Chapter-1

1. INTRODUCTION

The advancement in computer technology has revolutionized almost every aspect of our life. In earlier days data was not shared among different computers or devices. Now data and information is being shared among computers. The sharing of data among computers is referred as Data communication. This has increased the use of computer beyond the computer room. Data communication has enabled us to send and receive data and information from one computer other computer.

Sharing of information from computer to computer is possible if these computers are connected or linked with each other with any medium. Most computer systems are now connected together in some way to form what is known as Network. A computer network is interconnection of two or more computer systems located in same room, building, or at different places. Computer network enables the sharing of information, programs and hardware components. A computer network in an office, company or in a computer lab connects many computers and other devices to share data and information.

Compulsory components of any network are Sending device, Receiving device, Communication device, Transmission medium. Mainly we divide network into two main categories such as wired Network and wireless network. In wired network computers are connected with each other with wire i.e. wire act as medium. Local Area network (LAN), Wide Area Network (WAN) and Metropolitan Area Network (MAN) are three types wired networks. There is vast selection of cables used in wired communication i.e. coaxial cable, twisted pair cable and Fiber optic cable. Air acts as medium between the sending and receiving device in wireless network. It's up to the requirement either we use wifi, Bluetooth, infrared technology or any other spectrum of light to communicate data. The field of Wireless communication has experienced an unexpected and rapid growth and advancement in hardware as well in software. With the development in technology the means for communication also developed. Manual driving has changed in to automatic driving which leads in to a new era of safe and luxurious travelling standers and modes. Intelligent transport system is the famous example of modern automated and developed method of traveling

In wired network each user is directed connected with the main access point or with base station and has a fix infrastructure and design [1]. Opposite to it in MANET or in wireless communication there is no any fix infrastructure i.e. it doesn't rely on infrastructure for its

operations. The concept of Mobile ad hoc network traced back to the DARPA packet radio project in 1972.

The nodes in MANET communicate with each other while in moving state. Autonomous transitory mobile nodes communicate with each other over the wireless link. As shown in figure 1 Mobile nodes communicate the information by making autonomous network as in moving state they have no proper and fix position.

Nodes lie in range with other directly communicates while the other nodes which are out of range communicate with other nodes which are at distance through the nodes which are present in the middle act as router. The host in MANET moves frequently so the topology also changes with continues change in its position. It is multiple-hop network with no cellular infrastructure; Data is routed via intermediate nodes. Some MANETS are connected with local network while some connected with internet.

As Ad hoc network normally does not need back bone infrastructure support which is a time consuming as well as impossible to deploy in some certain conditions. Each node act as router which receives and forward the packets to and from other nodes [2]. MANET can be used to collect the sensed data collected by the sensors i.e. air pollution, temperature humidity and atmospheric pressure. By using VANET filling station, service station as well as the congestion of road can be detected. Characteristics of VANET includes Wireless communication, High Mobility of nodes, Limitless network size, frequent data transfer, life critic, abundant energy and better physical protection.

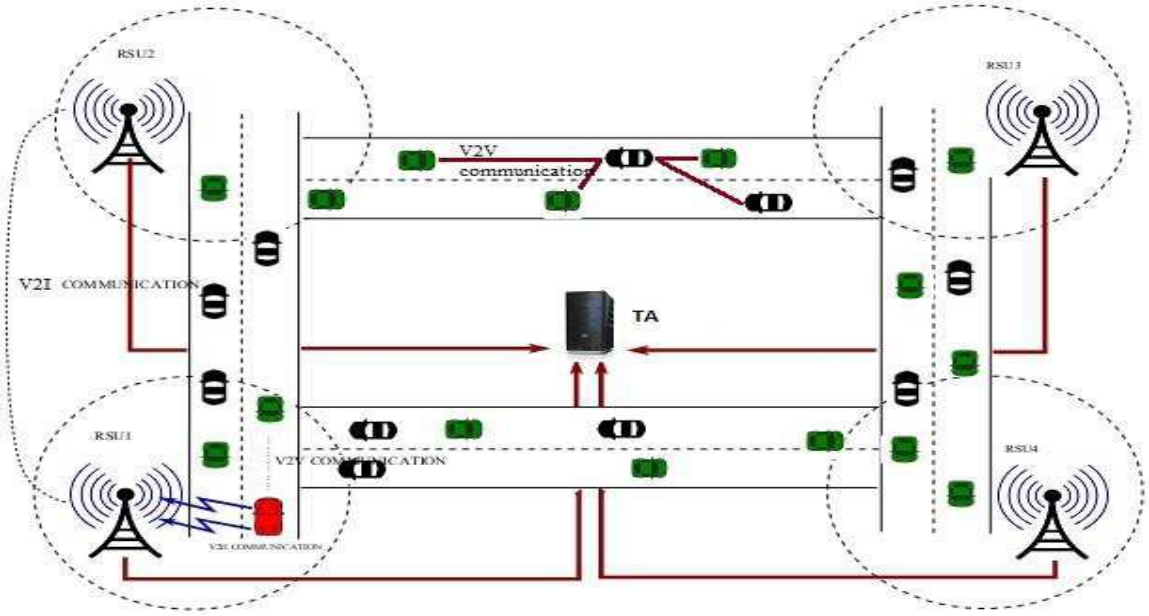

Fig.2.VANET Overview [6]

1.1.VANET (Overview)

Vehicular Ad-Hoc network is developed from MANET.As VANET nodes are fixed in vehicles called On board unit which communicate with each other and with the towers known as road side unit .It is wireless network which uses moving cars with radio signaling system operating in DSRC channels. As shown in figure 2 In VANET every participating cars considers as nodes and data be transmitted from one Vehicle to Vehicle (V2V) or node to node communication and Vehicle to RSU (V2RSU) communication. Vehicle ad-hock network is well known and modern type of network. It is widely used in vehicles to form intelligent transport system (ITS). VANET enabled vehicles installed with on board units. OBUs connect and communicates with the towers installed on road sides after a definite distance as per requirement called as Road side units (RSUs). By using a specific channel in DSRC OBUs and RSUs communicate with each other to share information and data.

Infect VANET is a heterogeneous hybrid network of internet service providers (provide internet)and cellular network. Vehicles in network frequently change their position and network topology. By using global positioning system OBUs and RSUs detect the data regarding the location. Network transmits information regarding road, traffic situation and about the information of the people who drove on the road. Like as in MANET vehicles move freely in network coverage area and stay connected with each other. Despite of MANET VANET nodes have a reasonable storage, processing as well as power capacities.

In VANET communication DSRC ranges from 5.850 GHz to 5.925 for signaling. For the safety and other purposes seven channels are used 178,172,174,176,180,182,184 with 10 MHz Dedicated Short Range Communication. DSRC is based on IEEE 802311A, 1609 while IEEE802.11P especially for Vehicular communication.

Likewise all networks VANET also utilize typical two types of communication happens in the network I.e. Vehicle to vehicle and vehicle to Infrastructure communications. Vehicles communicate with other vehicle in V2V communication. While in V2I communication vehicles communicate with the infrastructure i.e. with Road side units. In V2V communication IEEE 802311A standard is used. An Antenna installed on the vehicle act as sender as well as receiver in V2V as well as in V2I communication [3]. Vehicle communicates with other vehicle to transmit information regarding road situation as well as personal information.

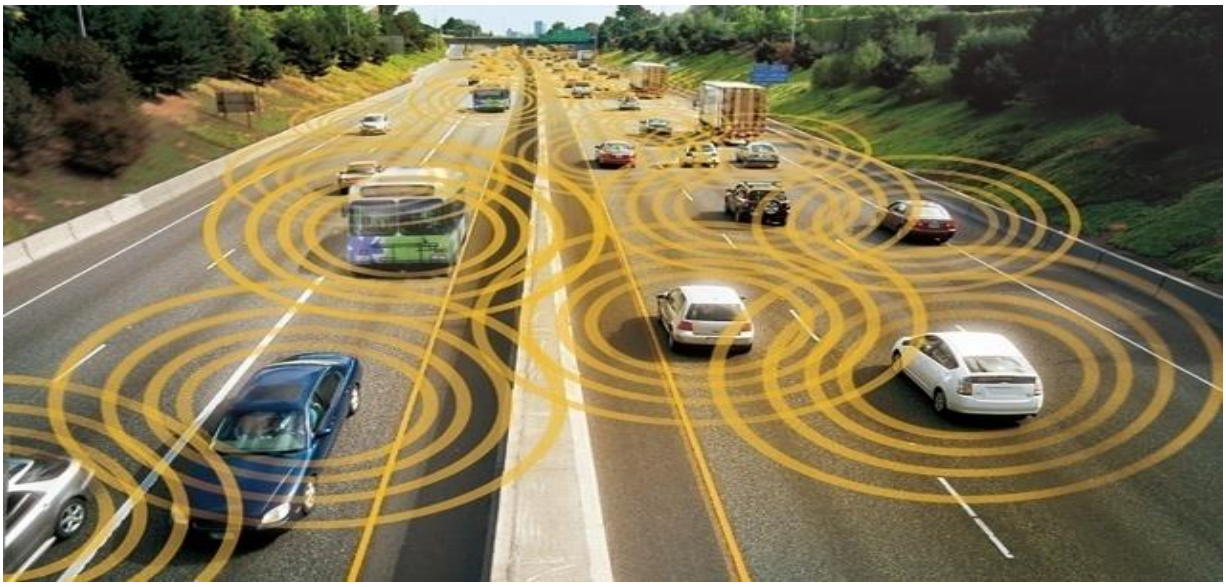

Fig.3. V2V communication [7]

1.2.V2V communication

In V2V communication vehicles communicate with other vehicle as given in figure. While communicating with other vehicle authentication is must. To ensure the safety of the VANET OBUs also be authenticate other vehicle before communicating. On Vehicle authenticate the nearest vehicle while the nearest one authenticates those vehicles which are near to it. By this ways OBUs authenticate and verify the vehicles to be connect and communicate.

Reliability and End-to- End delay are the most important factors in VANET applications security. As shown in figure 3Widely known that V2V (Vehicle to Vehicle) and (V2I) (vehicular to infrastructure) Communication links due to high-speed mobility tends to be short lived. Its basic and main purpose is to make sure of life safety application that save lives and improve traffic flow in VANET. To encourage DSRC development and usage of Private services are also allowed in to lower cost.

In VANET Communication Vehicle to road side unit communication is the most important part of vehicular communication infrastructure. It's important lies on urban and suburban areas i.e. the areas where the vehicle numbers on road is dense and thus results in life threatening situation. As due to the hardware deployment is not easy in rural area its coverage is preferably to be provided in urban areas, on major highways and motorways.

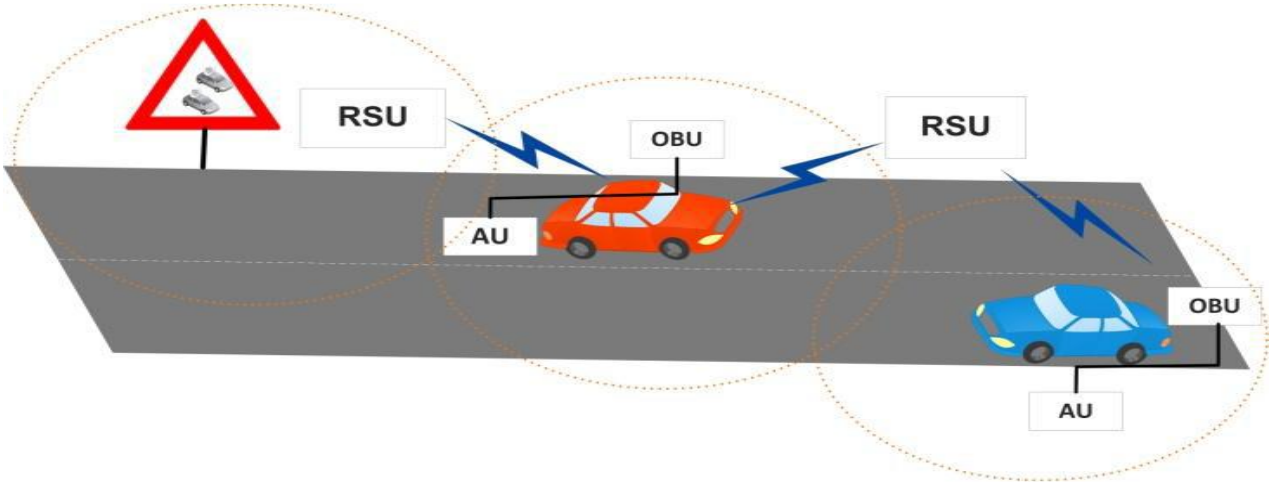

Fig.4. RSU communication [8]

RSU communication is the communication done between vehicles and road side units. Connection established between the OBU and RSU or may be with the vehicles within the range of RSU. As shown in Figure 4 RSU is in contact with the service providers and with other legal authorities provides services like HTTP, VOIP and access to the internet. Vehicles also can communicate with the far away vehicles by using road side unit as an intermediate node. Vehicle access internet and also give its location and information about the road situation.

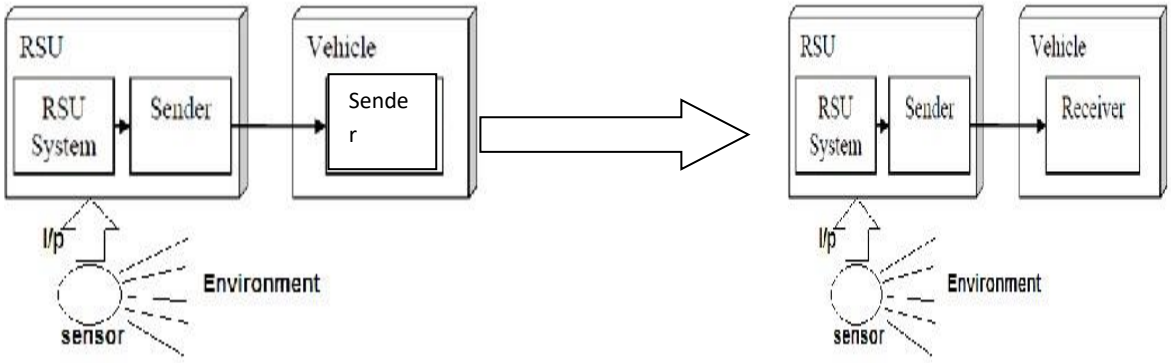

Fig.5.RSU to RSU communication[9]

1.3.RSU to RSU (R2R)

On board units also communicate with other OBUs with respect to the position. R2R communication is done to extend the communication range of the VANET for broadcasting and receiving of information about road by OBUs and to transfer the information to other RSUs and OBUs.

Global positioning system (GPS) and other services like wise are spreading in vehicular system for position awareness [4]. Due to the terrain and lack of infrastructure this utility is unable to be accessed and utilized from rural areas.

In modern time Intelligent Transport System is implemented to provide security and comfortable movement on road. This system is deployed to enable node to node and in network communication on road. Position of nodes can be detected according to the data shared after intervals. In Intelligent transport systems (ITSs) vehicles work as sender, receiver and router to communicate with either RSU or OBU. Short range radio interface equipped Vehicle that enables short range wireless ad hoc network to be formed. Vehicles also equipped with hardware that provide information regarding the GPS. Road side units are fixed and are connected with backbone network that facilitate communication. The number of the road side units depends on the protocol used for communication. The communication include inter vehicle, V2V and V2RSU based on up to date communication sensed by the surrounding network [5].

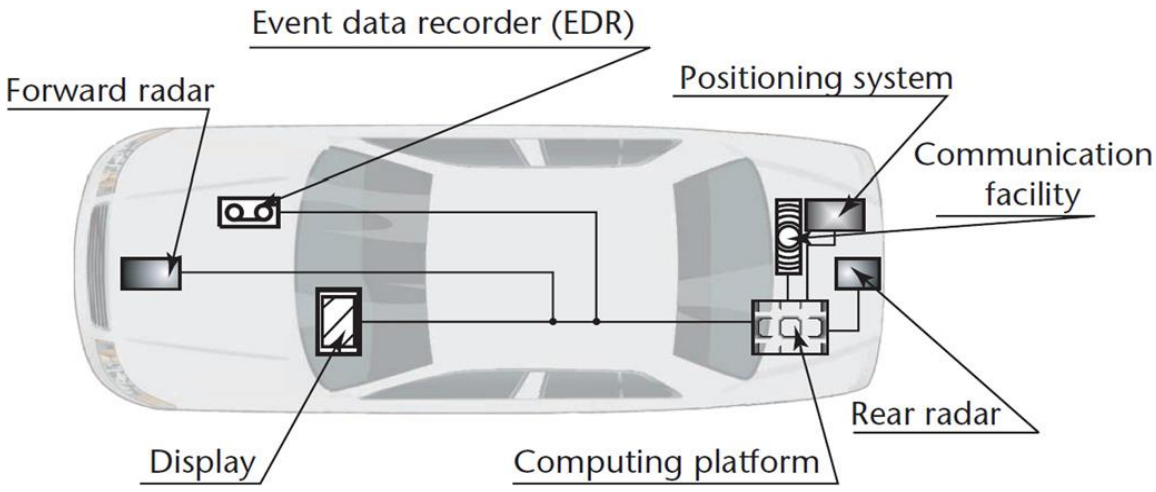

Fig.6. A Network Node [10]

OBU communicate with other OBUs to share on road situation, Its Global Position, Personal data as well as the data regarding the road congestion and accident.OBU also communicate with RSU which are towers at a reasonable distance along road.

VANET	APPLICATION TYPE	• SAFETY APPLICATIONS • INTELLIGENT TRANSPORT APPLICATIONS • COMFORT APPLICATIONS
	QUALITY OF SERVICE	• NON-REAL TIME • SOFT REAL TIME • HARD REAL TIME
	SCOPE	• LOCAL AREA NETWORK • WIDE AREA NETWORK
	NETWORK TYPE	• ADHOC INFRASTRUCTURE BASED
	COMMUNICATION TYPE	• V2V • V2I

Table.7. VANET Overall Description

We can categories VANET on the basis of its services. In the network as the communication medium is shared, limited bandwidth and un-reliable while the data delivery and information communication is very fast in vehicles. This requires mart and guaranteed protocols.
Technologies such as IEEE 802.15.4, IEEE 802.15.15 and IEEE (Zigbee) used in intra vehicle communication technologies that support the wireless communication.

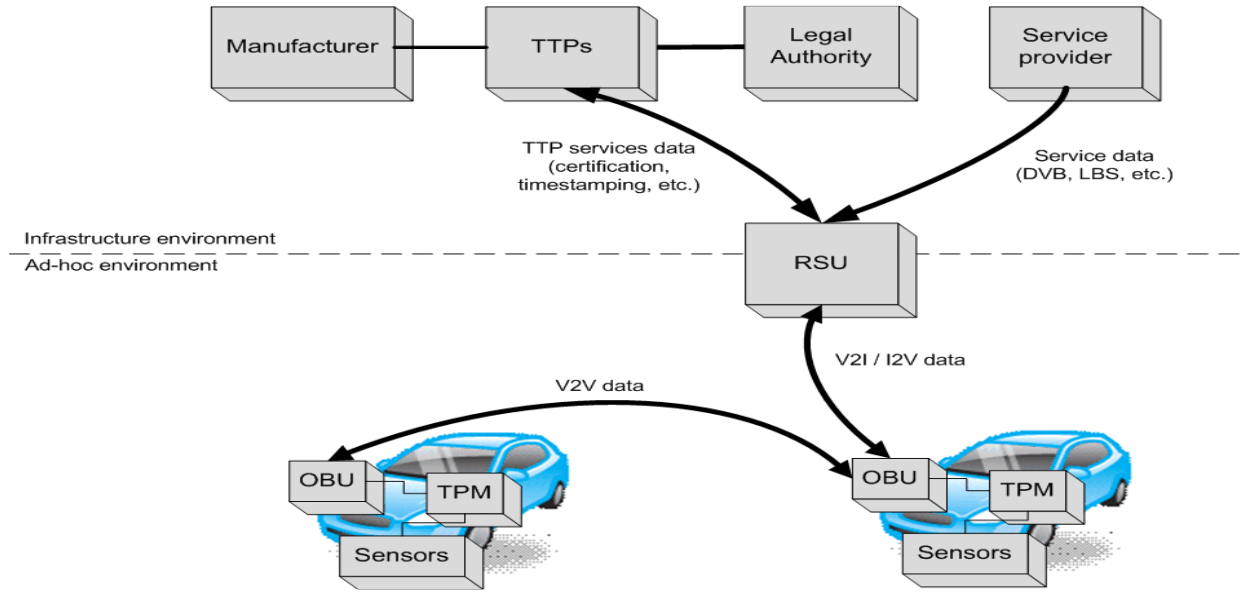

Fig.8. VENET Communication [12]

Towers equipped with necessary hardware's are deployed on road sides along with highways and roads which enables and support V2V and V2R communications.

RSU (Road side units) not only broadcast the Vehicles and traffic condition it also provide facility to drive thru Internet access i.e. it also provide facility to access internet. As in Fig 8 V2I communication infotainments services such as advertisements, parking and automatic trolling etc are also provided. Legal authorities and services providers are connected with the whole network via RSU which are continuously in contact with vehicles OBU [4].

As VANET are in continues dynamic position so it use Multi hop routing instead of static network connectivity. It uses different protocols at different situations. Mobile Ad-Hoc network is different in nature with respect to the others as it requires up-to date information for routing. It is complicated due to high speed movement of nodes. Protocols are used by considering area, application and topology.

The routing protocols in VANET are divided in five categories i.e. TBRP (Topology based routing protocol), CBRP (cluster based routing protocol), PBRP (Position based routing protocol), BRP (broadcast routing protocol) and GCRP (Geo cast routing protocol).In Topology based routing Link information exists in network is utilized for the transfer of packets from one node to other in VANET network.

Packets are continuously broadcasted to maintain the routing table so that the prepared routing table can be used for further use. It reduces the effort of VANET to re diagnose and to generate a topology. Position based routing: In this protocol use the global position of the node to communicate and to select the hope to communicate which is nearest with him. Nodes communicate with the node which is at nearest position according to the global positioning system. Broadcast routing: In this type of routing message is delivered at wide range i.e. beyond the transmission range. It is used to share about weather, traffic and emergency on the road. Massage is just broadcasted and the delivery report is not required by the receiver.

Cluster based routing: nodes are divided into squares to form clusters on the bases of geographical basis. One node which can be chosen as per situation acts as cluster head, broadcast the massage to tall nodes in the cluster. To provide the scalability virtually created infrastructure through the clustering of nodes. Geo cast routing: to reduce congestion and overhead packets are delivered within the specific geographic region. Location based multicast routing is basically Geo cast routing. A specific region is defined in which it broadcast the massage while the nodes outside the region are not alerted. DG-CASTOR, IVG protocols generally used for geo casting routing.

Security in VANET network is more critical issue than that of other networks as in VANET signal transmission is propagated wirelessly in open environment. In such a environment network can be easily accessed from anywhere the signals propagation area. The data transmitted in the network is life critical so it is mandatory that the data transmitted from sender node can be received at the receiver end without any change, Alteration or any addition. We discuss major types' attacks on VANET security on the basis of reaction and swear results after attack and try to evaluate the results and behavior of nodes at the time of attack [5].

1.4.Passive attacks

Passive attacks are less reactive as Active attacks as it have no affect on the functionality of the network. It only tries to use and discover the information traveling in the network. By sniffing network it involve in obtaining the routing information as well as users precious information and data. Attacker in this attack maliciously looks for sensitive information, passwords and other plain text that it can use in other attack and in hijacking. Passive attack is easily effective in the environment where no proper cryptographic standards are followed. Capturing of plain and unencrypted information including passwords, traffic analysis,

monitoring traffic and monitoring of the unprotected communication in network are some examples of passive attacks. As the passive attack does not change anything on user end so users are totally unaware of the attacks results in the disclosure of files and users information without the information and in notice of the user. Even it is difficult to detect the exact location of such a malicious node. As passive attack caused no disturbance in network so are very difficult to detect and resolve.

1.5.Active attacks

Active attacks try to disturb the operation of protocol. Its main goals are to limit the accessibility, Un-authentic access or illegally utilization of packets moving to other node. In this attack attacker break the system security and bypass it. This can be done by using various strategies and methods like worms, viruses Trojan horses or by implementing stealth. Active attacks are more swear then passive attacks because in active attack attacker breaks the security and can change or modify the information. Active attackers can introduce malicious code and can modify the information. User can be aware by these attacks as the attacker change the information.

1.6.Distributed attacks

Manufacturers and designers left some loopholes and backdoors in the hardware and software they designed and manufactured by intentionally or unintentionally. Attackers use these loopholes and backdoors to attack and access these hardware's and software's. Once the attacker accesses the device it can use it for any malicious purpose**.** This attack is very difficult to detect and restrict as the user have not too much know how of the hardware and software.

1.7.Insider Attack

Insider attack is such an attack done by inside, attacker may be present is the network. It is not mandatory that the insider attackers are malicious they can be non malicious as well. Malicious attackers in inside attack can access or deny the access of user, steal, or can damage information. Non malicious attackers can only access your information and does not alter or change the information or data. As the insider operating attackers are more dangerous than other attackers because they are operation within the network or from the OBU or RSU.

1.8.Close-in Attacks.

In close-in-attack the attackers are physically very close to the target. Malicious person attain the advantages for being close his target. Attacker gets closer to understand the network, topology, systems and the way network propagate. Famous form of Close-in-attack is social Engineering attack attacker get closer to the person related to the network either by physically or by using other ways of interaction like email, massages etc. The information reveals by socially interaction can be used in subsequent attacks to access the system maliciously. The information may be used to alter, change, modify or to re transmit the data after desired changing [6].

1.9.Phishing Attack

Phishing attack is the most famous trick to hijack the accounts by getting the users information by using many ways. In phishing malicious attacker create the clone of the original and popular website such as Facebook or PayPal. Attacker sends the link of the fake website to the user by using many ways I.e. by Email or by massaging and urges the user to click on the link. When the user clicked on the link clone or fake website open so that username and password of the user entered to login is delivered to the fake person who created the fake website. Information attained by phishing attack can be used to login the users account to access the personal information or to use it for some malicious activities

1.10. Hijack Attack

While in conversation in network two nodes communicate with each other when they are in active session. Communication is always done in session. In this attack attacker disconnect the one device from session and take over the session so the other device thinks as talking with the original device. Sender still believes that he is in conversation with real receiver and may send important and private information to the hacker. Hacker can also request the sender to share some specific information which can be used for any malicious activity by attacker [8].

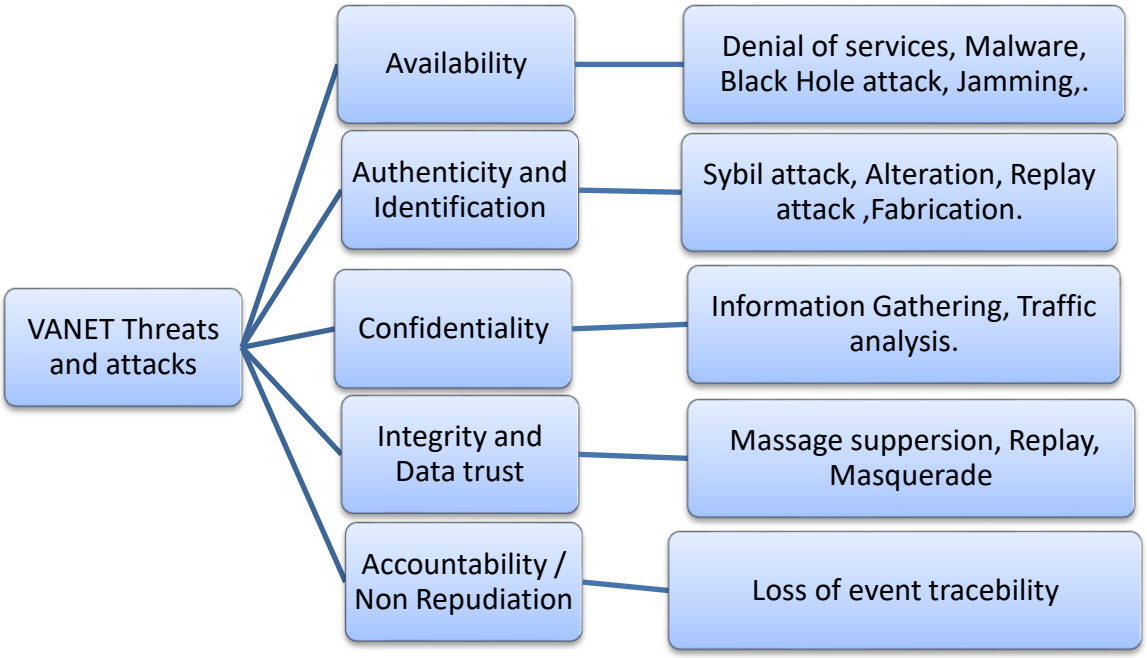

Fig.9. VANET Threats and attacks [13]

Vanet security is in alarming condition. We cover maximum threats and security issue under the umbrella of fine main categories.

Malicious attackers implementing fabrication attack can mislead or misjudges the vehicles which are about to communicate. As in Fig 9 These malicious attackers can transmit massages including warning massages, fallacious massages and fake massages as well over the network. Network by maintaining the privacy must detect the obligation and responsibilities of drivers. Safety in the network is crucial as it affects the life of passengers traveling on the automobile. It is to make sure that the vital information can't be changed or deleted. We discuss the above given threats of VANET in detail.

1.11. Availability

Availability refers to the condition when data or massage transfer in VANET disappeared i.e. due to any reason data loose occurs. There can be more than one reasons such as Denial of services, Jamming, Malware, Black hole attacks etc.

1.12. Denial of services

DOS (Denial of services) is the unavailability of services provided by the VANET. Attacker hack the network by sending unwanted massages and to reduce the efficiency of medium used by VANET to communicate. It is necessary to restrict unwanted and malicious users not

to breach network caused Dos attack. The strategy applied to apply Dos attacks is that the malicious cars at a time slot from different locations attack on RSU so that it can't communicate with other OBUs and RSUs. As the malicious car block the channel to communicate with other RSUs it broadcast a dummy massage ""Lane is closed ahead"" which case road accidents and other difficulties for RSUs [10].

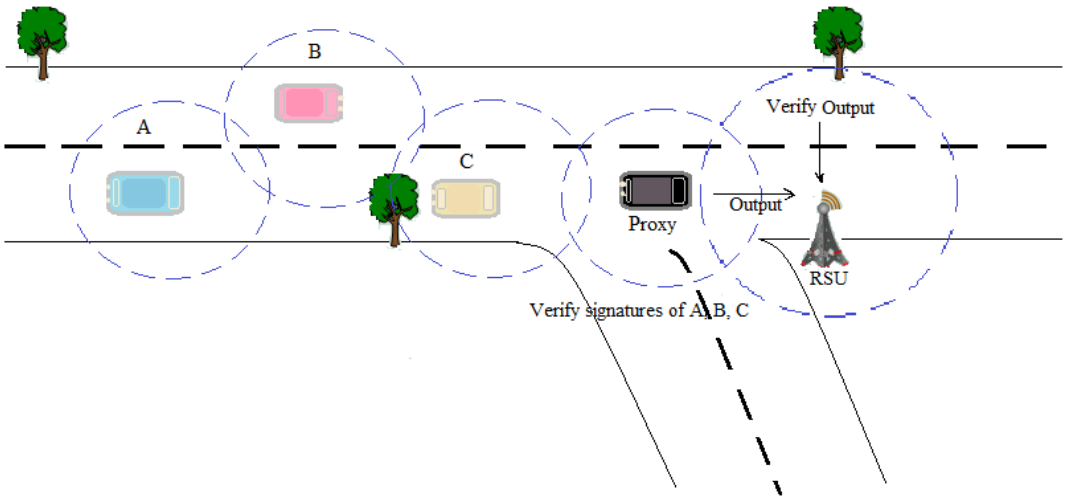

Fig.10.Movement in VANET [14]

1.13. Movement tracking

In this behavior malicious vehicle got the information regarding the position and speed of the other vehicles So that it can suppose and detect the future speed and position of the vehicle to effect their conversation and transmission [11].

1.14. Malware

Malware are the software which are malicious in their functionality i.e. specially designed to disturb the functionality of the device. Malware in MANET is responsible for the malfunctioning and transfer of information which can be used in malicious activities.

1.15. Black hole attacks

In this attack malicious node fascinates the source node to rout through it as it pretends to have the shortest path and provide the malicious and fake information to the source to destination nodes. So by this way node in network transmits data through the malicious node by considering it the shortest path between sources to the destination. This attack results in misuse of information transmits and move in network and also the forwarding of malicious packets and information to the other nodes [15].

1.16.Authenticity and Identification

In authentication and identification malicious cars un-authorized access and breach in network occurred. Attacker got access network by fake IDs and other authenticity information. Basic need is to restrict the unwanted cars or attackers to access the network.

1.17.Sybil attack

In this attack malicious car generate many IDs and transmit different massages from different locations so that the other cars on road access it many cars transmitting different massages. This caused problems while making decisions on road.

1.18. Replay attack

Unwanted vehicles jam the traffic in network while replays sending past massages. Malicious vehicle continuously send old and earlier user conversation and massages to a node to jam the traffic.

1.19.Fabrication

Malicious vehicle transmit retransmitting fake information to the network. The information consists of information such as fake or already used certificates, warnings and fabricated massages.

1.20.Alteration

In alteration attackers access the packets of data moving in network mainly un-encrypted packets can be accessed and utilized easily and change and alter either the whole of content of a part of content. As the alteration is done over the network so the destination node or RSU receive it after the attacker performs alteration in it.

1.21.Confidentiality

Confidentiality is to restrict the unwanted cars to use information or data transferred through the network. As Users in VANET enabled cars share their confidential data and other personal information with other users. It is to make sure that the transmitted data can be reached as it is sent by sender. No attacker can use it as it is broadcasted wirelessly. Network can be accessed easily.

1.22.Traffic analysis

Attackers continually analyze the data of the other vehicles such as their position speed and vehicle condition as well. Collected information in the result of analysis can be used for some malicious and unwanted activity. Attacker can judge the position after a specific interval and can distract or by fake instructions de route it. Attacker continuously record the traffic and all its attributes like speed, velocity, road condition and the continuous location of the targeted vehicle. After continuous record and analysis attacker can estimate and access the location and other attributes of the vehicle after a certain time that leads into future attacks and threat for the traffic.

1.23.Integrity and Data trust

1.23.1. Massage spoofing

Malicious vehicle broadcast false and fake information in the network to deceive then and to misdirect them; this caused accident and other issues in network. Eavesdropper vehicle send false data consisting of wrong information about network.

1.23.2. Replay

At time of sending massage attacker send the reply of the transmission of earlier information. By doing this it take advantage of sending massage. 802.11channel have not satisfactory protection against these attacks. As the attacker reuse the already used key for conversation it is easy to send bogus and fake massages into the system. The main goal is to prevent and confuse the managing authorities in identification of the vehicle in the case of accident, crash or hit and run.

1.23.3. Masquerade

In masquerade attack attacker act like in emergency to slow down or to mislead other vehicles. This can be done using alteration, replay attacks or by massage fabrication

1.24.Accountability / Non Repudiation

1.24.1. Loss of event traceability

Event traceability is the power of a vehicle to retrieve the identity of the vehicle which communicates with other vehicle. By using various tactics and methods attackers can block or disable the ability of vehicle to record event traceability.

Security of VANET is alarming and needs to be work on. Given parameters are important for the security of VANET infrastructure like authentication, anonymity and data integrity. if we want VANET secure and reliable authentication, anonymity and data integrity must to be kept on top priority [15].

Chapter-2

Background and Literature Review

2.1.0. SECURITY ISSUES IN VANET

Vehicular Ad-Hoc network operates wirelessly i.e. use wireless medium for communicate. Wireless medium is very much susceptible and exposed of attackers as the network can be accessed from anywhere by manipulation of wireless signals [18]. In this susceptible environment it is easy to perform Denial of Services (DOS) attacks on the network. Attackers attack the wireless communication medium to restrict the nodes to access the network and to communicate with each other. Channel jamming can also be caused by these types of attacks [19] [20]. There can be many goals of attacker's attacks on VANET network.

Mainly the attacker's main purpose is to restrict the node to utilize the network services and to restrict their connectivity and communication with other nodes and network. In the result of DOS attack genuine nodes are unable to communicate and lose their connection with the network i.e. they are unable to send or receive the lifesaving and important information and massages over the network. The network which is under attack not be available for genuine nodes for communication. In VANET data includes lifesaving and critical information related to the road situation or of other is to communicate between nodes and RSUs within critical time slot [21].

So DOS attack restricts the communication of data within the network causes very crucial and alarming situation. For the implementation of DOS attacks malicious attackers can use many different ways and techniques in the network. Attackers can jam a network channel either by injecting dummy and fake massages to prevent the other nodes to communicate inn network and prevent the data to travel in the network.

DOS attackers may jam the partially, selectively or completely the network. Mainly DOS attacks can be successfully achieved and implemented by using three ways or techniques for implementing DOS. Those are Channel jamming, Overloading of network resources and packets dropping. Dos attacks can be successfully implemented by targeting a specific portion or are in network [22] [23].

Dos attackers target special areas and target various situations in VANET which we can discuss below.

2.1.1. Make Resource Node Useless.

In this nature of attack attackers utilize and engage all the resources of the nodes so that no connectivity and other conversation be done within the network. This can be done either by sending continues massages which consume the resources of nodes for the verification or by continuously sending fake massage which keep node busy So that it cannot perform other tasks for communication within the network. There can be many situations and problem statements by which Dos attack is implemented for making resource node useless.

Case I) As in below given figure malicious node continuously send same massage of "Accident on the specific location" by continues and frequent same warning massages to the targeted node. Nodes have to process this large number of warning massage. So its resources remain busy and thus failed the communication within the network.

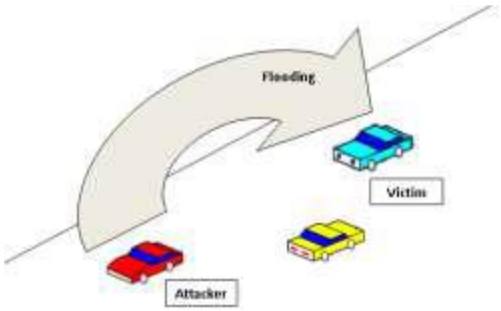

Fig.11. Make Resource Node Useless Case I[15]

Case II) In this case attackers target RSUs to implement Dos attack. Fig.11. Make Resource Node Useless Case I In this case attacker bombards multiple massages to the RSU so that the resources engage in checking and verifying the massages continuously received by the attackers [24].

As shown in Fig 11 RSU is engages to check the massages continuously do that it would be impossible for RSU to communicate or to check the massage sent by the genuine nodes in the network ultimately this practice caused the jamming of network i.e. denial of services as shown in figure bellow [25].

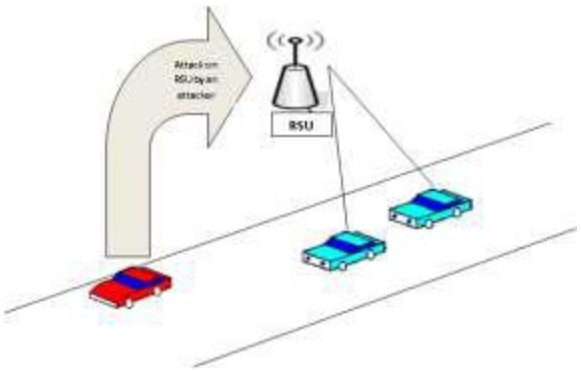

Fig.12. Make Resource Node Useless Case II[15]

2.1.1.1. CHANNEL JAMMING/ PHYSICAL LAYER.

This type of Dos attack is more crucial than that of first one. In this type of attack attackers genuine nodes and other network is unable to communicate as the channel of communication is jamming frequency. Channel can be blocked by the malicious attacker results in the failure of network communication channel jamming can be undergo by many methods mainly it can be done by two cases.

Case I) Attackers attack on network by sending high frequencies over the specific channel in a particular domain of node. As given in Fig 13 In that case when the particular channel containing higher frequency signal nodes are unable to communicate with each other. Jamming of the channel results the failure of network. Under attack particular domain of node neither can send nor receive data over the network. As this jamming is in a particular physical area so node in that area cannot communicate even they go beyond the jammed area i.e. a node can easily send or receive data only in that condition when it leaves the particular are under attack [26] [27].

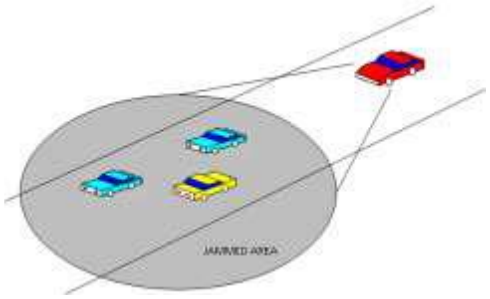

Fig.13. Channel Jamming Case I[15]

Case II) In this case attackers jammed the communication channel between RSU and node. It is the next level of channel jamming. Attacks are attacked by launching jamming attacks near RSU. Network breakdown occurred by this attack. In that case due to the unavailability of the channel nodes are unable to send or receive massage and life critical information by RSU. This attacks are more swear then that of first attack as RSU would be totally failed to share and communicate information and data with the on board units i.e. nodes. Channel jamming near to the RSU leads to the network failure results in critical condition.

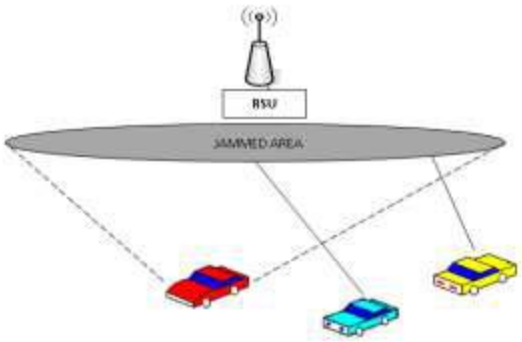

Fig.14. Channel Jamming Case II[15]

2.1.1.2. DDOS (Distributed Denial of services).

Distributed Denial of services is the next level and dangerous attack as comparative to other attack in VANET.

In Dos attacks attack is done by a single node or by single individual attacker. While in DDOS attacks attack can be done from more than one location i.e. multiple attackers from multiple locations attack at once on the VANET network for their malicious purposes. Generally attackers utilize other nodes by taking control on them and launch attack from multiple different locations. There can be two possibilities of DDOS attack [28][41].

Case I) In this case attackers use different time slots and different physical locations for sending massages to the victim. As this attack is practices from different location so the targeted node thinks that the different nodes are sending messages from different location tackle, process the massages individually[35]. The aim of this attack is to throw multiple of massages and engage the targeted node so that it would be un-available for other network. In fig 14 b Unavailability of the node results in the breakdown of network. By this attack such a

node is targeted which act as important and linkage between two network areas and in result jamming and breakdown occurs [28] [29].

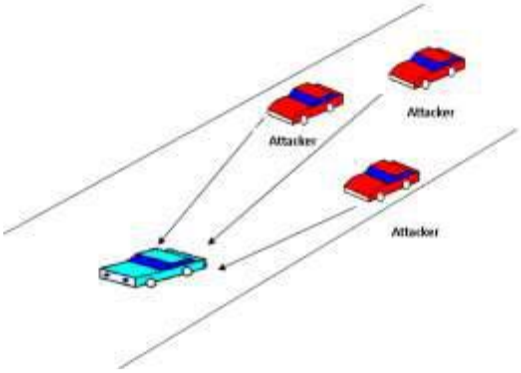

Fig.14.b. Channel Jamming Case I[16]

Case II) In this case Road Side unit is on target. Malicious individuals from multiple locations target multiple RSUs and send multiple massages to engage him to process only their sent massages [42]. Targeted RSU in the result of attacks remain busy in processing the massages send by the attackers and become un-variability for the network i.e. for nodes.

In that situation for whole network it seems un-available So that Nodes and other RSU fails to conversant and communicate with it results in the jamming and failure of the network. As the RSU also provide many other services with node communication. At the time of attack all these services are also unavailable for the network. The RSU is unavailable to respond the other node, thus results in DOS attack [30].

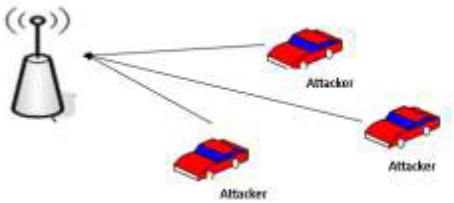

Fig.15.A. Channel Jamming Case III [17]

2.1.2. HYBRID DOS ATTACKS.

Dos attack is dangerous for VANET as it block the availability of network and cause breakdown. But it be more dangerous when DOS attack is practiced with some other attacks

i.e. Hybrid attacks. Other type of attacks use DOS attacks in hybrids fashion to attack on VANET network [31] [43]. We discuss modes of the producing this.

Case I) Network mode.

Denial of Services in VANET environment creates services problem when practiced in network node. Due to the flooding bandwidth of the targeted node can be jammed / blocked. In flooding attackers use network layer and produce vast number of massages and send to the targeted vehicle by doing this take-over the vehicle resources i.e. computing resources and creates the overloading and jamming in the original network. In the result life conscious and other important data can't be transmitted in the network on time. It can be more harmful in the case when driver make decision on this base of the data received by malicious attackers [44].

In this mode of attacks divert the vehicles path from its original path by misguiding him by sending malicious massages. Application mode hybrid attack results in the diversion of the vehicle toward the wrong path i.e. attackers change the vehicle from the right path to the path which is desired by the attackers for the node [32].

2.1.3. SYBIL ATTACK

A single malicious vehicles use and communicate in the network by using multiple identifications of different vehicles in this attack. This attack is practiced to create an illusion that there are multiple identities many different vehicles traveling on the road. These fake and multiple identities of vehicles are used for various attacks and many malicious activities in the network. By using multiple identities of different vehicles attackers create an illusion that there is large numbers of vehicles traveling on road. Every vehicle in the network which is creates using the false certificate and identification cab be involved in the Sybil attack [45] [46].

In VANET Sybil attack can be detected by using various methods. In the absence of no logical centralized authority Sybil attacks can easily be done. Detection is also difficult due to the same reason i.e. unavailability of centralized logical authority. Main purpose behind this practice is that the malicious nodes create it number of clones virtually and each node clone or node claims and forecast fake position so that it would be selected as data forwarder.

This attack comprises of using fake various identities to breach the network. When attack occurs fast change in position of the node moving continuously increase the difficulty of to detect the attack on time to detect the Sybil attack strong coordination is compulsory among the vehicles moving in the Vanet network. As the vehicles in network are freely moving and communicating with each other so having week coordination among them. In this situation it is slightly difficult to detect it. It is also difficult to verify and authenticate the vehicle simultaneously [33] [34].

There can be many methods and techniques to detect this attack some techniques are as under:-

2.1.3.1 Directional antennae.

In this technique massages are to be checked that can be sent either by malicious or by genuine node. The direction of the arrival of packets can be checked by this method. As the direction of the arrival of packets (massage) received to the node is calculated. In that case a fake and malicious node sends more than one massage to the node from the same direction. In the case of real neighbor massage could be of different direction [48].

2.1.3.2. Propagational model.

This model is more appropriate then the first one to identify the Sybil attack. In this model received signal power and the value of its claimed position is calculated. In the case of attack the signal power which can be calculated by considers its position as its position varies with respect to the value of the position sent by the vehicle [47]. In that case when a real and genuine node sends the message to the receiver its real GPS position in the network on the road and its position claimed by the sending node would be same. By calculating relative positional value receiving node can easily calculate the position of the node next to it and so on. Calculated and claimed position of the sending node is to calculate to verify the nature of the sender either it is genuine or malicious one [49]. As in the Vanet network mobility of the nodes is very fast and changes with the passage of time so it is difficult to calculate the relative speed. In some case this methodology is not suitable to detect the same attack [34] [34].

2.1.3.2. Resource testing.

We know the resources of the attackers are mainly more than that of the others so in this technique capacity of resources of the sender are checked to evaluate either the sender node is genuine or malicious and is attacker. In the network every node is equipped with the limited and calculated resources like power, processing power, sensing etc. In this technique a puzzle is given to the nodes which are communicating in the network and with the receiving node. As the malicious node is stronger, powerful in terms of his resources i.e. more processing speed then that of the typical nodes communicating in the network [36].

So malicious node can easily process and solve the given puzzle with in less time as compared to the other nodes in network. Genuine and real nodes take known time to solve the puzzle. By comparing and processing the processing time and processing speed node can easily diagnose the nodes with more resources as compared to the other nodes is malicious one and is in try to attack the network.

We have discussed various attacks in Vanet. Classification of the attacks helps to deal, identify and to restrict these attacks. Vanet network is a collection of vast category of nodes and services normally communicating with internal devices and external due to this verity serious threat of attacks are faced by the VANET [37]. In Vanet life threatening information moves so that user wants safety on the road while utilizing VANET. Given attacks and their classification is supposed to be helpful to identify the attacks [50]. It is not easy to restrict and minimize attackers but it is possible to implement such techniques which can help to identify the attacks and restrict them. In next chapter we purpose some techniques to identify the attacks and try to minimize the after affects of these attacks.

2.1.3.3. Ad-hoc on demand vector.

It enables multi-hope and self-starting routing between mobile nodes which are about to join the network. AODV allows the node to be in a rout when they communicate and doesn't urges them to remember these routes when they are not communicating. AODV by using destination sequence numbers avoid the counting to infinity [38] [39].

AODV defines three types of massages.

- RERR-:

In an active route massages are to be used to notify the breakage of a linkage in network.

- RREP-:

Finalizations of the routes by which the nodes are to communicate are finalized by using such a massage.

- RREQ-:

To establish a new route the initialization of the finding search such massages are used [40].

Research Methodology

Research methodology is quantitative of this thesis. It is used to quantify the problem by way of generating numerical data or data that can be transformed into useable statistics. Quantitative research is a more logical and data-led approach which provides a measure of what people think from a statistical and numerical point of view. For example, if you wanted to know how many of your customers support a proposed change in your products or service and how strongly (on a scale) they support it. Quantitative Research uses measurable data to formulate facts and uncover patterns in research. Quantitative data collection methods are much more structured than qualitative data collection methods [51].

The purpose of this research is to explore and analyses of the VANET and its security. To find the answer of the research questions and sub-questions the author has conducted the literature review. As per the data collected from articles, Books and other sources we analyze different possible threats, attacks and security related issues of VANET. We have to compare different rules and methodologies to made VANET safe and reliable for communication by getting information and knowledge by authors and researchers. After analysis some parameters are used to evaluate the efficiency of VANET.

This research is done to explore and to analyses the VANET and its security. To find the answer of the research questions and sub-questions the author has conducted the literature review. As per the data collected from articles, Books and other sources we analyze different possible threats, attacks and security related issues of VANET. We have to compare different rules and methodologies to made VANET safe and reliable for communication by getting information and knowledge by authors and researchers. After analysis some parameters are used to evaluate the efficiency of VANET. In this research by using different protocols used

in VANET we try to find the effects of black hole attack in VANET communication[52]. We run our proposed scenario and analyze its results by considering different situations.

2.2. Literature review

A number of research papers have proposed various methods and ways to analyze and to tackle with security and privacy issues of VANET. In this chapter we discuss already existing work done on the security and privacy of VANET. We analyze the major types of attacks and threats to the VANET. As we are working of security threats and issue of VANET so we analyze the already work had done on these threats by others researchers and authors.

1. Al. falasi, B. Ezendin (2013) proposed public key infrastructure approach in his research paper "Revocation in Vanet, A Survay". As PKI approach is very effective solution for the security related problems of VANET it is widely used and is adopted by the researchers. Certificate abrogation is the first part of PKI solution.

   Certificate abrogation is done of the vehicle which does some malicious activities in the network. Certificate abrogation is not only done by the certificate issuing authority but also by the neighboring vehicles which are in communication in the network along with that malicious vehicle.

   Author discussed various provocation and abrogation schemes adopted by the certificate issuing authority. Author overview and analyses the already stated abrogation approaches used to revocation of certificate by the certificate issuing authority and proposed new approach to terminate the certificate of malicious vehicle in the network used by the vehicle present in the network.
2. A. Hamieh, JB. Othman (2009) performs the Detection of Jamming Attacks by using Error Distribution. Author proposed a technique to detect jamming in VANET. In new scheme by using various measurements of the distribution of errors jamming can be detected. By the comparison and correlation between the correct exception time and the error exception time jamming attack can be detected. Author recommends this technique for reactive jamming. Specific jamming attacks are detected by using this scheme. Relationship and association between to specific random variables is defined as their correlation ship.
3. B. Vimal, K. Roshan, KB. Singh (2012) in his paper discuss and analyze VANET at the time of black hole attack. These attacks are analyzed by using four different scenarios to evaluate node-to-node delay, throughput and network load. In term of security protocol

should be dispensable and efficient. Vulnerability of the two protocols AODV and of OLSR is more severe and affects more when number of nodes is very high. In case of AODV severance is 5 to 10 percent while in case of OLSR it is 2 to 5 percent. As compared to OLSR throughput of AODV effected twice. The effect of malicious node on AODV is less then OLSR in case of network load. Author by using simulator Opnet concludes that then that of AODV OLSR is more vulnerable to black hole attack.

4. D. Dhumal, V. Tehre (2015) suggested an early alert system for the vehicle in the VANET. This system informs the vehicle about the accidental and swears condition of the road. Instead of broadcasting the alert and threat massage the system multicast the alert massages in the network reduced the congestion and accident chance on the road. This scenario ultimately results in the reduction of accidents.

   The fundamental undertaking is with whom to convey Priority Based Signal Management in Traffic System indicated how the Traffic Light Signal control, incorporating with the execute of Traffic Scheduling Algorithm which is utilized to pick up data from the vehicle position and the pace. The gained information from Road Side Units reschedules the movement light planning as per the activity condition for low or high-thickness street activity. In the event that the thickness of the street activity is high then Maximum thickness of movement permit most extreme default timing for movement lights. Least thickness of activity permit movement with least planning for activity lights.

   On the off chance that the activity rate on both side is Equal or crevice inside movement then as indicated by landing time activity light flag set to minimized. The reproduced results under high and in addition low-thickness street activity load. By using the early alert system road safety threats can be resolved at some extant.

5. Dhamgaye, (2012) discussed VANET security framework designs. Author also worked on designing of security framework. Effective cryptographic algorithms are required for the secure communication of VANET Network. To detect the malicious and attacker nodes in the network we need effective routing algorithms and communication frameworks. For safe and secure communication we only need crypto-graphical algorithms and methods but with this we also need a strong and effective framework that can detect the attacker, restrict and block them to communicate in network. In that case when an attacker successfully jammed a specific area in values of the both variables network exception time and error exception time varies as compared to the normal

values. By the Correlation of the values of both variables of both situations are undergone by a correlation process and comparison which in results shows either the network is normally functioned of there is any jamming.

6. JM. Horcas, M. Pinto, L, Fuentes (2014) discussed about secure and application oriented network design frameworks. In design frameworks security concerns and basic requirements of secure communication of VANET are considered. Authors analyze some technologies for the design of framework which provides a guideline for design. Author proposed a design framework which is security oriented.
7. Samiksh, A. Kaur , H. Kaur (2016) published analysis of security issues are discussed. Author discusses the saver result of Dos attack in VANET. Author provides a database of the attackers in which mainly the data of malicious activity model is given. User can identify the attack and trigger the model to tackle the attack
8. IA. Sumara, I. Ahmad. H, Hasbullah (2013) work in the same domain to provide the possible solution of the DOS attack. Author proposed the idea of using one more security layer already being used alternative solutions to tackle with DOS attack such as technology switching, channel switching, multiple transceivers and frequency hopping. No new crypto graphical scheme used in the given solution. While in already present schemes additional hardware of software is required so crypto-graphical scheme is introduced by which in the communication of RSUs and OBUs data can be encrypted and decrypted so that no malicious attacker can access it. In this scheme encryption and decryption is done while the keys is dispersed safely so that the malicious vehicle can't access the key as well. For the communication and dispersion of Key various techniques are used
9. H. Hasbullah, K. Verma, K. Ashok (2013) suggest an effective method to spot flooding attacks. This approach does not require any astronomically immense vicissitudes in OBU that makes it relatively facile to deploy. This approach is very effective and promising shows that the method is effective as well as efficient against the spoofing and flooding attacks. Its effectiveness depends on efficient data structures. The method is performed to achieve lower storage and computational costs with high level detection rate.
10. H. Godavari, Kudlikar, U. Nagaraj (2015) in his paper suggest that PKI scheme is time consuming as in Public key exchange scheme all the massages are to be checked and verified one after another to ensure the trustable communication in the VANET network. PKI failed to cope with the computational efficiency by this way. To overcome this

situation a new technique was also used known as Batch Signature Verification Scheme for Communication. In this scheme simultaneously multiple massages are verified.

But the speed of verification in this scheme is also very less as according to the DSRC protocol (Dedicated Short Range Communication). As per DSRC Road side unit must verify 2500-5000 massages per second. To attain this speed of verification is very difficult existing schemes are not suitable. To tackle this speed issue author proposed n new scheme for verification and authentication of massages named as Proxy Based Authentication Scheme (PBAS).

In this scheme RSUs, Vehicles and proxy vehicles function. By using verification functions proxy vehicle authenticate multiple massages at the same time i.e. verification of multiple massages is done by the special vehicle which is selected as proxy vehicle and is equipped by the various verification schemes and verification algorithms. Once the massage is verified by the proxy vehicle it is then send to the RSU for the verification of signature.

After the proxy vehicle verify the massages are sent to the RSUs for the signature verification. As the initial verification and authentication of massages is done by proxy vehicle so that the work load on RSUs decrease simultaneously. As the massages arrived from various proxy vehicles at RSUs it verifies their signature by using specially designed systematic and independent mechanisms. After the RSUs check their signature there validity level is also defined by RSUs.

In the proposed scheme PBAS work load of the RSUs is reduced due to the cooperation of vehicles which acts as proxy vehicles, as the signature is verified by the Proxy vehicle and send it in the form of output to the most nearby RSU. RSU checks the output of the proxy vehicle thus consuming les computational workload. In the design requirement following things must be kept in mind (1) computational efficiency requirements of the network must be kept on top priority (2) message integrity, authentication and Privacy must be fulfilled (3) Scheme should follow the process at any cost and in the presence of any amount of vehicles.

11. J.T. Isaac, S. Zeadally, J.S. Camara (2010) discusses some attacks and threats related to the security faced by VANET. They also proposed solutions for the reported security threats and vulnerabilities in VANET. Authors consider some various parameters to evaluate and to secure the VANET. It is said that ultimate security can be achieved by covering and monitoring the basic parameters such as key management, Location of

vehicle, anonymity and reputation. To keep the physical identity of vehicles undetectable from unauthorized nodes in network anonymity can be properly managed. Cryptographic conversation in the network is done by the generation, distribution and storage of the keys used in key management. Trust ability of the specific vehicle is evaluated by reputation. How much a vehicle is trustable and can we communicate with it?

12. H. Kaur , M. Bala , V. Sahni (2013) in their research work discussed the affect of black hole attack on network by using three routing protocols DSDV, DSR and ZRP by using some performance parameters. Competitive analysis and the affect of black hole attack is discussed in detail. DSDV and ZRP protocols are best as per there analyzes and same protocol is recommended for use as routing protocol.
13. K. Verma, H. Hasbullah (2014) author suggests the Bloom-filter-predicated detection method, which make the availability of services to the real vehicles in network. This method restricts the communication of malicious vehicles and allows utilizing services in VANET only to the genuine vehicles. With secure communication it also frees the portion of bandwidth used by falsified vehicles. This service requires less resource and is facile in deployment. As per the results in the detection of DOS attacks this method is effective and efficacious.
14. VD. Khairnar, DR K. Kotecha (2013) in his paper Analyze basics and important components of VANET network environment such as environment, standards and VANET architecture. MANET and cellular network are its originators so author listed some characteristics which distinguish it from them. For convenient and smooth communication routing strategies are required and favorable environment as well.
15. S. Malebary, W. Xu (2015) discusses jamming in VANET and suggested an algorithm to decrease the after effect and to detect the jamming. The detection method depends upon the Packet delivery ratio moved in VANET. By monitoring PDR in network it is suggested and is accessed either the network is working or is under jamming attack.

    Once the algorithm comes to know about the attack it broadcast a high priority warning massage to inform other vehicles in the network. Once a vehicle entered in jammed area its DPR value would be zero or very low so it would be considered as is under jamming attack. When a vehicle is detected under jamming attack then the state, direction, jamming area and jamming position would be broadcasted in the form of massage with very high priority. Author suggested the technique to detect the detection of jamming and

informing other vehicles about it. Author discussed only one type of jamming while attacker and malicious vehicle use different types and methodologies in jamming attack. Author also proposed two solutions and precautionary methods to tackle with Forging and Sybil attacks that use On board radar as eye of the vehicle.

16. K. Megha (2014) overview identified different communication models the current security issues and analyzed from the security point of view over VANETs. Author identified the current trends in data security proposed to solve not only traditional problems but also some context-specific ones (e.g. eviction of misbehaving vehicles from the VANET).
17. Minda Xiang et al (2012) suggested to remove the effects of DOS attacks in VANET. Protection node based strategy can be implemented to minimize the after effects of DOS attacks on VANET. Nodes are distributed into two levels i.e. lower level nodes and high level nodes. This distribution is called Hieratical Network Architecture. First node of the source which is selected as first layer at the time when attacker set a route for attack it is known as Remote Protection Node.

    As the node selected as Remote Protection Node from the source check and filter the packets which are broadcasted by the malicious node and in the case when the RPN come to know that the packets containing vulnerabilities it broadcast a massage to inform other nodes about that malicious node. As all the possible vehicles in the which are near to it in network are informed by malicious vehicle so by this technique effect of DOS and DDOS reduced but this technique increase the traffic load as it take allot of time for the whole process in broadcasting and evaluation of malicious attacks. Paper proposed a protocol to treat with jamming attack in VANET. The name of protocol is Wisper-net. This technique consists up of two components i.e. Wisper-net -Time and Wisper-net -Space.
18. H. Kaur , M. Bala , V. Sahni (2013) in their research work discussed the affect of black hole attack on network by using three routing protocols DSDV, DSR and ZRP by using some performance parameters. Competitive analysis and the affect of black hole attack is discussed in detail. DSDV and ZRP protocols are best as per there analyzes and same protocol is recommended for use as routing protocol.
19. Qian, (2015) discuss the different routing protocols in terms of different parameters which can affect the performance of VANET and evaluate quality of service parameters such as throughput and packet drop in city as well as highway scenario and it has been

found that ADV is best suitable for highway scenario. Author analyzes the performance of VANET and also evaluates its performance by considering various parameters.

20. K. Zaidi, M. Rajarajan (2015) analyze and discuss authenticity, security and privacy issues in VANET. Author recommends PKI based approach to tackle these issues. Conversation in the network is certified i.e. each massage move from OBU to RSU is RSU to OBU use its key and certificate issued from a trusted certificate issuing authority. Receivers either RSU or OBU checks the massage's certificate for the sender's key. That key is issued to verify the sander who sent the massage. It is also recommended that only the critical massages should be signed by OBU to prevent the future attacks in the network. The certificate of the malicious node should be blocked or provoked.

    The revocation of the malicious nodes can be done either by OBU or RSU as it depends upon the strategy used. For the revocation of malicious certificates three main types of strategies are being suggested. RCCRL (Distributed Revocation Protocol), RTPD (Revocation Temper proof device), DPR (Distributed of Revocation Protocol). Author suggests to use short time lived keys which can be expired once used by the receiver. These short timed lived keys are certified by the certificate issuing authority and preserved in OBUs and RSUs. While in conversation each session sender use different key for authentication. By using separate key the original and actual identity of the sender cannot be tacked. In any inconvenience situation only CA can trace the original and genuine identity of the sender. As in this technique OBUs and RSUs are to communicate continue sly with third parties like Service providers and certificate authority. By signing in by using the RSU keys the implementation of such a scheme would be expensive and easy to access by the attackers. Author also purpose other solution to resolve the attacks related issues but the main back draw of the such a practice is to require multiple handshaking between RSU and OBU to check the certificate of the vehicle or RSU sent the massage.

21. W. Xu, T. Wood, W.Trappe, Y. Zhang (2004) in his paper suggested two anti jamming methods special retreats and channel surfing. First technique is designed by inspiring little bit by frequency hopping technique. Frequency hopping technique is usually used to check and monitor the utilization of frequency allocated in the network. Channel surfing works at MAC layer while frequency hopping works at Physical layer in the network. In this technique it is to be sensed that either the channel in the network is jammed or not so if it is jammed vehicles can switch the channel to communicate.

When a node come to know that the channel is his channel of communication is jammed it switch its channel and broadcast a beacon massage over new frequency channel. When the node changes its channel other neighboring nodes detect the absence of the node in the channel so they also switch the channel to receive the beacon massages. Its neighbor nodes change the channel in search of beacon massage containing the information about the reason of the changing of channel. If the neighboring vehicles do not find any beacon massage they think that node just dispread or changed its position simultaneously. One the neighbor receives beacon massage it informs other vehicles in the network to change the channel and inform them about the jamming of initial channel.

In that case there would be two kind of switching in network either whole network changes its frequency channel or the nodes which are at the boundary of the jamming change its channel. In the first approach the nearby nodes change their channel and act as relays for the other vehicles in network. In second approach special retreat method reaction of the node after the jamming attack is different. In this method when a node come to know that it is being jammed it tries to escape from the jammed area and to avoid the partition from network is tries to remain in contact with the other nodes in the network.

When a node comes to know about the jamming area it tries to escape from that area and connect to the nodes present in the network specifically with its neighboring nodes. If a network continue sly move away from the neighboring nodes without sending imitational massage it ultimately move far from the network results in the partition from the network, So that I becomes impossible to stay connected with the network.

1. Wisper-net: -Time: - with the objective to decrease the control proportion of a measurable jammer to that of an arbitrary jammer.

2. Wisper-net -Space: - in which communication routs are adjusted continually to maintain a strategic distance from stuck zones and select ways with max PDR.

The assessment of the protocol demonstrates that Wisper-net decreases the working of jammers even an irregular one. The proposed convention has been executed on Fire-Fly. Firefly is a period synchronized continuous sensor system for assessment purposes. A few confinements have been seen after tests.

After some results it is observed that this protocol has some limitations in which it work properly and efficiently. One of the main issue comes to know after experiments is that Wisper-net is unable to work when a big network containing more than 500 nodes in

under attack. Little more research is required to enhance the efficiency of Wisper-net protocol to overcome the jamming attack.

The monitoring power of the radar is limited as it can watch and monitor only surroundings. A vehicle can see the position of the surrounding vehicle and the report of their coordinated it isolate the attacker. To tackle with replay attack in VANET two methods can be used. In first method timestamp is used for the entire vehicle to synchronize them. While in second data received is to be analyzed and comparison results in the identification and alarming of the critical situation.

Chapter No -3Experimental Work

3.1- Previous work.

We here discuss about previous work. We try to discuss about the work done in this domain till today.

- In 2013 Harmandeep Singh and Manpreeet Singh discuss effect of black hole attack on routing protocols including AODV, OLS and ZRP. They simulated 10 to 16 nodes and consider the results of behavior of these protocols when they are under attack and when they are in normal working. In their paper they analyzed that the behavior of DSDV protocol is not much different as compared to other.
- H. Kaur , M. Bala , V. Sahni (2013) in their research work discussed the affect of black hole attack on network by using three routing protocols DSDV, DSR and ZRP by using some performance parameters. Competitive analysis and the affect of black hole attack is discussed in detail. DSDV and ZRP protocols are best as per there analyzes and same protocol is recommended for use as routing protocol.
- Bossem and Azab in 2015 discussed effect of black hole attack by considering these routing protocols. Author discusses and performs survey of the effect of Black hole attack on the performance of VANET nodes by monitoring behavioral changes in some certain performance parameters.

3.2. -Proposed Work

In VANET attacks results in the alteration as well as the threat of malicious usage of personal data transferring in the network. As in chapter 2 we discussed many issues and security threats for the VANET network we choose Black Hole Attack for simulation and for analyses. Black Hole Attack results in the blockage of data flow or it can alter the data with malicious one. In this chapter we analyze the behavior of Black Hole Attack on the network.

We evaluate it by using various scenarios. As in Black Hole Attack genuine communication stops and the specific point used for inward and outward communication is hacked by some malicious node. To evaluate the Black Hole Attack in VANET network we use some protocols which are widely used in VANET for routing purposes. We chose this because Black Hole Attack infect effects the routing of nodes. How a Black Hole Attack reacts and affects the VANET? In next chapter we evaluate the affect of Black Hole Attack by considering three routing protocols i.e. DSDV, DSR and ZRP. We check and evaluate the

affect of Black Hole Attack on the VANET network by calculating and observing three characteristics of VANET network such as Network delay, Network Loads and Packet delivery ratio (PDR). The behavior of protocols varies with and without Black Hole Attack. To evaluate that behavior of the both protocols we consider and monitor the affect on the network. We consider these three characteristics of network or nodes.

We take these three protocols for the evaluation of the behavioral affect of Black Hole Attack. We monitor three characteristics of nodes such as Network delay, Network Delay and Packet delivery ratio (PDR). We simulate these three characteristics under different scenarios such as with lab of 50 nodes with and without Black Hole Attack.

NCTUns makes use of Linux network protocol to simulate network, transport layer networks, like TCP, ICMP, IP, and UDP. Slight modifications should be carried out on Linux kernel to enable timers used by kernel protocol stack of every node which is to be simulate to progress on their times which is based on the clock which is under control of NCTUns instead of the real world clock.

3.5- Black Hole Attack.

3.6- Performance Analysis.

3.3.- Black Hole Attack

Black hole attack in network is the point of place from where the incoming as well as outgoing traffic is blocked. Incoming and outgoing traffic is discarded from a specific point in such a way that the network can't get information about the exact problem [53]. In black hole attackers both sender node and receiver nodes without informing breach the transformation.

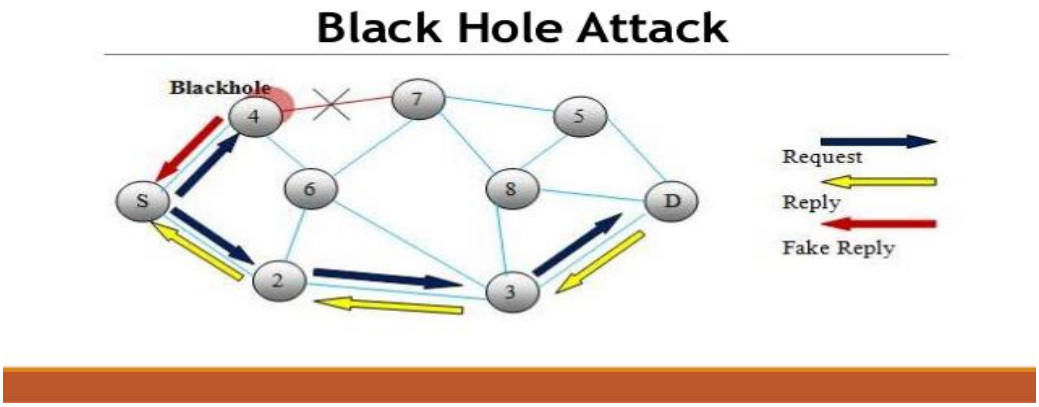

Fig.16.Black Hole Attack [30]

3.4- DESINATION SEQUENCED-DISTANCE VECTOR ROUTING (DSDV)

DSDV (Destination-Sequenced Distance-Vector Routing) is a proactive type of routing protocol widely used for routing in VANET. DSDV is mainly used to solve the routing loop problem. Routing table is based on sequence number each entry which consists up of the routing sequence is saved in table. DSDV is a proactive and table driven protocol to achieve the optimized link state routing. It reduce the traffic overhead MPR (Multipoint relay). It is proactive in nature [54].

It is designed for large size networks. MPR is designed to provide as accurate and optimized link as the network is dense and big. Multiple Relay helps to choose the shortest path for reaching toward the destination. All MPRs are required to inform their information about link state to their MPR sector heads. As the topological requirement occurs by a node it is periodically saved in the related MPR. DSDV typically use three types of control massages, Topology information (TC), HELLO, Multiple Interface Declaration (MID).

3.5-ZONE ROUTING PROTOCOL (ZRP)

Zone Routing Protocol is hybrid in nature as it can use both proactive and reactive routing in VANET network. As it cover the flaws and issues of both proactive and reactive routing. It speeds up the packet delivery and reduces the overheads and other hurdles by utilizing both routing techniques. If the massage destination is in the same origin of sender then proactive routing is used while in the case when the destination is far from the destination zone it utilizes reactive routing. Routing table is used to determine the routing route which would be more appropriate and safe as well as shortest [55].

In this each node regularly maintain a table in which information about the node is save which send the packet to other destination. Three types of control massages are used by ZRP i.e. RREQ whenever a rout is not available for the destination node a request for rout is broadcasted throughout the network, RREP whenever a anode has route of its destination but again want to be in session it unicast a massage to the destination to be in session for communication, RERR [56]. Whenever session or rout breaks between two nodes they send an error massage to each other to inform about the error in rout.

3.6- DYNAMIC SOURCE ROUTING PROTOCOL (DSR)

DSR is the set of instructions, massages and algorithms used to exchange packets from source to destination under some citrine routing pattern. Static routing allows routing only in static manner but DSR is more robust than that of static protocols. In case of static routing if a router or node become unreachable whole communication stops results in the failure of network. In DSR this disadvantage of static protocols are overcome. DSR switch the sent packets to the destination and put the routing information manually into routing table. This protocol not only determine the route as well as the maintaining a routing table it also determine and guide the sender to chose the best and shortest path in the case of the unavailability of first path [57]. DSR allow the dynamic topology change with the respect of requirement change as well as the breakage of first path. It has many distinctive functions among other protocols like.

- Discover new routes.
- Discover new remote routes.
- Manage and updation of routing table.
- Determined shortest and best route from source to destination.
- Discover new path in case of using old routing path.

Updation in the routing table is given a sequence number [58]. Every time with the updation of rout in routing table a specific sequence number is given to that updation.

We evaluate and analyze the performance of VANET with and without Black Hole Attack by monitoring certain performance measures which are given bellow:

- MOBILITY
- TIME PER SECOND.
- NETWORK LOAD
- NETWORK DELAY
- PACKAT DELIVERY RATIO (PDR

3.7.1-Scenario Description

Figure displays 50 vehicles nodes that are called OBUs in communication setup with in this scenario. As the OBUs change inside the network due to examine each protocols

performance, vehicles nodes display the network performance. While the performance of a below assumed scenario is being measured in vehicle to road-side-unit V2R, vehicle to vehicle V2V communication, inside the network vehicles nodes change to start VANET. In this thesis we used Random waypoint mobility model. Vehicles nodes are free to change their position and reach at randomly their endpoint with use of this mobility model.

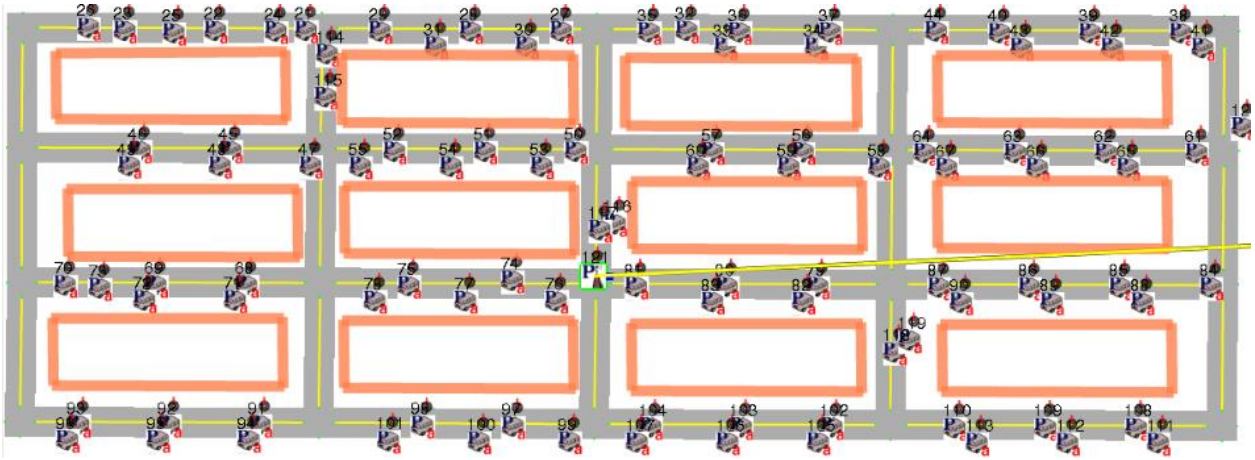

Fig.17.VANET Scenario[30]

3.7- Scenario for Simulation

VANET contain of movable nodes that route the Car representative mobility model which permits cars to track roads, to be alert of other, and traffic lights. Traffic lights on each corner of the road are fixed and nodes break or they retain moving according to the start of the traffic lights.

The following table displays the city area scenario vehicles nodes and simulation parameters.

3.8- VANET Routing Protocols

Following given are some important routing protocols used in VANET DSR, OLSR, DSDV.

DSR Dynamic Source Routing Protocol is source routing on-demand routing protocol designed for Ad-Hoc network to reduce the consumption of bandwidth utilized by control massages by eliminate the requirement of update in periodic table. DSR provide rout on demand so that a sender knows the complete route to its destination. Routes are saved in the route cache of the sender node so that is can be used whenever communication is required with the receiving node. Whenever node wants to send some data to any node it first of all check either the route of the desired node is present or note.

. DSDV Destination-Sequenced Distance Vector routing protocol used to increase convergence speed, solve routing loops problem and control overhead massages. In this node periodically update the routing tables of the neighboring nodes periodically.

DSDV protocol maintains a routing table that store information regarding address of the next hop and cost matrix of the routing path. Whenever the network topology changed updating occurred in the routing table.3.8.1- Security Based Routing Protocols

Chapter No- 4 Results and Discussion

4.1-RESULTS

This chapter emphasis on result and its study based on simulation performed in NCTUns simulator. Given figures present our simulated results in different network nodes which are under the Black Hole attack. In order to assess the performance of simulated based on black hole attack, also we can measure performance parameters of packet in end to end delay, through put as well as network load. Above given parameters for networks measuring are defined as “performance analysis”. For the analyses of the affect Black hole attack on VANET network. We simulate and analyze the network by considering some of the important characteristics of the VANET such as Mobility, Time, Network load, Network Delay and Packet Delivery Ration. We monitor the behavior of nodes with and without Black Hole Attack. For the analysis we monitor three important routing protocols used in VANET for routing i.e. dynamic source routing protocol (DSR), Destination sequenced-distance vector routing (DSDV), Zone routing protocol (ZRP). We here discuss these protocols and characteristics of VANET below. After simulation results we make comparative analyses of these results generated in the result of simulations.

4.2-ROUTING PROTOCOLS USED IN VANET.

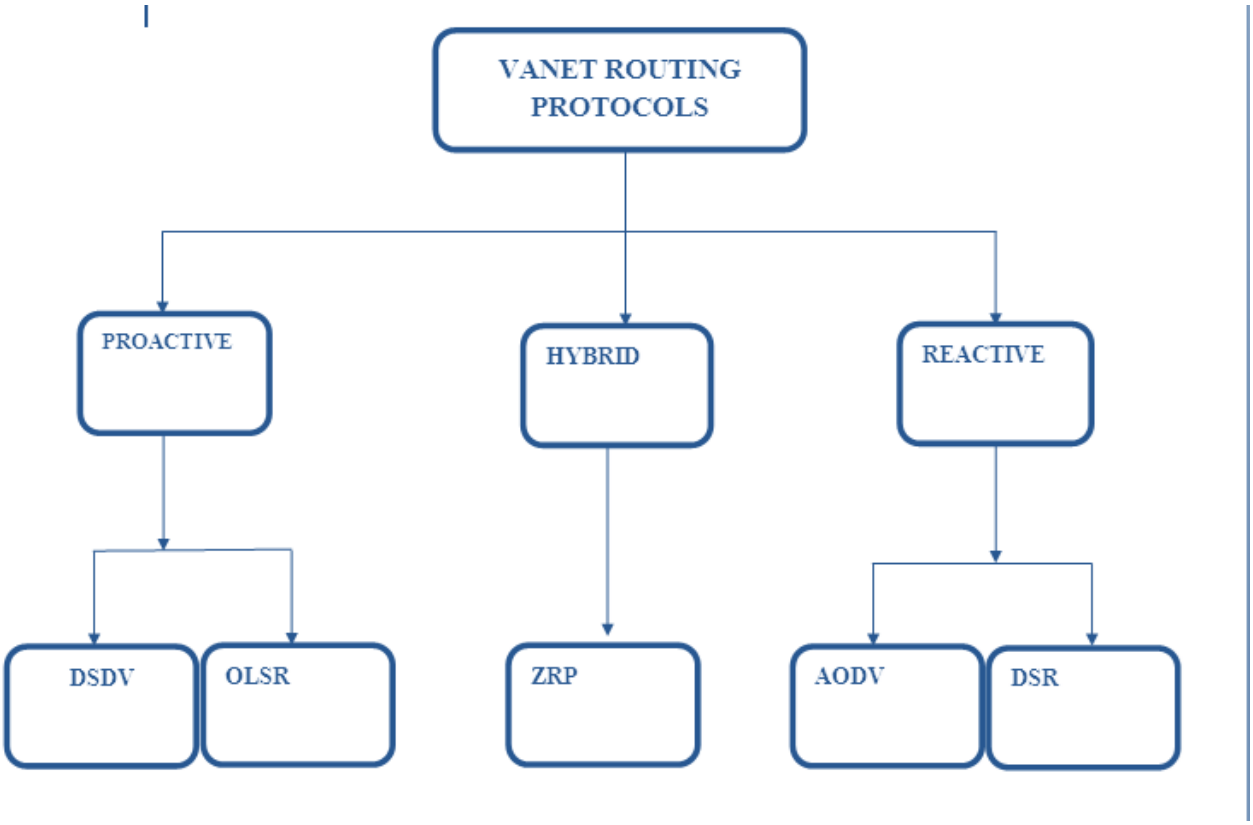

Fig.18. Routing Protocols Used In Vanet

Nature vise there are three main categories of VANET routing Protocols such as Proactive, Hybrid and Reactive. Further two protocols DSDV and DSDV are Proactive in nature; ZRP is Hybrid in nature while ZRP and DSR are Reactive protocols. For our simulation we used three protocols one from each category like DSDV from Proactive, ZRP from Hybrid and DSR from Reactive category. In below we discuss these three protocols one by one in detail. After simulation we perform comparative analyses of Black Hole Attack affect on various characteristics of VANET.

4.2.4-MOBILITY

In VANET network mobility is the distance covered by the packets per second. Mobility is the measurement of the travel or distance which a packet done from source to destination. A packet covered a specific distance at a certain speed which is represented as Meter per second (m/s).

4.2.5-NETWORK LOAD

Network load is the total amount of work has to be done by a system. In Vanet network load of a node consists of all the characteristics which we have defined in above description of VANET. Network load is the combination of all the inputs and outputs plus the processes done by the node. Network load in VANET network is the combination of the characteristics of nodes to transferring of data and information throughout the network and all the functionalities and all the processing's done by the nodes in the network. It is represented in bps.

4.2.6-NETWORK DELAY

Network delay is the specific time taken by packet or a signal to travel in network. It is the time taken by a packet to from source to destination; the certain time which it takes to travel is the delay. Delay varies with network to network.

Delay can occur due to many reasons such as distortion, noise and attenuation etc. Network delay is measures in Meter per seconds (m/sec).

4.2.7-PACKET DELIVERY RATIO (PDR)

Packet delivery ratio is the number of packets received by the receiver node which a sender transmits. It can be calculate by dividing the number of packets received by destination with the total number of packets sends by the transmitting node.

$$\textbf{PDR} = \frac{\textbf{Total number of packets received.}}{\textbf{No of Packet sent}}$$

4.3- SIMULATIONS

To analyze the affect of Black Hole Attack on the VANET we considered three routing protocols that are DSR, DSDV and ZRP. We monitor the behavior of these protocols in both cases i.e. when they are under attack and when they are in normal functionality (without attack). We simulations we take certain importance simulation parameters to simulate the behavior of the network.

Simulation Parameters

Model Family	VANET
Routing Protocols	DSR, DSDV, ZRP
Network Scale	City
Technology	Wireless Ad hoc
Operational Mode	802.11b
Simulation area	2000 x 2000 m
Simulation time	50 to 900 seconds
Number of scenarios	6
Number of nodes	50
Attacker nodes	15
node speed/mobility	50 m/s
Pause Time	1 sec
Trajectory	vector
Packet size(bits)	1024
Data Rate	20 mbps

Tabl.19. Simulation parameters

We first monitor the behavior of two performance parameters that are network load and time taken by the packets from sender node to reach at destination node.

4.4.1- NETWORK LOAD IN TERM OF TIME WITHOUT BLACK HOLE ATTACK.

Given below are the simulation parameters used to measure the network load and time required by packet to move from source to destination.

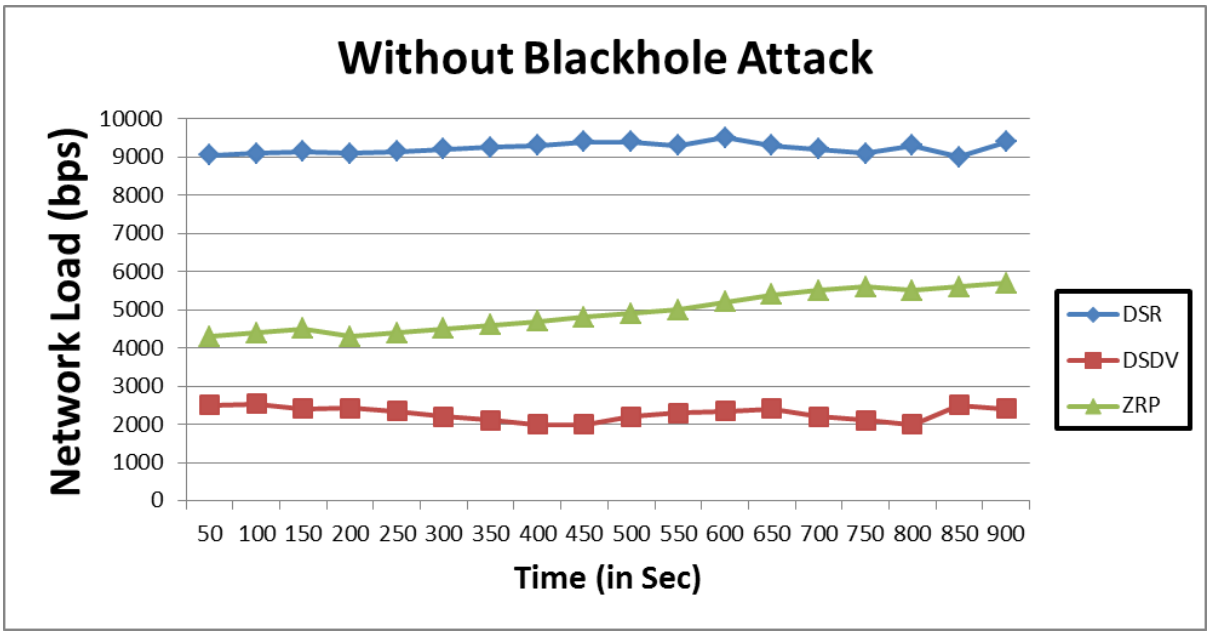

Fig.20. Network load without Black hole attack

In figure given above horizontally time is given in ascending order from 50sec to 900sec while vertically network load is also in ascending form from 0bps to 9000bps.

- Small parallelogram line represents DSR protocol.
- Triangle line showing ZRP protocol.
- Circled line showing DSDV protocol.

DSR in above given figure without black hole attack moves along with 9000bps in time 50sec to 900sec i.e. DSR remain constant at 9000bps at 550sec it slightly increases but at 600 sec it again come along 9000bps. So without attack DSR remain constant along 9000bps.

ZRP started from 4000bps and it deviated from 4000bps to 6000bps at 200sec. Its network load increased from 4000bps to 5000bps. At 500sec its Network load increase slightly from 5000 bps to 6000bps.

DSDV in start the network load is in between 2000-3000bps. DSDV moves at 400sec it slightly increases while at 800sec it again touches 2000bps. Overall it remain in roundabout of 2000bps.s

4.4.2- NETWORK LOAD IN TERM OF TIME WITH BLACK HOLE ATTACK

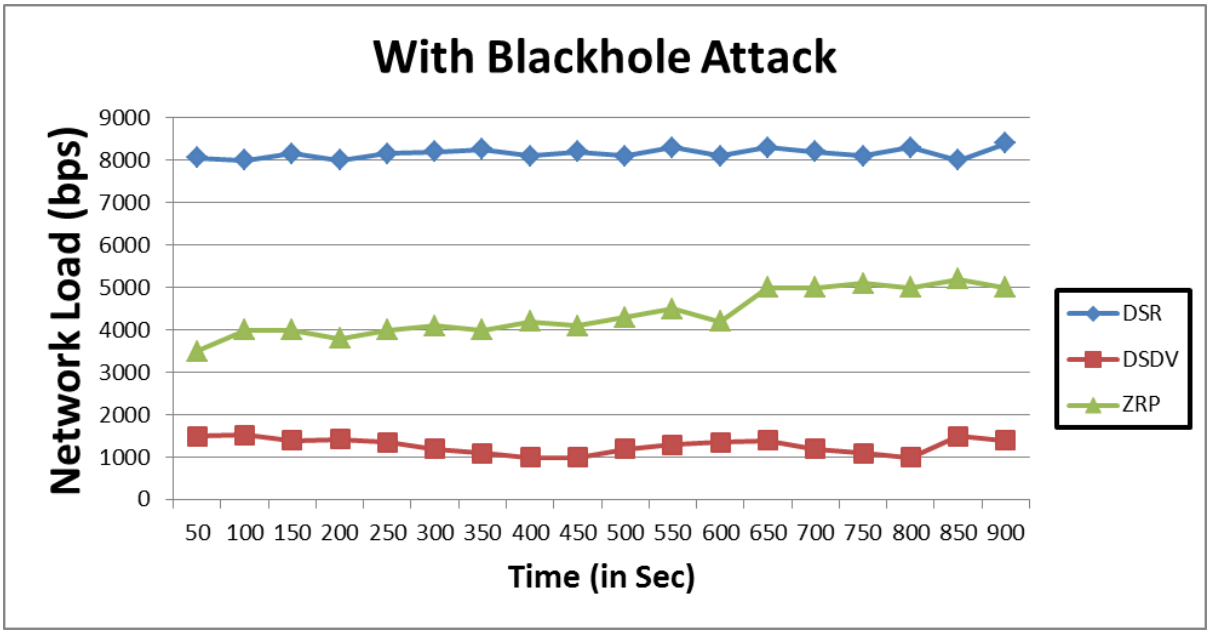

Fig.21.Network Load with Black Hole Attack

As shown in figure given above, DSR moves same as when it is not under attack. DSR in above given figure without black hole attack moves along with 9000bps in time 50sec to 900sec i.e. DSR remain constant at 9000bps at 550sec it slightly increases but at 600 sec it again come along 9000bps. So without attack DSR remain constant along 9000bps.

DSDV with attack also show the same behavior like when it is not under attack. DSDV in start the network load is in between 2000-3000bps. DSDV moves at 400sec it slightly increases while at 800sec it again touches 2000bps. Overall it remains in roundabout of 2000bps.

ZRP shows variations in its behavior when it is under attack. At start from time 50sec its network load is slightly above 3000bps with the passage of time its network load remain constant at 4000bps till 650sec. At 650sec its network load increase up to 5000bps and then it remain constant till 900secs.

4.4.3- NETWORK DELAY IN TERM OF TIME WITHOUT BLACK HOLE ATTACK

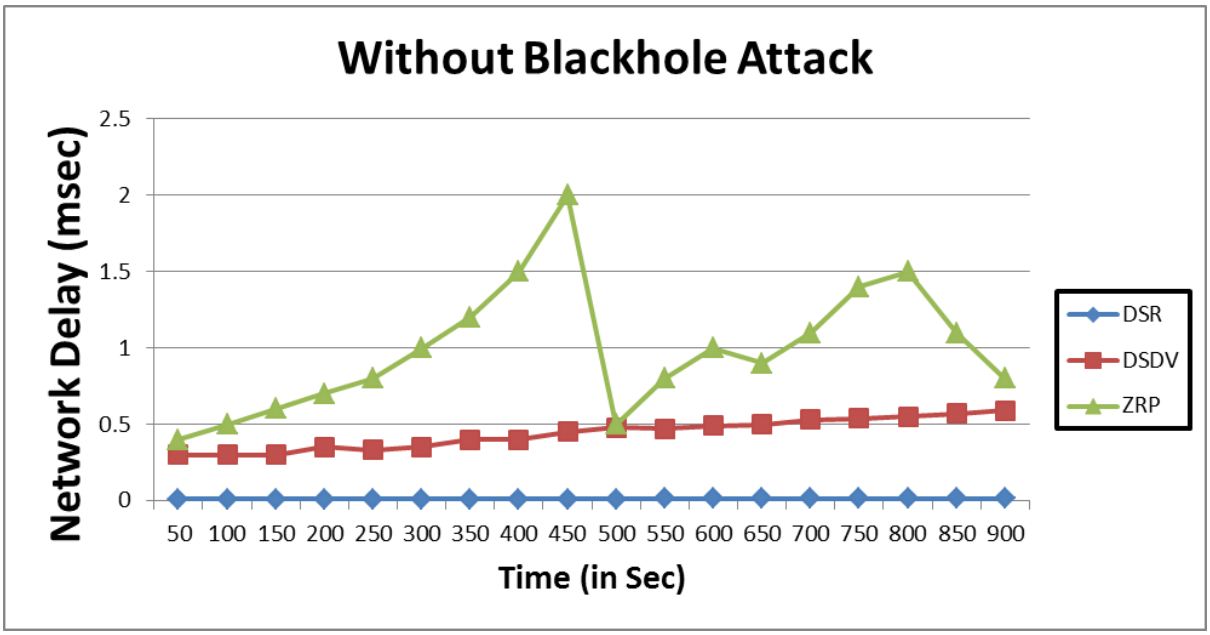

Fig.22. Network delay without black hole attack

As Shown in figure given above DSRs network delay is 0msec from time 50sec to 900 Hence it remain unchanged and no variation is noticed from the start of conversation in given time to then end.

At initial point the network delay of DSDV is slightly below from 0.5msec and is slightly above from zero. It means its network delay is less then 0.5msec at starting point. With the passage of time it continuously and slightly moves toward exactly 0.5msec at 500sec of time its Network delay is 0.5. After 500 sec network delay slightly increased from 0.5msec.

ZRP at time 50sec which is the initial time of communication the network delay is slightly below the 0.5msec. It touches at exactly 0.5msec at 100sec of time.

After 100sec it rapidly increases in network delay at exactly 450sec its network delay falls with high speed and again touches0.5msec of network delay. At 650msec it again touches 1msec and 105msec at 800sec of time.

4.4.4- NETWORK DELAY IN TERM OF TIME WITH BLACK HOLE ATTACK

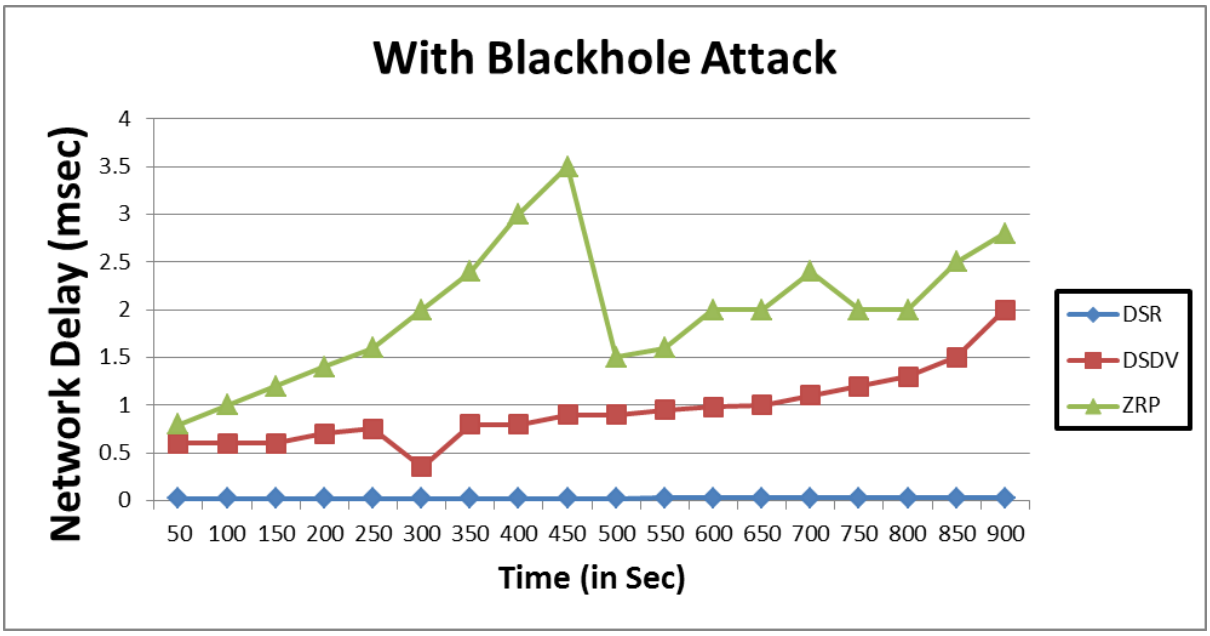

Fig.23. Network delay with black hole attack

As given above in figure behavior of DSR is same as when it is not under attack. DSRs network delay is 0msec from time 50sec to 900 Hence it remain unchanged and no variation is noticed from the start of conversation in given time to then end.

As shown in figure at time 50sec its network delay is exactly 0.5msec. With the passage of time at 300sec network delay of DSDV decreased from 0.5mec to 0msec. Again at 350sec its network delay increase and touches slightly below1msec .at exactly 650sec it start to deviation upward and at the end of time which is 900sec its network delay goes up to 2msec.

ZRP at time 50sec which is the initial time of communication the network delay is slightly below the 0.5msec. It touches at exactly 0.5msec at 100sec of time.

After 100sec it rapidly increases in network delay at exactly 450sec its network delay falls with high speed and again touches0.5msec of network delay. At 500sec it touches 1.5msec and as time pass it slightly increase till700sec .At 650msec it again touches 1msec and 105msec at 800sec of time. At the end of time that is 900 sec its network delay touches 2.5msec a slightly above from it.

4.4.5- PACKET DELIVERY RATIO IN TERM OF TIME WITHOUT BLACK HOLE ATTACK.

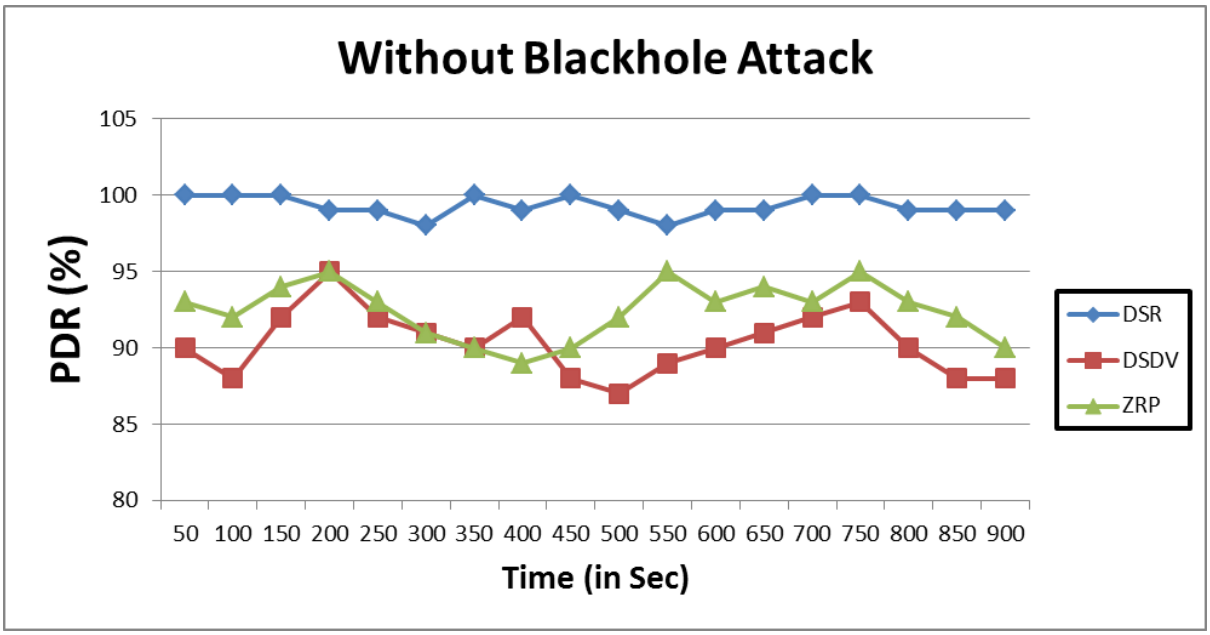

Fig.24. Packet delivery ratio without black hole attack

As shown in figure given above DSR without Black hole attack in the start of conversation at time 50sec have 100% PDR (Packet delivery ratio). With the passage of time PDR remain constant with little variations. Such as at time 300sec its PDR decrease from 100% and move toward 95% but after some time at 350sec it again touch 100% PDR. This variation occurs till the end of time.

Like as DSR ZRP in the start of time at 50sec having PDR in between of 90% and 95%. As it moves forward with the respect of time it goes up to 95% and fall back below 90% at exactly 550sec. At the end of time it again slightly decreases its PDR.

DSDV in start of time from 50sec is exactly at 90%. When it is at 100sec its PDR decreased down and at 200sec it increased up to 95% of PDR. After that with sight variations at 400sec of time it increase till between the 90 and 95%.at the end at time 900secits PDR again decreased between 90 and 95% of PDR.

4.4.6- PACKET DELIVERY RATIO IN TERM OF TIME WITH BLACK HOLE ATTACK.

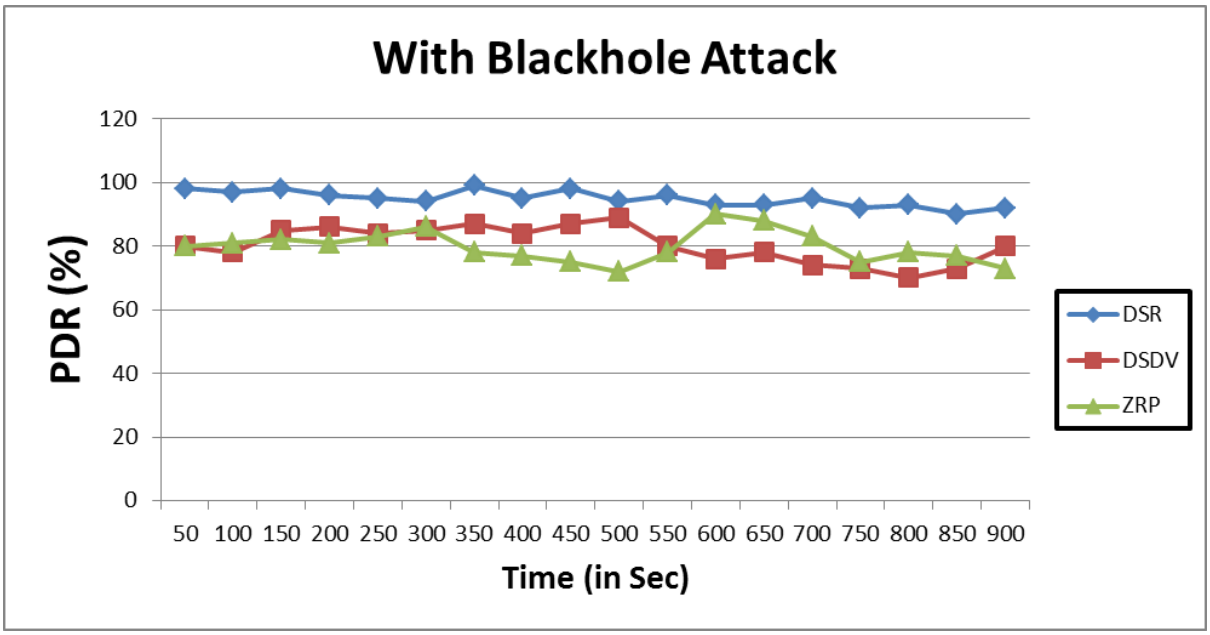

fig.25. Packet delivery ratio with black hole attack

DSR protocol under black hole attack shows a great variation with respect to the behavior when without attack. In start from 50sec of time its PDR is a little below from 100% of PDR as the time pass it decrease till 350sec of time after that it variants and remain in surrounding of 100% at the end it is below 100% of PDR.

ZRP under attack is at 800% of PDR in the start it remain in the surrounding and at 300sec it start to decrease ant decreased until at 300sec its PDR deviated toward 80% after 540sec it continuously drop and at the end of time 900sec it slightly deviates from 80% of PDR.

DSDV as shown in figure at the starting time at 50sec its PDR is at 80% and remain constant and in around of 80% till 30sec it derivate from 80% and go slightly toward 100% of PDR. At 500sec it decreases simultaneously till 600sec while at the end it again shows its PDR is exactly at 80%.

4.5. SIMULATIONS.

To simulate Black Hole Attack on the VANET we considered three routing protocols that are DSR, DSDV and ZRP. We monitor the behavior of these protocols in both cases i.e. when they are under attack and when they are in normal functionality (without attack). We simulations we take certain importance simulation parameters to simulate the behavior of the network. Simulation parameters are same but their values are different by above given simulations.

Simulation Parameters	
Model Family	VANET
Routing Protocols	DSR, DSDV, ZRP
Network Scale	City
Technology	Wireless Ad hoc
Operational Mode	802.11b
Simulation area	2000 x 2000 m
Simulation time	500 seconds
Number of scenarios	6
Number of nodes	50
Attacker nodes	15
node speed/mobility	10 to 100m/s
Pause Time	1 sec
Trajectory	vector
Packet size(bits)	1024
Data Rate	20 mbps

Table.26.Simulation parameters

4.5.1- NETWORK LOAD IN TERM OF MOBILITY WITHOUT BLACK HOLE ATTACK.

In first part of simulations we simulate the results as the performance parameters were at vertical while time was at horizontal. Likewise in first simulations we monitor same three protocols like DSR, DSDV and ZRP.

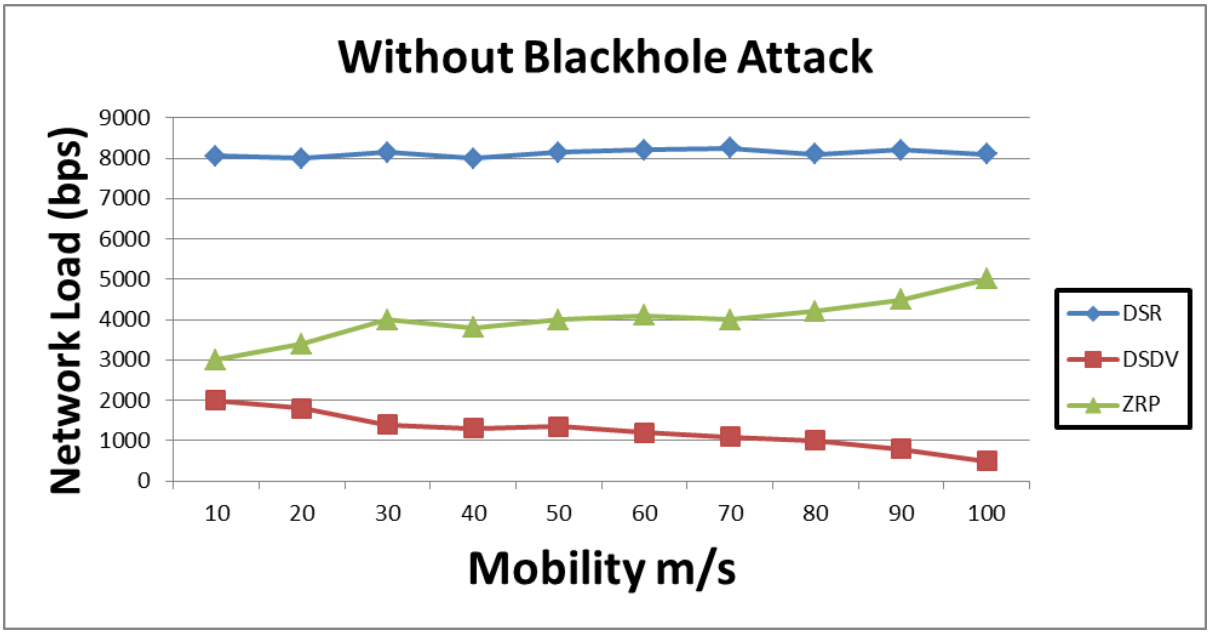

Fig.27. Network load in term of mobility without black hole attack

Network load is measured in bps and mobility measured in m/s. In the start at mobility there is 0m/s. Its network load is exactly at 8000bps. At mobility 30m/s it go away from line but with little variations remain along 8000bps of network load.

ZRP in start of conversation is at 3000bps while at 10m/s. When the mobility is 30 m/s its network load is 4000bps. While reaching at 70m/s it starts to decrease from 1000bps of network load. While the increase in mobility from 70m/s to 100ms its network load decrease simultaneously till it become in center of 1000bps and 0bps.

Network load of DSDV at exactly 10m/s network load is 2000bps. From here it starts decreasing till 40m/s of mobility. From here till 70m/s of mobility it remains almost unchanged and same. From 80m/s of mobility DSDV have 1000bps of network load. From 80ms of mobility its network load decrease slowly and ends between 1000bps and 0bps.

4.5.2- NETWORK LOAD IN TERM OF MOBILITY WITH BLACK HOLE ATTACK.

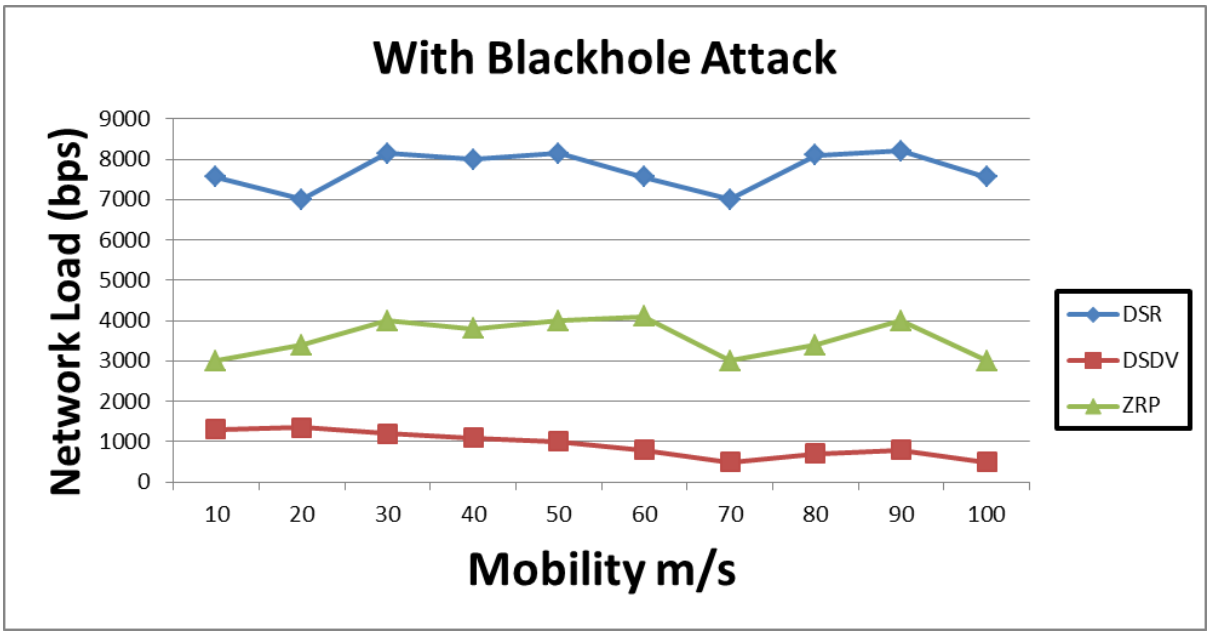

Fig.28. Network load in term of mobility with black hole attack

DSR at mobility 10 m/s its network load is in between 8000-9000bps. Its network load is 7000bps at mobility 20 m/s. From mobility 20 m/s it increased its network load till 8000 bps till 8000bps till 50 m/s its network load is 8000 bps. It slightly increases in its network load and at the end at 100 m/s its network load is bellow 8000bps.

DSDV at 10 m/s network load is at 1000bps with the increase in mobility till 50 m/s its network load remains same. While after 50 m/s its network load decreased below of 1000bps. At 70 m/s it again increases its network load and at 1000 m/s of mobility its Network load is between 0 and 1000bps.

ZRP when is under black hole attack at mobility 10 m/s its network load is at 3000bps. It's increased simultaneously after it till 30 m/s at 4000 bps of mobility. After 50 m/s it decreases slowly till 70 m/s up to 7000 bps. With the increase in mobility its network load remains constant but at the end at 100 m/s it remains between 8000-7000 bps.

4.5.3- NETWORK DELAY IN TERM OF MOBILITY WITHOUT BLACK HOLE ATTACK.

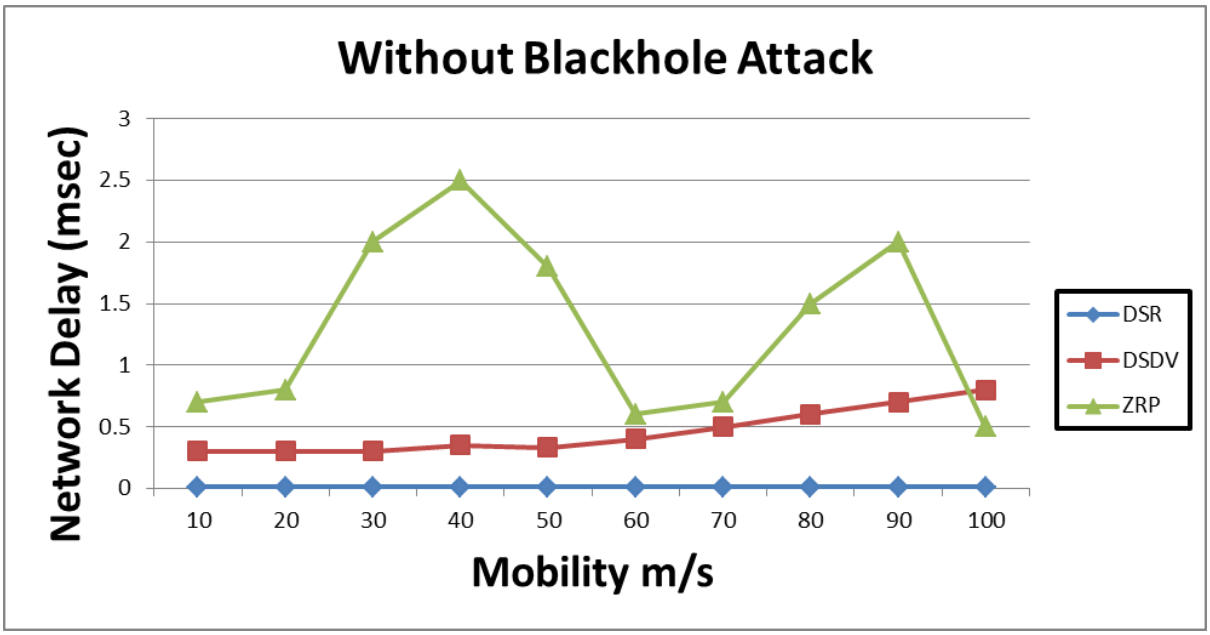

Fig.29. Network delay in term of mobility without black hole attack

DSR when is not under Black hole attack show zero variations from the start of conversation till the end i.e. from m/s to 100 m/s its network load remain 0msec.

DSDV form the start of conversation is between 1.5msec and 0msec. Network delay at the start of conversation at mobility 10m/s is between 0 and 0.5msec. from mobility 0m/s to 50m/s its network delay increase slowly till the mobility 100m/s it increase and reach between 1 and 1.5msec of network delay.

ZRP as shown in figure there is very large variation from start to the end. At mobility 10m/s the network delay is between 1 and 0.5msec network delay at 20m/s increase from 20m/s of mobility. It rapidly increases till the 40m/s of mobility its network delay is 2.5msec. From 40m/s it rapidly decreases and touché network delay at 0.5msec. Network delay increase from 60m/s of mobility till the 90m/s and network delay touches at 2msec. From 2msec of network delay it decrease till 0.5msec at the end of mobility 100m/s.

4.5.4- NETWORK DELAY IN TERM OF MOBILITY WITH BLACK HOLE ATTACK.

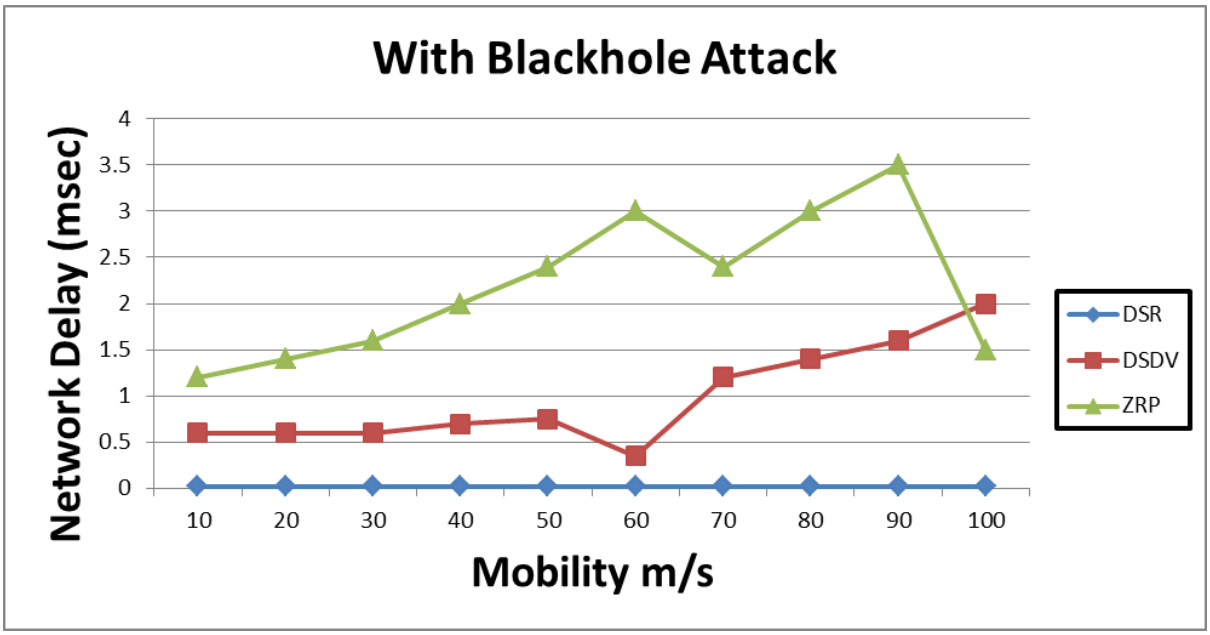

Fig.30. Network delay in term of mobility with black hole attack

DSR when under Black Hole attack show zero variations from the start of conversation till the end i.e. from m/s to 100 m/s its network load remain 0msec.

Network delay of DSDV at the mobility 10m/s is 0.5msec. From 10msec to 50m/s of mobility network delay remain same i.e. 0.5msec. From 50m/s of mobility it decrees its network delay and reach between 0.5m.s and 0m/s. From 60m/s network delay increase rapidly till the end of mobility 100m/s. Its network delay is 2msec. It means after black hole attack network delay is high then that of the behaviors shown without black hole attack.

Network delay of ZRP from the start of mobility at 10m/s is between 1.5msec and 1msec. From 10m/s if mobility to the 60m/s of the mobility it increase rapidly at exactly 60m/s to 70m/s its network delay decreased from 3 to 2.5msec. From it network delay increase till 3.5msec and from here it decrease to 1.5msec till the end.

4.5.5- PACKET DELIVERY RATIO IN TERM OF MOBILITY WITHOUT BLACK HOLE ATTACK.

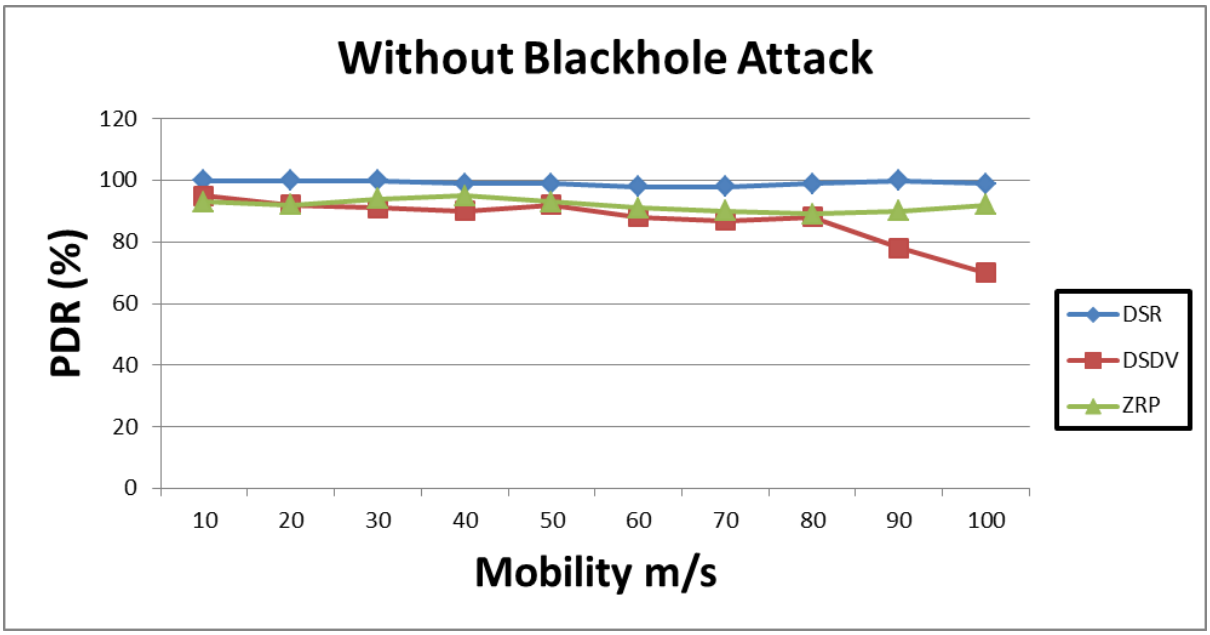

Fig.31. Packet delivery ratio in term of mobility without black hole attack

PDR of DSR from 50m/s of mobility is 100% form start. From 10m/s to 50m/s its PDR is at exactly 100%. From 50 to 80m/s it decrease in less PDR and after 80m/s it again reach 100% of PDR.

DSDV from the start of conversation from 10m/s it's PDR is less than 100%. From 10m/s to 50m/s of mobility it remains same with a very little variation. From 50m/s till and of conversation it decreases its PDR till between 60 and 80%.

ZRP from the start of conversation from 10m/s of mobility its PDR is between 80-100%. From 10m/s to 80m/s its PDR remain constant with a little variation. From 80m/s of mobility it increases in little PDR till the end i.e. 100m/s.

4.5.6- PACKET DELIVERY RATIO IN TERM OF MOBILITY WITH BLACK HOLE ATTACK.

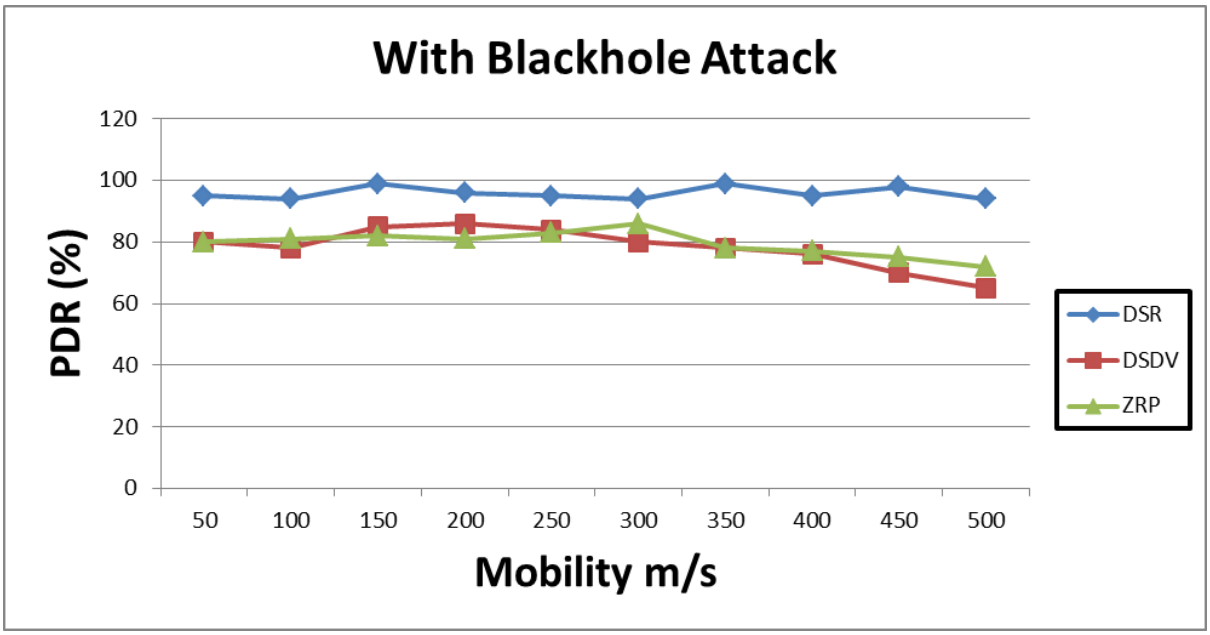

Fig.32. Packet delivery ratio in term of mobility with black hole attack

In this graph the interval of mobility is of 50 intervals as in 10 points of intervals variations cannot be clearly monitored.DSR from the start of conversation at 50m/s its PDR is little less than 100%. From 50 to 100m/s it remains unchanged. From here it increases till 100%. From 150m/s of mobility to the 350m/s it decreases to touch till 100%. From 350 to 450m/s it again touches 100% with little variation. From 450m/s to 500m/s it decreases from 100%.

DSDV in the start of conversation from mobility 50m/s its PDR is at 80%. After 50 intervals its PDR increase till the mobility 200m/s its PDR reaches between 80 and 100m/s. from 200m/s of mobility its PDR is 80%. After 300m/s of mobility its PDR decrease slowly and at the end of mobility at 500m/s its PDR is near to 60% of the mobility.

ZRP from the start of conversation at mobility 50m/s its PDR is 80%. Till the 250m/s of mobility its PDR is exactly 80% of ZRP. From 250m/s to 350m/s it remains along 80% of PDR. After 350m/s of mobility it decrease rapidly till 500m/s of mobility its PDR is between 80 and 60%.

6.6- COMPARISON

6.6.1-NETWORK LOAD

Network Load of DSR, DSDV and ZRP with and without Black hole attack with respect of time.

SR. No	Time/ Sec	DSR	DSR With attack	DSDV	DSDV with attack	ZRP	ZRP with attack
1	50	9000	9000+	2000+	1000+	4000	3000+
2	100	9000	9000+	2000+	1000+	4000+	4000
3	150	9000	9000	2000+	1000+	4000+	4000
4	200	9000	9000	2000+	1000+	4000	3000+
5	250	9000	9000+	2000+	1000+	4000+	4000+
6	300	9000	9000+	2000+	1000+	4000+	4000+
7	350	9000	9500	2000	1000+	4000+	4000+
8	400	9000+	9500	2000	1000	4000+	4000+
9	450	9000+	9000	2000	1000	4000+	4000
10	500	9000+	9000	2000	1000	4000+	4000
11	550	9000+	9000	2000	1000	5000	4000+
12	600	9000+	9000	2000	1000	5000+	4000
13	650	9000	9000	2000	1000	5000+	5000
14	700	9000	9000	2000	1000+	5000+	5000
15	750	9000+	9000	2000	1000+	5000+	5000
16	800	9000+	9000+	2000	1000+	5000+	5000
17	850	9500	9000+	2000+	1000+	5000+	5000
18	900	9500	9000+	2000+	1000+	5000+	5000

6.6.2- NETWORK DELAY

Network Delay of DSR, DSDV and ZRP with and without Black hole attack with respect of time.

SR. No	Time/ Sec	DSR	DSR With attack	DSDV	DSDV with attack	ZRP	ZRP with attack
1	50	0	0	0+	0.5+	0+	0.5
2	100	0	0	0+	0.5+	0.5	1
3	150	0	0	0+	0.5+	0.5+	1+
4	200	0	0	0+	0.5+	0.5+	1+
5	250	0	0	0+	0.5+	0.5+	1.5
6	300	0	0	0+	0+	1	2
7	350	0	0	0+	0.5+	1+	2.5
8	400	0	0	0+	0.5+	1.5	3
9	450	0	0	0+	0.5+	2	3.5
10	500	0	0	0+	0.5+	0.5	1.5
11	550	0	0	0.5	0.5+	0.5+	1.5+
12	600	0	0	0.5	1	1	2
13	650	0	0	0.5	1	0.5	2
14	700	0	0	0.5	1+	1+	2.5
15	750	0	0	0.5	1+	1+	2
16	800	0	0	0.5+	1+	2	2
17	850	0	0	0.5+	1+	1+	2.5
18	900	0	0	0.5+	2	0.5+	3+

6.6.3- PACKET DELIVERY RATIO (PDR)

Packet Delivery Ratio of DSR, DSDV and ZRP with and without Black hole attack with respect of time.

SR. No	Time/ Sec	DSR	DSR With attack	DSDV	DSDV with attack	ZRP	ZRP with attack
1	50	100	80+	90	80	90+	80
2	100	100	80+	85+	80	90+	80
3	150	100	80+	90+	80+	90+	80
4	200	95+	80+	95	80+	90+	80
5	250	95+	80+	90+	80+	90+	80+
6	300	95+	80+	90+	80+	90+	80+
7	350	100	100	80+	80+	90+	60+
8	400	95+	80+	80+	80+	85+	60+
9	450	100	100	80+	80+	85+	60+
10	500	95+	80+	80+	80+	85+	60+
11	550	95+	100	80	80	85+	60+
12	600	95+	80+	60+	60+	90	80+
13	650	95+	80+	80	60+	90+	80+
14	700	100	80+	60+	60+	90+	80+
15	750	100	80+	60+	60+	90+	60+
16	800	95+	80+	60+	60+	90+	60+
17	850	95+	80+	60+	60+	90+	60+
18	900	95+	80+	80	80	85+	60+

6.6.4-NETWORK LOAD

Network Load of DSR, DSDV and ZRP with and without Black hole attack with respect of Mobility.

SR. No	**mobility/ m/s**	**DSR**	**DSR With attack**	**DSDV**	**DSDV with attack**	**ZRP**	**ZRP with attack**
1	10	8000	7000	2000	1000+	3000	3000
2	20	8000+	7000+	1000+	1000+	3000+	3000+
3	30	8000	8000	1000+	1000+	4000	4000
4	40	8000+	8000	1000+	1000	3000+	3000+
5	50	8000+	8000	1000+	1000	4000	4000
6	60	8000+	7000	1000+	0+	4000	4000
7	70	8000+	7000+	1000	0+	4000+	3000+
8	80	8000+	8000	1000	0+	4000	3000+
9	90	8000+	8000	0+	0+	4000+	4000+
10	100	8000	7000+	0+	0+	4000+	3000+

6.6.5-NETWORK DELAY

Network delay of DSR, DSDV and ZRP with and without Black hole attack with respect of Mobility.

SR. No	mobility/ m/s	DSR	DSR With attack	DSDV	DSDV with attack	ZRP	ZRP with attack
1	10	0	0	0+	0.5+	0.5+	1+
2	20	0	0	0+	0.5+	0.5+	1+
3	30	0	0	0+	0.5+	2	1.5
4	40	0	0	0+	0.5+	2.5	2
5	50	0	0	0+	0.5+	1.5+	2+
6	60	0	0	0+	0+	0.5	3
7	70	0	0	0.5	1+	0.5+	2+
8	80	0	0	0.5+	1+	1.5	3
9	90	0	0	0.5+	1.5	2	3.5
10	100	0	0	0.5+	2	0.5	1.5

6.6.5- PACKET DELIVERY RATIO (PDR)

In Fig 31 and 32 we have simulated Packet delivery ratio (PDR) of DSR, DSDV and ZRP with and without Black hole attack with respect of Mobility. In Fig 31 we have simulated PDR with respect to the Mobility. We measure the behavior of three protocols with rest of 10 intervals of Mobility as well as with 50 intervals. We have changed the interval number because the simulation was showing a small deviation and there would be difficult to analyze it.

4.14- Conclusion and Future work

Communication access in VANETs has been a subject of great concern from last few decades. However, recently both researchers and industrialists have been motivated to show greatest interest in providing real-time high data rate communication and throughput to vehicles. The main goal of this work was to propose, analyze and evaluate the VANET security issues. This research work utilizes simulator NCTUns carried out for end to end delay, throughput and network load. We have analyzed and done the comparative analysis of Reactive protocol DSR, Proactive protocol DSDV and Hybrid routing protocol ZRP with attack and without attack using performance metrics of Network load, network delay and packet delivery ratio. The performance of DSDV is best in presence of black hole attack and without attack than DSR and ZRP with attack and without attack in almost every case. By using protocols we evaluate the affect of Black Hole attack and its results on the node. Comprehensive analysis has been made on the basis of results generated by the simulator. This work can be further extended by analyzing the different VANET protocols. In future we plan to extend my work on the black hole detection and prevention schemes using some kind of security and routing protocols and algorithm.

Bibliography

[1] ASLAM , B .(2009). *NETWORKING AND SECURITY SOLUTIONS FOR VANET INITIAL DEPLOYMENT STAGE.* Orlando, FL.: University of Central Florida Press.

[2] Arvin, R .(2011). *Performance Evaluation of VANETs using simulation tools*. Ahmedabad,IN.: Nirma University Press.

[3] Babar, S. Mahalle, P. Stango, A. Prasad, N. Prasad , R.(2014*). Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT).* Aaborg, DK.: Aalborg University Press.

[4] Boxill. L, Y. (2000). *An Evaluation of Traffic Simulation Models for Supporting ITS Development*. Rajasthan, IN.: Kota Press.

[5] Cunha ,FD. Boukerche, A. Villas ,L. Vianam ,AC. Loureiro , F. (2015). *Data Communication in VANETs: A Survey, Challenges and Applications*.Strasbourg,F.: Le Meilleur des Mondes Press.

[6] Dahiya, P. Deswal ,S .(2014). *Performance Analysis of Advanced FMIPv6.For Handover Management In VANET.* Haryana, IN. IJIRSET Press.

[7] Daniel, G. Xavier, L .(2011). *Performance evaluation of VANETs over high speed environments using NCTUNs*. New York, USA.: IET Press.

[8] Dhamgaye, A. (2012). *Infrastructure design for VANET security*. Seoul, Korea.: IJCSN Press

[9] Dhumal, D. Tehre , V .(2015).*Early Alert System in VANET.* Nagpur, IN.: IJERG Press.

[10] Deng.H, Li.W, Agrawal, D, P. (2012). *Routing security in wirelessAd-Hocnetworks*. Ohio, USA.: IEEE Communications Press.

[11] Etal,MX.(2012).*WisperNet: Anti-Jamming for Wireless Sensor Networks.* Pennsylvania. DE.: University of Pennsylvania Press.

[12] Falasi,Al. Ezendin , B .(2013). *Revocation in Vanet, A Survey.* New York, USA.: IET Press.

[13] Godavari, Kudlikar, H . Nagaraj ,U.(2015). *A Survey on Various Security Schemes in Vehicular Ad hoc Network.* Pune,IN.:Pune University Press.

[14] Goswamim,A.Geol, R. (2012). *Security and Privacy in Vanets.* Nagpur, IN.: IJEAT Press.

[15] Godavari , H. Kudlikar, Nagaraj ,U.(2015). *A Survey on Various Security Schemes in Vehicular Ad hoc Network.* Pune,IN.: IJIRCCE Press.

[16] Hasbullah, H . Verma, K. Ashok , K .(2013). *Affective defense method against UPD spoofed flooding traffic of Denial of Service attacks in VANET* . New York, USA.: IET Press.

[17] Hamieh,A. Othman ,JB.(2009).*Detection of Jamming Attacks in VANET using Error Distribution.* New York, USA.: IET Press.

[18] Horcas, JM. Pinto, M. Fuentes ,L .(2014).*An Aspect-Oriented Model transformation to weave security using CVL*. New York, USA.: IET Press.

[19] Isaac, JT. Zeadally,S. Camara ,JS. (2010) .*Security attacks and their solutions for VANET*. . New York, USA.: IET Press.

[20] Jagdale,B. Prof. Patil, P. Prof. Lahane, P. Prof. Javale, D .(2012). *Analysis and Comparison of Distance Vector,DSDV and AODV Protocol of MANET.* Pune, IN.: IJDPS Press.

[21] Jain, A. Sharma , D .(2016). *Approaches to Reduce the Impact of DOS and DDOS Attacks in VANET.* Rajasthan, IN.: Kota Press.

[22] Jérôme, H. Marco, F. (2014). *Vehicular Ad hoc Network mobility extension to the CanuMobiSim framework*. Torino, IT.:Torio state Press

[23] Kahina, A. Oumaya, B. Alexandre, C .(2011). *Routing Mechanisms Analysis in Vehicular City Environment* in *Vehicular Technology*. Ohio, USA.: IEEE Communications Press

[24] Khairnar, V D. Dr. Pradhan , SN .(2010) . *Mobility Models for Vehicular Ad-Hoc network Simulation.* Ahmedabad,IN.: Nirma University Press.

[25] Khairnar,VD. Khairnar, DR. Kotecha , K. (2013).*Performance of Vehicle-to-Vehicle Communication using IEEE 802.11p in Vehicular Ad-Hoc network Environment. Ahmadabad,IN*. IET Press.

[26] Malebary, S. Xu ,W. (2015) .*A Survey on Jamming in VANET*. Columbia,SC. University of South Carolina Press.

[27] Mary ,SR. Maheshwari ,M. Thamaraiselvan , M. (2014). *Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA).* Chennai, IN.: IJEAT Press.

[28] Malebary , S. Dr. Xu, W.(2015). *A Survey on Jamming in VANET.* South Carolina, USA.: Columbia Press.

[29] Megha , K. (2014).*Security Analysis in VANETs Survey*. Pune, India.: IJERT press.

[30] Mokhtar, B. Azab ,M .(2015).*Survey on Security Issues in Vehicular Ad Hoc Networks.* Alexandria , EG.: IEJ Press.

[31] Mrs. Megha ,K. (2012). *Security Analysis in VANETs: A Survey*. Pune,IN.: IJEAT Press.

[32] Mr. raj ,S. M Mr. Kirubakaran ,S. Dr. Valarmathy, S. Mr. Kumar. EP .(2013*). Performance of TCP Variants in VANET*.Tamil Nadu, IN.: IJAIEM Press.

[33] Nasir ,MK. Hossain ,AS. Hossain ,Md. Ali, Md. (2013). *Security Challenges And Implementation Mechanism For Vehicular Ad Hoc Network.* New York, USA.: IET Press.

[34] Pouyan,A. Alimohammadi , M.(2014). *Sybil Attack Detection in Vehicular Networks*. Semnan, IR.: HRPUB Press.

[35] Park,S. Aslam,B. Turgut,D. Zou ,C .(2012). *DEFENSE AGAINST SYBIL ATTACK IN VEHICULAR AD HOC NETWORK BASED ON ROADSIDE UNIT SUPPORT*. Orlando, FL.: University of Central Florida Press.

[36] Qian, V. (2015). In *Design Secure and Application Oriented*. Gaithersburg, US.: Gaithersburg press.

[37] Raw, R. Kumar, M. Singh , N.(2013). *SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET.* Delhi,IN.: IJNSA press.

[38] Raghuwanshi, V. Jain , S .(2015). *Denial of Service Attack in VANET*: A Survey.Bhopal,IN.: IJETT Press.

[39] Rasheed, A. Dr Qayyum, Ajmal,S .(2013). *SECURITY ARCHITECTURE PARAMETERS IN VANETS.* Islamabad, PK.: Muhammad Ali Jinnah University Press.

[40] Rahbari,M. Jabreil , A .(2011). *EFFICIENT DETECTION OF SYBIL ATTACK BASED ON CRYPTOGRAPHY IN VANET*. Shabestar, IR.: IZU Press.

[41] Samiksh. Kaur , A . Kaur ,H .(2016) .*Overview of types of attacks in VANET*.Mohali,IN.: ECL Press.

[42] Saini ,M. Mann,S .(2010). *Handoff Schemes for Vehicular Ad-Hoc networks: A Survey*. Jaipur,IN.: Banasthali University Press.

[43] Serageldin ,A. Alturkostani ,H. Krings,A .(2013). *On the Reliability of DSRC Safety Applications: A Case of Jamming*.Moscow,RU.: University of Idaho Press.

[44] Sedjelmaci ,H . Senouci , S M. Ali, M.(2014). *An Efficient and Lightweight Intrusion Detection Mechanism for Service-Oriented Vehicular Networks.* New York, USA.: IET Press.

[45] Sumara , IA. Ahmad,I . Hasbullah ,H . (2013) .Behavior of attacker and some new possible attacks in Vehicular Ad hoc Network (VANET) . New York, USA.: IET Press.

[46] Shie, Yuan. Wang. Chih, L. (2008). *NCTUns 5.0: A Network Simulator for IEEE 802.11(p) and 1609 Wireless Vehicular Network Researches*. South Carolina, USA.: Columbia Press.

[47] Tonguz ,O. Wisitpongphan, N. Bai, P. Mudalige,V. Sadekar.(2012). *Broadcasting in VANET*. Warren, USA.: Carnegie Mellon University Press.

[48] Tongu , O. Wisitpongphan , N. Bai ,F. Mudalig ,P . Sadekar ,V.(2008). *Broadcasting in VANET*. Warren,USA.: IEEE Press.

[49] Verma ,K. Hasbullah, H .Kumar, A .(2014) .*An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VANET.Ajmer,IN.:IJEAT Press.*

[50] Verma,K. Hasbullah ,H .(2014).IP-CHOCK (filter)-Predicated Detection Scheme for DoS attacks in VANET. New York,USA.: Gaithersburg press.

[51] Vimal ,B. Roshan,K. Singh , KB. (2012). *Performance Analysis of Black Hole Attack in Vanet*. Bihar, IN.: Modern education and modern press.

[52] Wei, L. Kai, Y. Meng, L. (2011). *Bus Assisted Connectionless Routing Protocol for Metropolitan VANET*. Orlando, FL.: University of Central Florida Press.

[53] Xavier, R. Diego, P .(2011). *Perfomance evaluation of Manhattan scenarios for VANET*. PFC, UPC, 2011. Ohio, USA.: IEEE Communications Press.

[54] Xu, W. Wood, T. Trappe, W. Zhang ,Y.(2004).*Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service.* New Jersey, USA.: The State University

Press.Y, Kim. I,Kim.(2013). *Security Issues in Vehicular Networks.* Macomb,USA.: IET Press.

[55] Zaidi, K. Rajarajan ,M.(2015) .*Vehicular Internet: Security & Privacy Challenges and Opportunities.* London,UK.: City University Press.

[56] Zeadally, S. Hunt,R. Chen,Y. Irwin,A. Hassan ,A.(2010). *Vehicular ad hoc networks (VANETS): status, results, and challenges*. Washington DC, USA.: University of the District of Columbia press.

[56] Zhou,T. Choudhury,R. Ning,P. Chakrabarty, K .(2011). *Sybil Attacks Detection in Vehicular Ad Hoc Networks.* Durham, USA.: IET Press.

[57] Kaur, H . Bala , M . Sahni , V.(2015). *Performance Evaluation Of Aodv, Olsr And Zrp Routing Protocols Under The Black Hole Attack In Manet.* Jalandhar, IN.: Ctiemt Press.