forwarding of packets, (ii) the detector, which is in charge of detecting the misbehaving of monitored nodes, (iii) the isolator, basically responsible for isolating misbehaving nodes detected by the detector, (iv) the investigator, which investigates accusations before testifying when the node has not enough experience with the accused, and (v) finally the witness module that responds to witness requests of the isolator. These modules are based on new approaches, aiming at improving the efficiency in detecting and isolating misbehaving nodes with a minimum overhead. They also mathematically analyze their solution and assess its performance by simulation, and compare it with the watchdog, which is a monitoring technique employed by almost all the current solutions.

CHAPTER 3

PRESENT WORK

3.1 Problem Formulation

In MANET inside and outside attacks are possible, which disgrace the performance of the network. In Inside attacks a node within the network become malicious node and it launched attacks on network. In outside attacks a malicious node which is outside the network, it become the member of the networks and then launched the attack on network. A passive outsider eavesdrops on all communication and aims to compromise privacy. Selective packet Drop attack is the partial denial of service attacks which is triggered by the malicious nodes in the network. In the past, many techniques have been proposed to isolate Selective attacks from the network. When this attack is triggered in the network, end to end delay increase as steady rate and throughput of the network reduced. In our work, we work on to detect and isolate Selective Packet Drop attack In AODV Protocol.

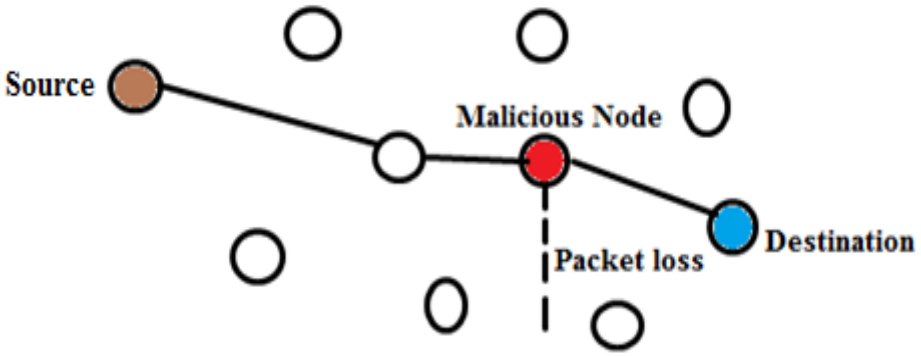


Figure 14. Show Packet Loss Due to malicious Node

In fig:12 there are nodes in the network one act as source and other act as destination. Suppose source sends packet from source to destination. It sends 10 packets. There is a malicious node at the centre which drops the packet and only forward few packets. This problem arise the packet loss problem. To overcome this problem a novel technique will be proposed that is Diffie-Hellman.

3.2 Objectives

Following are the various objectives of this research work:

1. The study focus on analysis of Selective packet Drop attack in MANET and its consequences.
2. To study the previously proposed plans suggested for counter measurement of Selective Packet Attack
3. The aim of the study to detect the Selective Packet Drop in MANET using AODV protocol.
4. Analysing the effects of Selective Packet drop attack in the light of Packet loss, throughput and end-to-end delay in MANET.
5. To propose new scheme to detect malicious nodes in the network which are responsible for triggering the Selective packet Drop attack in the Network.
6. Simulating the detection of Selective packet Drop attack using AODV protocol in MANET using NS-2 tool.

3.3 Research Methodology

Proposed technique is to detect packet drop attack in MANET and improve the performance of the network. The concept use in the proposed technique is based on the monitoring mode and key exchange technique. Our challenging schema is work in 2 parts. (I) Key exchange and (II) Monitoring mode technique.

We have embedded the Diffie Hellman key exchange algorithm authentication procedure. In network, it defines the source node and destination node. To establish secure channel between communicating parties, each party select a random prime number g and n, selected numbers become public keys of both parties. The source node become master and destination node become slave, master and slave select their private keys ‘a’, ‘b’ respectively. The master calculates new value “M” from their selected public and private numbers.

$M= g^a \bmod n$

The Slave calculates new value “S” from their selected public and private numbers

$S= g^b \bmod n$

The Master and slave exchange their calculated “M” and “S” values through intermediate nodes. When Slave receives “M” and Master receives "S” both parties will calculate mode inverse value.

When master receive value “S” from slave and calculate new value “K1” from the received “S” value.

$K1=S^a \bmod n$

Slave receives value “M” from master and calculates new value”K2” from the received “M”

$K2=M^b \bmod n$

After calculating “K1” and “K2”, both parties establish secure channel, by calculated new key “K”. If both communicating parties have same “K1” and “K2” values, secure channel is established between Master and Slave.

$K=K1+K2$

When secure channel is established between master and slave, communication starts between both parties. The communication between Master and Slave is encrypted with public keys. Each parties use their own private keys to decrypt the communication.

The following figuren explains the above work, how the embedded Diffie-Hellman works in network.

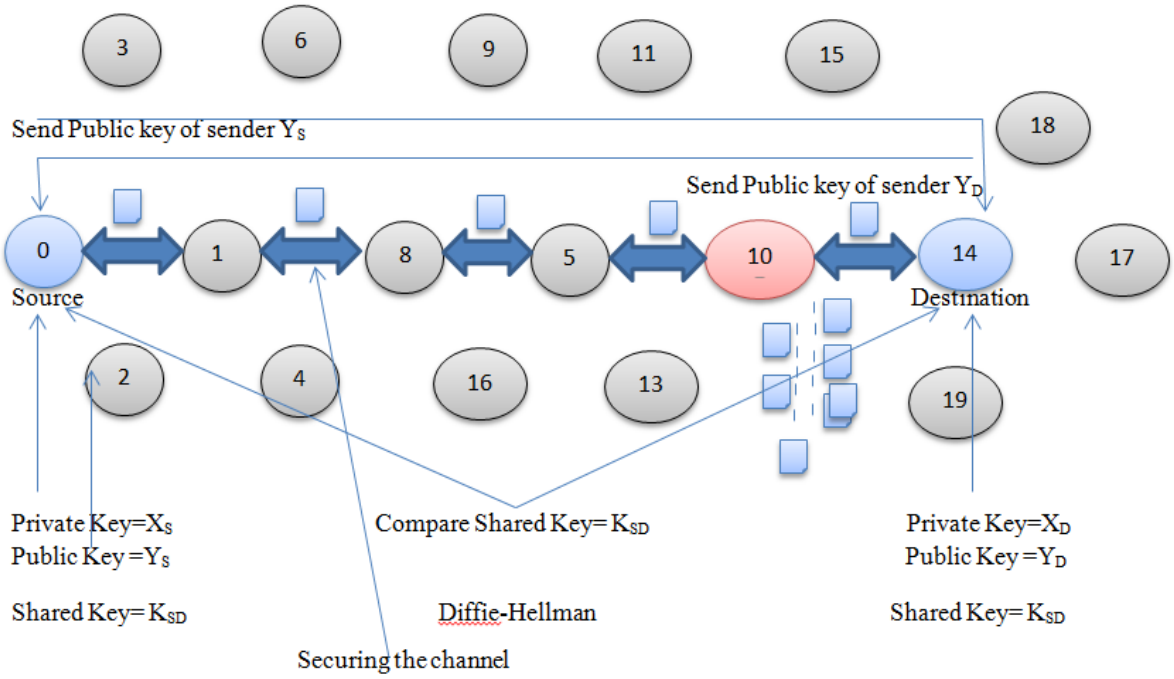


Figure 15. Key Scheduling Process

In the present work we have to apply Diffie-Hellman technique to detect malicious node in the network. First of all a secure channel will be established with the help of Diffie-Hellman technique. After the establishment of the channel, communication begins. Now source sends private key "A" to the source and when destination receive it, also send "B" to the source. When packet reaches to malicious node it does not have key "B". Then this path will not be established due to present of malicious node. Now another path will be choose for communication where there is no malicious node. The secure path will be established after the exchange of the key. Now sender and receiver match their shared key if it match then sender continue the communication towards the destination. If the shared key does not match then source flood the ICMP message in the network and call the monitor mode technique.

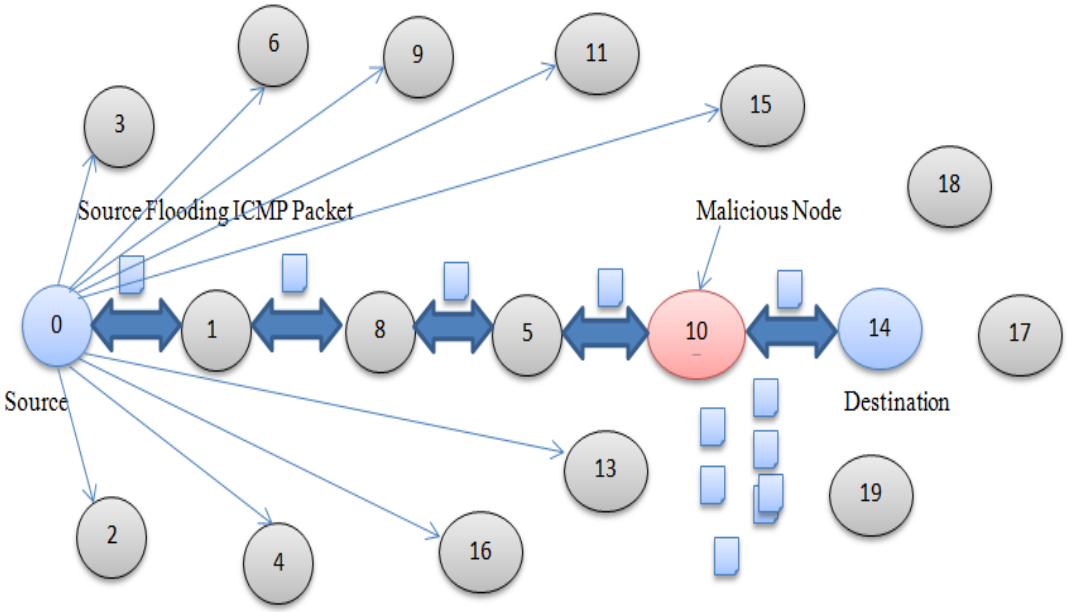


Figure 16. Flooding ICMP packets

Monitor Mode: When the source floods the ICMP packet all the node in the network apart from node who are participated in the routing become a passive node. This node starts the monitoring on the path which is use for routing. Each monitoring node send request to node which is in path. If the replay did not comes in particular time stamp it considered as malicious node and all the information about malicious node is send to the Source node. Now Source node deploy the new path and secure it by deffiee-hellman and communication start between the source and destination.

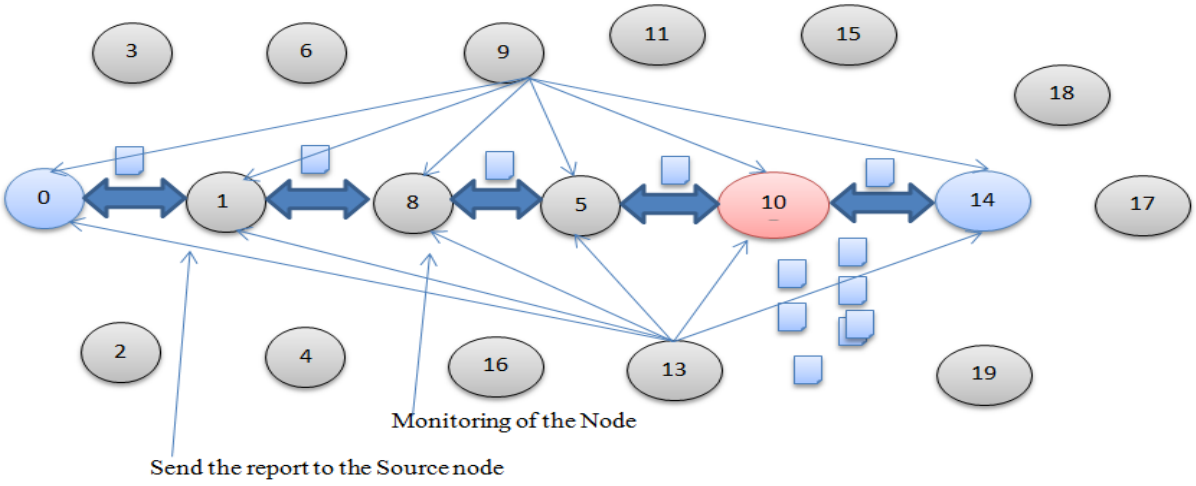


Figure 17. Initiate the Monitoring Mode Technique

3.3.1 Flow Chart

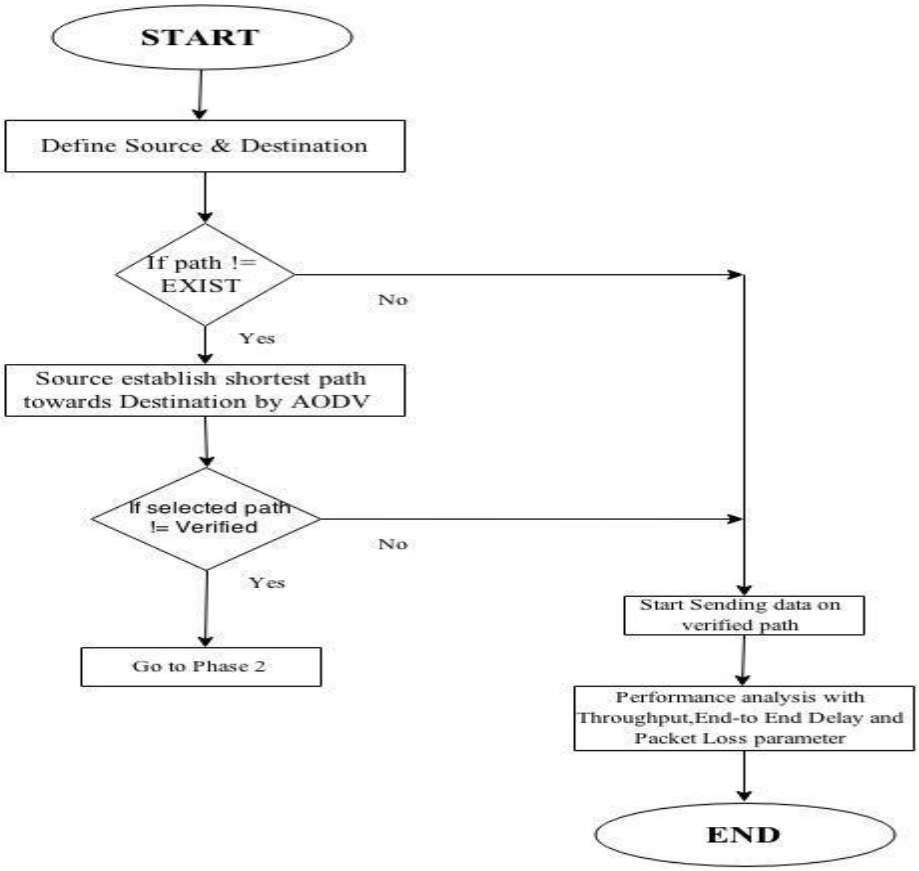


Figure 18. Phase 1 of KEAM Algorithm

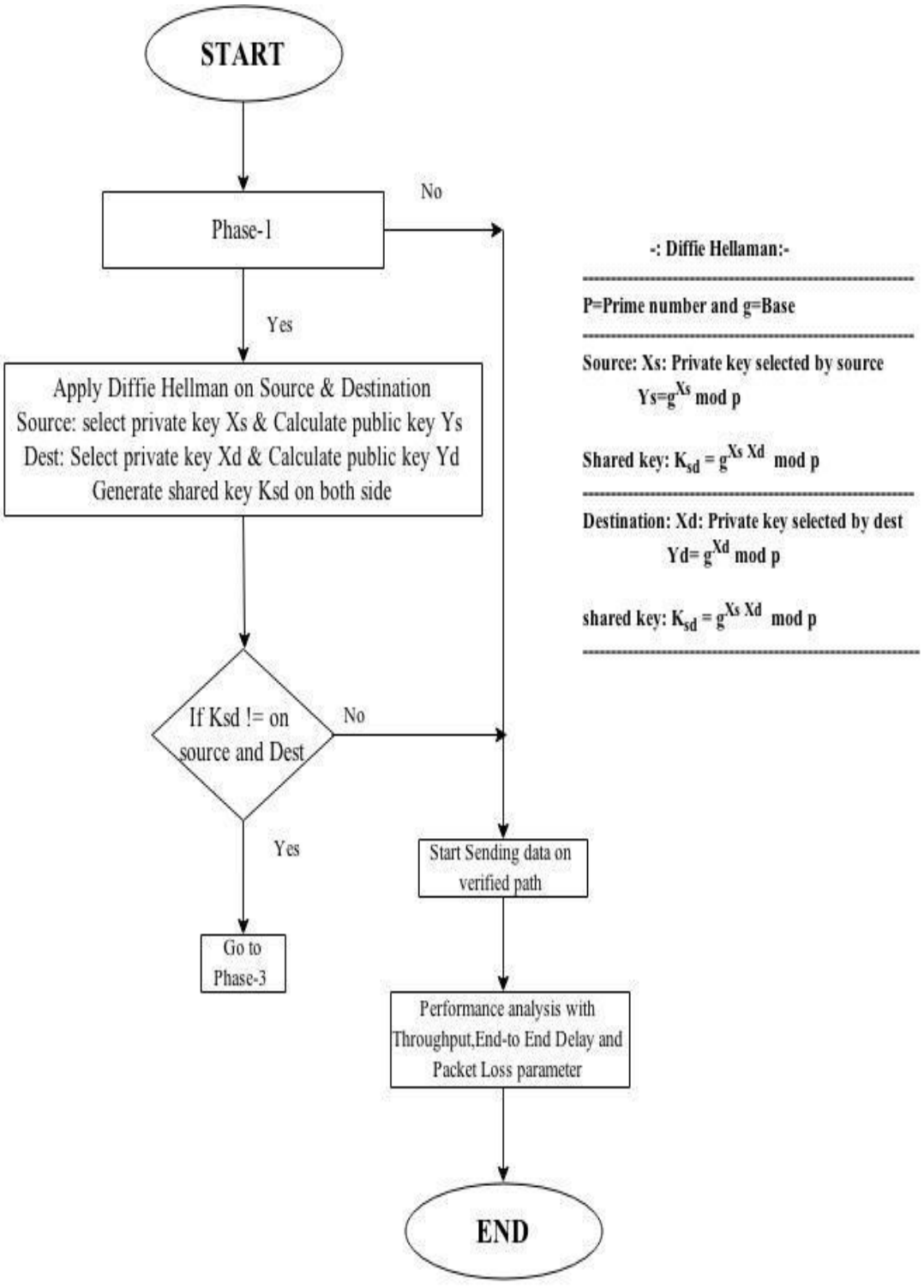


Figure 19. Phase 2 of KEAM Algorithm

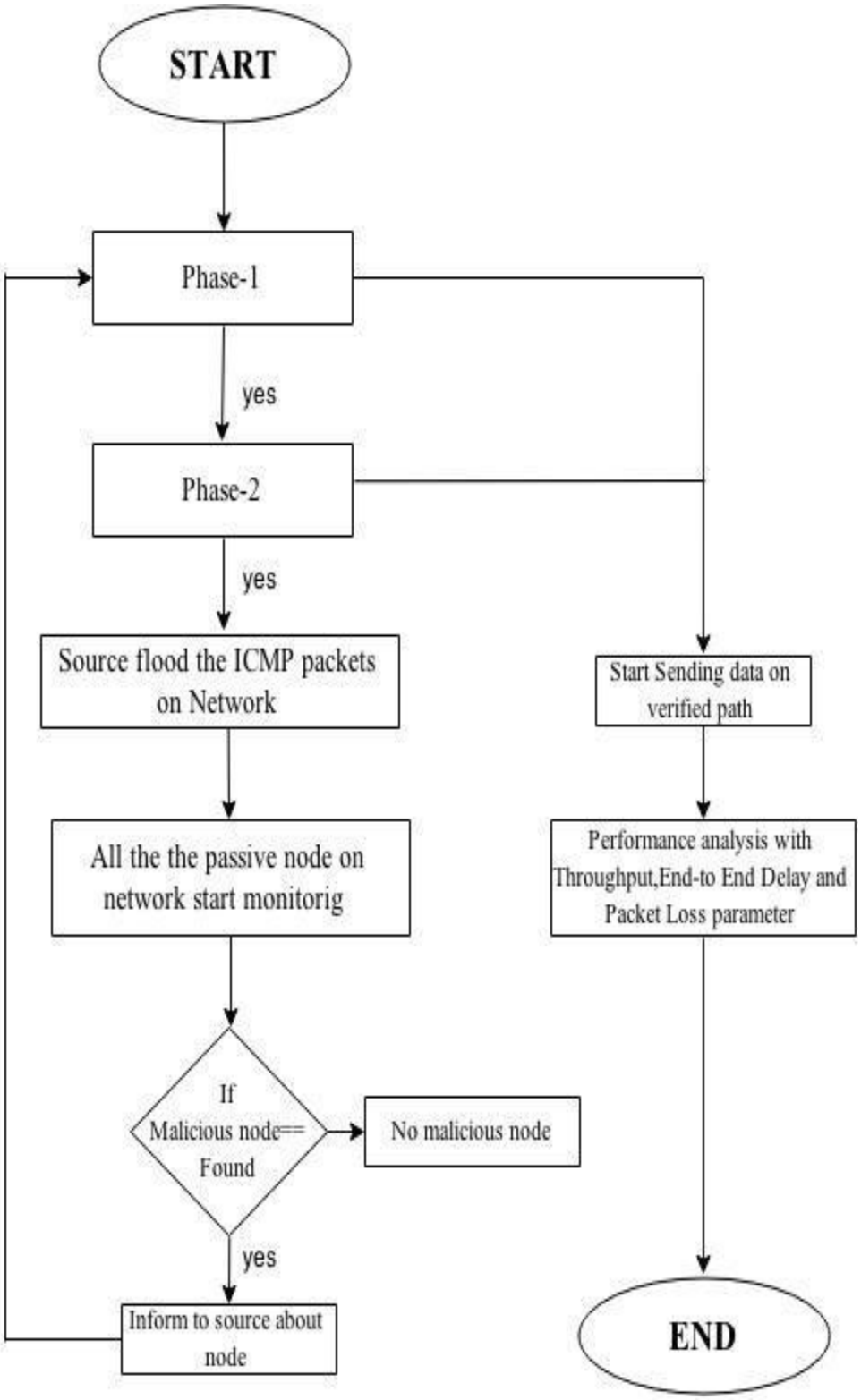


Figure 20. Phase 3 of KEAM Algorithm

CHAPTER 4

RESULTS AND DISCUSSIONS

4.1 Simulation Environment

NS2 Overview: NS-2 is an open-source simulation tool running on Unix-like operating systems. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired, wireless and satellite networks. It has many advantages that make it a useful tool, such as support for multiple protocols and the capability of graphically detailing network traffic. Additionally, NS-2 supports several algorithms in routing and queuing. LAN routing and broadcasts are part of routing algorithms. Queuing algorithm includes fair queuing, deficit round robin and FIFO. NS-2 started as a variant of the REAL network simulator in 1989. REAL is a network simulator originally intended for studying the dynamic behaviour of flow and congestion control schemes in packet-switched data networks. In 1995 ns development was supported by Defence Advanced Research Projects Agency DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. The wireless code from the UCB Daedelus and CMU Monarch projects and Sun Microsystems have added the wireless capabilities to ns-2.

Depending on user's requirement the simulation are stored in trace files, which can be fed as input for analysis by different component:

- A NAM trace file (.nam) is used for the ns animator to produce the simulated environment.
- A trace file (.tr) is used to generate the graphical results with the help of a component called X Graph.

❖ **Number of nodes:** This parameter in the above table is used to represent number of nodes that are used for conducting the simulation.

❖ **Pause time**: this parameter represents the time interval for which the nodes can be paused in the network during simulation.

Table 5. Simulation Parameter

Parameter	Value
Terrain Area	800 m x 800 m
Simulation Time	50 s
MAC Type	802.11
Application Traffic	CBR
Routing Protocol	AODV
Data Payload	512 Bytes/Packet
Pause Time	2.0 s
Number of Nodes	23
Number of Sources	1
No. of Adversaries	1

- **Traffic type:** Network traffic can be of two types viz. Variable Bit Rate (VBR) and Constant Bit Rate (CBR). The CBR traffic can suffer a maximum delay of T.
- **Simulation time**: Simulation time is the duration of time for which the simulation is carried out.

4.1.1 NS-2 Program Invocation

NS2 can be invoked by executing the following statement from the shell environment:

>>ns [<file>] [<args>]

where <file> and <args> are optional input argument. If no argument is given, the command will bring up an NS2 environment, where NS2 waits to interpret commands from the standard input (i.e., keyboard) line-by-line. If the first input argument <file> is given, NS2 will interpret the input scripting <file> (i.e., a so called Tcl simulation script) according to the Tcl syntax. Finally, the input arguments <args>,each separated by a white space, are fed to the Tcl file <file>. From within the file <file>, the input argument is stored in the built-in variable "argv".

As shown in Fig. 20 , the general simulation steps can be tailored to fit with the NS2 framework. The key NS2 simulation steps include the following:

Step 1: Simulation Design

The first step in simulating a network is to design the simulation. In this step, the users should determine the simulation purposes, network configuration, assumptions, the performance measures, and the type of expected results.

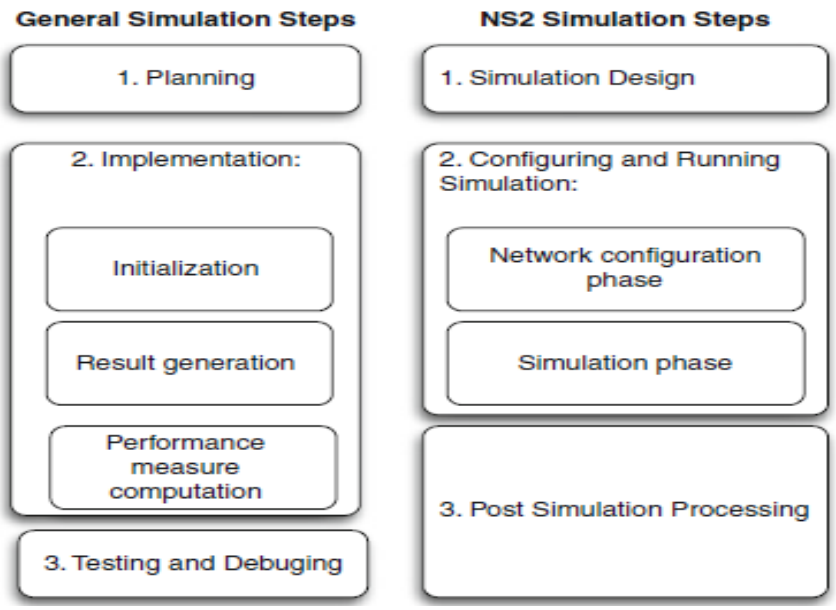


Figure 21. comparison of general simulation steps and NS2 simulation steps

Step 2: Configuring and Running Simulation

This step implements the design in the first step. It consists of two phases:

- **Network configuration phase:** In this phase, network components (e.g., node, TCP and UDP) are created and configured according to the simulation design. Also, the events such as data transfer are scheduled to start at a certain time.
- **Simulation Phase:** This phase starts the simulation which was configured in the Network Configuration Phase. It maintains the simulation clock and executes events chronologically. This phase usually runs until the simulation clock reaches a threshold value specified in the Network Configuration Phase.

In most cases, it is convenient to define a simulation scenario in a Tcl scripting file (e.g., <file>) and feed the file as an input argument of an NS2 invocation (e.g., executing “ns <file>”).

Step 3: Post simulation Processing

The main tasks in this steps include verifying the integrity of the program and evaluating the performance of the simulated network. While the first task is referred to as debugging, the second one is achieved by properly collecting and compiling simulation results.

4.1.2 Network Animation (NAM) Trace

NAM trace records simulation detail in a text file and uses the text file to play back the simulation using animation. NAM trace is activated by the command "$nsnamtrace-all $file," where "ns" is the Simulator handle and "file" is a handle associated with the file (e.g., "out.nam" which we create in any prog.) which stores the NAM trace information. After obtaining a NAM trace file, the animation can be initiated directly at the command prompt through the following command:

>> nam filename.nam

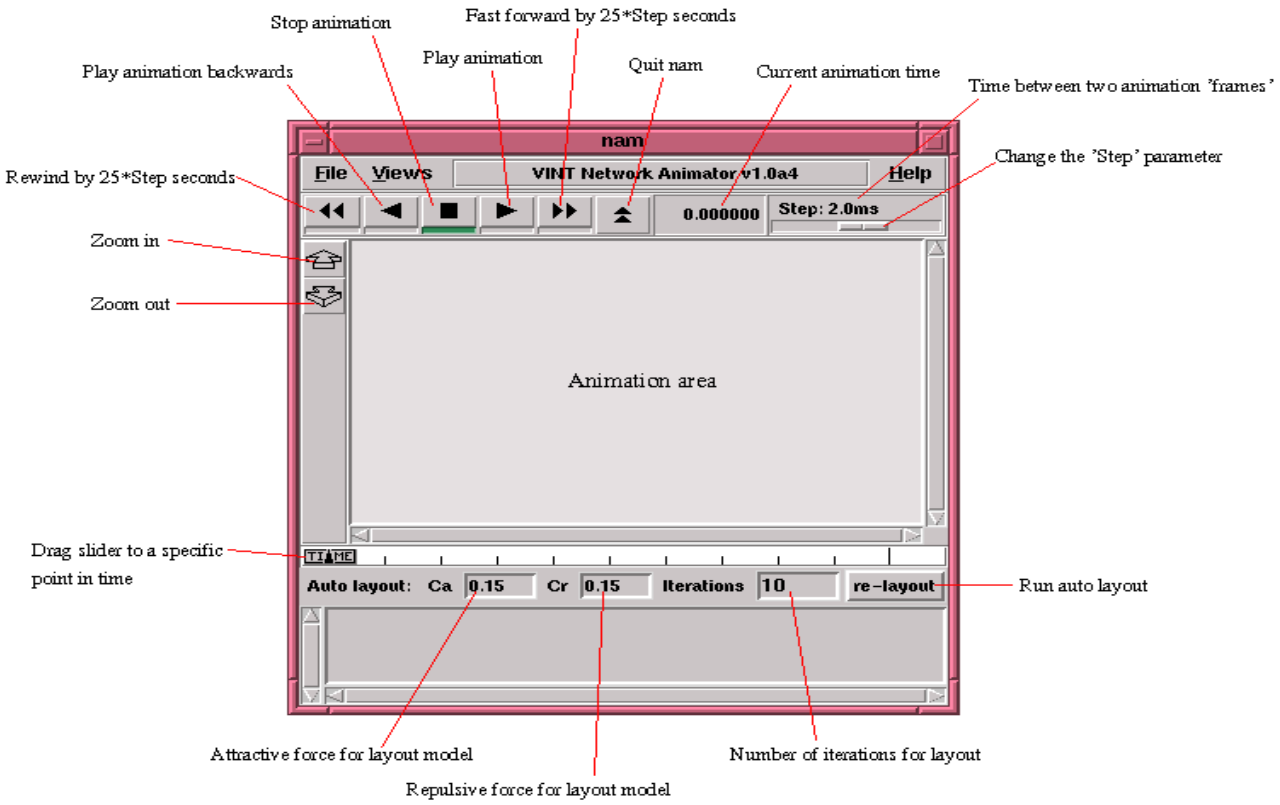


Figure 22. NAM Console

4.1.3 Wireless Mobile Node Architecture

The picture below shows the architecture of a Mobile Node. It is an extension of a regular node. The part below the dotted line is the extension. This extension consist of several blocks. The network stack for a mobilenode consists of a link layer(LL), an ARP module connected to LL, an interface priority queue(IFq), a mac layer(MAC), a network interface(netIF), all connected to the channel. These network components are created and

plumbed together in OTcl. Clasifier is use for forwarding the packet. Each component briefly describe here:

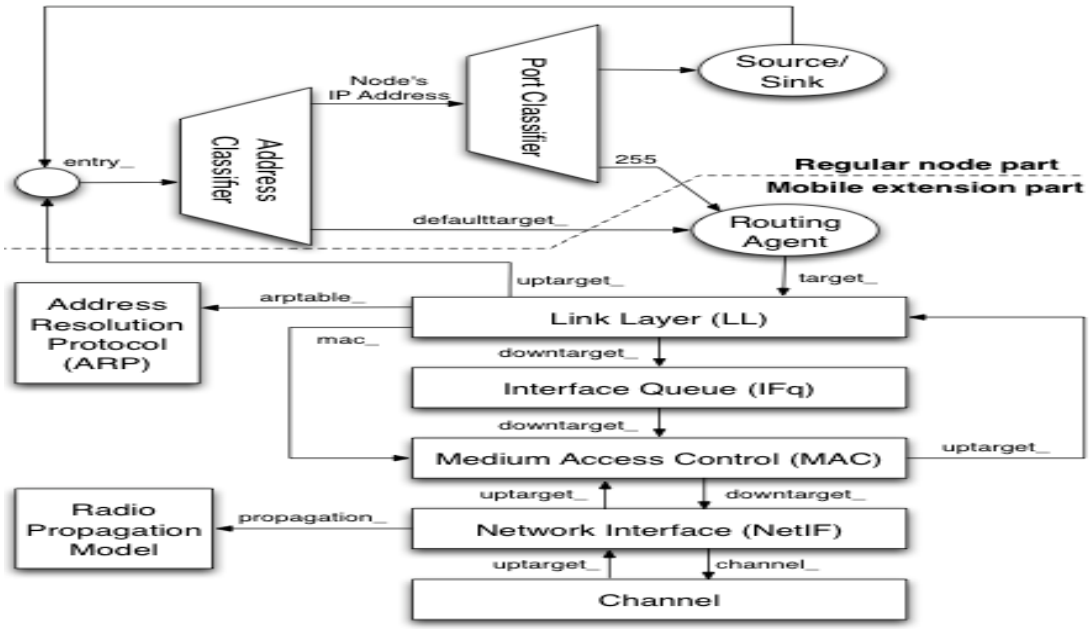


Figure 23. Mobile Node Architecture

1) **Routing agent**: A routing agent tells the node how a packet should be transmitted (e.g., who is the next hop node?) It works with routing protocol responsible for propagating routing information throughout the networks.
2) **Link Layer:** This Models bandwidth, packet transmission time, propagation delay. The only difference being the link layer for mobile node has an ARP module connected to it which resolves all IP to hardware (Mac) address conversions. Normally for all outgoing (into the channel) packets, the packets are handed down to the LL by the Routing Agent. The LL hands down packets to the interface queue. For all incoming packets (out of the channel), the mac layer hands up packets to the LL which is then handed off at the node_entry_ point.
3) **Interface Queue:** This module models buffer management. The class PriQueue is implemented as a priority queue which gives priority to routing protocol packets, inserting them at the head of the queue. It supports running a filter over all packets in the queue and removes those with a specified destination address.
4) **Medium Access Control (MAC)** : Models the MAC layer. Ns-2 has used the implementation of IEEE 802.11 Distributed Cordination Function(DCF) from CMU.

5) **Network Interfaces** : It is in this module where actual transmission takes place. It works with the radio propagation model to simulate packet transmission error. The Network Interphase layer serves as a hardware interface which is used by mobile node to access the channel. The wireless shared media interface is implemented as class Phy/WirelessPhy. This interface subject to collisions and the radio propagation model receives packets transmitted by other node interfaces to the channel. The interface stamps each transmitted packet with the meta-data related to the transmitting interface like the transmission power, wavelength etc. This meta-data in packet header is used by the propagation model in receiving network interface to determine if the packet has minimum power to be received and/or captured and/or detected (carrier sense) by the receiving node.
6) **Channel**: This module is in fact not a part of a mobile node. It is the part which is shared among all neighbouring mobile nodes. A mobile node puts the packet being transmitted on this module. The destination node reads the channel and picks up the packet belonging to itself from this channel
7) **Address Resolution Protocol (*ARP)* :**This module translates hardware addresses into network (i.e., IP) addresses The Address Resolution Protocol (implemented in BSD style) module receives queries from Link layer. If ARP has the hardware address for destination, it writes it into the mac header of the packet. Otherwise it broadcasts an ARP query, and caches the packet temporarily. For each unknown destination hardware address, there is a buffer for a single packet. In case additional packets to the same destination are sent to ARP, the earlier buffered packet is dropped. Once the hardware address of a packet's next hop is known, the packet is inserted into the interface queue.
8) **Tap Agents** : Protocol Entity. Agents that subclass themselves as class Tap defined in mac.h can register themselves with the mac object using method installTap(). If the particular Mac protocol permits it, the tap will promiscuously be given all packets received by the mac layer, before address filtering is done.
9) ***Radio Propagation Model*** It uses Friss-space attenuation (1/r2) at near distances and an approximation to Two ray Ground (1/r4) at far distances. The approximation assumes specular reflection off a flat ground plane.
10) ***Antenna*** An omni-directional antenna having unity gain is used by mobile nodes.

4.1.4 Trace File Format

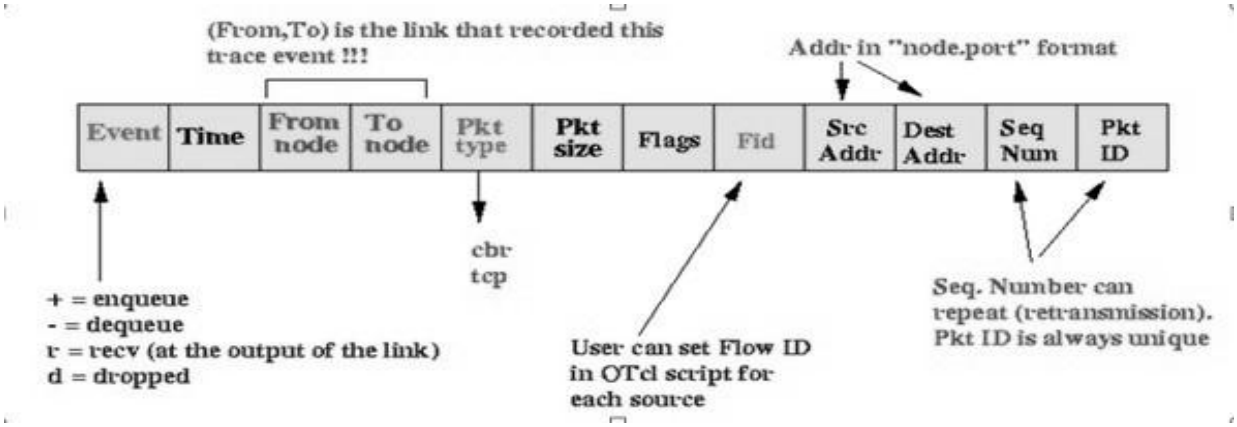


Figure 24. Trace Format

1) Type Identifier:

   "+": a packet enque event

   "-": a packet deque event

   "r": a packet reception event

   "d": a packet drop (e.g., sent to dropHead_) event

   "c": a packet collision at the MAC level

2) Time: at which the packet tracing string is created.
3) Source Node and Destination Node: denote the IDs of the source and the destination nodes of the tracing object.
4) Packet Name: Name of the packet type :CBR/TCP
5) Packet Size: Size of the packet in bytes
6) Flags: A 7-digit flag string

   "-": disable

   1st = "E": ECN (Explicit Congestion Notification) echo is enabled.

   2nd = "P": the priority in the IP header is enabled.

   3rd : Not in use

   4th = "A": Congestion action

   5th = "E": Congestion has occurred.

   6th = "F": The TCP fast start is used.

7th = "N": Explicit Congestion Notification (ECN) is on.

7) Flow ID : It is use for analysis purpose: it is also used where specifying stream colour for the NAM display.
8) Source Address and Destination Address: the format of these two fields is "a.b", where "a" is the address and "b" is the port.
9) Sequence Number: Assign to packet for analysis purpose.
10) Packet Unique ID: It shows the unique id of the object

4.2 Initialization of Network Deployment

The simulation for the projected method has been carried using network animator and the operating system used is Ubuntu. our Simulation is conducted within the network Simulator(NS) 2.35 environment on platform with GCC 4.3.4 and Ubuntu 14.04.1 shows in fig: 25. In NS 2.35. we make configuration with 23 nodes and flat grid size of 800x800m.Simulation is made with use of AODV routing. we generate the result in NS-2 with use of reference node technique.

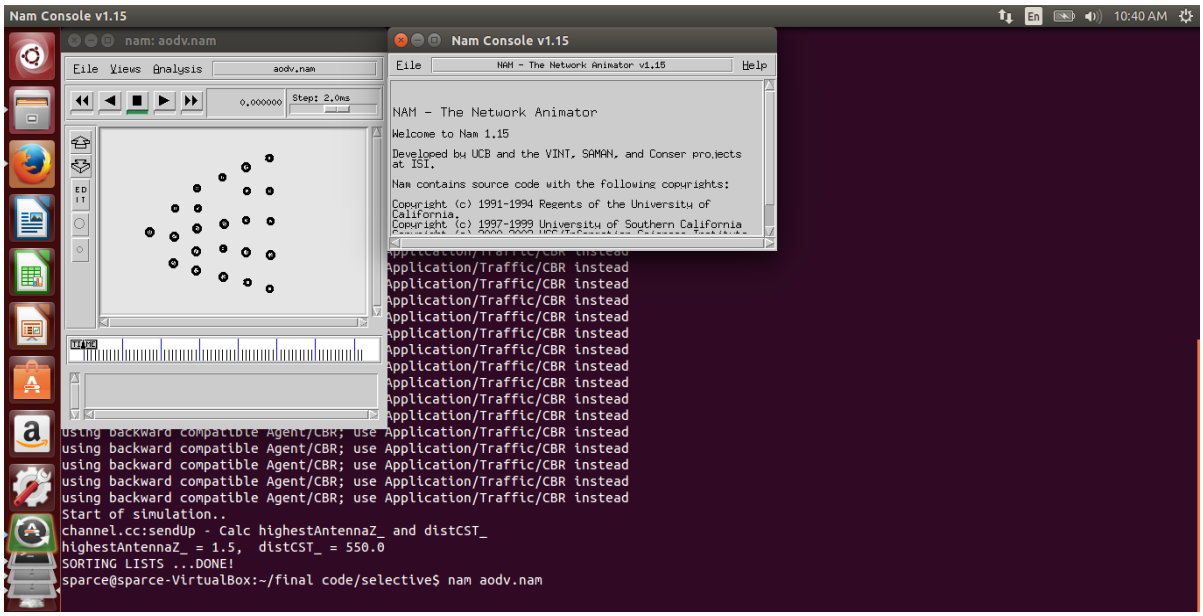


Figure 25. Execution of Namespace for 24 Nodes

The Figure 25. shows when we executing tcl script in Terminal with >> ns prog.tcl it will first initialize all the background process for generate the network. Then enter the >> nam. prog.nam command in terminal it will start animation of network by generating one pop-up

menu of NAM it shown in fig 25.

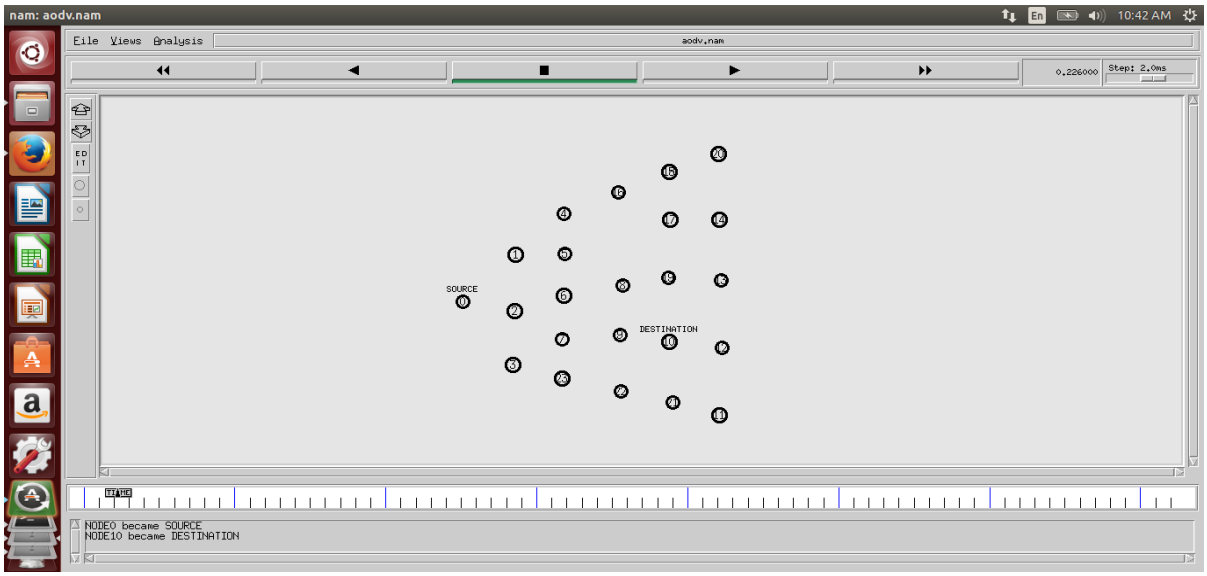
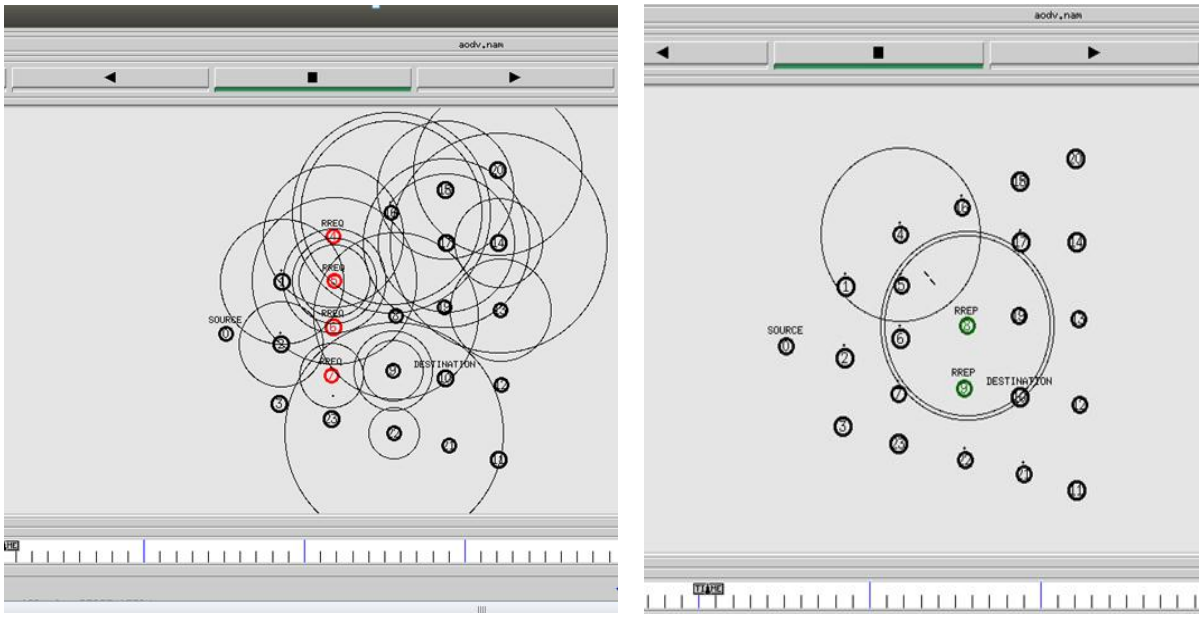


Figure 26. Deployment of Network with Source and Destination

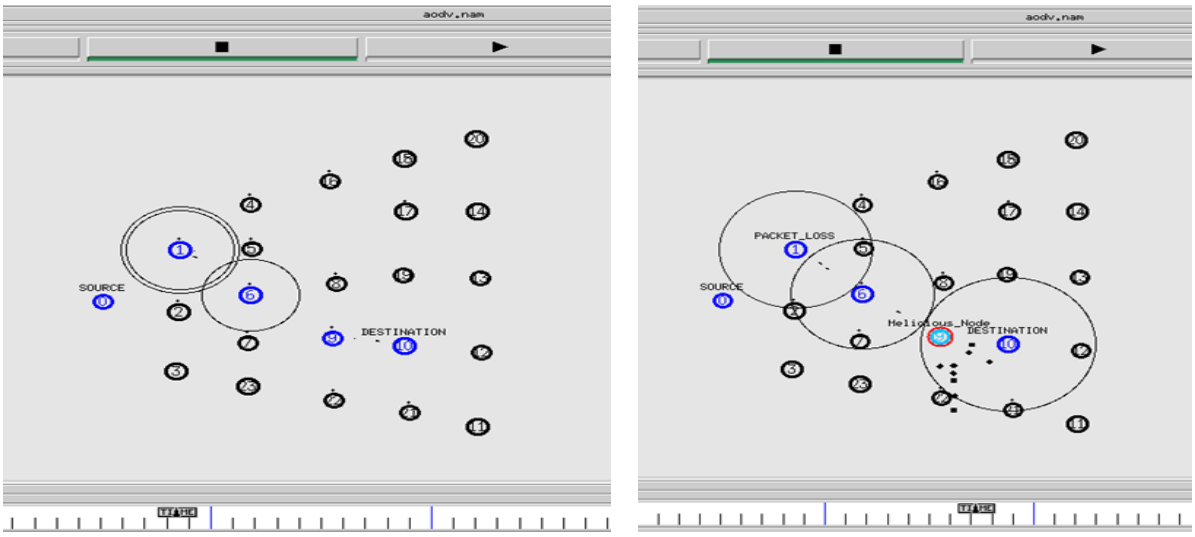
In Fig 26: shows that all the 23 node are fixed on X Y Z coordinate and deploy an Ad-Hoc network, 2 nodes are labelled as source and destination in the network. This animation has a start, stop, forward and rewind, previous and next button. It also provides Zoom in and Zoom out facility to see the simulation. Even we can drag the time slide window to check the simulation of any point of time.



(a) (b)

Figure 27. (a)Flooding of RREQ from source to all adjacent node (b)RREP Route Replay Packet

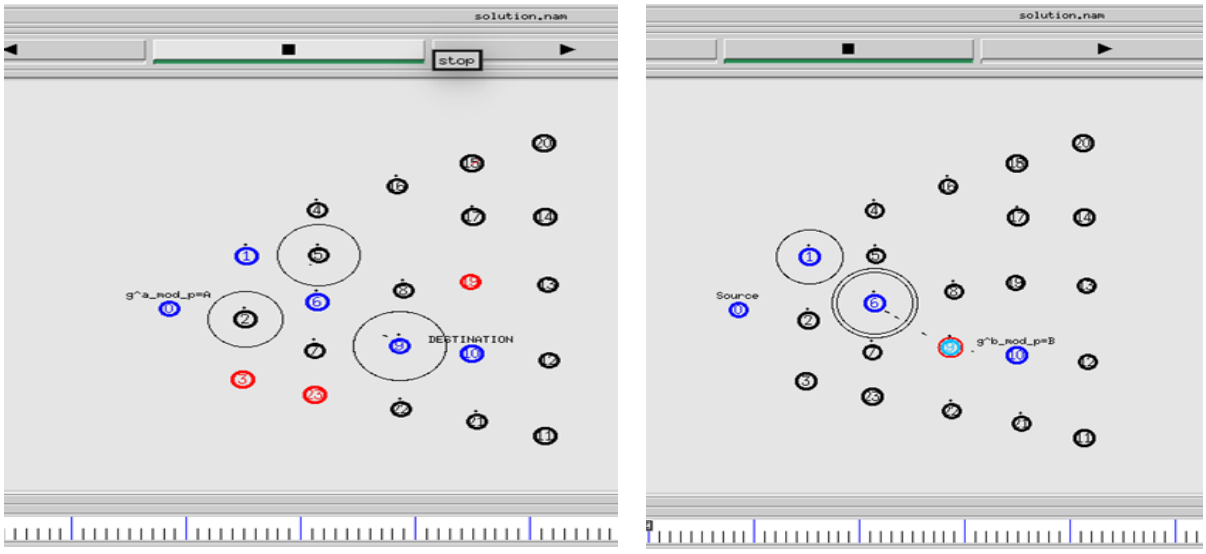
Figure 27 Shows that source node flood RREQ to its neighbour node so route to destination could be possible. The blue and red node with circle shows that neighbour node further broadcast RREQ and RREP to its intended node so that path could be establish between Source and Destination.



(A) (B)

Figure 28. (a) Shortest Path by AODV (b) Packet Drop by Malicious Node

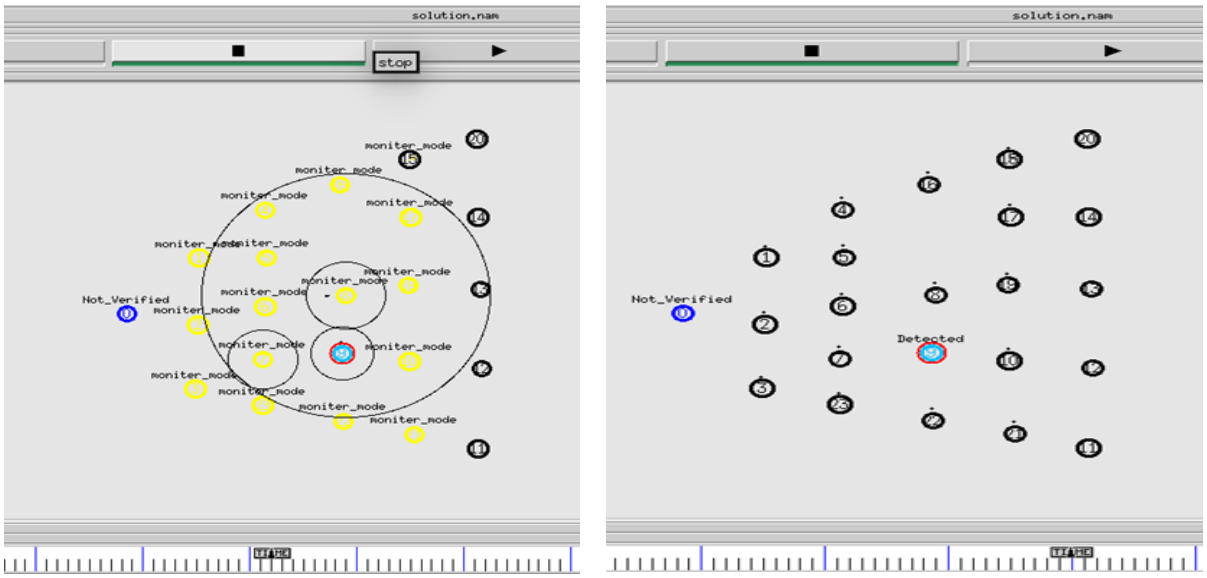
In Figure 28 (a) we can see that shortest path establish between two end nodes which is mark as blue node and (b) shows that the malicious node continuous dropping the packet on selective path for certain time period and the result is packet loss in path.



(a) (b)

Figure 29. (a)(b) Source and Destination exchange own public key by Diffie-Hellman

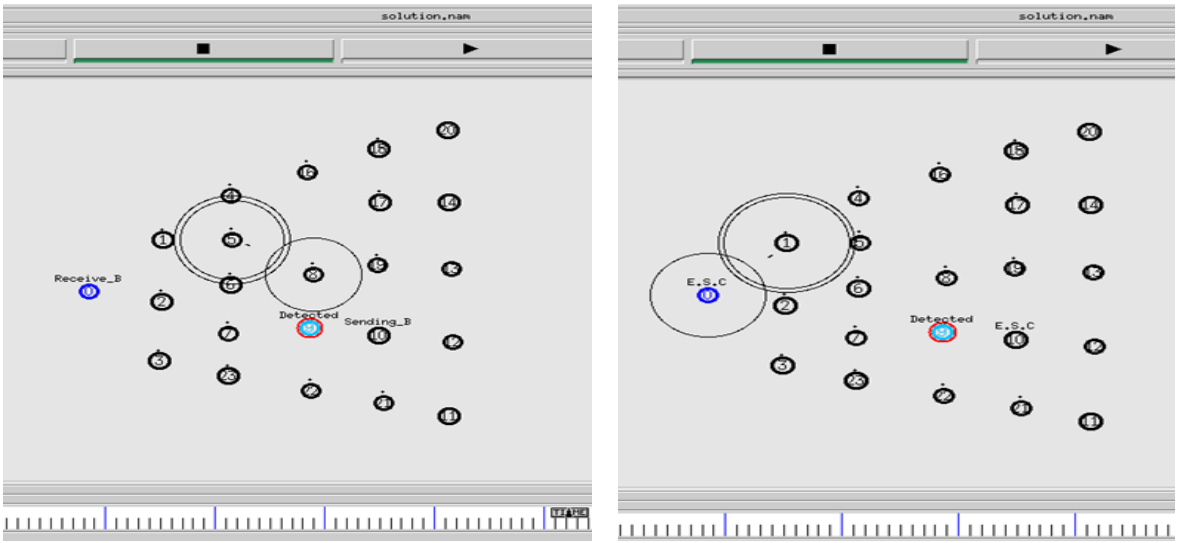
Figure 29: give the solution to Isolate and Prevention of given attack. By Diffie-Hellman algorothm Source and Destination slect privvate key, calculate public key and exchange it at baoth the side to generate shared key.



(a) (b)

Figure 30. (a) Monitor mode technique (b) Detecting and Labelling Malicious Node

Now if the shared key is not match on source and destination then source flood ICMP packet in network to start Monitor mode technique which is shown in figure with yellow node. If the node does not give replay to monitornode then it will be disclouse as malicious node mark as red node in figure 30.



(a) (b)

Figure 31.(a)Key Exchange between Source and Destination (b) Acceptance of Shared key

When malicious detected source again find new shortest path by AODV and make the channel secure by Diffie-hellman key exchange can show in fig 31 (a). At source and destination we can see that E.S.C (acceptance) label in fib 31 (b) which show that both are ready to start communication.

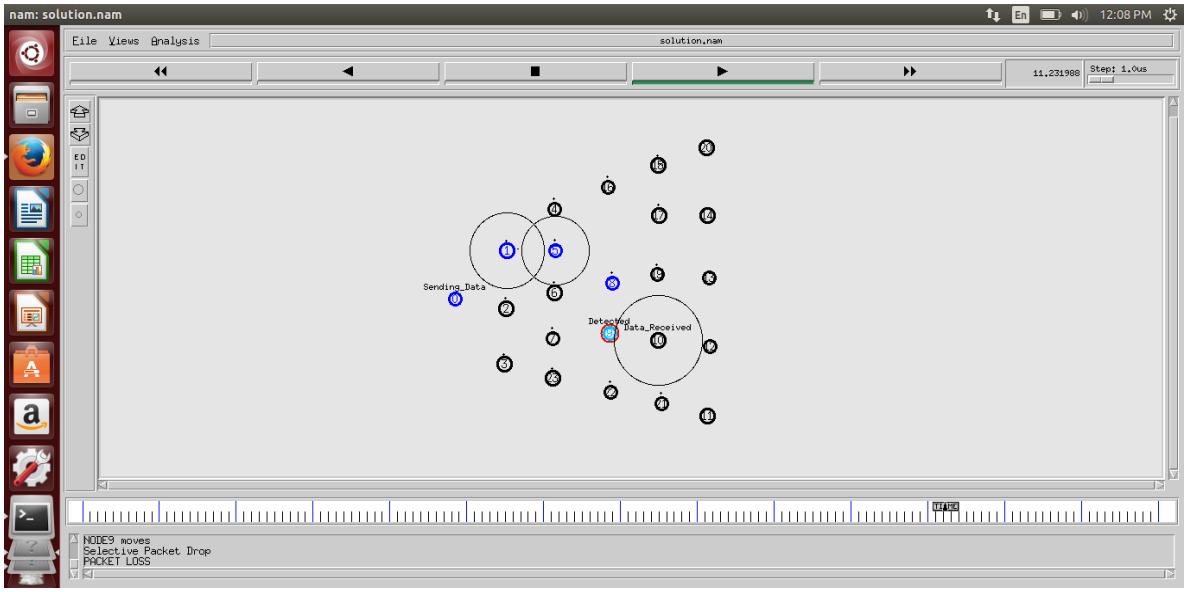


Figure 32. New Secure Path Establish Between Source and Destination

New secure and shortest route deploy between source to destination and data transmission start and bot the end send and receive data which is shown in fig 32.

4.3 Graphs

The graphs are used to signify the variation in throughput and end-to-end delay using the proposed method. Green line characterizes the change in case of the new scenario and red colour represents the conventional method. These two parameters are a widely used for validating the confirming the use of particular methods. Throughput can be defined as the number of packet data received per unit time whereas end-to-end delay defined as the time taken between sending of a packet and it's receiving on the destination.

Figure 33. shows the change in end-to end delay after deployment of the proposed method. It shows that our proposed KEAM schema reduce 90% of end-to-end delay while packet is going to transmit from source to destination In the previous schema, the delay starts linearly increasing when there is presence of malicious node in the path mark as green line whereas in

absence of malicious node delay first decrease but the new path deploy because of malicious activity it will be not as much shortest then previous so at some point of time the peak of the graph increase and decrease because of delay which mark as red line in graph.

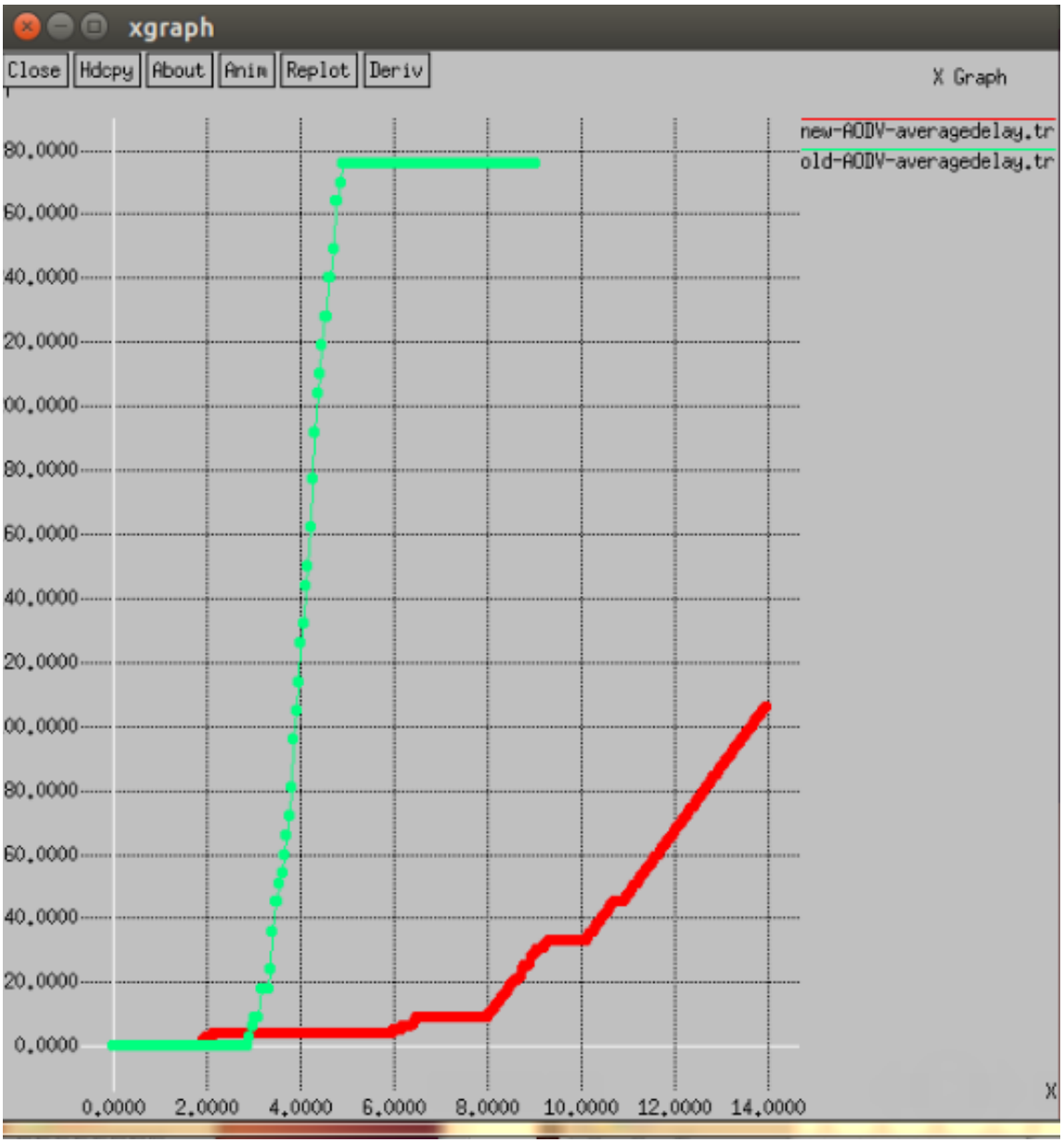


Figure 33. End-to-End Delay

Fig 34. represents the average throughput after applying proposed method. As the delay in the network is minimum because of isolation of malicious node, so throughput of the network is linearly increased after some pint of time. From graph we can see that when number of packet increase throughput is gradually increase with time in our proposed schema shown by red line. While green line represents previous schema when the malicious node

present in the network at that time packet continuous drop so the line is constant for some period of time.

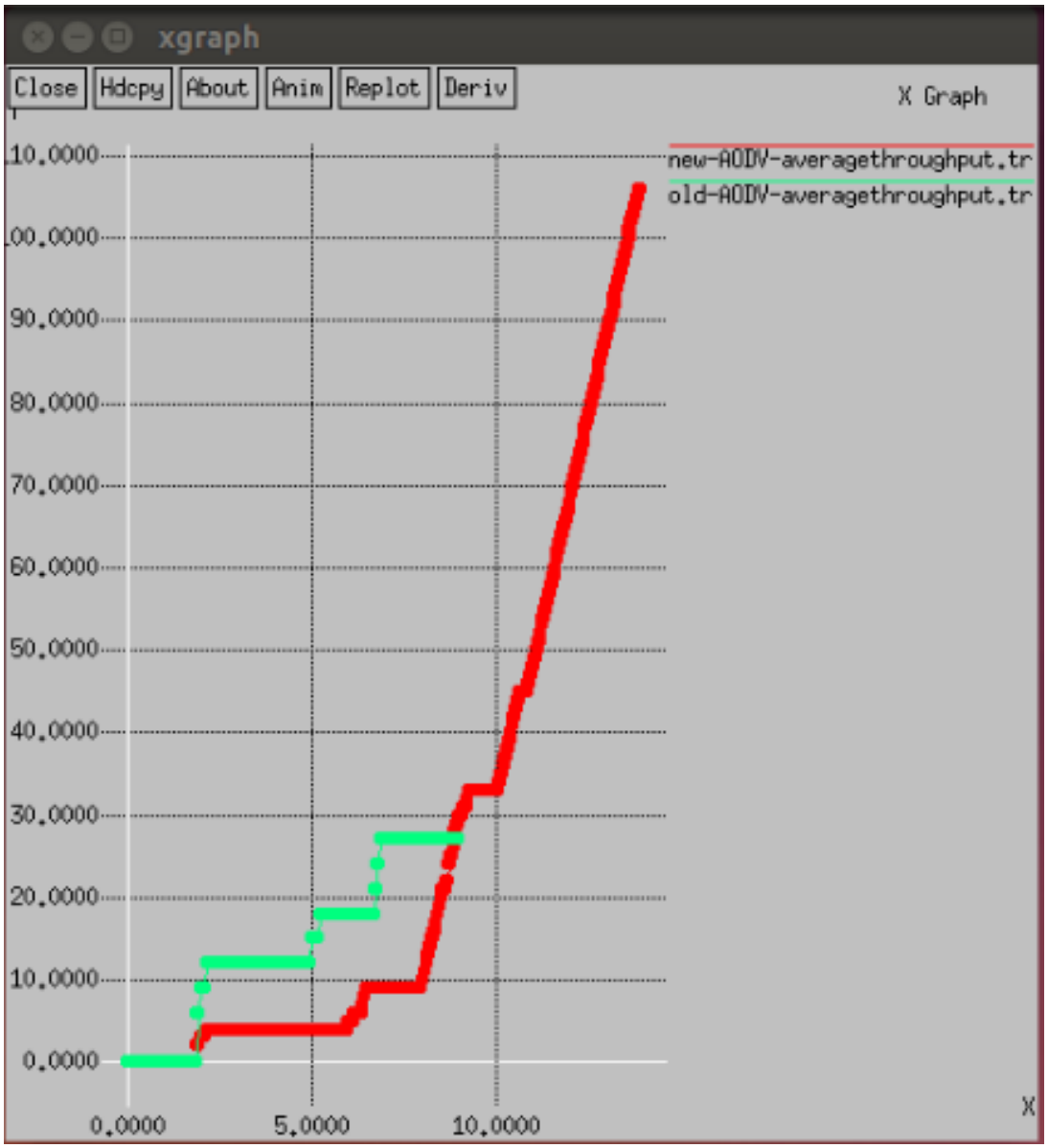


Figure 34. Average Throughput

Calculating the Throughput of the system , we have used the following formula:

Throughput = Packet received * 8/ Amount of packet forwarded (over some point of time).

As we have applied the Diffie-hellman and monitoring algorithm for setting up the path then packet loss is less as compared to the previous scenario. We make the channel secure so final

result comes is maximization of throughput and minimization of packet loss. In previous schema malicious node continuously dropping the packet so final output is major loss of packet . In fig 35: we see that the green line is continuously increase because of dropping of the packet and red line constant after some time because of securing of channel.

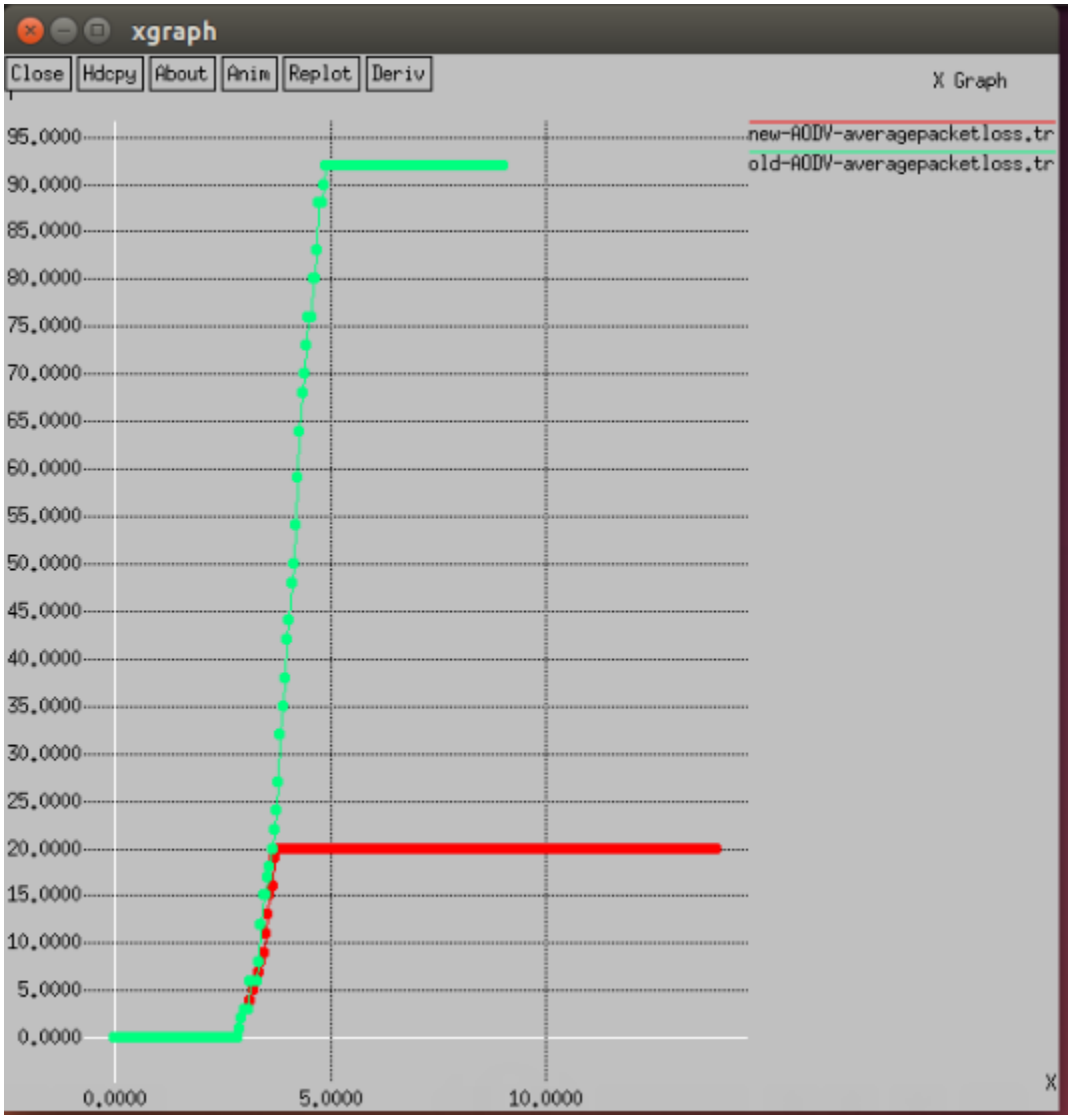


Figure 35. Average Packet Loss

CHAPTER 5

CONCLUSION AND FUTURE WORK

Mobile ad-hoc network have been wast area of research work from past few years because its widely used application in battlefield and business purpose. Due to openness and dynamic topology network is vulnerable from attacker.In this paper we proposed and evaluated two network layer schema Key Exchange and Monitor node-KEAM , which can easily deploy to source initiated routing protocol such as AODV. The schema detects the malicious node from routing path in network so when new route establish it would be free from malicious activity and the result improvement in the packet delivery ratio and minimize the end-to-end delay .Simulation show that monitor node technique easily detecting the misbehaving node and increasing the throughput.

We would continue our future work in the following direction: Make further improvement in the acknowledgement and key exchange model posted in this report and take other decision factor for our model. Comprehensive performance evaluation will be conducted in the light of multiple packet drop attack.

REFERENCES

[1] Sunil Taneja, Dr. Ashwani Kush and Amandeep Makkar, "End to End Delay Analysis of Prominent On-demand Routing Protocols", IJCST Vol. 2, Issue1, March 2011.

[2] Andul Haimid ,Bashir Mohamed, thesis, "ANALYSIS AND SIMULATION OF WIRELESS AD-HOC NETWORK ROUTING PROTOCOLS"2004.

[3] Giovanni Vigna, Sumit Gwalani ,Kavitha Srinivasan ,Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool for AODV-based Ad-hoc Wireless Networks", 2004.

[4] Sevil Sen, John A.Clark, Juan E.Tapiador,"Security Threats in Mobile Ad Hoc Networks", 2010.

[5] Rusha Nandy, "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme" Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011).

[6] Wenjia Li and Anupam Joshi,"Security Issues in Mobile Ad Hoc Networks- A Survey",2005.

[7] Gene Tsudik,"Anonymous Location-Aided Routing Protocols for Suspicious MANETs", 2010.

[8] Karim El Defrawy, and Gene Tsudik , "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs" ,IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 9, SEPTEMBER 2011.

[9] Seung Yi, Robin Kravets,"Key Management for Heterogeneous Ad Hoc Wireless Networks",10th IEEE International Conference on Network Protocols (ICNP'02) 1092-1648

[10] Pradeep kyasanur,"Selfish MAC layer Misbehavior in wireless networks", IEEE on Mobile Computing,2005

[11] Yixin Jiang Chuang Lin, Minghui Shi, Xuemin Shen"Multiple Key Sharing and Distribution Scheme With (n; t) Threshold for NEMO Group Communications", IEEE 2006

[12] Caimu Tang ,Dapeng Oilver "An Efficient Mobile Authentication Scheme for Wireless Networks", IEEE.

[13] Thongchi Chuachan and Somnuk Puangpronpitag ,"A Noveel Challebge & Response Scheme Agaist Selective Forwarding Attacks in MANET", IEEE, 2013

[14] Ahmed M.Abd EL-Haleem and Ihab A. Ali,"TRIDNT:THE TRUST-BASED ROUTING PROTOCOL WITH CONTROLLED DEGREE OF NODE SELFISHNESS FOR MANET",IJNSA,Volume-3,No.3,PP.189-203,May 2011.

[15] K.Sangeetha,"SECURE DATA TRANSMISSION IN MANETS USING AODV", IJCCER, Volume-2,Issue 1,PP. 17-22, 1 January 2014.

[16] Bo Sun Yong, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", EPMCC, 2004

[17] Kashyap Balakrishna, Jing Deng and Promod K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", IEEE Communication,pp.2137-2142.

[18] Sushma Yalamanchi and K.V. Sambasiva Rao "TWO-STAGE AUTHENTICATION FOR WIRELESS NETWORKS USING DUAL SIGNATURE AND SYMMETRIC KEY PROTOCOL" International Journal of Computer Science and Communication (IJCSC), n Vol. 2, No. 2, pp. 419-422,July-December 2011

[19] S.Sharmila and G. Umamaheswari," Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", International Journal of Computer Applications Volume 39– No.4, February 2012

[20] Hui Xia, Zhiping Jia, Lei Ju ,Xin Li and Edwin H.-M. Sha," Impact of trust model on on-demand multi-path routing in mobile ad hoc networks",Computer Communication-Elsevier, pp.1078-1093,2013

[21] Hung-Min Sun ,Chiung-Hsun Chen and Yu-Fang Ku ,"A novel acknowledgment-based approach against collude attacks in MANET",Elsevier,pp.7968-7975,2012

[22] Djamel Djenouri and Nadjib Badache,"On eliminating packet droppers in MANET: A modular solution",Elsevier,pp.1243-1258,2009.

APPENDIX

LAN :	Local Area Network
KEAM:	Key Excahnge and Monitoringx
WAN :	Wide Area Network
MANET :	Mobile Ad-Hoc Network
WSN:	Wireless Sensor Networks
WMN:	Wireless Mesh Networks
AS :	Autonomous System
DSN :	Destination Sequence Number
AODV :	Ad-Hoc On-Demand Distance Vector
DSR :	Dynamic Source Routing
CHGSRP:	Cluster Head Gateway Routing Protocol
ZHLSRP:	Zone base Hierarchical Link State Routing Protocol
WRP :	Wireless Routing Protocol
ZRP :	Zone Routing Protocol
RREQ :	Route Request
RREP :	Route Replay
RERR :	Route Error
CORE :	Common Open Research Emulator
CW :	Contention Window
PKI :	Public Key Interchange
ACK:	Acknowledgement
TCP:	Transmission Control Protocol