Survey of Different Attacks Against Routing Protocols in Ad Hoc Environment

Ashish Patil
Ramrao Adik Institute of Technology,
India

Nilesh Marathe
Ramrao Adik Institute of Technology,
India

Pooja Padiya
Ramrao Adik Institute of Technology,
India

ABSTRACT
The Wireless network is attracting users as well as researchers because of aspects like, ease of access, easy and quick to setup, and freedom from wires and cables. It is of two types, the Infrastructure-based wireless network, such as WLANs (Wireless Local Area Networks); And the Infrastructure-less wireless networks, such as Ad Hoc network. The Ad hoc network is a network which can be setup in-a-minute without any infrastructure. There are two types of ad hoc network namely, Mobile Ad-Hoc Network (MANET) and Vehicular Ad-Hoc Network (VANET). Routing in MANET is facing challenges like, Dynamic topology, low battery power. Whereas VANET has issues like, highly mobile nodes (high speed vehicles), Low communication range, periodic communication with road-side units, GPS communication for physical location of a vehicle, etc. This study focuses on routing in MANET and VANET, and found some issues and vulnerabilities in it. The attacker takes advantage of assumption of cooperativeness in Ad hoc network routing and launches an attack. As VANET inherits some of the properties of MANET, so both have some common attacks against routing. This study compares the routing protocols as well as the attacks on both MANET and VANET Scenarios.

Keywords
Ad hoc network, Attack, MANET, Routing, VANET.

1. INTRODUCTION
A fixed Infrastructure can be expensive, time consuming, or impractical. Therefore the Wireless network is evolved and growing fast. The Wireless network is a network set up by using Radio Signals frequency to communicate among computers and other network devices. There are various type of wireless networks such as Cellular network, Wi-Fi Network, Ad Hoc Network, etc. refer fig. 1.

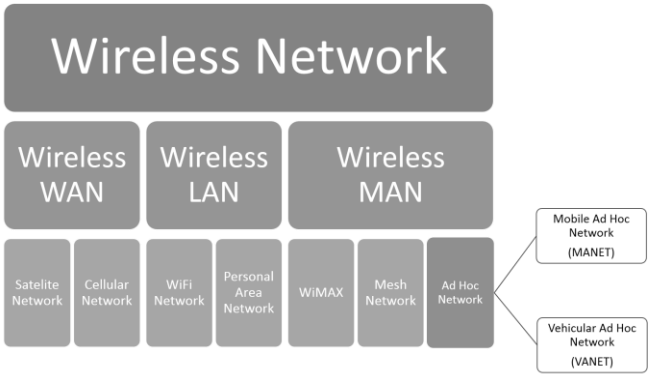

Fig 1 Wireless Network

The word 'Ad hoc' is Latin, which means "For this day or for this only". Due to increasing demand of wireless network and devices the wireless network has become interesting to today's researchers, especially the AdHoc Network. The Ad hoc network is a network having no infrastructure such as routers in wired network. The intermediate Node forwards packet to the destination. This study will be focusing on Ad Hoc Network and its type viz. Mobile Ad Hoc Network (MANET) and Vehicular Ad Hoc Network (VANET).

In Mobile Ad Hoc Network (MANET) nodes are mobile in nature, they operate co-operatively without any infrastructure. Node mobility results in dynamic topology.

The Vehicular Ad Hoc Network (VANET) is special kind of MANET. VANET facilitates wireless communication among the vehicles and vehicle to infrastructure. VANET utilizes GPS to discover path to target vehicle. VANET helps in scenarios like accidents, traffic jams by notifying driver about these situations and suggests alternate route. VANET helps to improve road traffic by limiting speed of the vehicle as per the traffic rules, maintaining lane, free passage for emergency vehicles (a police vehicle or ambulance).

2. LITERATURE REVIEW
MANET and VANET

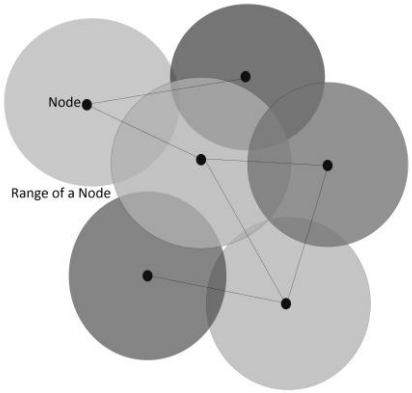

Fig 2 MANET Architecture

The MANET, refer fig. 2 [3], has mobile nodes, among which one is the source, one is the destination and some of others are intermediate nodes (also called as routers). The network is decentralized, therefore the routing decision has to be made at every node [3].

Whereas in VANET, as shown in fig. 3 nodes are vehicles and Road Side Units (RSUs). The RSU is connected to global network. The in-vehicle domain refers to a network logically composed of an OBU and one or more Applications Units (AU) inside a vehicle. An AU is a device that contains single or a set of applications.

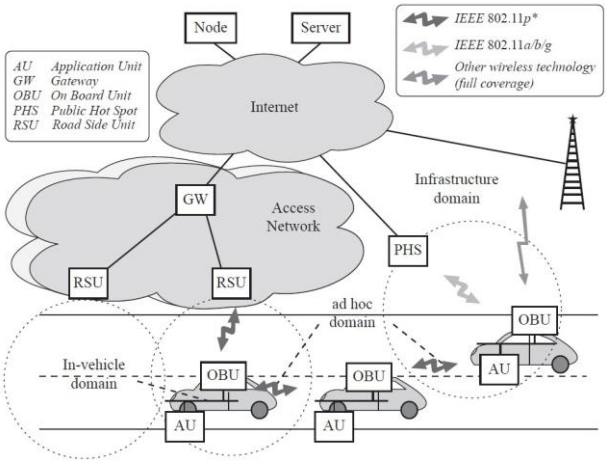

Fig 3 VANET Architecture

It utilizes the OBU for communication. An OBU has wireless communication capabilities. Vehicle uses OBU to communicate with the external world. The infrastructure domain consists of RSUs and gateways connected to internet. Vehicle may access internet through RSUs.

3. RELATED WORK

The network which is completely mobile which require little or no infrastructure is coined with the term MANET (Mobile ad hoc network). These MANETs have several properties like dynamic topologies, limited bandwidth, limited energy and many more.

Vehicular ad hoc network (VANET) is special form of MANET. VANET environment consists of various components like vehicles, road side units (RSUs), Gateways etc. VANET has its own routing protocols to suit its unique characteristics.

Kannhavong et al. reviewed each type of protocol in MANET. They discovered link spoofing attack and colluding misrelay attack with their solutions .There are attacks like Black hole, Worm hole, flooding, impersonation, modification and replay attack [5].

The MANET is still vulnerable to attack because, it assume that the node involved in routing operation are cooperative. There are various security threats to MANET, here Amara et al. has classified those as passive attacks and active attacks. Passive attacks are not intended to interrupt the routing process or any damage to the network. But they may capture some valuable information by monitoring the network silently. Whereas active attacks are mean to damage network traffic and nodes in it to break down the network. Amara et al. has listed 19 attacks against routing in MANET. Author has proposed countermeasures for listed attacks using IDS [6].

Samara et al. has analyzed attackers and attacks on VANET, attacks like DoS Attack, message suppression attack, Fabrication attack, alteration attack, Replay attack, etc. Attackers like, Selfish attacker and prankers. VANET has its own challenges like Mobility, volatility, Privacy, liability, etc. which makes it very popular in researchers. Samara et al. also discussed about current real time solutions proposed by recent researches, e.g. VPKI (Vehicular Public Key Infrastructure) [9].

Sherali et al. discussed the importance of VANET by identifying its application in various critical domains like, safety related applications (ambulance and police service). The detailed structure of VANET is describes how Vehicle-to-Vehicle and Vehicle-to-infrastructure communication happens, and what are the roles of various units in vehicles, domains. Every system is not fully protected and secured so VANET has its vulnerabilities which causes an attack, such as Message based attacks. Message based attacks like, Bogus information attack, cheating with sensor information, Black hole, Masquerading, Replay attack, DoS attack, Illusion attack, etc. and other attacks like Worm hole, GPS Spoofing attack, Sybil attack, etc. Sherali et al also listed some security solution to these attacks [8].

4. ROUTING IN AD HOC NETWORK

MANET Routing

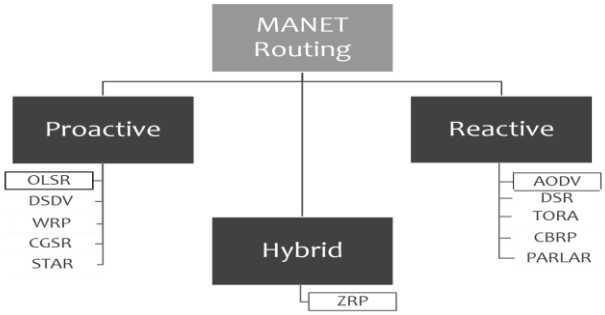

Fig 4 Routing in MANET

A. Proactive Routing Protocol

It uses tabular approach. It maintains topology information in tabular format called routing table. It helps to find shortest path between source and destination. This table is periodically broadcasted in order to maintain latest topology information.

Proactive routing protocol is beneficial when node mobility is less in MANET and it also helps to decrease time required to discover route and setting up the route. But proactive routing protocols are not suitable for large network, because more space is required for routing table to maintain whole network information. More bandwidth is needed to share such table with other nodes in network. Network with highly mobile nodes is also not suitable to proactive protocols because more bandwidth will be utilized to share frequent changes in a network. This needs a lot processing and memory.

1. Optimized Link State Routing (OLSR)

The OLSR is pure Link state routing protocol under proactive routing. It maintains routing table and broadcasts it periodically. Its uses concept of selective flooding by introducing Multi-point relays (MPRs) refer fig. 5. Each node stores information about its MPRs. And each MPR has information about MPR selector. There is a special criteria for selection of MPRs. A neighboring node with highest degree of links or having highest number of neighbors is selected as MPR. This improves connectivity and reachability between nodes. MPR is responsible for announcing topological information. Control packets are flooded/ forwarded via MPRs. This helps in reducing redundant flooding of packets in network [1].

B. Reactive routing protocol

The reactive routing protocols or on-demand routing protocol is designed to overcome problem in proactive.

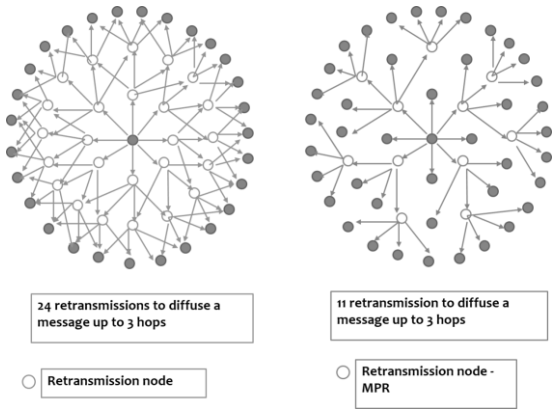

Fig 5 Flooding and Selective Flooding

Route is discovered on demand basis. Very first phase of reactive routing is route discovery process. As route is discovered at the time of communication, there is no need to maintain any tabular info. In route discovery process, route request is broadcasted with destination address. This route request is forwarded until destination is reached. Once destination receives route request it sends back route reply to source. After retrieving route reply source starts actual data transfer.

The reactive routing protocol has low routing overhead but needs more time to discover and setup route. It is not suitable for large networks with highly mobile nodes, because the routing information just gathered may become stale as it moves start actual data transmission. In reactive protocols path is stored in packet header, as number of router node increases packet size increases, this leads to inconvenience in routing.

1. Ad hoc On-demand Distance Vector (AODV)

This is reactive distance vector protocol. It uses control messages such as, route request (RREQ), route reply (RREP), route error (RRER). As shown in fig. 6, the source (S) broadcasts RREQ to discover route to destination (D) and RREP is kind of acknowledgement from destination (D) saying that it has received RREQ packet. It is necessary to reach RREP to source within predefined time for successful communication, otherwise route is rediscovered. If any link fails between source and destination then respective intermediate node will send back RRER to source, and on retrieval of RRER source removes route entry of that destination and resends RREQ through alternate route. It also utilizes sequence number in order to check the freshness of the packet [7].

C. Hybrid Routing Protocol

The hybrid protocol works as proactive for shorter distance and reactive for larger distance. E.g. Zone routing protocol (ZRP). It works proactive within the zone and reactive between the zones.

It helps in reducing disadvantages of proactive and reactive protocols. Hybrid protocol has low routing overhead for father away destination and low latency to discover routes within short range. The only disadvantage of hybrid protocol is that it is very complex.

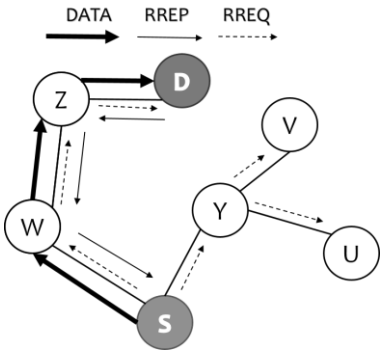

Fig 6 AODV Routing Protocol

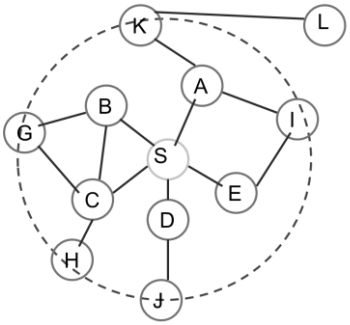

Fig 7 Zone Routing Protocol

1. Zone Routing Protocol (ZRP)

In ZRP, Each node has its own routing zone. Zones may overlap with each other. Fig. 7 shows zone for node S. Zone has perimeter nodes, here perimeter nodes are K, I, H, G, and J. Node S maintains routing information limited to zone (hence works as proactive within zone) and discovers route for the nodes in out of zone (same as reactive routing). Here each zone has radius (in hops), that defines zone area. K-Zone routing defines zone is up to K no. of hops. K is zone radius here. In our case zone radius is 2; that means every node which is 2 hops away from node S is in the S's zone. Here Zone radius plays a very critical role because if zone radius too large, route propagation becomes a problem. Too many frequent changes are shared within zone which leads to bandwidth wastage. And if zone radius is too small then reachability issue comes out for nodes in outer area which leads to high overhead [2]. ZRP uses neighbor discovery protocol (NDP) to detect new neighbor or loss of connectivity. NDP utilizes HELLO messages. It also uses border resolution protocol (BRP) in order to query perimeter nodes, this is called 'border-casting'.

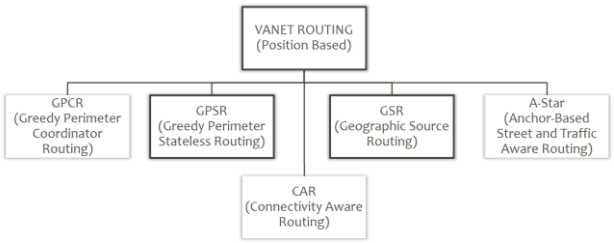

Fig 8 Routing in VANET

5. ROUTING IN VANET

A. Position Based Routing

Although VANET is special form of MANET, it has some unique characteristics therefore MANET protocol does not suit VANET environment. Vehicle in VANET communicate with

respect to traffic direction i.e. vehicles heading to same direction communicates with each other. In order to send some information vehicle discovers target location by using GPS technology. This is called Position based routing.

The position based routing maintains location table which stores information in the form of vehicle ID and geographic location. The position based routing is comprised of following:

i. Beaconing

ii. Location service

iii. Forwarding

Following are the routing protocols for VANET (also refer fig. 8).

1. Greedy perimeter stateless routing (GPSR)

GPSR uses nearest neighbor of destination in order to communicate. This is called Greedy perimeter forwarding. Every node is aware of its position and neighbors which helps to the destination efficiently. It uses greedy forwarding and perimeter forwarding.

In greedy forwarding node tries to send data packet to the nearest node of the destination, this helps to ensure packet delivery. But sometimes there no common node within the range of both source and destination, in this case greedy forwarding fails. Therefore perimeter forwarding helps to reach out to destination.

Perimeter forwarding uses right hand rule. Right hand rule helps to traverse through such void region by forwarding packets in clockwise direction. This packet is transmitted until the source node is reached through destination. This forms a perimeter of an arbitrary shape, therefore called as perimeter forwarding.

2. Geographic Source Routing

GSR protocol is designed to overcome disadvantage of GPSR which fails because of radio obstacles. GSR considers geographical map of road as topology. This improves routing efficiency in VANET. It uses Dijkstra's algorithm to discover shortest route. Junction points on the roads plays important role in routing. These junction points are called as 'Anchor points' (AP).

The APs are responsible for routing decisions at the junction. These Aps are included in path header. Greedy forwarding is used between APs. Source broadcasts query in order to get location of target vehicle, this may utilize more bandwidth. Whole path is inserted into header, which makes it is not suitable for long distance communication.

6. ATTACKS ON THE MANET AND VANET

MANET and VANET has some common attacks on both the networks. Most Common attacks are as follows:

1) Denial of Service (DoS) attack

2) Replay Attack

3) Black Hole Attack

4) Worm Hole Attack

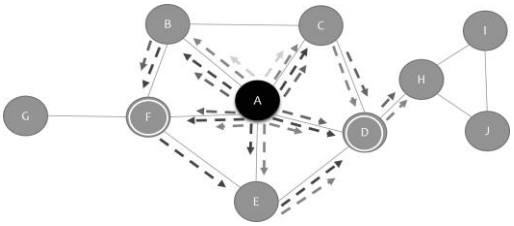

Fig 9 DoS attack against OLSR

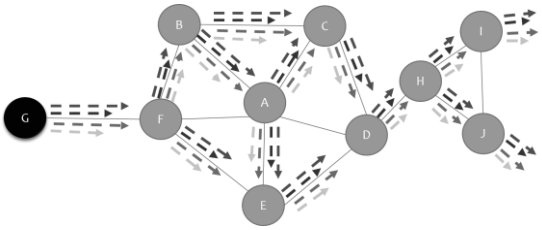

Fig 10 DoS attack against AODV

7. MANET Scenario

A. Denial of Service (DoS) attack

This attacks aims to slowdown the network and eventually causes network breakdown. In this attack network is flooded with the special messages so that it will multiplex the attack.

In case of AODV (see fig. 10), a malicious node can exploit nature of route request (RREQ) message. It will generate high amount of RREQ messages pointing to the destination which does not exists. Because no one will reply to the RREQs, these RREQs will flood the whole network. And this results in draining node's battery power and bandwidth wastage.

Same may happen with OLSR Protocol using HELLO messages as shown in fig. 9.

B. Replay Attack

As name suggests it replays previously captured valid control packets in order to disrupt the routing in MANET. In case of AODV, preciously captured RRER messages can be utilized to disturb the routing process with the forged sequence number. In case of OLSR, previously captures Hello messages can be utilized to make routing entries stale.

C. Black Hole Attack

In a Black hole attack, an attacker injects fake routing info so that other legitimate nodes will communicate through it [6]. As shown in fig. 12, the attacker sends fake RREP (with forged sequence number) in response to RREQ received from source node S. and obviously RREP sent by attacker Y will reach early than the valid one.

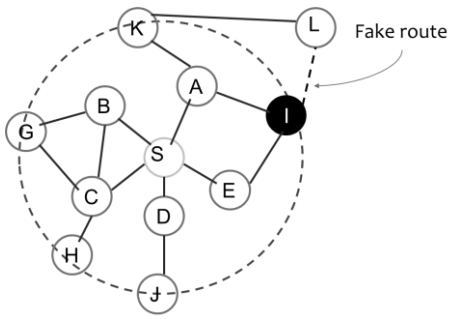

Fig 11 Black hole attack against ZRP

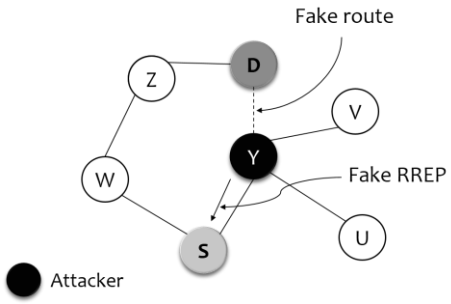

Fig 12 Black hole attack against AODV

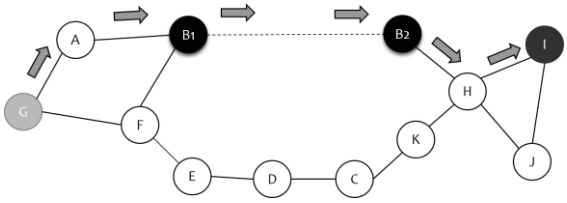

Fig 13 Worm hole attack against AODV

This is how it diverts all the network traffic and drops all the received packets. In case of OLSR protocol attacker advertises himself as he's having links to many other nodes so that legitimate node will select attacker as its MPR and causes traffic to flow only through it so it can drop every packet in the network. Same may happen with ZRP as shown in fig. 11.

D. Worm Hole Attack

A wormhole attack is one of the most dangerous attacks in MANETs. In this two or more attackers collude to launch an attack. They form a tunnel between them. This tunnel is nothing but the high speed network. So that they can advertise themselves as they are having shortest route to destination and divert all the traffic through them. After diverting all the network traffic through them, they may monitor and steal information that is going through it [6].

In fig. 13 node G sends RREQ to find node I, which captured by one of the two attackers. Then that RREQ packet is sent to second attacker B2, which will rebroadcast that packet near destination node I.

In response node I sends back a RREP through B2-B1. This forms communication path G-A-B1-B2-H-I. This is how attackers participates in every communication in the network.

VANET Scenario

The probability for attacks are very high. The major idea of the attacker is to generate harms for legal users, and as an outcome services are not easily reached and thus denial of services [4].

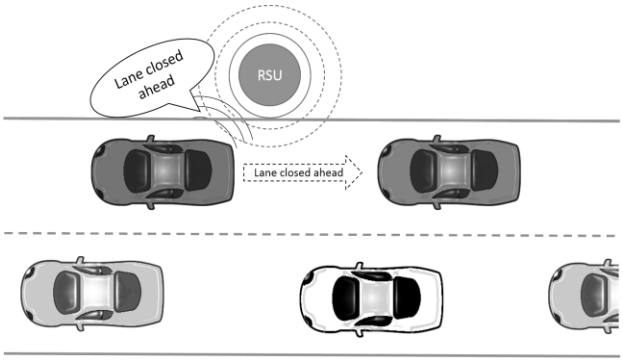

Fig 14 DoS attack against VANET

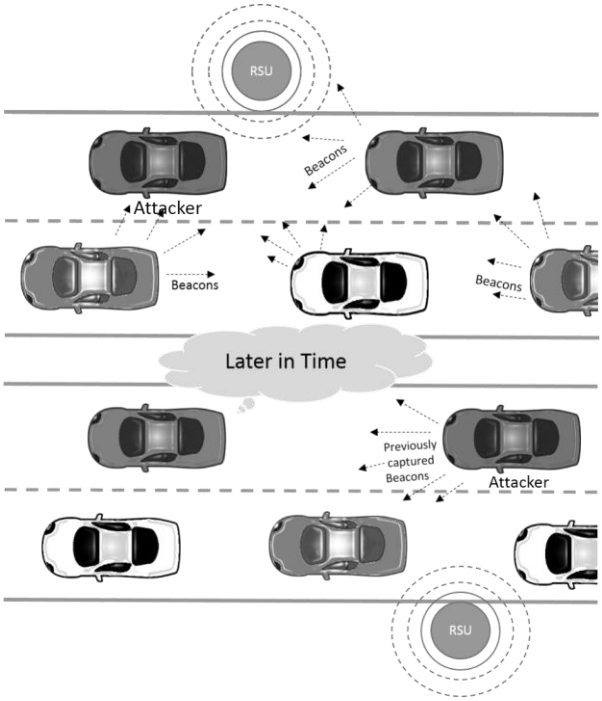

Fig 15 Replay attack against VANET

A. Denial of Service (DoS) attack

In this attack attacker utilizes control messages in order to cause traffic jams or accidents. Considering scenario in fig. 14 attacker sends out 'lane closed' message to the vehicle behind, so that it stops and sends the same message to the vehicles behind this causes traffic jam on that road. Or else attacker may jam network so that vehicle may not exchange any safety or control messages [8], [11].

B. Replay Attack

In VANET scenario, attacker replays previously captured beacons as shown in fig. 15. Beacons has information regarding vehicle ID and vehicle geographic location. Replaying these beacons results in false change in location table of other vehicle who is listening to these beacons. So the information in vehicles location table becomes stale [8].

C. Black Hole Attack

In this attack one or set of vehicles drops all the received packets. So important messages like 'accident ahead' will not reach to vehicles behind the attackers. All traffic will keep on moving to the place where accident happened and this situation may get worse, refer fig. 16.

D. Worm Hole Attack

In this attack, pair of attacker vehicle forms very high speed network. Packet captured form first vehicle is sent to another through tunnel, as shown in fig. 17. Attacker at the other end replays those control packets. Those replayed control packets are mean to disrupt the traffic. They may replay messages like accident ahead, or lane closed or beacons to poison the location table [11].

8. COMPARATIVE ANLYSIS

Table I describes comparative analysis of three types of protocols in MANET, Proactive (OLSR), Reactive (AODV), and Hybrid (ZRP). And Position based protocols in VANET. Every protocol is designed for special environment.

Table 1 Comparison of Routing protocols in ad hoc network

Protocols / Parameters	MANET			VANET	
	OLSR	AODV	ZRP	GPSR	GSR
Protocol type	Proactive	Reactive	Hybrid	Position based	Position based
Environment	Any	Any	Any	Urban/ Highway	Urban/City
Messages used	Hello, TC	RREQ, RREP	RREQ. RREP, RERR	Position Request	Position Request
Overhead	Path info, MPR info, MPR Selector info	Route discovery	Inter-Zone route discovery	Node Discovery, neighbor's info	Node discovery, Path overhead (as entire path included in Header), Local Maxima
Frequency of Updates	Periodic	On Demand	Periodic & On Demand	On Demand	On demand
Utilizes sequence no.	No	Yes	Yes	No	No
Utilizes HELLO msgs	Yes	No	Yes	No	No
Critical Nodes	MPR	-	Peripheral nodes	-	Anchor Point
Message utilized for an attack	Hello, TC	RREQ, RREP, RRER.	RREQ, RREP, RRER.	Position Req. msg	Position Req. msg
Attacks possible	DoS Attack, Black hole Attack, Worm Hole Attack, Replay Attack				

Table 2 Comparative analysis of attacks against ad hoc routing

Attacks \ Parameter	Attacker	Motivation	Type	Affected security aspect	Message utilized for attack	Protocol
DoS Attack	Insider / outsider	to bring down the network	Active	Availability	HELLO, Route Req., Traffic Control msg, Position Req.	AODV, OLSR, ZRP GPSR, GSR
Black Hole Attack	Insider	To drop packets	Active	Availability	Traffic Control msg, Route req./ response	
Worm Hole Attack	Insider / outsider	to make victim to choose attacker as one of the nodes in path to monitor / Listen traffic. path to monitor / Listen traffic.	Active / Passive	Availability		
Replay Attack	Insider / outsider	to confuse authorities and prevent identification of vehicle	Active	Integrity		

Every protocol has its own messages like AODV has RREQ and RREP. These protocols also has overheads, such as OLSR has tables to store information like Path, MPRs and MPR selectors; AODV has overhead of Route Discovery (reactive property); ZRP's overhead depends upon the zone radius, if it's too small then it has Inter-zone routing overhead, and if it's too large then it has Intra-zone routing overhead; GPSR has overhead of beacons and GSR has overhead of beacons and path, because entire path is stored or maintained in header. The frequency of updates should be as latest as possible to ensure delivery of data. To ensure the recentness of path some of protocols makes use of Sequence number. The critical nodes are those who plays important role in routing such as, MPR in OLSR Protocol and Peripheral nodes in ZRP.

Table II describes comparative analysis of attacks possible on each kind of protocol in MANET and VANET scenarios. Attacker are of two types Insider and outsider. Every attacker has motivation to attack, such as Black hole has motivation of dropping packets to block information broadcast. Active attack that interrupts traffic, and Passive attack that silently monitors traffic without interrupting it. Attacker smartly uses messages to attack, which defines signature of an attack. And every attack is responsible to harm one or more security aspects [9].

9. CONCLUSION

Initial part of this research is about analyzing each type of routing protocol for MANET and VANET and to find routing issues. By this study DoS attack, replay attack, black hole attack, and worm hole attack are the most common attacks against these ad hoc networks. Later part of research is to find the cause and impact of attacks over MANET and VANET. The comparative analysis provides a detailed review on routing protocols as well as on attacks against them. This will help researchers to find new solutions or improve proposed solutions in order to make ad hoc networks more secure and reliable. These solutions may focus on combined parameters of comparative study to tackle attacks.

10. REFERENCES

[1] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, Oct. 2003

[2] Gupta, Kriti, Maansi Gujral, Nidhi "Secure Detection Technique Against Black hole Attack For Zone routing Protocol in MANETS," *International Journal of Application or Innovation in Engineering & Management 2.6* (2013).

[3] Gupta Rachika, "Mobile adhoc network (MANETS): Proposed solution to security related issues," *Indian J.*

Computer Science and Engineering (IJCSE), vol. 2, no. 5, pp. 748-46, Nov 2011.

[4] Jhariya Mahendra Kumar, Piyush Kumar Shukla, Raju Barskhar. "Assessment of Different Attacks and Security Schemes in Vehicular Ad-hoc Network," *International Journal of Computer Applications*, vol. 98, no. 22, pp. 24-30, Jul. 2014.

[5] Kannhavong, Bounpadith, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, "A survey of routing attacks in mobile ad hoc networks," *Wireless communications, IEEE,* vol. 14, no. 5, pp. 85-91, Oct. 2007.

[6] Abdelaziz, Amara Korba, Mehdi Nafaa, and Ghanemi Salim. "Survey of routing attacks and countermeasures in mobile ad hoc networks," *2013 UKSim 15th International Conference on Computer Modelling and Simulation*, pp. 693-698, 2013.

[7] Perkins, Belding-Royer, Das. "Ad hoc on-demand distance vector (aodv) routing," RFC 3561, Jul. 2003.

[8] Jesus Tellez, and Sherali Zeadally, "Security in Vehicular ad hoc network", *Dynamic Ad Hoc Networks – IET telecommunication series 59*, ch. 3. 2013.

[9] Samara, Ghassan, Wafaa AH Al-Salihy, R. Sures. "Security Analysis of Vehicular Ad Hoc Nerworks (VANET)," *2010 Second International Conference on Network Applications Protocols and Services (NETAPPS)*, pp. 55-60, 2010.

[10] Surmukh Singh, Sunil Agrawal. "VANET routing protocols: Issues and challenges," *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, pp. 1-5, Mar. 2014.

[11] Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit. "An Analytical Study of Routing Attacks in Vehicular Ad-hoc Networks (VANETs)," *International Journal of Computer Science Engineering (IJCSE)*, vol. 3, no. 4, pp. 210-218, Jul. 2014.

[12] Sreenath, N., A. Amuthan, and P. Selvigirija. "Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs," *2012 International Conference on Computer Communication and Informatics (ICCCI)*, Jan 2012.