Black hole detection and prevention in AODV

Dissertation

Submitted in partial fulfillment of the

requirement for

the award of the degree of

MASTER OF TECHNOLOGY

in

Electronic and Communication Engineering

By

Mehak Kaushal

Reg. No. 11307232

Under the Guidance of

Mr. Gunjan gandhi

Assistant Professor

School of Electronics and Communication Engineering

Lovely Professional University, Jalandhar-Delhi G.T. Road (NH-1),

Phagwara, Punjab, India-144411

(April, 2015)

CERTIFICATE

This is to certify that the Dissertation titled "Black hole detection and prevention in AODV" that is being submitted by "**Mehak Kaushal**" in partial fulfillment of the requirements for the award of MASTER OF TECHNOLOGY, is a record of bonafide work done under my guidance. The contents of this Dissertation, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for award of any degree or diploma and the same is certified.

Mr. Gunjan gandhi
(Assistant Professor)
Dissertation
LPU, Punjab.

Objective of the Dissertation is satisfactory / unsatisfactory

Examiner I

Examiner II

ACKNOWLEDGEMENT

I acknowledge with gratitude the tremendous inputs of my guide Asst. Professor **Mr. Gunjan gandhi**, Lovely Professional University, for both initiating and motivating me in to research. It has been excruciating at times, as I have had to dwell upon the unheard and the unknown essential vitals to this research.

I am also grateful to **Prof. Bhupinder Verma,** Dean - Electronics and Communication Engineering, Lovely Professional University, Punjab for providing the facilities required for accomplishment of my Dissertation work at the university.

I am also grateful to the faculty of department of electronics and communication for continuous support, guidance and inspiration for effective and successful completion of this rewarding research.

I am also grateful to my parents and my friends who supported me in all my efforts.

Place: LPU, Jalandhar — Mehak Kaushal

Date: April, 2015 — Reg.No: 11307232

CERTIFICATE

This is to certify that "Mehak Kaushal"bearing Registration no. 11307232 has completed objective formulation of thesis titled, **"Black hole detection and prevention in AODV"** under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the thesis has ever been submitted for any other degree at any University.

The thesis is fit for submission and the partial fulfillment of the conditions for the award of Degree of **Master of Technology** in **Electronics & Communication Engineering**.

Signature of Advisor:
Mr. Gunjan Gandhi
Lovely professional university
Date:

DECLARATION

I, **Mehak Kaushal**, student of **Master of Technology** under Department of Electronics and Communication Engineering of Lovely Professional University, Punjab, hereby declare that all the information furnished in this Dissertation report is based on my own intensive research and is genuine.

This thesis does not, to the best of my knowledge, contain part of my work which has been submitted for the award of my degree either of this university or any other university without proper citation.

Date: **Mehak Kaushal**

Reg. No.: 11307232

ABSTRACT

Currently, the wireless sensor network is facing four major issues namely security, power management, localization, routing and deployment techniques. Out of these in security, energy conservation and coverage efficiency are the main issues. Security is the main constraint of wireless sensor networks (WSNs) due to the routing algorithms we use in AODV. We will study the AODV routing protocol and use some algorithms to improve the AODV routing and to make the AODV routing protocol more efficient and reliable and prevent the threats of attacks. AODV is the ad-hoc on demand routing. The black hole worm hole and the grey hole attacks are more prone to the wireless sensor networks. These attacks deteriorate the working of the network by not providing the end to end delivery to the destination nodes. So to avoid these attacks we use clustering to detect the black hole attacks and to stop the attacks from the malicious nodes. Moreover to increase the security of the network we would like to apply the HOOSC scheme on the network so that the signcryption of the data can be done. It enhances the security issues present in the network and give us efficient and the reliable network.

Table of contents:

LIST OF FIGURES:

CHAPTER 1

INTRODUCTION: Wireless sensor networks consist of sensors which are spatially Distributed to monitor the surroundings and to provide the feedback to the main location. These are providing a bridge between the physical and the real worlds. In the past decade wireless sensor networks have gained much more attention from the actual users and the researchers. In simple words sensor networks are something that is known by sense perception. Sensors are the principle part of the wireless sensor networks. The size of the sensor nodes is as small as possible it would vary from a tiny dust particle to the size of the shoe box. So that it becomes easy to deploy the more nodes. So, that the system becomes reliable. Basically wireless sensor network consists up of large no of sensor nodes. These sensor nodes are deployed in a very dense manner. There is no need to pre determine the location of sensor nodes. This will allow us the deployment of nodes which would be random in nature. A mode that sense is basically comprises of the controller part, the device used for receiving and transmitting and the main power supply.

Fig1. The sensing nodes

Sensing, processing and communication, when they add up in tiny device n give rise to the major applications. The design constraints for wireless sensor networks should be limited amount of energy, short -communication range means low bandwidth and limited processing and storage in each node. Lifetime is the primary factor of all sensing nodes. Lifetime reduced due to the collisions overhead packets and the idle listening. Energy efficient routing is used to increase the lifetime of sensor nodes, but the nodes on the forwarded path near to the base station are deployed. Data redundancy is also a main objective of WSN's. Nodes do the work collaborate and when the data is sensed by multiple nodes, then data redundancy should check that they have certain level of

correlation or redundancy. Each node is having their own GPS but if see it practically it is not viable so for the sake of simplicity, we assign GPS to some of the nodes and they helps the neighboring nodes to find out their position.

(QOS) is also a design objective for the WSN's in the terms of packet delivery latency and packet loss. Some of the challenges that are faced by WSN's are the limited energy capacity, sensor locations, limited hardware resource, and data aggregation. Data aggregation means that a sensor node produces significantly redundant data and that data is aggregated on the single node. The basic key elements of WSN's are given below:

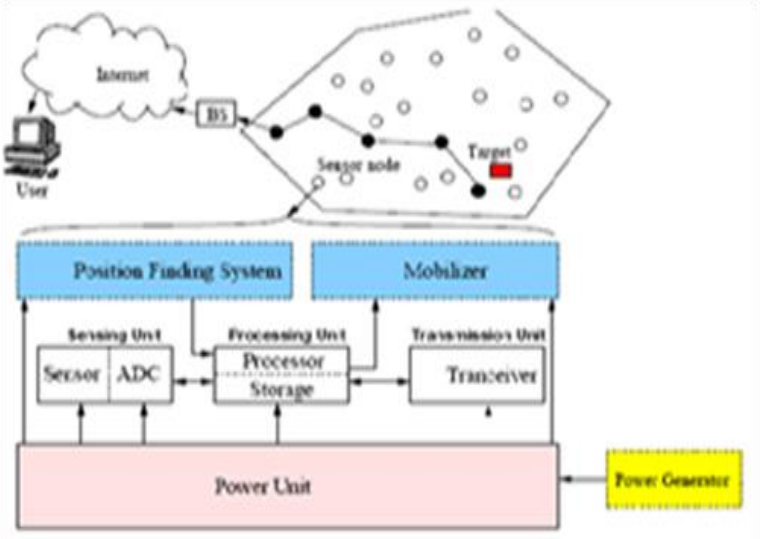

Fig2. Components of sensor node

Now let us explain each and every component very carefully. As per the diagram the sensor node is made up of four components a unit that senses a unit for processing, a unit that transmits and receives and the power unit. The components belongs to the particular application are position finding system, a power generator and the Mobilizer. Sensor unit is further composed of sensors and ADC. ADC's are used to convert the analog data into digital data. The digital data is then sending to the processing unit which is associated with small storage unit.

The processing unit keeps the data for a while and then passes it to the other nodes for the sensing task. The transceiver unit connects one node to the other nodes or we can say that to the network. The active and passive optical devices or a radio frequency device

may be used in transceiver. RF communication is used in most of the ongoing research projects because the packets which are being conveyed are having small size, small data rate and the frequency reuse is high due to short communication distances.

Next one of the important units is the power unit which may be supported by batteries or solar cells etc. The knowledge of finding the location and deploying the node with high accuracy is mandatory in sensor networks so we use another block known as location finding system. Mobilizer is a device it is used to move the nodes wherever they are needed for an assigned task. Mobilizer makes the nodes environment friendly. Wireless sensor network can broadly used in military and civilian applications.

Some of the major applications of the WSN's are as follows:

1. Vehicular telematics: An advanced architecture of vehicular telematics is AHVN. It is an integrated architecture between ad hoc networks and existing cellular wireless networks. Multi hop vehicular connectivity is being used in this model. Physical characteristics of the roads and the false hop characteristics of the initial connection. Then we come to the failure probability of vehicular telematics in V2V system.V2V means vehicle to vehicle, we use interoperability in this. We will hand over the failed criteria to communicate with the V2R networks (vehicle to roadside). VANET's are been created by using the vehicle nodes. V2R is playing an enhanced version by taking the base stations, vehicular nodes and the access points are connected to internet. Intelligent transport system is used to update the information and the solutions for the safety purposes.
2. Biomedical signal monitoring: as we know about the revolution of the WSN field. It has provided its vast contribution to the medical field. Let us know about the concept of the biomedical signal monitoring, in this application we can take care of the patient even if we are distance apart from him. This is the revolutionary concept in the medical field. The main objective of this is application is to develop the medical the instruments, prototype for the acquisition, processing and transmission of the biomedical signals.
3. Event detection: much work has been done in the fields of tracking. Instant tracking of events will be done through the WSN's. Collaborative event detection and tracking is done through the WSN which means (CollECT). However some of the issues which are not being addressed yet are the data dissemination and

routing in the wireless heterogeneous sensor network. In this crisp values are being used which characterize the event. In case of multiple event detection. Sometime it is tough to detect the data due to the noise components then a scheme named as compressed sensing is used, which gives us the efficient recovery of the data. It is used to reconstruct the source signal which contains multiple simultaneous events.

4. Military applications: WSN plays a vital role in the military applications by military command, control, communication surveillance and the intelligence. Basically for military uses it provides us a C4ISRT approach. In military, energy consumption is much more because of data or corrupting control devices are attacked. And that's why the nodes will move out from the network. Correct modeling and the energy efficiency of the nodes are yet to be explored. We can use the WSN in the object tracking and detection we need high detection probability, low false alarm rate and bounded detection delay.
5. Industrial applications: WSN gives us very advantageous applications in the industrial field. Distributed architectures are being used in the industrial application and they are dependable inexpensive and flexible. We can improve the system performance by interfacing the sensors and the actuators are directly deployed to the communication network. For the safety purposes in coal mines we use many sensors of gas, temperature wind speed etc. when the value exceeds the given threshold value an alarm will occur. GPRS technologies have been reduced the investment on the layout that is underground. GPRS provides the timely ensure and the rapid and accurate transmissions in underground mining zones and this is how the efficiency is being improved.
6. Intelligent parking: As in metropolitan cities, traffic issues are very common. Vehicle owners or drivers face problems in finding vacant place to park their vehicles. Due to which traffic is generated on roads and parking lots. So to overcome the traffic congestion, parking management systems have been deployed using wireless sensor networks. Parking can be made easy by deploying sensor nodes in the parking lots. The sensor nodes collect the data and then this information is processed to find the parking time of vehicles, payment of parking lot etc. Hence beneficial to the parking lot managers and the vehicle owners. Hence traffic can be controlled by using WSNs.

OSI model: The foundation for wireless sensor network is the OSI model acronym for open system interconnection. It is a networking framework. It is used to implementing the protocols in seven layers. It is ISO standardized. It is seven layered structure as shown in fig.3

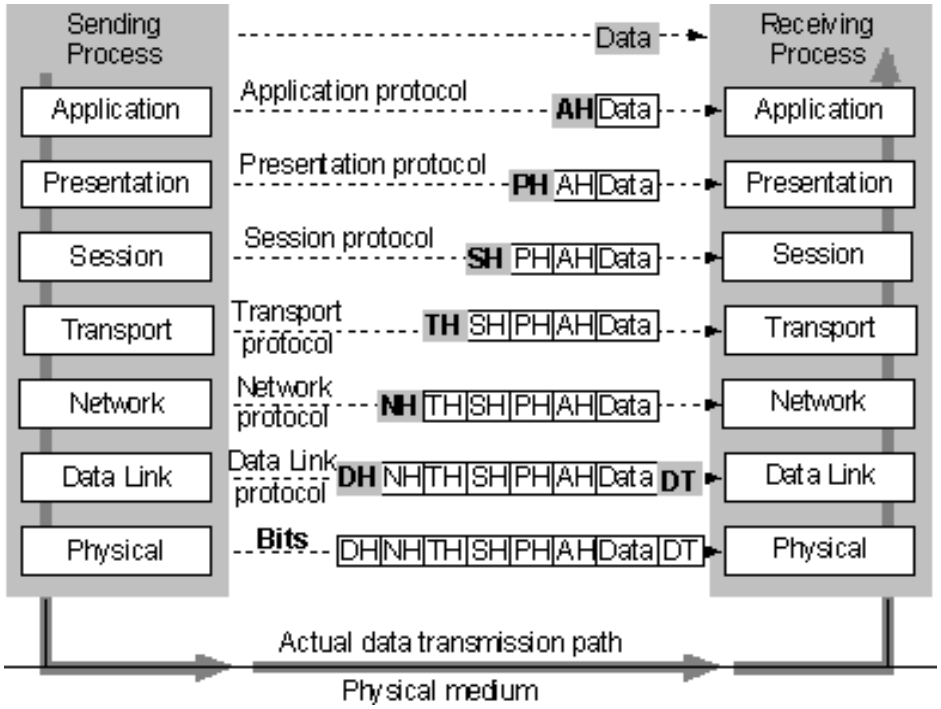

Fig3. Various layers of OSI model

Let us discuss each and every layer of OSI model in brief. Each layer can communicate with the layers above and below to it like transport layer may communicate with network layer and session layer. The development of each layer takes independently and this adds up to the flexibility to the network. As the data is passed through each layer some of the relevant data is get attached to the data that is passing through the layers. This process is known as Encapsulation.

1. Physical layer: This layer is dealing with the bits. Coordination of bits is done by this layer. Launching of bits takes place in physical layer. It tells us about the physical characteristics of the interface used between the devices and the transmission medium. This layer throws a light on which transmission medium we are using. It tells us about the representation of bits (0 and1). Bits are being encoded in to optical or electrical signal in this layer. This layer helps to synchronize the sender and receiver at the bit level. Physical layer tells us the basic idea that which topology is being used, which line configuration is

being used either it is multipoint or point to point or which mode is being used e.g. half duplex, full duplex.

2. Data link layer: this layer basically deals with the frames. This is two party communication and exchanging frames between the two nodes. This tells us that how we can move information between multiple devices by using the same logical network based on physical device addressing. It makes the physical layer error free to the upper layer (network). The basic purpose of the data link layer is to organize the bits into logical groups called frames. This layer is further categorizing into two sub-layers: LLC (logical link control) and MAC (media access control). These layers are responsible for error control and flow control. MAC is used to carry the address of each device on the network. It is 48 bit address which is burned on the network interface card. The work done by the physical layer is to control the flow error and the access. It is also responsible for making the frames (framing) and it proves the physical addressing. Access control tells us that, when two devices are sharing the same link then access control tells us that which device is having control over the link.

3. Network layer: this layer dealing with the packets. This layer is responsible for the delivery of packets from source to the destination. Until the packets are received at the final destination the buffering of packets takes place in the network. The basic purpose of this layer is "Routing". It tells how the information can be moved to the multiple independent networks based on network layer addressing. If the system are fetching information from the same link then there is no use of network layer, if systems are attached to the different links then the network layer must be inevitable. It defines the route discovery (the selection of routes) n provides the logical addressing. The physical address is implemented at the data link layer and handles the addressing problem locally but if the packet passes the boundary then we need logical addressing. This layer adds up a header to the packet coming from upper layer with source and destination logical addresses. Routing is an important concept in network layer. In a large network routers or switches route the packets to their final destination.

4. Transport layer: This layer is responsible for the process to process delivery of the entire message. Network layer is used for the delivery from host to destination. Network layer does not recognize the relation between packets but the transport layer tells us about the arrival of whole message. It oversees the flow and error control as well from process

to process. It establishes an end to end relation between the source and destination. The data unit belongs to transport layer is TPDU (transport protocol data unit). As we know there are several processes which are running simultaneously in the computer, the transport layer header contains the port address which ensures the source to destination delivery n give the specification of the process. Transport layer provides the segmentation n reassembly which means that the bits are divided into segments and then the segments are assigned with the sequence numbers that makes easy to reassemble the segments on the time of arrival. We can also confirm the loss of packet during the transmission. The control also a duty of transport layer, it may be connection oriented or connectionless. Connection is established with the destination machine if it is connection oriented and if it not connectionless then each segment is treated as independent packet and deliver to the transport layer of the destination machine. It also has the ability for flow control and error control.

Session layer: It is responsible for the ongoing communication between two parties which is called a session across the network. As long as the session is staying, the application on either side of the session can transmit the data or send packets. It manages the session setup and tears down it when the session ends. It keeps an eye on the session identification, so that only designated members can interchange their information and the authentication remains safe. It provides us a dialogue box which provides us the two way communication. It permits the traffic to go both sides or in the one direction at a time. Token is being provided for avoiding the same operation held at a same time. The side that is having the token is allowable to perform the critical operation. It's another service is synchronization , which means that the file that is being crashes while transmitting and not being able to perform the transfer and the process is repeated for the complete transfer. To avoid this kind of problems, we use the synchronization, which add up the checkpoints to the data stream, so that after the crash only the data after the checkpoint has to be repeated. The data unit of this layer is SPDU (session protocol data unit).

Presentation layer: It manages and responsible for the format of the data during network communication. Its main concern is over the syntax and the semantics of the information transmitted. Its work is to convert the data into the generic format when it is in the outgoing process. When the data is in incoming process, this layer converts the incoming data into the format that is understandable by the receiver end. Each computer is having its own code to representing data. So the presentation layer makes it possible for the

computers with the different codes to communicate. It provides common communication services like data compression, reformatting and encryption. Data compression is used to decrease the size of data that is being transmitted and the cryptography is used for the security purposes (privacy and authentication). The data unit of this layer is PPDU (presentation protocol data unit).

Application layer: it mainly provides us the user interface that is used to connect the human or software to access the network. It is helpful to the services like e-mail, remote file access and transfer, shared database management etc. the data unit of this layer is APDU (application protocol data unit). Its main purpose is the file transfer means file is being moved between different systems, reading deleting and writing of remote files. It also manages the remote file storage and this process is known as network virtual terminal. In this layer, through simulation of real terminal we can access applications in different remote computer systems. It provides the facility for the electronic exchange of documents e.g. e-mails. The directory service is used to match the names with addressing information.

ROUTING IN WIRELESS SENSOR NETWORKS: The process of moving a packet from source to destination is called routing. The routing is done by the devices called routers. The basic feature of internet is routing. Because with the help of routing, we can transfer the data from one computer to another and finally to the destination machine. Intermediate devices are acting as routers (computers). Routing table is used to identifying or analyzing the best path. We can move from source to destination with the help of the routing tables. Sometimes we got confused in routing and bridging. Basically bridging is done at low level and mostly it is implemented on the hardware part, but the routing is at higher levels and can perform much complex functions. Routing emphasizes on the software part which is of more concern. Now the question arises, how the routers can identify the best path for doing their job? How the paths have been created? This job is done by routing protocols. Routing protocols suggests a path to the routers that how they will communicate. Routing protocols suggests us the choice of route. Each router is having the information of the networks attached to it directly. Firstly, routing protocols establishes the contact with the neighboring nodes and then the data is transmitted thoroughly. This is how the routers come to know about the topology of the network. Basically there are three types of routing protocols:

(a) *Flat based routing*

(b) *Hierarchical based routing*

(c) *Location based routing.*

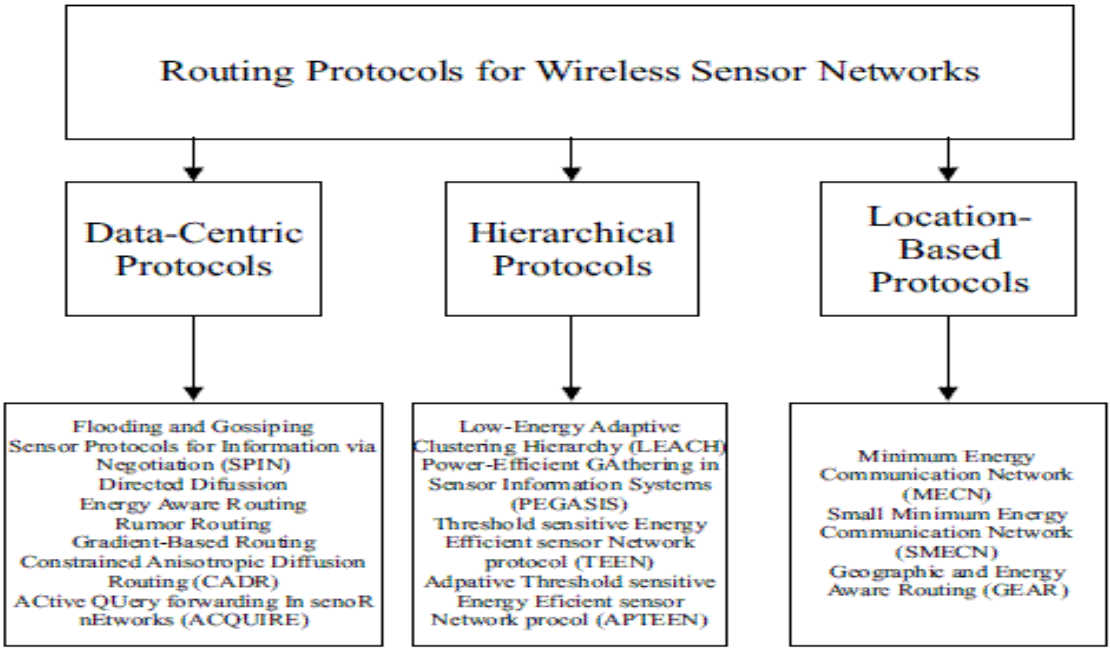

Fig.4 routing protocols for wireless sensor network

*Flat based routing***:** In flat based routing huge amount of sensor nodes are required. Every node has some its own role in flat based routing. As we know, the number of nodes required in flat based routing is very large so it is not possible to assign the identification to each and every node. So in that case we provide GPS to some of the nodes within the network so that the neighboring nodes come to know their own address. Therefore in this we requires a *data centric approach* in which a base station is required to send the query to a group of particular nodes in a particular region and waits for the response. Some of the e.g. of the flat based routing are energy aware routing (EAR), direct diffusion (DD), sequential assignment routing (SAR), minimum cost forwarding algorithm (MCFA), sensor protocols for information via negotiation (SPIN), active query forwarding in sensor networks (ACQUIRE), ad-hoc on demand distance vector routing (AODV).

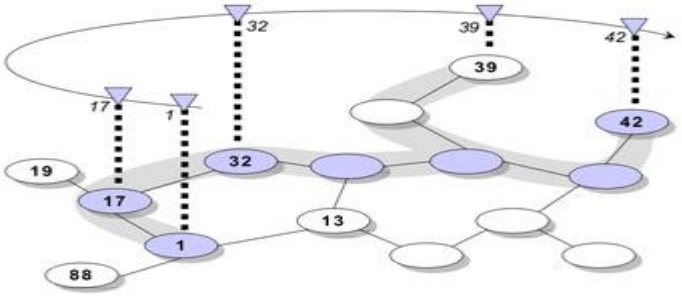

Fig.5 flat based routing

Hierarchical based routing: when the communication is needed efficiently then the best match for that is hierarchical based routing. In this clusters are being used as commonly known as the cluster based routing. This routing technique is energy efficient technique because in this the nodes having the higher energy are randomly selected for the main tasks like processing and sending the data. While the other nodes (low energy nodes) are only used for sensing and it uses to send the data to the cluster heads. It enhances the scalability of the network life time and minimum energy. In this routers are arranged in a well manner which decreases the complexity of the network. Some of the e.g. of the hierarchical based routing are hierarchical power active routing (HPAR), threshold sensitive energy efficient sensor network protocol (TEEN), power efficient gathering in power info systems, minimum energy communication network (MECN), adaptive power threshold sensitive energy efficient sensor network protocol (APTEEN), low energy adaptive clustering hierarchy(LEACH).

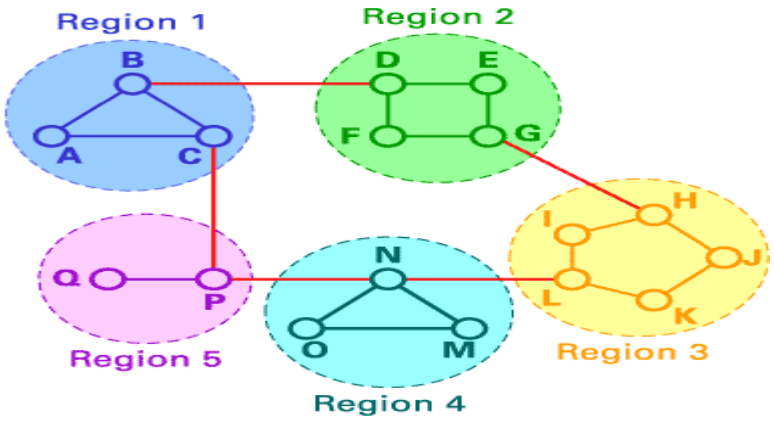

Fig.6 Hierarchical based routing

Location based routing: In this kind of routing the nodes are randomly scattered in the area in which networking is to be done and we know the positions of the deployed nodes with the help of GPS. The signal strength is the main parameter in the location based routing because with the help of signal strength we come to know about the distance between the nodes. Distance can be estimated by calculating the signal strength from those nodes and coordinates and calculates by exchanging the information between the neighboring nodes. Basic examples of these routing protocols are: sequential assignment routing (SAR), ad-hoc positioning system (APS), geographic adaptive fidelity (GAF), greedy other adaptive face routing (GOAFER), geographic distance routing (GEDIR).

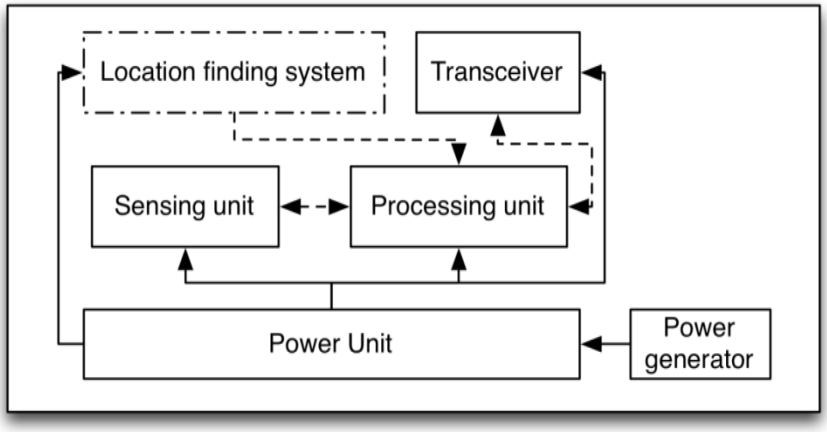

Fig7. Location based routing

AODV: AODV is a flat based routing protocol and as in flat based routing the routers or nodes are placed without any hierarchical manner, so it is known as ad-hoc protocol. AODV routing protocol is mainly used for wireless sensor networks which are ad-hoc in nature such as MANET's i.e. mobile ad-hoc networks. Basically in AODV, the network remains still until the transmission or link is needed. When a node needs a route or path to transmit data, it sends the request for the path in the whole network. The nodes present in the network, receive the request and send the replies in the form of temporary routes. The node which is waiting for the connection, checks for the temporary paths and selects the path to the destination node. The path selected by the source node is reliable and contains less number of hops. After the data has been transmitted, the path is terminated. In AODV protocol, the route is created whenever needed, so the energy can be saved and network becomes efficient. When there is a failure in the network, a routing error message is circulated in the whole network. The source node receives the routing error message and repeats the process for creating a new route. In AODV, the temporary route requests sent by the nodes are having a unique sequence number so that the routes are not repeated

again and again. Every route request has a certain lifetime, so that they are not retransmitted after their lifetime ends. But due to this feature, when a link fails, the new route request takes time to be sent because it takes time twice to lifetime to retransmit the same route request. AODV routing protocol decreases the traffic during communication and is simple and hence no complex computation is required for it.

In AODV routing protocol, the process of creating or discovering the route and terminating the route or connection is based on a mechanism in which routing messages are circulated in the whole network. These routing messages are RREQ, RREP and RERR. These messages are circulated during the discovery and termination of the routes. RREQ stands for route request. Whenever a node present in the network needs to send the data or information, it needs a route for it. As we know in AODV as the name suggests, the route is created whenever the data is to be sent. So the source node sends the route request message i.e. RREQ message in the whole network. When the RREQ message is broadcasted in the network, the destination as well as the intermediate nodes sends the route replies i.e. RREP message to the source node. The source node receives the RREP message from the nodes. Each route reply message consists of a sequence number. The source node selects a path with less intermediate hopes and hence the connection is established. If there occur a path failure, the intermediate node will send the RERR message i.e. route error message to the source and the process of detection and termination of the path will be repeated again. As in AODV the shortest path is selected for communication. In AODV routing, there arise many problems like data aggregation, congestion, energy consumption, grey hole/ black hole effect which effect the routing in AODV. Hence to overcome these problems we use various algorithms or techniques. We will study further about these problems and how to avoid these problems. So as to make the AODV routing more energy efficient and reliable. Hence we will use algorithms like spanning tree, cooperative based AODV, MST, distance vector routing etc. techniques to mitigate these problems being faced in AODV and to make the AODV more efficient.

The literature review of the AODV routing says that it is an on demand routing protocol which is finding the route when the demand arises. Control messages are being used in the ad hoc on demand vector routing these are:

(a). RREQ – ROUTE REQUEST

(b). RREP – ROUTE REPLY

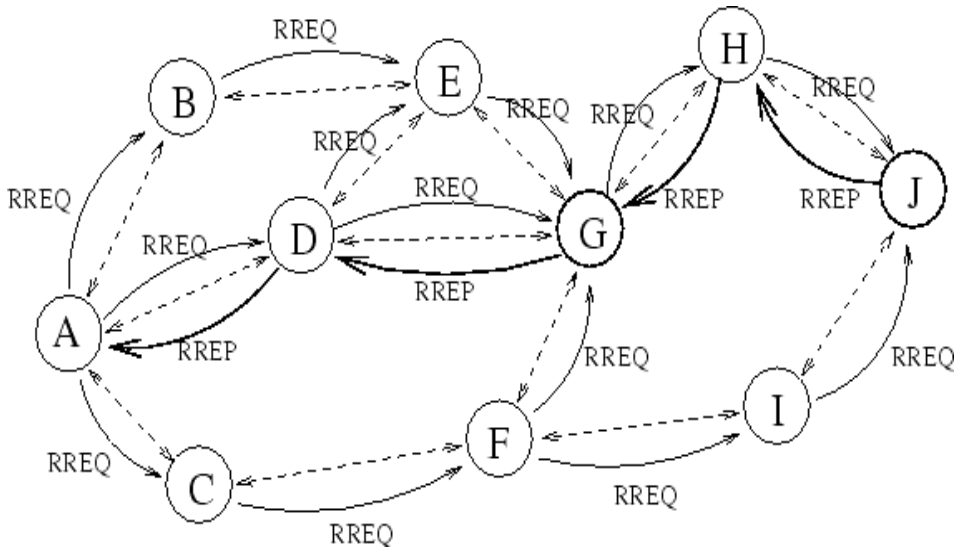

Figure8. Routing in AODV

We have seen a rapid growth for the wireless sensor networks in the research area also in mobile and ad hoc networking. We need to have new set of networking for efficient and end to end communication. There are many advantages provided by the mobile ad hoc networks in battle field and the recovery of the disaster. The TCP/IP structure is followed by MANET to provide the reliable communication. As we know that there is mobility of the nodes and limited resources (power supply) is there so we have to suffer from various challenges in MANET. Routing is the dominant research area in the MANET. There are some challenges along with the problem of routing that are mentioned under:

Security: This is the primary concern associated with the AODV. Security is the key feature for any network. This area is not explored yet to the limits. There are many attacks that are faced by the AODV like black hole attack, grey hole attack, worm hole attack (malicious attacks). There are many techniques proposed by the authors to detect and mitigate the effects if the attacks. As a result of these attacks denial of service came into existence. Cryptographic techniques and the encryption techniques are being used to solve this problem. By using these techniques the data should be confidential enough and the problem of the denial of service would be overcome. These attacks deteriorate the service of the network by dropping the packets, denial of service by altering the information in the packets there are many techniques to solve the security issues but till now this problem is indeed one of the serious problem of AODV.

Quality of service: quality of service means the fare use of various resources offered by the network. It is characterized by some factors (jitter, throughput and loss). The

parameter is defined by the QOS that which is better. Quality of service is also an important challenge in the domain of wireless sensor networks. AODV has a challenge to provide quality of service with least delay and bandwidth. In quality of service there are many factors that are included like end to end delivery of the packet, packet loss, effective and efficient use of the protocols. As there is lack of resources and the frequent change of the topology, that is why the quality of service is becomes a challenging task in AODV. Some of the changes have been done and the AODV-D provides better quality of service.

Scalability: As in large ad-hoc networks, large numbers of nodes are deployed. Hence it becomes difficult to provide service at acceptable level. So parameters like end to end delay, throughput etc. must be considered. Scalability is basically the ability of the network to provide efficient service even if large number of nodes is present in the network. So it is required to optimize the routing in ad-hoc networks to improve the scalability factor and to make the communication more reliable.

Energy efficiency: In ad-hoc network, nodes are placed without any hierarchy. And the routes are created as per requirement. Whenever the sender wants to send the packets, it broadcasts the route request message in the network and the nodes present in the network send the route reply messages with their unique sequence numbers. Hence the route with less hop count is selected. Now as the ad-hoc networks are established in remote areas, so nodes which are deployed in the network must have longer lifetime i.e. longer battery life. In AODV routing protocol, the path with less hop count is selected for transmission of packets. So if this path is selected as shortest path again and again for faster transmission, the nodes present in the path may exhaust faster, creating a network failure. Hence the network will be disconnected and communication will be stopped. Hence an energy efficient network is required to make the communication more reliable. Battery lifetime time should be maximized to increase the lifetime of the network.

Now the concept comes about the black holes that come under the issue of security, it is also a severe attack on the network among the other attacks. In this what happens, that the a malicious node captures the path towards themselves by making a claim that this malicious node is having highest sequence number and also having the smaller hop count to the destination. In such a case the source node sends all of its data packets to the malicious nodes and this will never transmit the data packets to the original destinations

that is why an interruption causes among the source and the destination nodes and the communication will suffer. The AODV recognize the RREP with higher number as the fresh ones. And then the source nodes sends the information and the communication gets interrupted. Same as the black holes there arises another attack known as grey hole, in gray holes the whole packet is not dropped only the part of the packet is dropped. We can overcome the problem of balck holes and the grey holes by using the AODV routing protocols. In AODV routing protocols what haapens that the source not do not transmit all the packets and waits for all the route replies from the neighboring nodes. then the source node compare all the route replies from the neighnboring nodes which is having the same next hop as the other alternative routes. This is the method we can detect the black holes.now another method known as (PCBHA) prevention of cooperaion balck hole effect tells about the precense of the black hole by the threshold values. We can grey holes by two thresholds one is counter threshold and second threshold stage is query based that uses the acknowlegement from the intermediate nodes. intrusion detetction is also used to detect the grey holes each node is maintained by one hop. Larger bandwidth is required for the IDS (intrusion detection system).

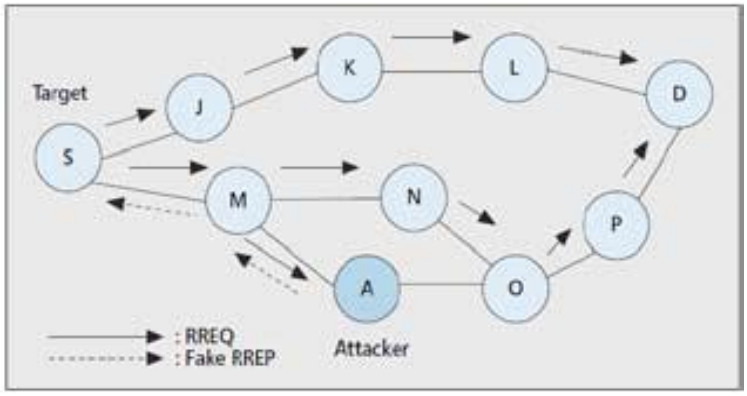

Fig9. Black hole attack

CHAPTER: 2

LITERATURE SURVEY: The main issue in wired and wireless networks is network security; it is the main requirement in the emerging field. The main attributes which should be satisfies in any network are authentication, confidentiality, access of integrity and non repudiation. Black hole attacks are prone in MANET's (Mobile Ad-hoc Network). MANET is a self configurable, self deployable and infrastructure less network in which nodes are continuously moving and creates dynamic topology. Mobile ad hoc network (MANET) is a collection of mobile hosts without the required intervention of any existing infrastructure or centralized access point such as a base station. The nodes of MANET do not require any infrastructure to communicate with one another. MANET's are used basically in the conditions where the wired and wireless infrastructure is inaccessible, overloaded, and destroyed. E.g. disaster relief applications and tactical battlefields. MANET is not dependent on the fixed infrastructure where each node acts as an intermediate switch. The transmission of data or we can say that routing is done through different routing protocols. It is the recent active field and is getting spectacular attention because of self configuration and self maintenance, but security is the main issue which should be kept under consideration to protect the communication from the hostile environment. The present status of a node should be broadcasted to its neighbors before the source node wants to communicate with the target node. Because the current routing information is not known to the other nodes.

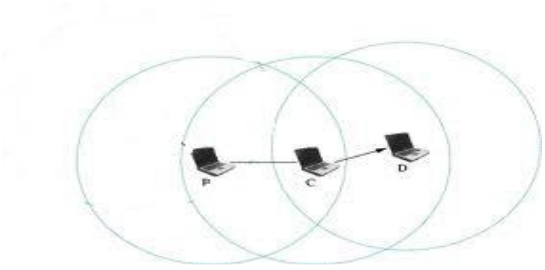

Fig10.MANET

Basically there are three routing protocols named as:

Proactive routing protocol (table driven): it is also known as table driven protocol. In this type of routing protocol the nodes flashes their routing information to the neighbors periodically. Each node should have to manage its table by its own. The table should

consist up of the number of hops, information of adjacent nodes and the reachable nodes. Each node should have to maintain the records of the neighbors as long as the network topology changes. The disadvantage of this protocol is that the overheads have been created in this protocol as the network size increases and the advantage is that the network status flashes immediately when any malicious node joins the network.

Reactive routing protocol: This is also known as on demand routing protocol. The reactive routing only starts when the nodes are willing to send the data packets. The advantage is that the wastage of bandwidth can be reduced by using on demand routing protocols. The disadvantage is that this routing protocol suffers from certain packet loss. The main types of reactive protocol are AODV (ad hoc on demand distance vector) and dynamic source routing protocol (DSR).

Hybrid routing protocol: This protocol is the merged form of reactive and pro active routing protocol. It overcomes the limitations of both the protocol. These routing protocol forms a hierarchical or layered network. At the initial step of hybrid routing proactive routing is employed and gathers the unfamiliar information then to maintain the routing information reactive routing is being used. The type of hybrid routing is zone routing protocol (ZRP) and temporally ordered routing algorithm (TORA) [6]. TORA is highly distributed adaptive routing protocol. The operation is held under dynamic multi hop network. In TORA, to initiate the route the QUERY packet is send to all the neighbors. The QUERY is rebroadcasted through the network until it reaches the destination node. The recipient will broadcasts the UPDATE packet which contains the height list of the nodes with respect to the destination. When this UPDATE packet propagates in the network then each node which so ever is receiving this packet will set its height value higher than the value of neighbor from which the UPDATE packet received. When a node detects a network partition, it will generate a CLEAR packet that results in reset of routing over the ad hoc network.

AODV (ad hoc on demand vector routing) is reactive king of routing and generates the routes on the demands of routes. The key objective of the AODV is route discovery and route maintenance. AODV is one of the most efficient routing protocols for the MANET as it is very dynamic in nature, self starting it also supports multi hop routing and it automatically detects the hidden routes and nevertheless it is loop free. The discovery of

route is initiated when the source node wants to find the route or when the lifetime of the existed route is expired. Each node is having its own sequence number which is increased by one when the topology changes. The topology used in AODV is multi hop. The three basic requests which are being followed by the AODV are RREQ (route request) RREP (route reply) RERR (route error). This process is started by broadcasting the RREQ packet to the neighboring nodes which rebroadcasted by the neighbor nodes until the sought route has been discovered. When RREQ is received by the nodes, some of the intermediate nodes which are having the fresh enough route or itself the destination nodes broadcast the RREP to the source node. Fresh enough route means the destination sequence number of sought node is greater than the destination sequence number of the source node itself. If the source node is getting multiple RREP's then the RREP packet with largest destination sequence number will be chosen and if the destination sequence number is same for two RREP's then the packet with the smallest hop count will be taken into account. RERR [9] is broadcasted when the node is having not any route to the destination. The node which does not have any connection to the destination node will put the address of the destination node in to the list and send the RERR to the other nodes. Then other nodes will check out for the route to the destination node by checking the route map and current list of RERR. If there is not any route present in the table then the RERR sent to the source node. In this way the source node gets the RERR packet.

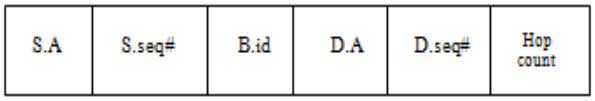

Fig11. Packet format for AODV

The problem of black hole attack is the serious problem that is faced by MANET's. In this attack a malicious node acts as the next node in the routing table and advertises that it is having the shortest path for the transmission of data, and then the interception of data takes place. If the reply of malicious node reache before the reply of the actual node then the forged route has been created and the denial of service, packet drop and other processes are been carried out by the malicious node. Black hole effects are of two types:

1. *Single Black Hole Attack*: in this type of attack an individual node acts as black hole node which hysterics into the route between source and destination. This node belongs to

the data route. When any possibility of attack occur, this node make it active data route element.

2. *Cooperative black hole attack*: as the name suggest, in this a group of nodes acts as malicious node or we can say that malicious node acts in group. Various nodes swallow the packets send by the source node. The initiative steps of this type of attack are likewise single black hole attack and afterwards a chain of attacks from different nodes has been created n therefore the networks gets corrupted easily and gradually.

*Dropping attacks***:** we can classify the dropping attacks as *persistent and intermittent* dropping attack. An attacked connection is called the victim connection and the packets that are being dropped by the attacker are called the victim packets. There are different types of dropping pattern in each victim connection.

Periodic packet dropping (perPD): in this pattern, we would take into account the three main parameters named as (K, I, S) where K is total number of victim packets in the connection, I is the consecutive interval between two packets and S tells us about the position of the first victim packet. Take an example (K=4, I=7, S=4) it depicts that the 4^{th} packet will be dropped, once every 7^{th} packet and starting from the 4^{th} packet seen by the attacker. The attacks created by the malicious nodes slow down the working of the TCP layer.

Retransmission packet dropping (RetPD): it is quite obvious that the intruder will drop the retransmission of specific packet. In this pattern K and S will be taken into consider ability. As S denotes the victim packet K is the number of times the dropping of retransmission packet. For instance a pattern is (3, 8) then the attacker will drop the 8^{th} packet and retransmission will be done 3 times. When the retransmitted packet lost, then the TCP slows down and exponentially start to back out its value. This value is known as (retransmitted timeout value) RTO. We can say that after some consecutive retransmissions being dropped, the destination node has to wait for long time. This period is known as idle period. No packets send in this period.

Random packet dropping (RanPD): this is also known as natural dropping. These patterns have limited number of effect on TCP's performance. Because in this pattern,intruder will randomly choose the value of K which has to be dropped.

DETECTION AND PREVENTION SCHMES OF BLACK HOLE ATTACK IN AODV:

*A.)Detection, prevention, and reactive AODV (DPRAODV)**:*** The concept of ALARM is used in this technique while in other techniques the dynamic threshold value has been used. The RREP sequence number is being checked whether it is higher than the entrance value or not. If the RREP sequence number is higher than the entered vale. Then the sender is considered as an attacker and the name of the node is updated in the black list and the ALARM is being broadcasted to its neighbors who are having the black list. As a result from the all phenomena the RREP from the malicious node is blocked. DPRAODV are highly used to detect the black hole and as well as it we used to prevent the black hole attack by updating the entrance value. The advantage of using this technique that is offers us a higher packet delivery ratio than the actual AODV. The disadvantage of this technique is that it is used to find the single black holes rather than the cooperative black holes

B.)Neighborhood based and routing recovery scheme: This technique is used to create the reliable path to the destination and it also discovers the black hole effect. In this method, we will encounter the black hole by two methods: detection and response. We will simulate it with ns2 and come to know that there is not even a problem of overheads. Neighborhood based method is used to detect the black hole and used to identify the nodes which are not confirmed and the routing recovery scheme is used to build the correct path. In this scheme modify route entry is being send by the source node to create the new path. In this particular scheme the time for detection is small and the throughput is comparatively high. This scheme does not work under the conditions where the cooperative black hole attack is forged.

C.)REWARD against malicious nodes: REWARD (receive, watch, redirect) basically a routing algorithm in which we use a distributed database for the detected black holes attacks. This database keeps the record for the areas and nodes which are supposed to be suspicious. Two types of messages are being used by this technique names as: MISS and SAMBA. When the destination receives any query then it send the RREP to the source node. Assume that the destination nodes do not receive the packets within a specified time then the destination node broadcast a MISS message (material for intersection of

suspicious sets). The destination nodes will copy entire nodes which are involved in the query message to the MISS message. The most probable reason for not getting the packet is the black hole attack. Nodes that are listed under the MISS message are suspicious nodes all the nodes will collect the MISS message and they start to intersect the misbehaving participant nodes in the route. Another reason for not receiving the packet may be collision but the proper organization of nodes can tackle this problem. But the problem arises in dense network where the suspicious nodes may get avoided. This problem can be overcome by path matrices. The path with the highest metric should be selected. If after some destinations the destination nodes receives the same data packets. Each node is transferring the packets to both immediate neighbors. One node is forwarding and one node is back warding. If nay node performs a black hole attack and drops the packet it will surely be detected by the next node in the path. The watcher will wait for a time period and then transmit the packet by changing its path along with broadcasting the SAMBA (suspicious area mark a black hole attack) message. SAMBA message provide the location of the black holes attack.

D.) Distributed cooperative mechanism (DCM): This technique is used to mitigate the problem of collaborative black hole attacks. As the nodes are working with collaboration so this can detect the multiple black hole attack. The DCM is consists up of four sub modules named as local data collection, local detection, cooperative detection, global reaction. In the local data collection phase a table is designed and maintained by each n every node in the network. Overhearing packets are being determined by the nodes to evaluate whether there is malicious node is present or not. If one suspicious node is detected, then the check packets are being sent to the cooperative nodes. If the value of inspection is positive then the suspected node is remarked as the normal node otherwise the detection node starts the cooperative detection procedure and makes a notification to all the neighbors to participate in the decision. Network traffic is going to be increased in this method. Task for the global reaction phase is to execute a notification system and send warnings to all the nodes in the network. There are reaction modes in the global reaction phase; the first reaction phase notifies all the nodes in the network. Along with this overhead communication is being lost. Each node is concerned with its own black hole list and makes other transmission path through other node. The advantage of this technique is that it offers us a higher data delivery ratio.

E.) Intrusion detection system (IDS): It is the detecting mechanism which is used to detect the attacks against the wireless sensor networks. Intruders may be legitimate users or from outside the network. Intrusion detection system looks for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent. The main designs that are for intrusion detection system are: the misuse detection design, hot based, network based and the anomaly detection design. Intrusion can be done through buffer overflows, unexpected combination, unhandled input and race conditions. Anomaly based IDS is the usage of network with noise characteristics. Anything that would be distinct from the noise would be regarded as an intrusion activity. The disadvantage of this design model is that sometimes it may create the false alarms and hence the effectiveness would be compromised. The signature based IDS is programmed to interpret a certain series of packets. Most signature analysis is based on pattern matching algorithms. In this method, IDS looks for the sub string within a stream of data and carried out by packets. And it identifies those network packets as vehicles of attack.

*F) REACT***:** This technique is used for finding out the collaborative black hole attack in the MANET's. It identifies individually the misbehaving nodes in the network that refuses to carry the data because that node is suspicious or malicious node. We can assume that there are two node disjoint path in any network. The identity of each node which is engaged in the path is known to the source. And then the pair wise key is used to protect the communication between the source and the intermediate node. Let's take an assumption that there are k intermediate nodes on the path between S to D. As in reactive method, when any packet drop occurs the destination node will reply back to the source node about the packet drop. Source node will select a node ni and verify that it correctly receives the packet from the previous hop. Source node will send an audit request through another path which is not same as the previous one. Audit request identifies a group of packet sequence number and ni will be asked to generate the behavioral proof by using the bloom filters Then the behavioral proof of the packets will be generated by using bloom filter. Bloom filter is much smaller than the length of the whole packet. After generating the behavioral proof in signs the request and send it to S. the source node will generate its own behavioral proof based on the selected packets .then the comparison of both the behavioral proofs is done one behavior proof is from s and other is from ni .if the proofs are similar then S concludes that the misbehaving node is in between ni to D. And if it is not so then the misbehaving node will b in between S to ni This approach will not

store the overheads and large communication. The process is continued till the two neighboring nodes are left in the suspicious set.

*G.) DRI and cross checking***:** this technique is used to find out the collaborative or we can say that cooperative black hole attack in MANET's. In this technique the AODV is enhanced with an additional feature known as DRI table (data routing information).in these two additional requests are being added known as FREQ FREP. Each node will maintain its own DRI table. 1 represents for true and 0 stands for false. The keywords of this technique are "from" and "through" means from which node data is coming n through which node the data is coming. The entry 1;1 in the table implies that the node 1 has successfully transmitted the data from or through node5. The entry 0;0 means that the data is not routed successfully from and through node 3. Let us create a scenario, where SN stands for source node IN stands for intermediate node NHN stands for next hop node.SN will broadcast RREQ and will get back RREP from the node and packets are being sent to that node. Intermediate node sends next hope node and DRI table to the source node. In the next step, the SN crosschecks its own DRI table with the DRI table that has been sent through the intermediate node to check the honesty of the intermediate node. SN will send request to the intermediate node's next hope node and asks for the routing information including the NHN, the NHN's DRI and its own DRI table. In the last step comparison is being done by the source node to find out the presence of the malicious node in the route. The disadvantage of this scheme is that the mobile nodes have to maintain extra database for the past routing information.

H.)Multiple base station technique for finding black hole attack: It is very advantageous to use multiple base stations in WSN. The advantage by using the multiple base stations are decrease in energy consumption, scalability will be highly achieved and gradual computing accuracy with high accuracy. Instead of transmitting the data through the network we will send the agents through the network. the importance is more for the data delivery to the base station than to prevent the data capture by adversary .we are emphasizing on the packet delivery to the nodes which can be done by having various base stations to improve the likelihood of packets from the source node reaching at least one base station in the network. It will ensure us high packet delivery ratio. Multiple base stations to handle the flow of large amounts of, heterogeneous data from the network and several Optimization techniques have been designed for query Allocation and base station

placement. So by using the multiple base stations we can maximize the delivery ration in the presence of the black holes. Source node can route the data packets to all the base stations in the network. Base stations are connected over by the wired network. We assume that the SNs in the network can be compromised by an external adversary and programmed to analyze the packets they receive and drop them instead of forwarding them to the BSs. We refer to a compromised SN as a black hole node. The adversary is capable of compromising more than one SN in the network, thus creating one or more black Hole regions. In addition, the compromised nodes are capable of colliding with other compromised nodes in their neighborhood or in other black hole regions to analyze the captured packets. We assume that the SNs in the black hole region do not perform their environment sensing tasks as they are compromised.

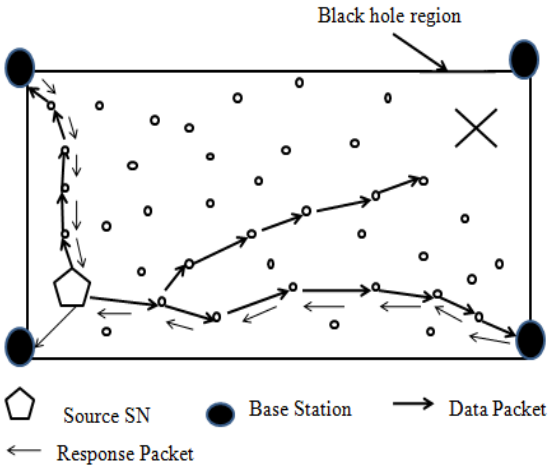

Fig11. Data delivery success improved with multiple base stations

I.)BAAP (black hole avoidance protocol): we can detect the black hole attack in the network without using any external hardware. This protocol proposes ad hoc on demand multipath distance vector (AOMDV) .Correct path is established by the nodes by having proper legitimacy with the neighboring nodes. Intermediate node will create a route in which that node will not participate whose legitimacy ratio value is more than the threshold value. The packet loss in AODV is 90% while in BAAP [22] it is 15.6% to 21.3% in the presence of two three malicious nodes.

J.) Honey pot scheme of detection: In honey pot detection scheme, topological knowledge is used to detect the spurious advertisement of routes. Trip of the network is done by some deployed roaming software and luring of attackers is being done by

sending route requests advertisement. This is how; enough valuable knowledge is collected by using intrusion logs. But the drawback of this algorithm is that it is not for MANET this is used by WMN as it is not proactive phenomena and the honey pot is not having the centralized authority.

Some other techniques to detect and mitigate the effects of the black hole attack:

SAODV: it represents the solution to the black hole attack ad hoc on demand vector routing. In solution AODV the source node will not send the data packets instantly in fact the source node wait for the other route replies from the other neighboring nodes until the threshold time remains active. CRRT (collect route reply table) is used for collecting all the route replies. Then in CRRT, it is checked that there is any repeated next hop node is present or not. If the next hop node is there in the CRRT then it would be safe to transmit the data packets.

Real time monitoring: in this method we will check the neighbors of the RREP node creator and these are known as suspected nodes. Now it's the duty of the neighbor node to visualize the packets send by the suspected node. Neighbor node is counting two counters named as F count and R count. Addition of 1 takes place in the f count counter, when the neighbor node sends the packet to the suspected node. Now overhearing takes place by neighbor node when the suspected node will forward the packet and the r count is increased by the value 1. If the source node is receiving RREP from the node, it sends the data packets over the path to know that the node is malicious or not. Neighbor node is sending the packets to the suspected node till the f count reaches to the threshold. And when the r count becomes zero, RREP creator is identify as the malicious node and is blocked in the network.

Detect and overcome black hole effect: we can detect and overcome the black hole effect by modifying the original AODV. The node who originates the RREP must be honest. If the node is first to receive the RREP it may send directly it to the source node based on the opinion of the neighbors of RREP originator nodes. The neighboring nodes are requested to send an opinion about the RREP originator nodes. After receiving the reply, the source node comes to know that this is an honest node because RREP originator nodes have delivered many packets to the destination. If RREP originator nodes are

having many received packets but do not move it further and the RREP packets are more in number then this node may also considered as the misbehaving node.

Comparison of destination sequence number: This method is used to prevent black hole effect in the AODV: All the RREP's from all the intermediate nodes are collected by the source node. The entry received by the source at the very beginning is marked as first entry in route reply table. The destination sequence number which is supported by the first entry is compared with the source sequence number. Now, if the sequence number is very less than the destination sequence number of the first entry then the node is to be considered as the malicious node. And this node is removed from the table. Now the path is selected from the remaining entries that are arranged in order by DSN. The node which is having the highest DSN is selected for route.

Secure route discovery to avoid black hole effect: in this method, different threshold values are assigned for different environmental conditions like small large and medium. The threshold value that is assigned to the environments is having some percentage of maximum sequence number. Two extra function units are being added to this first one is that the source node is using the threshold value to check the RREP from the neighboring nodes and second unit is that the destination node use the threshold value that is defined to check the RREQ message from the source node. If the destination sequence number of RREP exceeds its value from the threshold value then the node is considered to be malicious node

Calculation of peak value to detect black hole effect: during the route discovery process malicious nodes are being detected. In this process three parameters are being used that are 1.RREP sequence number 2. Routing table sequence number 3.number of replies received during the tome interval. Peak value is the maximum value of any RREP sequence number. If the peak value is less than the RREP value then that node is considered as the malicious node

We are proposing a solution to overcome the consequences of black hole effect by using the HOOSC scheme. In this proposed solution we are encrypting the data first and then send the data to the destination node. By using this technique intruder nodes cannot retrieve the information stored in packets. Multi hop routing technique is being used in the HOOSC scheme which means that the transmission of packet from source to

destination is done through the intermediate nodes. HOOSC scheme allows the sender in the identity based cryptography to send a message to the public key infrastructure. We are using 5 algorithms in this scheme. Those five algorithms are named as below:

a.) SET-UP
b.) IBC-KG
c.) PKI-KG
d.) Off-sign crypt
e.) On-sign crypt
f.) Unsigncrypt

CHAPTER: 3

PRESENT WORK:

Problem formulation: As we have discussed all about the ad hoc on demand vector routing and the challenges that are associated with the ad hoc on demand vector routing. The major threat that has been discovered from the survey of the literature is the black hole attack. Like black hole attack there are many other attacks like worm hole attack grey hole attack etc. the results of these attacks is denial of service and the packet drop. The problem is how to save the packets from dropping, for this we proposed a infrastructure known as Clustering. Cluster heads have been chosen by using the CA authority. CA authority provides a digital certificate to the nodes and the keys are being generated by the CA, by using the technique of clustering we can tackle the problem of the black holes attack. Because when the clusters are being generated the total network is divided into clusters and each cluster is having its own cluster head. As we have studied that the cluster head is generated by using the CA the governance of whole cluster is governed by the cluster head. This is how the burden in the network is decreased as cluster head is only responsible for the movement of the nodes. All data about the nodes is incorporated with the cluster head, as the cluster head is having all the information regarding the nodes of its own cluster then the cluster head will surely know about the malicious node and restrict the passage of data to the malicious node. This is how the packet drop can be reduced. And to enhance the security of the network we have incorporated a scheme named as HOOSC scheme heterogeneous online offline sign crypt ion. This is an encryption scheme. The packets that are to be transmitted are in the encrypted form. This scheme is divided in to five phases. The PKI (public key infrastructure) and IBC (identity based cryptography) are being used in this encryption scheme. This is how more secure network can be created that even if there is any security threat that we can overcome with the encryption schemes. Our basic problem is the drop age of the packets which can be mitigated by choosing the clusters and cluster heads. Then to enhance the security we use the HOOSC scheme. By using the digital certificates we can provide confidentiality to the network. The basic meaning of the digital certificate is the passports on the web. Digital certificates are issued by the certification authority. And these certificates are then used in the asymmetric key cryptographic applications. Digital certificates establish the relation between the user and her public key. This give us

the insurance that particular user can use particular public key. Digital certificates are uniquely assigned to the users.

Objective:

- To mitigate the effects of black hole attack.
- To use Clustering to detect the black hole attack node.
- CA is used to find out the cluster head
- To use HOOSC for security enhancement.
- To use the public keys for the nodes that would be secure.

Methodology: The flowchart of the work which we have done in our course by using ns2.

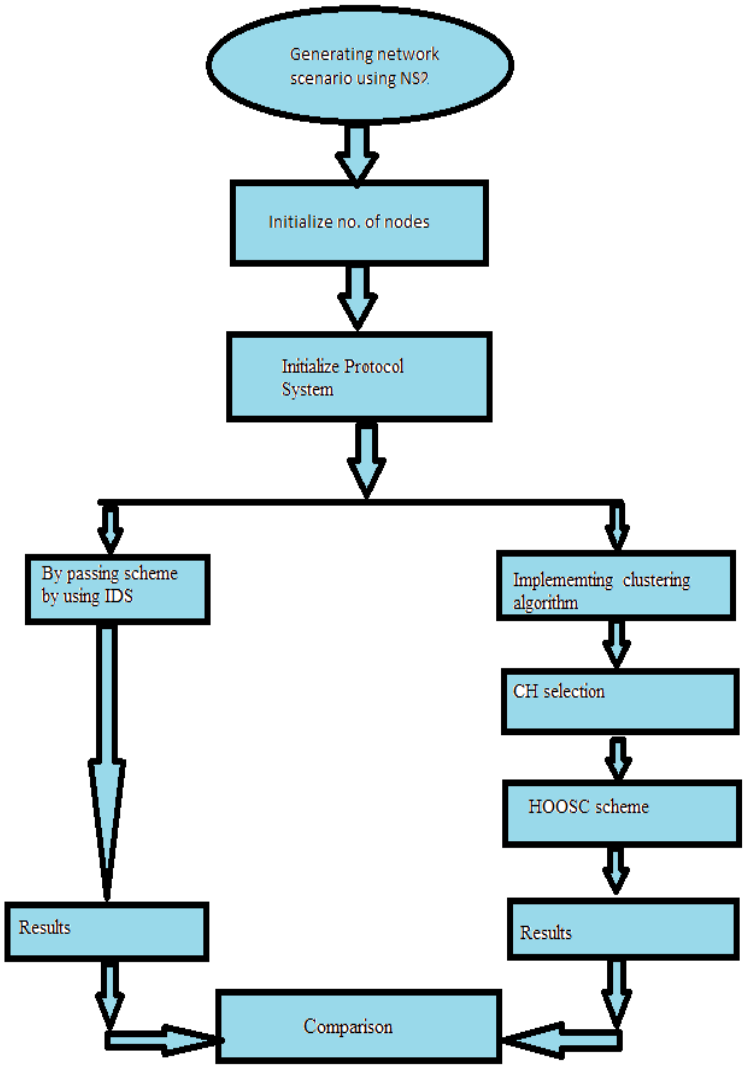

Fig.13 flowchart of black hole detection and encryption

This flowchart gives an idea that how the work have been done by the steps. Now let us explain the whole scenario one by one. The work we have done in the dissertation1 is to detect the black hole node attack. Then we have bypassed the nodes which are suspected nodes and creating the problem of black hole attack. By adjoining the concept of

clustering we can stop the black hole attack up to some extent. Then an encryption scheme is associated to enhance the security aspects. Now we will explain how the work is carried out in this scheme:

1. *Generating network scenario in ns2*: it is an open source and freely distributed.ns2 is used to support networking research and education. We can design our protocol and compare it with other protocols with an ease. New designs that are launched are also supported by the network simulator.tha languages that are used in the network simulator 2 are c++ and OTcl. We can easily configure our network parameters in ns2. There are many parameters that are defined at the starting of the programming that how to proceed the programming, the network area, the no of nodes, the topology all are being discussed prior to the simulation. The main part of the ns2 is c++, we can implement the designs through the c++.The packet flow is done through the c++ on a single node. We can comment out the existing protocols by using the ns2 or we can change also. We are using 2 languages because both are equally important. The c++ is used to run the programs faster which the otcl cannot and on the other hand otcl is used to code the programs faster but runs slowly. So both languages are playing a vital role in ns2. There are various protocols that are been supported by the ns2 that are listed below:

    - It can support unicast multicast and the hierarchal routing.
    - Transportation is done through TCP and UDP.
    - The queuing disciples that are used are drop tail and RED (random early drop).
    - Web, ftp, telnet and CBR are the sources for traffic sources.

NAM (network animator) is based on the graphical user interface. We can see the animations here. Traffic and topology is generated first in the pre processing and then the simple trace analysis is carried out which is carried out by the awk or tcl files. The processing of the ns2 is done by the steps which we are going to discuss. In the first step the event is created then we will turn it on to the tracing. After that a network is being generated and the simulation is ready to proceed. Then the routing algorithms are used to set up the routing, like which type of routing we want to have in the network. Errors are

being inserted to the network and the transport connection is created (TCP UDP). We will adjoin the traffic agents with this like CBR traffic agent. The format for the file is like:

<Event> <time> <from> <to> <pkt_type> <pkt_size> <flags> <fid> <src> <dst> <seq> <uid>

In ns2 the topology is defined first as it is a basic facility and the relationship between two is defined. Containers and helpers are used to facilitate this process. Then models are established e.g. UDP, point to point devices and links and applications. Then the node and the link configuration are come into existence. The values of the models are defined by default. Sometimes attribute system is used to set the values of the models. Execution is done on the logged data and the requested data. Once the execution is done then the performance analysis done and the graphical interpretation can be visualized in a very fine way.

2. *Initialize no of nodes*: Once the network scenario is created using ns2tool we will initialize the no of nodes in the network the selection of no of nodes in the network is based on the type of protocol and the topology.
3. *Initialize the protocol system:* After selecting the no of nodes in the network we will initialize the protocol system. As we are working on ad hoc networks, we will initialize the AODV protocol system.
4. *By passing scheme by using IDS:* The base paper I have chosen for my research is "Performance of an intrusion detection system in an ad hoc network under the black hole effect" gives us the idea that how the performance of the system can be increased by using the IDS and we can remove the black holes too by using IDS. IDS can remove the denial of service which was created by the malicious effect. IDS can also deal with the impersonation, which means that if the data to be send is in encrypted form with its private key, but it can be decrypted by any public key. This is known as impersonation and can be avoided by using the IDS. If the receiver will not be able to decrypt the message then the packet is lost and the sender is not considered as the real source. In this way we will detect the malicious nodes and can remove the effect of the black holes. By using this method we can find out the node that is creating the problem and we block that node. The simulator we will use for the research is MATLAB. As we saw the results of the base paper then we come to know that how throughput of the system is high by using the IDS. Throughput of the system with IDS

under the black hole effect is good. In the fig of the base paper this is also shown that how the packet drop are less in number by using the IDS. The overall network performance is good by using the IDS. After these attacks the data is heavily affected. The packet drop is directly depends on the black hole effect. More the nodes are found as black holes more the data packets will be lost. The data packet loss is decreased by using the IDS in AODV protocol.

5. *Result analysis of IDS:* we have analyzed the results in the base paper and with those results we can by-pass the malicious node. But bypassing is not only the solution to this problem, still our network is under the threat and this threat is security threat. So to mitigate this problem we will choose to have clusters in the network and for each cluster one cluster head is selected by using the certification authority. By the help of the cluster head we can detect and overcome the problem of black hole attack and the HOOSC scheme is used to enhance the security features by encryption.
6. *Implementing clustering algorithm:* the grouping of nodes to do a specific task is known as clustering. Scalability and higher efficiency is achieved by using the cluster formation and we can enhance the lifetime of the battery. Data fusion and the aggregation of data are possible by implying clusters and that's why it leads to significant power savings. There is a leader for every cluster and the leader is known as the cluster head that is used for the data aggregation and the data fusion. And the sensor nodes are taken as the members of the cluster. The formation of the cluster is having a two level hierarchy in which the cluster head is from higher level and the cluster members are from the lower level. The data transmission is done periodically and the sensor nodes used to send the data to the corresponding cluster head nodes. Aggregation of the data is done in clustering (that's why the relayed packets are decreased in no) and the data through intermediate nodes or by using another cluster head nodes is send to the base station. Sa the data transmitted by the cluster head nodes is at higher distances so the energy used in this is obviously high then common transmission. Therefore to overcome the problem of the energy a periodic reselection of the cluster heads takes place. This is how each and every node probably may get the chance to become a cluster head. The CH nodes are basically an interface between the sensor nodes and the base station. The base station is a place where the data processing takes place. Cluster head node does the aggregation of data before sending it to the base station. We can say that the CH is the sink for cluster nodes and the base station is acting as a sink for the cluster heads. Replication is done as many times as it

is needed and creates multiple layers. Actually the clusters are the critical parameter with regard to the efficiency. There are two type of clustering intra cluster communication and inter cluster communication. In intra cluster communication the communication is done between the sensor node and the CH of the cluster. In inter clustering the sensor nodes are high in number but the cluster heads are limited to the number.

7. *CA selection:* Nowadays the cluster heads are been selected by the CA (certificate authority). They provide a digital certificate. A digital certificate is a small file. By using the digital certificates we can resolve the problem of exchanging the keys. A digital certificate is used to exchange the keys by preventing the keys from the man in the middle attack. CA authority is used to provide the digital certificate to the nodes. The main CA is VeriSign and Entrust. These certificates are used in the asymmetric key cryptographic applications. The structure of the digital certificate is defined by the X.509.the certificate contains the version, certificate serial number, subject name and the subject unique identifier. As we know that the MANET's are more prone to the security threats so we have to choose a cluster head which can detect the malicious node to avoid the attacks. When the concept of the CA is used the secret key is provided to all the nodes. When any node wants to send the data it broadcasts a message that is R2mod N to all the nodes and the challenge is for the node that is having the same data. If this node also sends the same data, but with the key to the cluster head. Then the comparison of both data from the nodes is carried out. If it is same then is considers as the normal node otherwise it may be taken as the malicious node. When the malicious node is found out then the revocation of the certificate is done and the normal nodes get free to move in the network and the security is increased by using this method. Revocation of the certificate is done just to confirm that this is the authenticated certificate or not. To carry out the process of revocation we have some lists to carry out the whole procedure. The lists are warned list, black list, both the lists hold the accusing and the accused nodes resp. certificate authority generates a certificate and send it to all the cluster heads. Then the generation of the master key is done by cluster heads and master key is send to the members with in the cluster. Subordinate keys are generated by all the cluster members by using the master key of the particular CH. There are n numbers of master keys .n is the number of the cluster members. The subordinate keys are n in number and they are matched with the

master key of that cluster head. If it matches with the master key then the node is considered as the normal node otherwise it is taken as the malicious node.

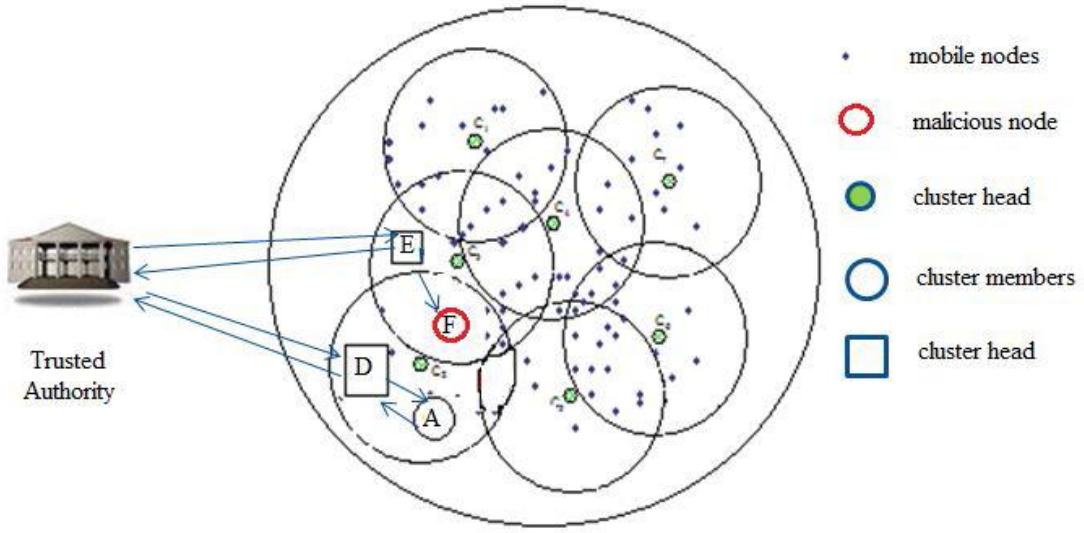

Fig 14. Clusterd network

8.HOOSC scheme: WSN are consists up of tiny sensor nodes with one or more than one base station and with the limited no of resources. The base station is acting as an interface between the sensor nodes and the network user. Base station is used to provide the data to the users in WSN. If we want to read the data anywhere in the world, then we have to integrate the WSN over IOT. Integration of this task can be done through three ways that are front end proxy solution, gateway solution and TCP/IP overlay solution. By doing this we can gain the end to end delivery of the data. Confidentiality and integrity of the message can be kept safe by using these types of techniques. HOOSC scheme is used to maintain the integrity and the confidentiality of the data and thus it provides us a secure network. PKI public key infrastructure and IBC identity based cryptography are used at the sensor node and at the internet host resp. these are the two main infrastructure of the HOOSC scheme. The signcryption is done in this scheme. It means that the public key encryption and the digital signature are done in one single step. In the PKI certificate authority issues the certificate. This certificate builds up a link between the public key and the identity of the user by using the signatures. There are no of certificates in the PKI and this is the solely disadvantage of the PKI to manage all the certificates and revocation. At the IBC side the public key is directly generate from the identity of the user e.g. telephone numbers, email id's etc. secret keys are been generated by the third party known as PKG (private key generator).the main advantage of the IBC is that in this

we do not have to manage all the certificates. The main work that is carried out by the HOOSC scheme is to split the signcryption in two phases: offline phase and the online phase. Light computations take place in the online phase and the heavy computations are being carried on the offline phase. This approach is known as signature then encryption approach and it provides us confidentiality integrity and authentication.

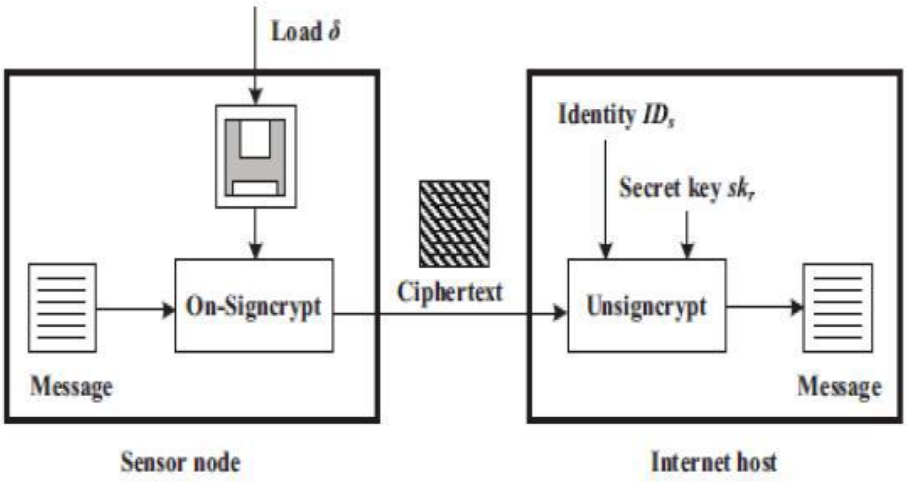

Fig 15.steps for secure communication

8. *Comparison:* we have discussed two methods in detail like IDS (intrusion detection system) and the HOOSC (heterogeneous online offline signcryption) scheme. What we have analyzed that by using the IDS we only by pass the malicious node but that is not the termination of the attack. After some time the node can enter in the broadcasted area and again will claim that it is this node (malicious node) will provide the least hop count and having the highest sequence number and gain the packet. In the HOOSC scheme we have enhanced the security by practicing the clusters in the network by choosing the cluster head using the certification authority. Then after the comparison we come to know that the packet loss and the denial of service are decreased in the case of HOOSC scheme. Along with the detection of the malicious node that is done by the clustering. We have gained the confidentiality and the data integrity of the data.

CHAPTER: 4

RESULTS AND DISCUSSION: In the results and discussions we will give the practical scenario of the study which we have done and give the enhancements to the work. After the detailed study of the techniques we have used in the report and by simulating it on ns2 we have got some results which are shown below:

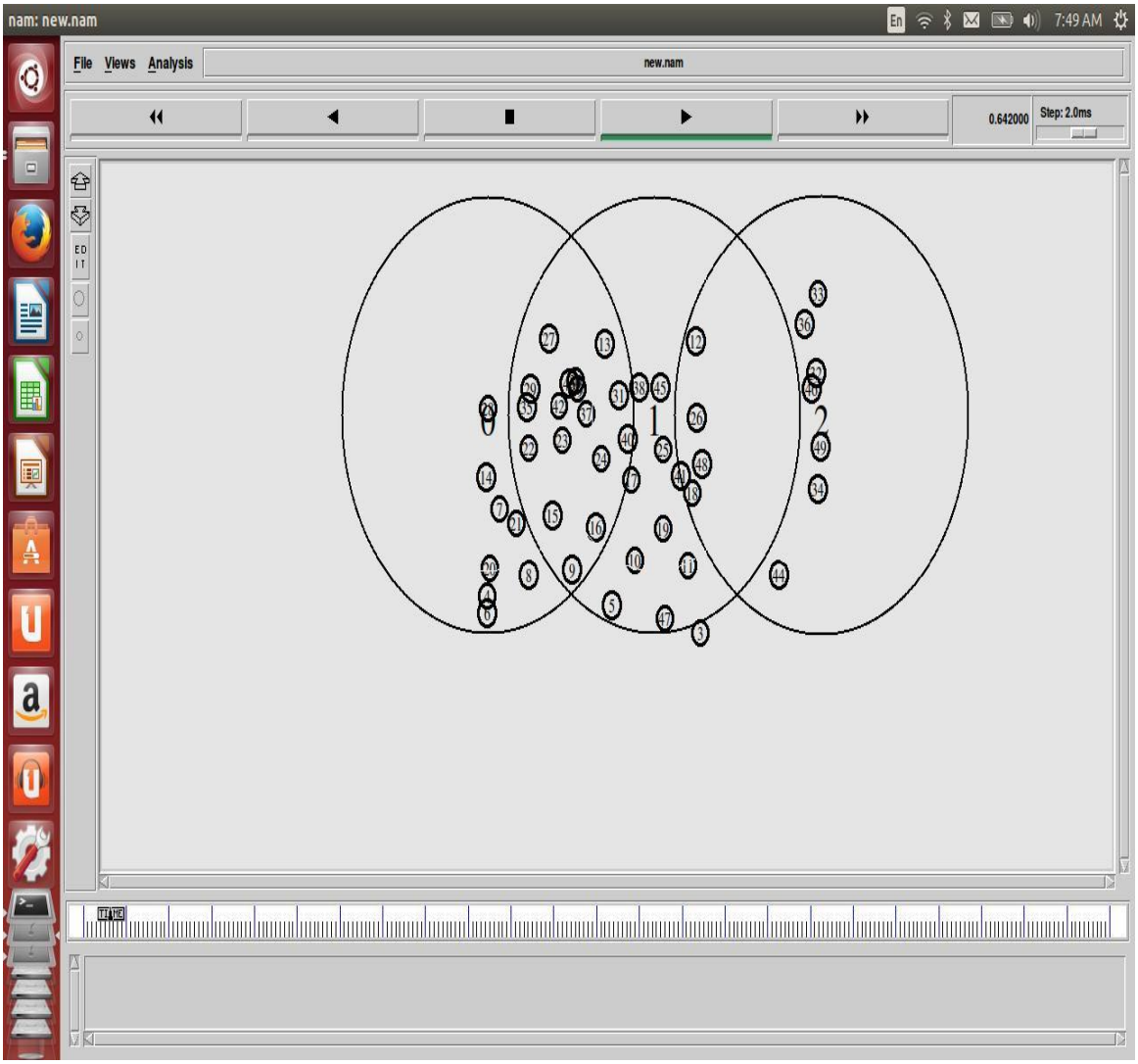

Fig16. Formation of clusters

In this figure, the clusters are being made on the basis of range based clustering. The clusters are made so that the traffic of the network can be controlled. Clusters are made on the basis of different parameters like distance between the nodes to all the nodes the routing algorithm we used etc.

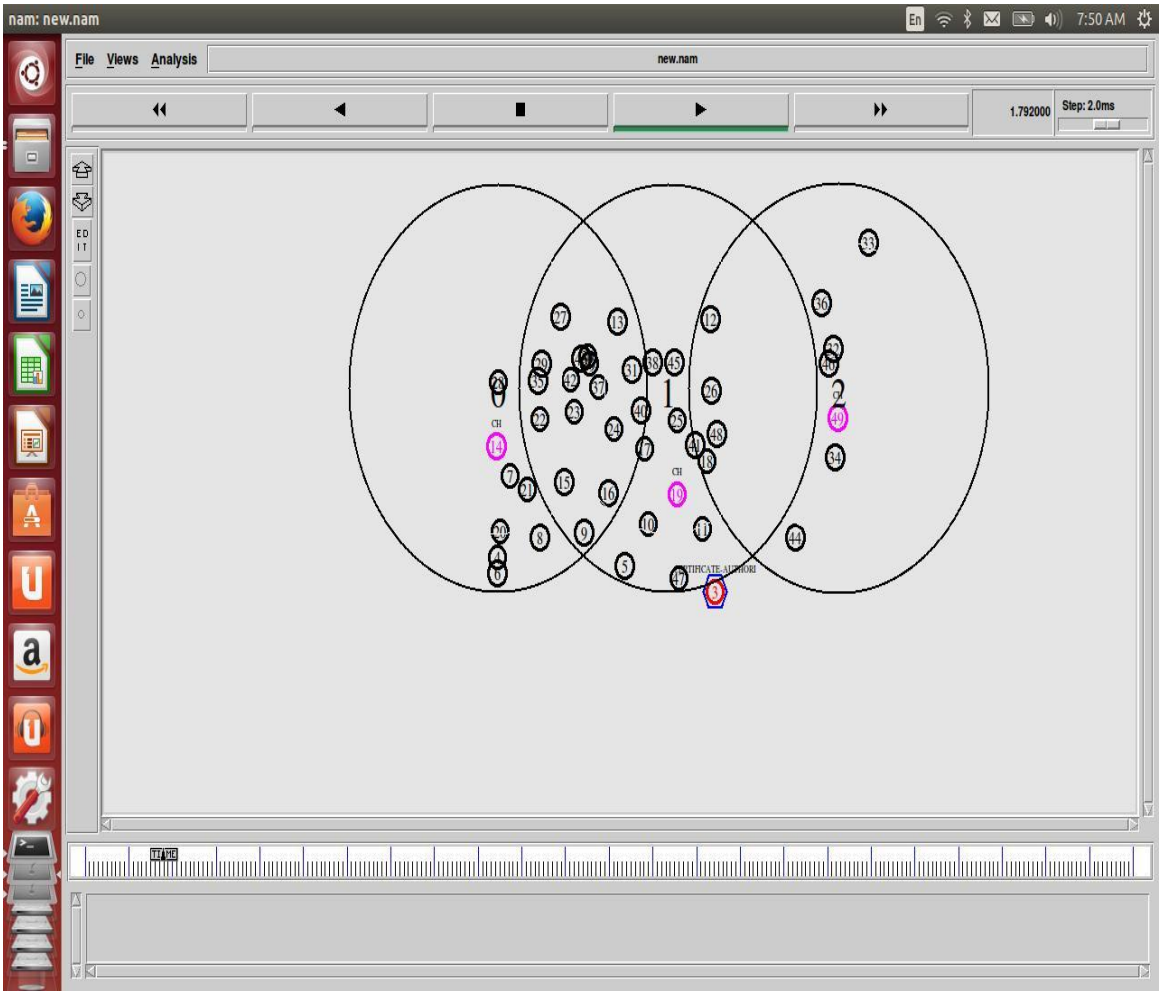

Fig.17 the selection of the cluster head

The cluster heads are selected in this fig. the cluster head is having the information of each and every node present in the network. The 14 19 and 40 node is selected as the cluster head which is highly responsible for the cluster members.

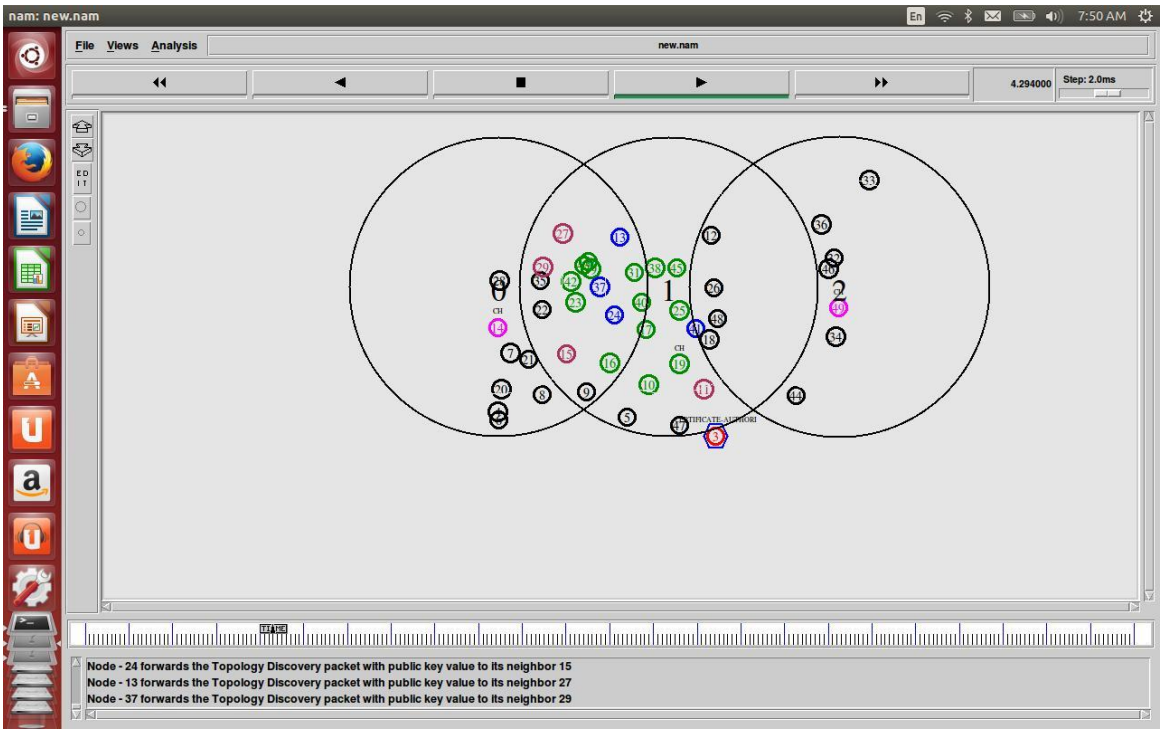

Fig18.Assigning of keys

Now let us come to the security issue, we used HOOSC scheme to assign the keys that are public. In this animation the nodes which are green in color are getting the keys this is how all the nodes in the network will get the keys and the security problem can be overcome.

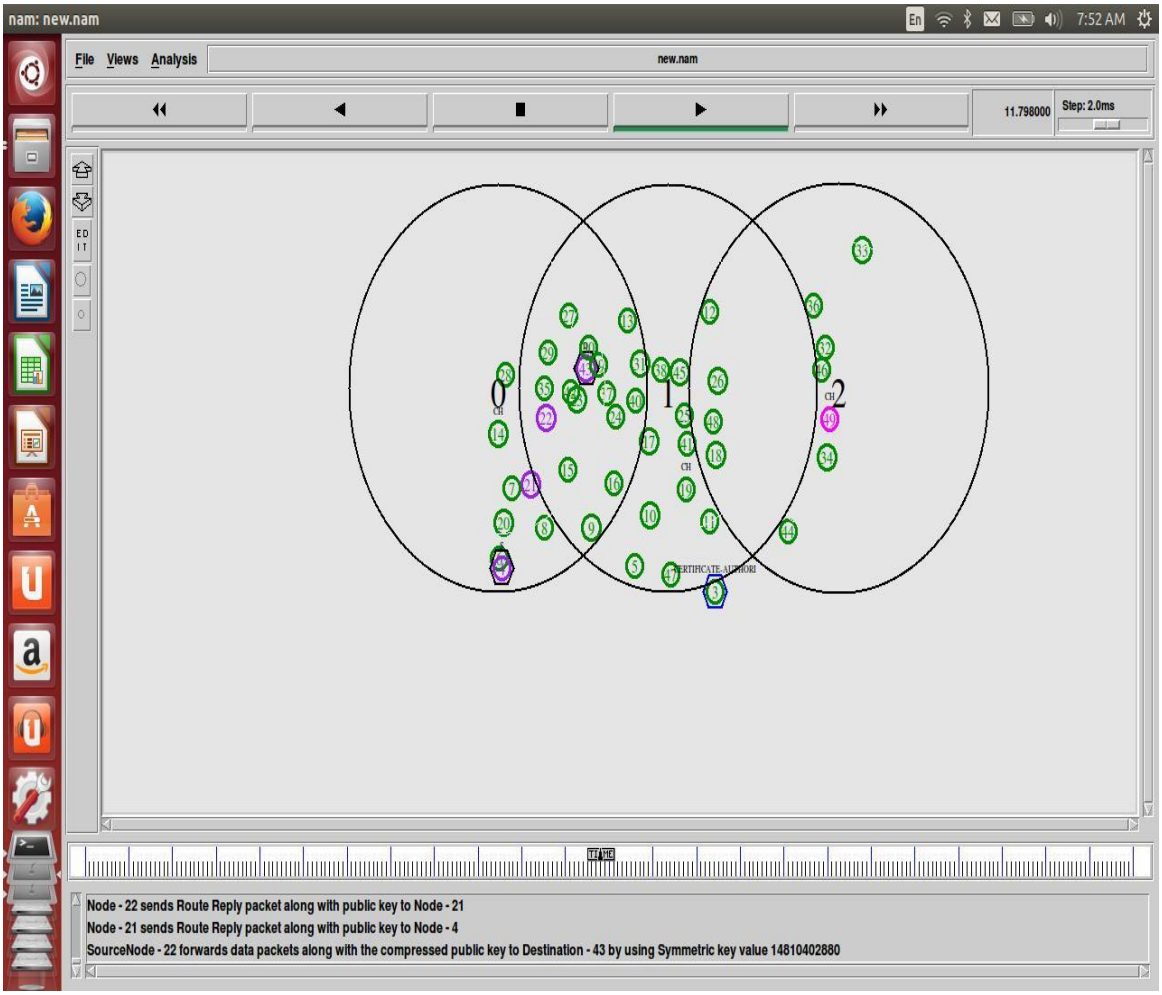

Fig.19 route maintenance in the cluster

Routes are maintained on the basis of the smallest path and the least hop count and the nodes having highest sequence number are used to offer the path to the sender node and the data will flow from this route. We are having least possibility to get the malicious node here. Because the cluster heads are detect and stop the transmission through the node which is to be suspected.

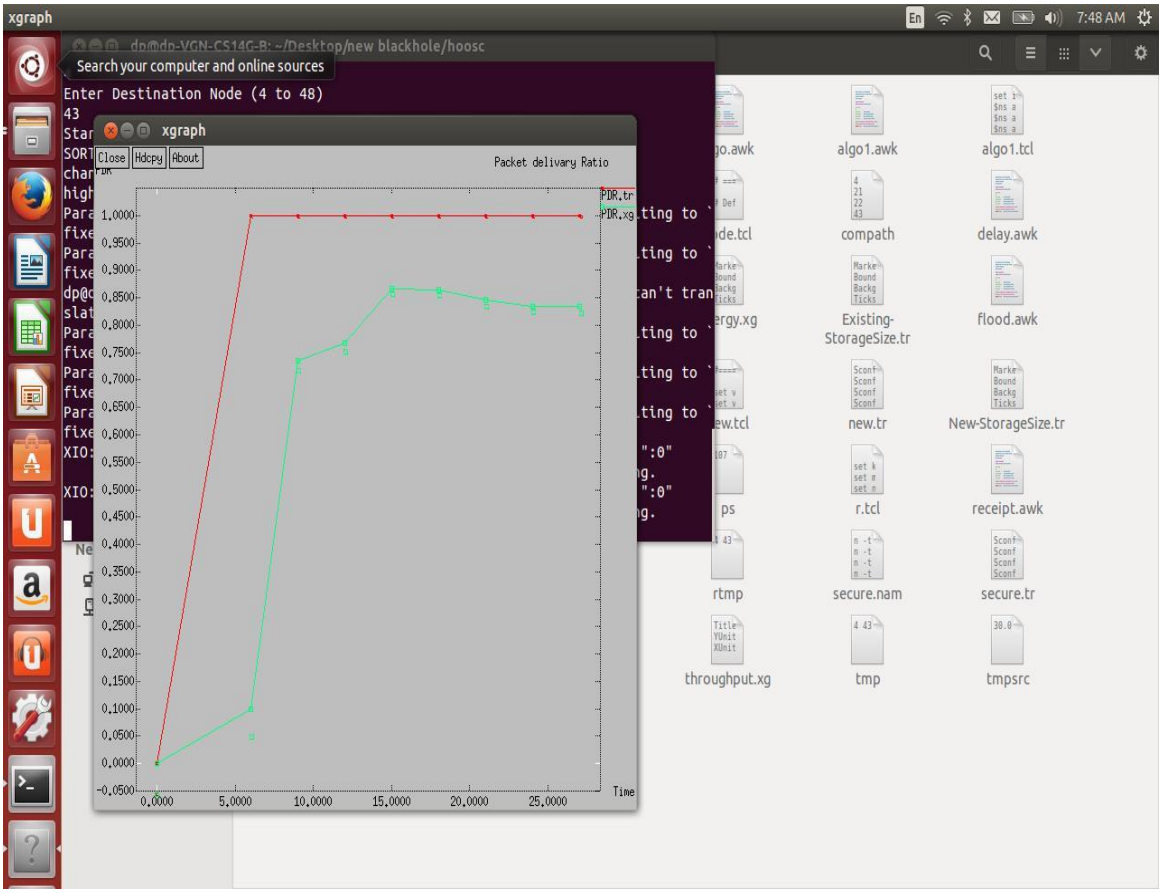

Fig 20. Packet delivery ratio by using HOOSC

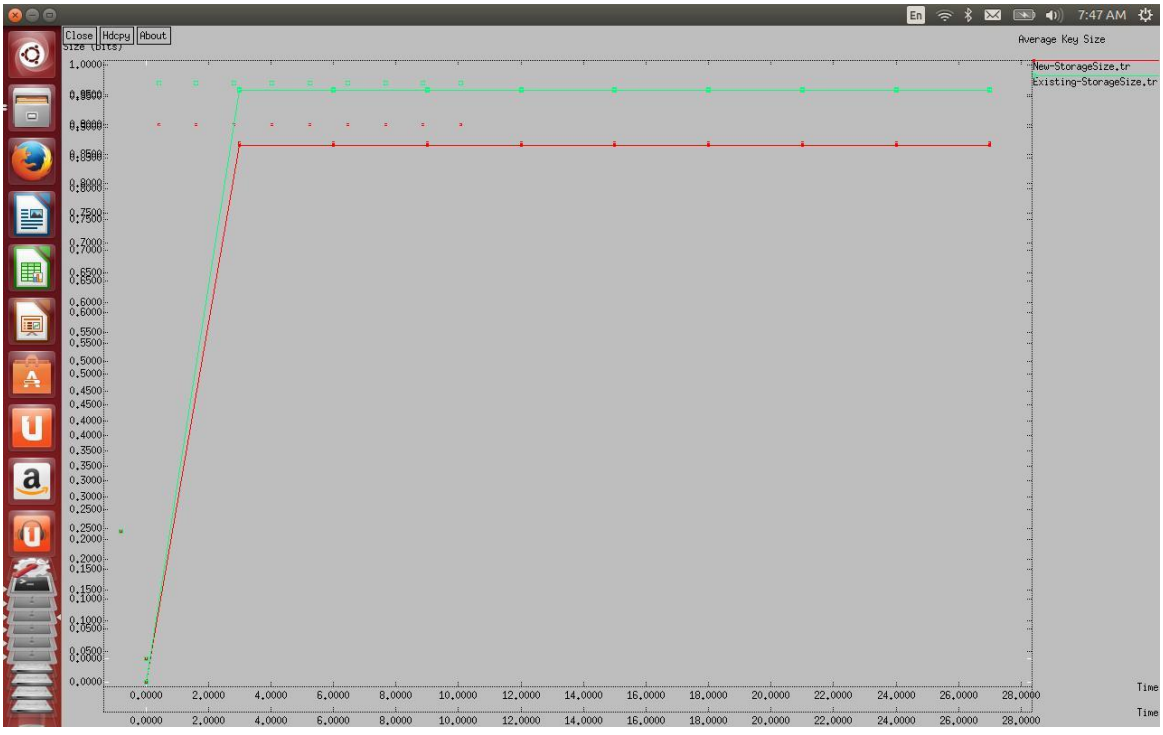

Fig21.The key size for the nodes

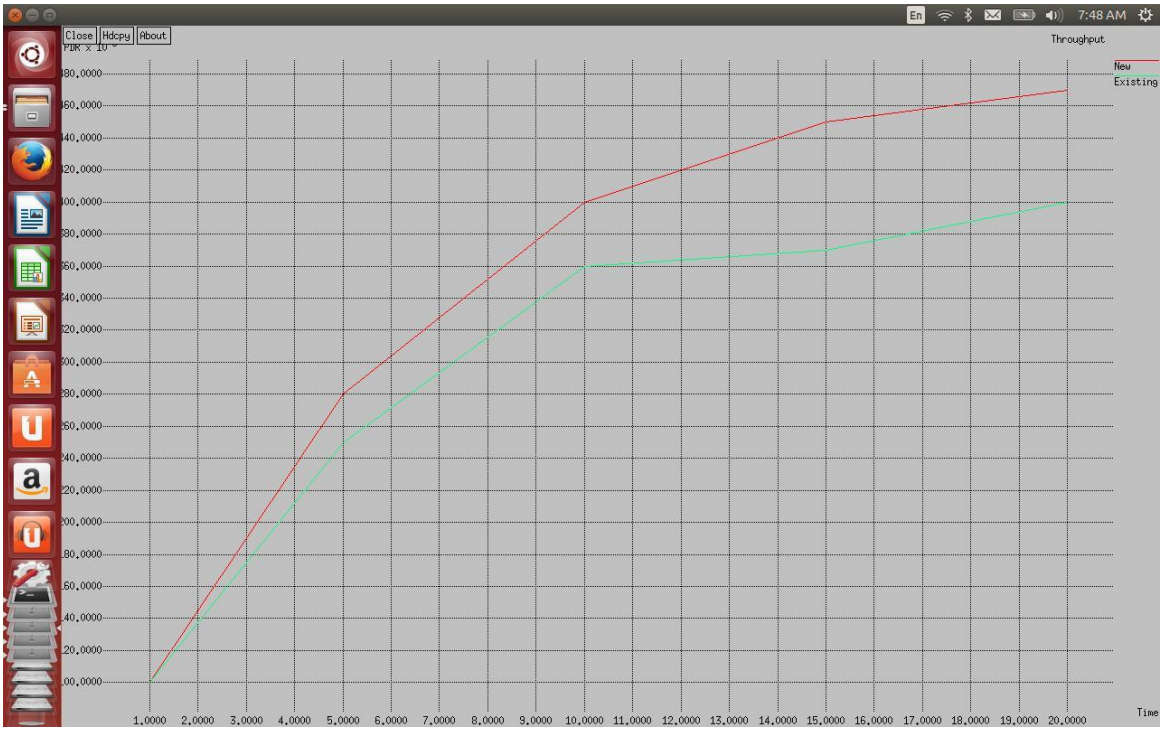

Fig.22 Throughput of the network by using HOOSC

CHAPTER: 5

CONCLUSION AND FUTURE WORK: As we have studied all the research and have got the practical results, so from all the discussions and result we come to a point that we can detect and stop the black hole attack by using the clustering by the CA and enhance the security by the HOOSC scheme that Even if the of the packet can be taken by the malicious nodes then the data could not be altered because of the signcryption we done in the HOOSC scheme. We will signcrypt the data .this is all we have concluded from the study that it gives us better packet delivery ratio and the through put. The future work that can be done in the future is that we can apply the whole scenario on other attacks like worm hole attack and grey hole attack. Another approach that we can choose is, we can change the making of clusters. Means the clusters we use in pre defined techniques are range defined clustering so the algorithms can be changed to do clustering. Mitigation of attacks can be done by the clustering and the HOOSC scheme on the different attacks that attacks the security of the systems. We can get better results for worm hole, grey hole etc and increase the factors like through put, end to end delivery ratio and Packet loss.

.

CHAPTER: 6

REFRENCES:

[1] Xiaobing Zhang, S. Felix Wu, Zhi Fu, Tsung-Li Wu," Malicious Packet Dropping: How It Might Impact the TCP Performance and How We Can Detect It".

[2] Payal N. Raj and Prashant B. Swadas. (2009), DPRAODV: A dynamic learning system against back hole attack in AODV based in: international journal of computer science Vol. 2, 2009.

[3] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao. (2011), A survey of black hole attack in wireless mobile ad hoc networks in: human centric computing and information sciences; a Springer open journal.

[4] Z. J. Hass and M. R. Pearlman, "Zone Routing Protocol (ZRP)", Internet draft available at www.ietf.org.

[5] D. Bertsekas and R. Gallager. (2002), Data Networks in Prentice Hall Publ., New Jersey.

[6] V. Park and S. Corson, Temporally Ordered Routing Algorithm (TORA) Version 1, Functional specification IETF Internet draft, http://www.ietf.org/internet-drafts/draft-ietf-manet-tora-spec-01.txt,1998.

[7] P.Samundiswary and P.Dananjayan.(2010), Performance analysis of trust based AODV for wireless sensor networks In: international journal of computer applications Volume 4– No.

[8] Mangesh Ghonge, Prof. S. U. Nimbhorkar , Simulation of AODV under black hole attack in MANET In: international journal of advanced research in computer science and software engineering" ISSN: 2277 128X.

[9] Sakshi jain. (2014), Review of prevention and detection methods of black hole in AODV based mobile ad hoc networks In: international journal of information and computation technology Volume 4, pp. 381-388.

[10] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. (2007), Detecting black hole attack on AODV based mobile ad hoc network by dynamic learning method In: international journal of network security Vol.5, No.3, PP.338–346.

[11] Nidhi Chhajed and Mayank Sharma. (2014), Detection and prevention schemes for black hole attack in WSN In: international journal of advanced research in computer science and software engineering Volume 4, Issue 11.

[12] Xiaobing Zhang, S. Felix Wu, Zhi Fu, Tsung-Li Wu," Malicious Packet Dropping: How It Might Impact the TCP Performance and How We Can Detect It".

[13] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao(2011), A survey of black hole attack in wireless mobile ad hoc networks In: human centric computing and information sciences; a Springer open journal.

[14] Amin Mohebi and Prof.Dr.simon scott.(2013), A survey on mitigation methods to black hole attack on AODV routing protocol In: Vol.3, No.9, 2013 ISSN 2225-0603 (Online), www.iiste.org network and complex system.

[15] Zdravko Karakehayov(University of Southern Denmark Mads Clausen Institute) Using REWARD to detect the black hole attack in WSN .

[16] Chanchal Aghi and Chander Diwaker.(2013) , Black hole attack in AODV routing protocol In: international journal of advanced research in computer science and software engineering Volume 3, Issue 4, ISSN: 2277 128X .

[17] Mozmin Ahmed and Md. Anwar Hussain ,Performance of an IDS in an ad hoc network under black hole and grey hole attacks.

[18] Weichao Wang, Bharat Bhargava and Mark Linderman, defending against collaborative packet drop attacks on MANETs.

[19] Chander Diwaker, Chanchal Aghi and Kulvinder Singh., Detection and prevention of black hole attack in MANETs In: international journal of emerging technologies in computational and applied sciences ISSN (Online): 2279-0055 .

[20] Ms.B.R.Baviskar, Mr.V.N.Patil., black hole attacks in wireless sensor network by using multiple base station using of efficient data and encryption algorithms In: international journal of advent research in computer and electronics.

[21] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard., prevention of cooperative black hole attack in wireless ad hoc networks.

[22] Jaspreet kaur and bhupinder kaur. (2014), BHDP using fuzzy logic algorithm for WSN under black hole attack In : international journal of advanced research in computer science and management studies, Volume 2, Issue 9.

[23] Amanpreet Kaur, Manjot Kaur Sidhu, Diminution of MANET attacks by HOOSC scheme In: International journal of science and research.

[23] Anjaly Joy and Sijo Cherian, Black hole attacks and its mitigation techniques in AODV and OLSR In: international journal of computer science and engineering technology.

[24] Bhoomika patel and khusboo trivedi, A review-prevention and detection of black hole attack in AODV based on MANET In: international journal of computer science and information technology ISSN:0975-9646.

[25] Ms. Twincle G. Vyas and Mr. Dhaval J. Rana, Survey on black hole detection and prevention in MANETs In: international journal of advanced research in computer science and software engineering.

CHAPTER: 7

APPENDIX: