Volume 6, Issue 12, December 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Routing Protocols and Attacks in Vehicular ADHOC Network (VANETs): A Review

Er. Jayant Vats[*]
Research Scholar,
Shri Venkateshwara University,
Gajraula, Uttar Pradesh, India

Dr. Gaurav Tejpal
Professor,
Shri Venkateshwara University,
Gajraula, Uttar Pradesh, India

Dr. Sonal Sharma
Associate Professor
Dept. of Comp. Applications
Uttaranchal University, Dehradun, India

Abstract— ***Primary purpose of this paper is to develop a comprehensive understanding of VANETs; second to classify various types of existing protocols like topology based routing protocols, reactive adhoc based routing protocols, position based routing protocols, broadcast routing protocols, geocast routing protocols and cluster based routing protocols; third to discuss various types of attacks like gray hole attack, black hole attack, phony details attacks sybil attacks and DOS to classified routing protocols. This paper seeks to discuss briefly the challenges faced in imparting the various routing protocols. For this paper 50 papers has been studied from year 2007 to year 2016***

Keywords— ***Routing Protocols, Attacks in Vanets***

I. INTRODUCTION

Increasing vehicles on roads leads to much kind of problems arises such as traffic congestion, accidents on roads, air pollution which causes serious damage to humanity. To overcome all these kind of problems, the research introduces us with the new technology called VANET (vehicular ad-hoc network)[2]. Vehicular Adhoc Networks is considered as a special type of mobile adhoc networks (MANETs) [14]. VANETs shows us the complete information regarding roads that is how to travel on roads with safety, which speed should be followed ,which lane is more safe, also detects the problem occurs due to environment conditions such as flood , fading , raining due to which the signal drops in between and the complete information is not reached to the user[18,36]. VANET uses cars as mobile nodes. VANET turns every participating car into a wireless router or node allowing cars approximate 100 to 300 meters of each other. The first systems that will integrate this technology are police and fire brigade to connect with each other of safety purpose by introduction the technology of VANETS [15]. The vehicles tend to move in an organized fashion rather then moving at random the proposed scheme of VANET is based on the collaboration among users through their mobile devices that is smart phones by providing the update information about nearby traffic so that they can manage their lane to travel [24]. Creating the data about the traffic control with the help on GPS and NAVIGATION the driver gets the full information about the traffic ahead. The small units across the roads can avoid many accidents the unit such as Road Side Unit (RSU) which directly connected to the user to update the traffic information and secondly On Board Unit (OBU) which shows the information on the car board that the vehicle in the front and one side or at the back travels with how much speed and the distance maintained from your vehicle [41].It shows the complete information about all the vehicles that travel in the same lane or nearby lane VANET is based on wireless technologies such as mobile data or wifi connections. The major intend of VANETs is to absolute the users choice on the road and build their drive safe and comfortable [36].

II. ANNUAL DISTRIBUTION OF PAPERS

For the review of this paper we have studied the papers of the following years as mention in the table below:

Years	No. of the Papers
2007	01
2008	01
2009	01
2010	07
2011	07
2012	03
2013	06
2014	06
2015	08
2016	10

III. VANET ARCHITECTURE

VANET architecture[24] is defined as it is clearly shown in the below figure that the cars are moving in a secured and specified path each of vehicle is defined it paths through the Road Side Unit (RSU) [18,22] through the Security key is defined to each of individual car so that the user can define the correct path. For example, if all the vehicles are running smoothly on the road by well defined setup of path suddenly a car overtakes the other and the lane changes by default the car got hit to the other car and the crash of two vehicles occurred then the automatic message about this accident will reach the other user through internet and they can control their vehicle direction and speed so that the accident should be avoid and they can change their path easily to get secured lane. On Board Unit [41] can help to figure out the problem and it also gives the whole information on board screen of the vehicle which is next to you. The sensors are placed by the road side which gives u the complete data or information regarding the entrance of new user and the exit of any of the user.

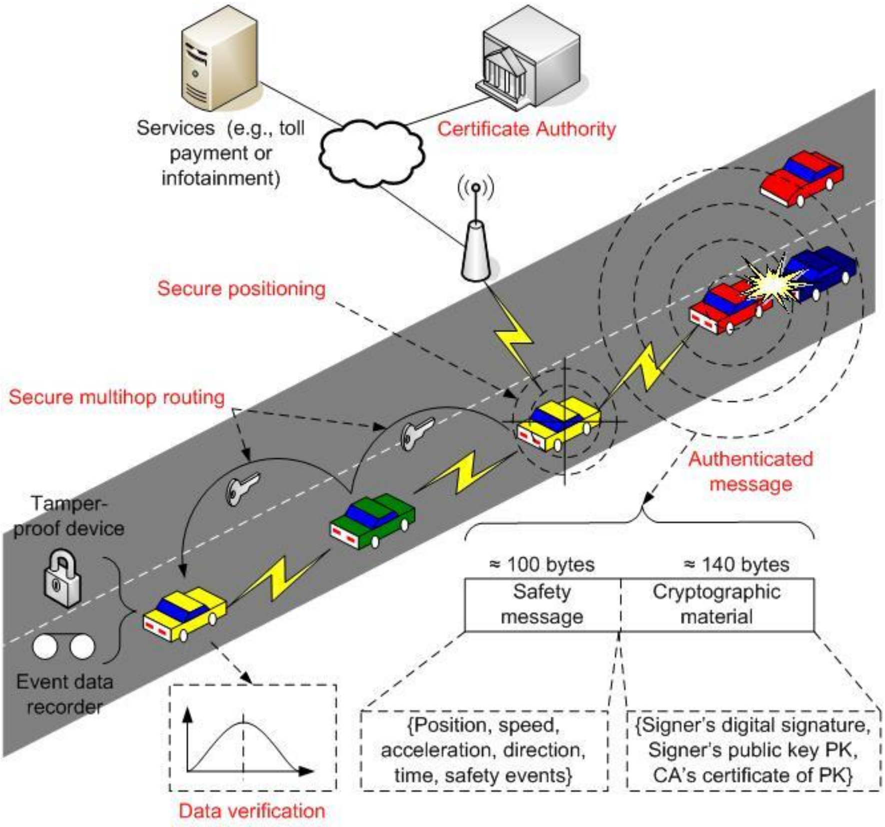

Fig 1: VANET Architecture [24]

IV. VANETs SECURITY REQUIREMENTS

Three properties regarding security that cannot be ignored are confidentiality, integrity, and availability [11, 22].

A. Confidentiality

In VANETs, the definition of confidentiality refers to "confidential communication" [29]. In a group, none except group members are able to decrypt the messages that are broadcasted to every member of group; and none (even other members) except a dedicated receiver member is capable to decrypt the message devoted to it.

B. Integrity

It ensures that data or messages delivered among nodes are not altered by attackers. This concept in VANETs often combines with the concept "authentication" to guarantee that: A node should be able to verify that a message is indeed sent and signed by another node without being modified by anyone. In order to gain this property, Data Verification is also required: Once the sender vehicle is authenticated, the receiving vehicle performs data verifications to check whether the message contains the correct or corrupted data.

C. Availability

The network should be available even if it is under an attack without affecting its performance. This concept of VANETs is not different from itself in other kinds of networks but not easy to ensure because of the mobility in high speed of vehicles.

D. Traceability And Revocability

Although a vehicles real identity should be hidden from other vehicles, there should be still a component (e.g., Trace Manager) that has the ability to obtain vehicles' real identities and to revoke them from future usage.

E. Non-Repudiation

Drivers must be reliably identified in case of accidents. A sender should have mandatory responsibility in transmitting the messages for the investigation that will determine the correct sequence and content of messages exchanged before the accident. Real-time constraints since vehicles are able to randomly move in and quickly move out to a group of a VANET for a short duration, real-time constraints should be maintained.

F. Low Overhead

All messages in VANETs are time critical. Thus, "low overhead" is essential to retain the usefulness and validity of messages.

V. BASIS ELEMENTS OF VANET

A. Road Side Unit (Rsu) [15]

It is the small kind of device which is fixed along the road side which helps to locate the nearby junctions and parking the RSU is a network which is dedicated shoot communication based on radio technology so that the other user can also get the same information and forward to other user.

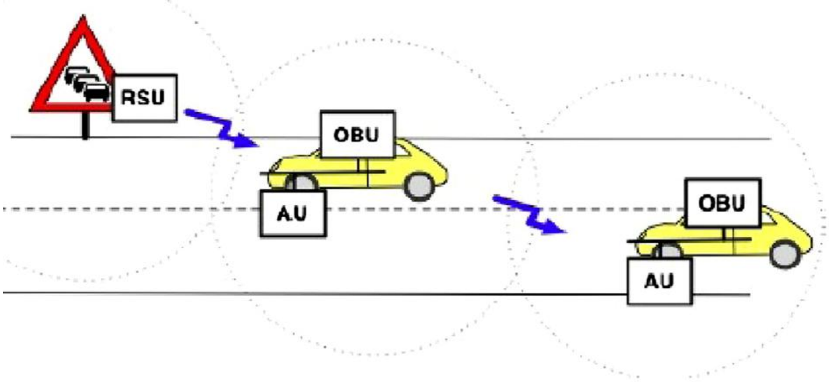

Fig2: RSU as information source [15]

B. On Board Unit (Obu)

It is a device placed on the board of the vehicle so that it can get the information through RSU to define the particular range of vehicle and lane. The main function of OBU is to define the area geographically routing network and congestion control network, transfer message and data security

C. Application Unit (Au)

The application unit detects the message which is forward by OBU .it is inbuilt function in the vehicle so that the provider or user can access the right information. This application also used to run the internet.

VI. VANET CHARACTERISTICS

A. Safe Driving

VANETs provides [19] the safe driving as it provide the complete information to the user about the traffic jams so the according to the provided information the user can adjust the path and drive safely and smoothly.

B. Improving Passenger Comfort

VANET technology also help to improve the user and traveler comfort as it provide the complete information on their mobile phones through mobile data and GPS setting so that the traveler can get the full information whether the driver runs the car in a proper manner or not.

C. Random Change In Network Topology

VANET also helps to define the random change in the network topology as if the vehicle is running on the highway where the number of vehicles is very high and congested. It helps by providing the data so that the user can adjust on that network

VII. CHALLENGES IN VANETs

A. Bandwidth Limitations

It is the main issue in the VANET [29] technology that the center coordinator is absent which can cause the problem in communication nodes the limited range of the bandwidth is (10- 20 mhz). The proper use of bandwidth helps us to get the message on time and reduces the time delay.

B. Signal Fading

This problem occurs due to signal loss or fading is also the problem as it occurs due to the uncertain change in the environment condition by raining or wind blow which breaks the signal and user is unable to get the information

C. Connectivity

Connectivity also effect the signal some time as if the user travels on the congested are or on highway where the signal changes at random on that way it is touch some time to get the signal for further information.

VIII. ROUTING PROTOCOLS IN VANETs

In VANET, the routing protocols are classified into five categories: Topology based routing protocol, Position based routing protocol, Cluster based routing protocol, Geocast routing protocol and Broadcast routing protocol. Vehicular multi-hop ad hoc networks (VANETs) enable the exchange of information between vehicles without any fixed infrastructure. The varying conditions in VANETs introduce high requirements on the routing protocols being used. Thus, we developed a reasonable free way mobility model and evaluated the performance of AODV, DSR, FSR and TORA in typical freeway traffic scenarios on the basis network simulations. The outcomes show that AODV performs best in all the simulated traffic situations, accompanied by FSR and DSR, while TORA is inapplicable for VANETs

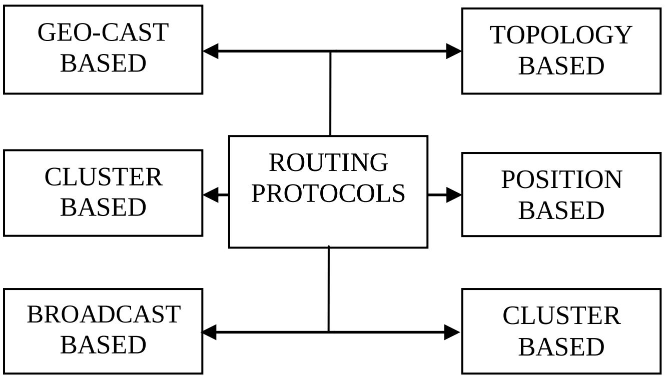

Fig 3: Routing Protocols in VANETs

A. Topology Based Routing Protocols

These routing protocols use links information that exists in the network to execute packet forwarding. They're further split into Proactive and Reactive.

1. *Proactive routing protocols*

The proactive routing implies that the routing information, like next forwarding hop is maintained in the background aside from communication requests. The advantage of proactive routing protocol is that there's no route discovery since the destination route is stored in the background; nevertheless the disadvantage of the protocol is that it provides low latency for real-time application. A table is constructed and maintained within a node. To ensure that, each entry in the table indicates the next hop node towards a particular destination. In addition it contributes to the maintenance of unused data paths that cause the decrease in the available bandwidth. The various kinds of proactive routing protocols are: LSR, FSR

- Fisheye State Routing: It is similar to link state routing protocol (LSR). Each node maintains a topology table on the basis of the latest information received from neighborhood nodes. It uses different exchange period for different entries in routing table to reduce how big is control messages in large networks. The disadvantage in FSR routing is how big is the routing tabling increases with upsurge in network size. Route discovery may fail if the destination node lies out of scope of source node. Because of high mobility in VANET, route to remote destination become less accurate.
- Optimized Link State Routing Protocol: It is an optimization of a natural link state protocol for mobile adhoc networks. Each node in the network selects some neighbor nodes called as multipoint relays (MPR) which retransmits its packets. The neighbor nodes that aren't in its MPR set can only read and process the packet. This procedure reduces the amount of retransmissions in a broadcast procedure.
- Destination Sequence Distance Vector Routing: DSDV protocol it can be an earliest ad hoc routing protocol, it implements the length vector strategy and uses a shortest path algorithm to implement. DSDV protocol guarantees the loop free routs, excludes extra traffic due to frequent updates. DSDV increases the overhead in the large network; due to unnecessary updating broadcast even when there is no change in the network topology.

2. *Reactive/Ad Hoc Based Routing [15]*

Reactive routing opens the route only when it's essential for an ode to keep in touch with each other. It maintains only the routes that are now in use; as a result it reduces the burden in the network. Reactive routing consists of route discovery phase in which the query packets are flooded in to the network for the trail search and this phase completes when route is found. T he various forms of reactive routing protocols are AODV, PGB, DSR and TORA

- Ad Hoc On Demand Distance Vector (AODV): AODV is a source initiated routing protocol and uses HELLO messages to spot its neighbors. Source node broadcasts a route request to its neighbors which fill forward to the destination. Then the destination unicast a route reply packet to the sender. Every node maintains broadcast-id which increments for new RREQ. Whenever a RREQ arrives at a node, it checks the broadcast id if it is less than or corresponding to previous message then it will discard the packet.

- Dynamic Source Routing (DSR): It uses source routing rather than based on intermediate node routing table. So routing overhead is always dependent on the path length. The limitation of the protocol is that the route maintenance process does not locally repair a broken link. The performance of the protocol briskly decreases with increasing mobility.
- TORA: TORA is a reactive, highly adaptive, efficient and scalable distributed routing algorithm based on the concept of link reversal. TORA is proposed for highly dynamic mobile, multi-hop wireless networks. The main feature of TORA is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. The protocol has three basic functions: Route creation, Route maintenance and Route erasing.

B. Position Based Routing Protocols

Position based routing consists of class of routing algorithm. They share the property of using geographic positioning information to be able to select the following forwarding hops. The packet is send without any map knowledge to the main one hop neighbor, which will be closest to destination. Position based routing is beneficial since no global route from source node to destination node need to be created and maintained. Position based routing is broadly divided in two types: Position based greedy V2V protocols, Delay Tolerant Protocols.

- Zone Routing Protocol: In ZRP, some type of assertive course-plotting practice (IARP) is probably included in intra-zone television broadcasting including a inner-zone reactive course-plotting practice. (IARP) is probably included in intra-zone communication. Foundation sends information right to a new retreat whenever either every bit as are often throughout equivalent course-plotting industry otherwise IERP reactively causes some type of direction discovery. ZRP is designed so that you can reveal snare free strategies to your destination. The idea makes use of border casting tactic to develop multicast plants in order to deluge a question packets instead of regular inundating so that you can find out retreat route.
- HARP: The idea isolates total technique into non-overlapping zones. The idea is designed to create a mild direction via a new hitting the ground with your destination for a new enhance delay. The idea applies direction breakthrough involving regions and specific areas in order to reduction inundating within technique, and judge greatest direction in line with the tranquility criteria. In HARP course-plotting is done on 2 steps: intra-zone and even inter-zone, dependant on the placement in touch with destination. The idea makes use of assertive and even reactive benchmarks around intrazone and even inter-zone course-plotting respectively.

C. Broadcast Routing Protocols

Broadcasting routing enables packets to flood into the network to all available nodes inside the broadcast domain. Broadcasting routing is widely in VANETs, it mainly used in the route discovery process, some protocols (like AODV) allow nodes to rebroadcast the received packets. This routing scheme allows packets to deliver via many nodes which may achieve a reliable packet transmission, however it could consume the network bandwidth by sending replicated packets, so each node need to identify which packet is replica (it has received it before) to discard.

- Density-Aware Reliable Broadcasting Protocol: DECA is a density aware protocol; it uses beacon messages to get knowledge about its neighboring nodes and to share information between nodes. It is a reliable broadcast protocol utilizes store and forward transmission scheme.
- Position-Aware Reliable Broadcasting Protocol POCA similar to DECA protocol, it select certain neighbor nodes to rebroadcast a packet, however in this protocol the selection of rebroadcast nodes is based on their position; other unselected nodes stores the packet and startup a waiting timer, if the time is over and no rebroadcast received, they rebroadcast the packet by themselves. POCA provided a good reliability in higher density
- Distributed Vehicular Broadcast Protocol (DV-Cast) In this protocol, each node monitors the status of its neighboring connectivity all the time, in order to broadcasts to them. DV-CAST deals with different classes according to many aspects; such as: traffic state, connected state of the neighboring nodes, light traffic, and normal traffic. It uses the periodic beacon messages to get information about the network topology.

D. Geo Cast Routing Protocols [18]

Geo cast routing is actually a spot based multicast routing. Its objective is to provide the packet from source node to all or any other nodes in just a specified geographical region (Zone of Relevance ZOR). Geo cast is considered as a multicast service in just a specific geographic region. It normally defines a forwarding zone where it directs the flooding of packets in order to reduce message overhead and network congestion due to simply flooding packets everywhere.

- Inter- Vehicular Geocast (IVG): The purpose of IVG is to inform vehicles located in a risk area called multicast group about any danger on the highway (e.g., when an accident occurs). To achieve this goal, risk area is determined considering the precise obstacle location on the road and the driving directions which can be affected. The damaged vehicle broadcasts a message alert to the multicast group. The neighbors receiving the message test its relevance according to their location by report to the risk area. All the neighbors belonging to the risk area calculate a differ time back off that promotes the furthest node to be a relay to rebroadcast the message. This relay selection technique makes the use of periodic beacons unnecessary.

- Abiding Geocast: Abiding Geocast that allows a periodical delivery of a Geocast message in Ad Hoc Networks. Three solutions are provided. First, the use of a server that stores Geocast message (Unicasted from the source).Then the server uses a Geocast protocol to deliver periodically the Geocast message to the destination zone. Second, a node is elected in the relevant destination area in order to store the Geocast message and retransmit it periodically or by notification. Third, the neighbor approach consists to allow all nodes to store the Geocast message. Handover is done on entry and message delivery by notification.
- Distributed Robust Geocast (DRV): Distributed Robust Geocast protocol the zone of relevance ZOR as all nodes satisfying a set of geographical criteria for which the Geocast message still pertinent, and zone of forwarding ZOF the set of nodes eligible to forward the Geocast message. DRG takes place in the manner that each vehicle when receiving a Geocast message tests its relevance according to its location; if the vehicle belongs to the ZOR then it read the message, else, if the vehicle is in the ZOF then it forwards the message, else, the message is dropped.

E. Cluster Based Routing Protocols

Cluster based routing is preferred in clusters. A group of nodes identifies themselves to be always a part of cluster and a node is designated as cluster head will broadcast the packet to cluster. Good scalability can be provided for large networks but network delays and overhead are incurred when forming clusters in highly mobile VANET. In cluster based routing virtual network infrastructure must be created through the clustering of nodes in order to supply scalability.

- Cluster Based Routing**:** In this routing every node determines best neighbor cluster header to be able to send information to another hop by making use of regional data. The cluster header forwards LEAD data to their neighbors with coordinate of its grid and the position of cluster header. In the street area the grid can behave as a cluster header. Any time when the header is departing the grid that transmit LEAVE data including their grid location. The beginner node saves till a latest cluster header will be chosen. The latest cluster header employs these details with regard to information redirecting.
- Cluster-Based Directional Routing Protocol: It separates the vehicles into clusters along with those vehicles that are planning to follow a same path to form a cluster. The sender transmits data to the cluster header and further it transmits the data to header that are incorporated with identical cluster together with the location. Finally the particular location header transmits data towards the location. This cluster header choice and preservation can be exact as CBR however they look at speed and path of a car
- Hierarchical Cluster Routing Protocol (HCB): It represents a hierarchical cluster routing protocol intended for large mobility adhoc networks. HCB is two-layer connection architecture. In HCB, intra-cluster routing is accomplished individually in every cluster. Cluster heads changing account details regularly to allow inter-clusters redirecting.

IX. SECURITY ISSUES IN VANETs

Security in VANET is a challenging problem for researchers in the era of cyber threats. The message passing from one vehicle to another vehicle may be hacked by an intruder who creates vulnerability in the systems performance. In this section, security challenges, security requirements, attackers on VANETs and various attacks in the VANET are studied**.**

A. Security Challenges In Vanets:

The challenges of security must be considered during the design of VANET architecture, security protocols, cryptographic algorithm etc. The following list presents some security challenges:

B. Real Time Constraint

Most of the applications in VANET require time critical messages, like collision avoidance, hazard warning and accident warning information etc. Hence strict deadlines for the delivery of messages must be met.

C. Data Consistency Liability

In VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency.

D. Location Awareness

The increased reliance of VANET on GPS or other specific location based instruments may affect its applications in case of occurrence of any error.

E. Low Tolerance For Error

Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause danger.

F. Key Distribution

In VANETs, security mechanisms implemented reliant on keys. Each message is encrypted and need to decrypt at receiver end either with same key or different key. Keys distribution among vehicles is a major challenge in designing a security protocols.

G. Incentives

Manufactures are interested to build applications that consumer likes most. Very few consumers will agree with a vehicle which automatically reports any traffic rule violation. Hence successful deployment of VANET will require incentives for vehicle manufacturers, consumers and the government is a challenge to implement security in VANET.

H. High Mobility And Volatility

Computational capability and energy supply in VANET is nearly same as the wired network node but the high mobility of VANET nodes requires the less execution time of security protocols for same throughput that wired network produces.

I. Tradeoff Between Authentication And Privacy

For the authentication of the messages that are to be transmitted, it is required to track the vehicles for their identification. This is not feasible as most consumers will not like others to know about their personal identification. Therefore this has to come in balance and a tradeoff must be maintained between the authentication and privacy of the nodes.

J. Network Scalability

The scale of the vehicular network in the world is exceeding continuously and as this number is growing, another problem is arising.

X. ATTACKERS ON VANETs

Attacker create problem in the network by getting full access of communication medium DSRC. Here we are discussing some properties and capability of the attackers which has been mentioned in studies [10, 36].

A. Insider

This type of attackers who is an authentic user of the network and have detail knowledge of network. Insider attacker might have access to insider knowledge and this knowledge will be used for understanding the design and configuration of network. When they have all information about the configuration then it's easy for them to launch attacks and create more problem as compare to outsider attacker. It can create problem in the network by changing the certificate keys. We can simply say that insider attacker is the right man doing the wrong job in the network.

B. Outsider

The outsider attacker is considered as an authentic user of the network. It is a kind of intruder which aims to misuse the protocols of the network and the range of such attacks are limited. Outsider attacker also has a limited diversity for launching different kind of attacks as compare to insider attacker.

C. Coverage Area

Coverage area is the main property of attacker when they launch any kind of attacks. Attacker could cover the main area of road, and it depends on the nature of the attacks. Basic level attacker has controlled one DSRC channels and covers the range of at most 1000 meters but the extended level attackers are more organized and cover more area using of hundred DSRC channels.

D. Technical Expertise

Technical expertise of the attacker makes them stronger for creating attacks in the network. It is difficult for attacker to mount attacks on cryptographic algorithms. Chance is low for attacker to compromise the infrastructure network and data capture from restricted area of network. Attacker having ability to extracts the program code and secret keys of the computing platform of OBU and RSU by launching physical attacks.

XI. ATTACKS PROCESS MECHANISM

In this process, we explain in detail the different attacks and communication between the authentic VANET user and attacker. The detailed steps are as follow:

STEPS
The Attacker

1. Launches first class attack to other vehicle in the network. Sybil attack is the example of this attack.
2. Also launches first class attack to infrastructure. DOS attack is an example of such attacks.
3. Receives safety message from other vehicle.
4. Receives safety message from infrastructure.
5. Alters the content of the message and passes this message to other vehicle.
6. Forwards wrong message to infrastructure.
7. Launches timing attacks to other vehicle.
8. Launches some social attack to nearby vehicle.

Monitors the communication between the vehicles or infrastructure and achieves his/her benefit

XII. ATTACKS IN VANETs

Security is an important issue for routing in VANETs, because many applications will effect life-or-death decisions and illicit tampering can have devastating consequences. Security is an important issue for routing in VANETs, because many applications will effect life-or-death decisions and illicit tampering can have devastating consequences. The characteristics of VANETs make the secure routing problem more challenging and novel than it is in other communication networks. Another challenge related to routing is efficient data dissemination and data sharing in VANETs.

In order to get better protection from attackers, it is essential to have the knowledge about the attacks in VANET against security requirements. These attacks are based on

(i) Identification and Authentication
(ii) Attack on privacy
(iii) Attack on availability
(iv) Routing attacks

A. Attack On Identification And Authentication

a. Impersonate

In this attack, attacker assumes the identity and privileges of an authorized node, either to make use of network resources that may not be available to it under normal circumstances or to disrupt the normal functioning of the network, usually this attack is performed by active attackers and attacker could be insider or outsiders. This attack can be performed by following two ways:

- False Attribute Possession: In this scheme an attacker steals some property of legitimate user and later with the use of attribute claims that it is who (legitimate user) that sent this message. By using this type attack a normal vehicle can claim that he/she is a police or fire protector to free the traffic.
- Sybil Attack [18, 37]: Sybil attack is the creation of multiple fake nodes broadcasting false information. In Sybil attack, a vehicle Install with On Board Unit (OBU) sends multiple copies of messages to other vehicle and each message contains a different fabricated identity. The problem arises when malicious vehicle is able to pretend as multiple vehicles and reinforce false data. There are several technique proposed to encounter Sybil attack in VANETs such as statistical and probability, signal strength and session keys. However, each of these schemes has advantageous and disadvantageous due to dynamic characteristics, weather conditions and system design. One of the interesting method proposed are based on statistical and probability algorithm integrated with signal strength as an input data. The different between received signal strength and estimate signal strength is claimed by positioner calculated. It is analyzed by AS using statistical and probability algorithm. A framework to detect Sybil attacks in nodes has been proposed using Certificate Authority (CA). Two main steps involve in the processes are system initialization and attacks detection where public key and private key are used during system initialization to sign in the message.

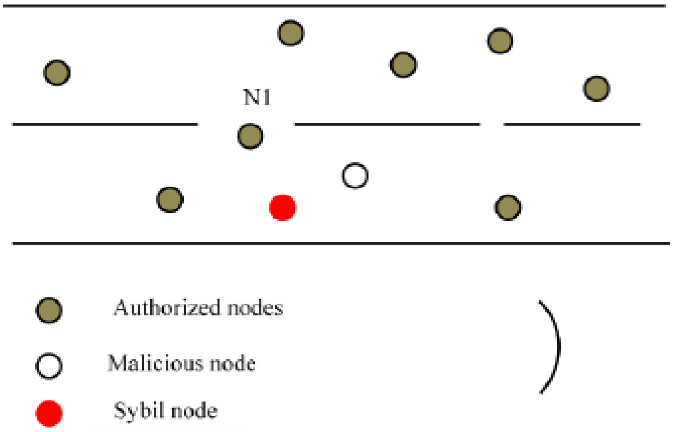

Fig 4: Sybil Attack [27]

B. Attack on Privacy

- Session Hijacking**:** Most authentication process is done at the start of the session. Hence it is easy to hijack the session after connection establishment. In this attack attackers take control of session between nodes.
- Identity Revealing: Generally a driver is itself owner of the vehicles hence getting owner's identity can put the privacy at risk.
- Location Tracking: The location of a given moment or the path followed along a period of time can be used to trace the vehicle and get information of driver.

C. Attack on Availability

- Network Denial of Service: Denial of Service (DOS) attacks aims to make the network unavailable to its legitimate vehicles. DOS attacks can be carried out in following ways [10].

- Jamming Attack: Jamming attacks can affect VANET availability, because a jammer can block warning messages e.g. accident warning, road hazard, emergency vehicle etc. The consequences of not receiving these messages can result in failing to slow down, rerouting or stopping the vehicle, which can jeopardize drivers' and passengers' safety. It is difficult to detect jamming reliably and the impact can be devastating.
- Distributed Dos Attack: DDOS attacks are number of attackers in the network. That attacks from different location with different timing slots. It is dangerous than the DOS attack because these is only one attacker which can be easily find But in DDOS attack there are number of attacker in the network

Case I: V2V communication: In this case, attacker sends message to victim from different locations and may be use different time slots for sending the messages. The attacker may change time slots and the messages for different nodes. The aim of attacks is to achieve network unavailability by bringing the network down at a target node. For example there are three attackers nodes (blue color car) send some messages to a target node in front (yellow color car). After some time the target node cannot communication with any other nodes in the network.

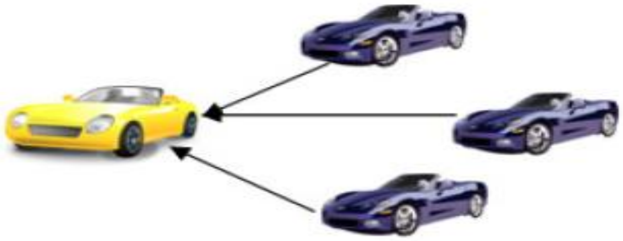

Fig 5: DDOS ATTACK V to V Communication [47]

Case II: V2I communication: In this case, the target of attack in the VANET infrastructure (RSU). There are three attackers in the network and lunch attack on the infrastructure from different location. When other nodes in the network want to access the network, the infrastructure is overloaded

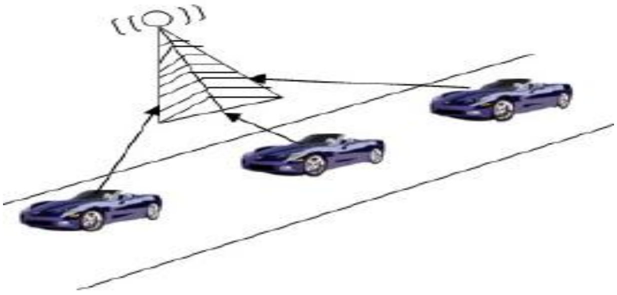

Fig 6: DDOS ATTACK V to I Communication [47]

XIII. ROUTING ATTACKS IN VANETS

In this type of attack, the attacker either drops the packet or disturbs the routing process of the network. Following are the most common routing attacks in the VANET.

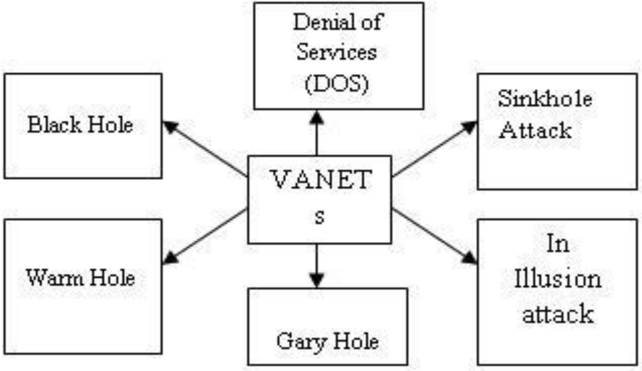

Fig 7: Routing Attacks in VANETs

A. Black Hole Attack [28]

A black hole is an area where the network traffic is redirected. However, either there is no node in that area or the nodes reside in that area refuse to participate in the network. In a black hole attack, a malicious node introduces itself for having the shortest path to the destination node and thus, cheats the routing protocol. Instead of taking a look on routing table firstly, this hostile node advertises rapidly that it has a fresh route for the route request. In consequence, attacker node wins the right of replying to the route request and thus it is able to intercept the data packet or retain it. When the forged route is successfully established, it depends on the malicious node whether to drop or forward the packets to wherever it wants figure illustrates an example where the node A wants to send data packets to node F but does not know the route to F. Therefore, A initiates the route discovery process. As a malicious node, D claims that it has active route to F and pretends that it must be next-node if A wants to send packets to F. Depending on the routing protocol (e.g., Ad hoc On-demand Distance Vector (AODV) or Optimized Link State Routing (OLSR)), an attacker builds its own method to fits.

B. Worm Hole Attack

In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two adversaries are called wormhole. It can be established through a single long-range wireless link or a wired link between the two adversaries. Hence it is simple for the adversary to make the tunneled packet arrive sooner than other packets transmitted over a normal multi-hop route.

C. Gray Hole Attack

This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively. It can be performed by three ways.

1. Malicious node may drop incoming packets while allow some packets to pass
2. Malicious node may behave as normal for some time and malicious for a certain time
3. Malicious node may drop incoming packets from some specified nodes for some time and later on it behaves as a normal node. These different types of behavior make attack difficult to detect.

Gray hole attack finally disrupts the network's performance by interfering with the route discovery process.

D. Denial Of Service (DOS) Attack

This type of attack can be done by the network insiders & outsiders. An insider attacker may jam the channel after transmitting dummy messages & thus, stops the network connection. An outsider attacker can launch a DOS attack by repeatedly disseminating forged messages with invalid signatures to consume the bandwidth or other resources of a targeted vehicle. The impact of this attack is that, VANET losses its ability to provide services to the legitimate vehicles. Figure shows the whole scenario when the attacker A launches DOS attack in vehicular network and Jams the whole communication medium between V2V and V2I. As a result, authentic users (B, C, and D) cannot communicate with each other as well as with infrastructure.

E. In Illusion Attack

In this attacker tries to purposely manipulate his/her sensor readings for giving falsifies information about his/her vehicle. As a result, the system reaction invokes and false traffic warning messages are broadcast to neighbors. The impact of this attack is that it can easily change the driver's behavior by spreading the wrong traffic information & can cause accidents; traffic jams and reduces the vehicular network efficiency by dropping the bandwidth consumption. Existing message authentication & message integrity approaches cannot secure networks against this attack as the malicious vehicle directly manipulates & misleads the sensors of its own vehicle to produce & broadcast the wrong traffic information

F. Sinkhole Attack

In Sinkhole attack, a malicious vehicle broadcasts the fake routing information so that it can easily attract all the network traffic towards it. The impact of this attack is that it makes the network complicated & degrades the network performance either by modifying the data packets or by dropping them. Figure illustrates a Sinkhole attack in which a malicious vehicle drops the data packets received from a legitimate vehicle & broadcasts fake routing information to the legitimate vehicles behind it.

Table 1 Comparison of Routing Attacks with their Effects & Security Requirements

Routing Attacks	Impact/Effect	Security Requirements
Denial of Service (DOS) Attack	Reduce the performance & efficiency of the network	Availability
Black Hole Attack	Reduce the performance & efficiency of the network	Availability
Wormhole Attack	Prevent the discovery of valid routes & cause data packets to be lost	Authentication & Confidentiality
Sinkhole Attack	Make the network complicated, either by modifying the data packets or by drooping them	Availability
Illusion Attack	Cause car accidents, traffic jams & reduce the performance of the network in terms of bandwidth utilization	Authentication
Sybil Attack	Take over the control of whole network & inject false information in it like traffic congestion, accident etc	Authentication

Table 2 Summary of Routing Protocols and Attacks in VANETs

S.No.	Paper	Objective	Routing Protocols in VANETS	Attacks in VANETs
1)	**Overview of Various Attacks in VANET** [36]	In this paper author gives the comprehensive study of various attacks in VANET and comparison of various attacks in VANET	N/A	Denial of Service Attack (DOS), Distributed Denial of Service Attack (DDOS Attack), Sybil Attack, Node Impersonation Attack.
2)	**Various Attacks in VANETs : A Review** [46]	In this paper author gives various attack in VANET and their effects on the Network	Topology Based routing protocols like: AODV protocol (Adhoc on demand distance vector routing) ,(Dynamic source routing) DSR, LAR protocol (Location aided protocol)	Black Hole Attack, Grey Hole Attack, Warm hole Attack, Sybil Attack
3)	**Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study** [44]	In this paper, various dimensions of VANETs including its emerging applications, security issues, challenges, security threats	N/A	Attack on Identification and Authentication, Attack on privacy, Attack on availability, Routing attacks, Attack on non-repudiation:
4)	**Security Analysis of Vehicular Ad Hoc Networks (VANET)** [8]	In This paper, a various types of security problems and challenges of VANET been analyzed and discussed	N/A	Different types of Attacks Like: DOS Attack, Message Suppression Attack, Fabrication Attack, Alteration Attack, sylib attack.
5)	**VANET Routing Protocols: Pros and Cons** [11]	This paper presents the pros and cons of VANET routing protocols for inter vehicle communication.	Topology Based Routing Protocols, Geographic Routing Protocols	N/A
6)	**A Survey on Routing Protocols and its Issues in VANET** [13]	This paper gives a brief overview of different routing algorithms in VANET along with major classifications. The protocols are also compared based on their essential characteristics and tabulated.	Topology based protocols, Position based protocols, Geocast based protocols, Cluster based protocols, Broadcast based protocols, Infrastructure based protocols	Comparison of Routing Protocols like: DSR, AODV, TORA, ZRP, OLSR
7)	**A Survey of Vehicular Ad hoc Networks Routing Protocols** [24]	This Paper represents the general outlines and goals of VANETs, investigates different routing schemes that have been developed for VANETs, as well as providing classifications of VANET routing protocols	Topology based protocols Like: DSDV,OLSR,AODV., Position based protocols Like: Delay Tolerant Network (DTN) Protocols, Geocast based protocols Like: Robust Vehicular Routing (Rover), Cluster based protocols Like: Cluster-Based Directional Routing Protocol (CBDRP), Broadcast based protocols, Infrastructure based protocols	N/A
8)	**Intelligent Intrusion**	This paper presents an intelligent Intrusion		New Intrusion detection system for the detection

	Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks [50]	Detection System (IDS) that relies on anomaly detection to protect the external communication system from grey hole and rushing attacks.	N/A	of grey hole attack
9)	**Vehicular Ad hoc Network (VANETs): A Review** [35]	This paper provides a survey of routing protocols for VANETs. It covers application areas, challenges and security issues prevailing in VANETs.	Features of different Routing Protocols Like: DTN, BEACON, OVERLAY, Reactive Protocol, Proactive	N/A
10)	**Various Types of Attacks in VANETs** [40]	VANETs can be disturbed by attackers for different reasons such as: fun, creating disorder in functionality of networks and etc, In this paper author introduce VANET and then concentrate on different attacks which are happening in this network.	N/A	Denial of Service attacks (DOS), Attacks against the authenticity of the messages, Attacks against privacy of messages, False attacks and false attack detection.
11)	**Classes of Attacks in VANET** [10]	In this paper, author proposed five different classes of attacks and every class is expected to provide better perspective for the VANET security. The main contribution of this paper is the proposed solution for classification and identification of different attacks in VANET.	N/A	Network Attack, Application Attack, Social attack, Monitoring attack, Timing Attack
12)	**Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)**[19]	This paper presents several existing security attacks and approaches to defend against them, and discusses possible future security attacks with critical analysis and future research possibilities	N/A	Denial of Service (DOS), Masquerade, Black Hole Attack, Malware and Spam, Timing Attack, Man in the Middle Attack (MiMA), Global Positioning System (GPS) Spoofing,
13)	**VANET Routing Protocols: Issues and Challenges** [33]	We have In this paper a tendency to survey a number of the recent analysis leads to routing space. In the different sections author present various existing routing protocols with their merits and demerits.	Position Based Routing Protocol, Topology Based Routing Protocol, Broadcast Based Routing Protocol, Cluster Based Routing Protocol, Geo Cast Based Routing Protocol	N/A

XIV. CONCLUSION

This paper shows the review on the VANET's and the issues faced by the VANET's in routing protocols, attacks, communication domains, architecture components and its characteristics. This paper also shows the great deal of study of VANET's technology and the challenges faced in imparting the various routing protocols and routing attacks.

REFERENCES

[1] Fan Li and Yu Wang, University of North Carolina at Charlotte, "*Routing in Vehicular Ad Hoc Networks: A Survey"* IEEE Vehicular Technology Magazine, 2007 pp 12-22

[2] SUN Xi , LI Xia-miao*," Study of the Feasibility of VANET and its Routing Protocols"*, IEEE, 2008,pp 1-4

[3] Juan Angel Ferreiro-Lage, Cristina Pereiro Gestoso, Oscar Rubiños, Fernando Aguado Agelet, *"Analysis of Unicast Routing Protocols for VANETs",* Fifth International Conference on Networking and Services, 2009, pp 518-521

[4] Yuyi Luo, Wei Zhang, Yangqing Hu, *"A New Cluster Based Routing Protocol for VANET",* IEEE Second International Conference on Networks Security, Wireless Communications and Trusted Computing 2010, pp 176-180

[5] Prabhakar Ranjan , Kamal Kant Ahirwar, *"Comparative Study of VANET and MANET Routing Protocols*", International Conference on Advanced Computing and Communication Technologies, 2010, pp 517-523

[6] Yun-Wei Lin, Yuh-Shyan Chen And Sing-Ling Lee, *"Routing Protocols in Vehicular Ad Hoc Networks: A Survey And Future Perspectives"* Journal of Information Science And Engineering, 2010 , pp 913-932

[7] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, *"Security Analysis of Vehicular Ad Hoc Networks"* ,Second International Conference on Network Applications, Protocols and Services 2010, pp 57-60

[8] J.T. Isaac, S. Zeadally J.S. Camara, *"Security attacks and solutions for vehicular ad hoc networks",* In Special Issue on Vehicular Ad Hoc and Sensor Networks, IET Commun., 2010, Vol. 4, Iss. 7, pp. 894–903

[9] Irshad Ahmed Sumra,Iftikhar Ahmad, Halabi Hasbullah, *"Classes of Attacks in VANET",* IEEE 2011

[10] Bijan Paul, Md. Ibrahim, Md. Abu Naser Bikas, "*VANET Routing Protocols: Pros and Cons*" , International Journal of Computer Applications, Volume 20– No.3, April 2011, pp 28-34

[11] Rakesh Kumar, Mayank Dave, *"A Comparative Study of Various Routing Protocols in VANET",* International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011, pp 643-648

[12] Jagadeesh Kakarla1, S Siva Sathya1, B Govinda Laxmi2, Ramesh Babu B, *"A Survey on Routing Protocols and its Issues in VANET"*, International Journal of Computer Applications, Volume 28– No.4, August 2011, pp 38-44

[13] Pooja Rani , Nitin Sharma, Pariniyojit Kumar Singh, *"Performance Comparison of VANET Routing Protocols"*, IEEE, 2011

[14] Farzad Sabahi, *"The Security of Vehicular Adhoc Networks",* Third International Conference on Computational Intelligence, Communication Systems and Networks", IEEE,2011, pp 337-342

[15] Shaikhul Islam Chowdhury, Won-Il Lee, Youn-Sang Choi, Guen-Young Kee, and Jae-Young Pyun, *"Performance Evaluation of Reactive Routing Protocols in VANET"*, 17th Asia-Pacific Conference on Communications (APCC) 2nd – 5th October 2011, pp 559-564

[16] Salim Allal, Saadi Boudjit, *"Geocast Routing Protocols for VANETs: Survey and Guidelines",* Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE, 2012, pp 323-328

[17] Ahmad Yusri Dak, Saadiah Yahya, and Murizah Kassim, *"A Literature Survey on Security Challenges in VANETs",* International Journal of Computer Theory and Engineering, Vol. 4, No. 6, December 2012, pp 1007-1010

[18] Mohammed Saeed Al-kahtani, *"Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)"*, IEEE, 2012

[19] Mostofa Kamal Nasir , A.K.M. Kamrul Islam, Mohammad Touhidur Rahman and Mohammad Khaled Sohel,*"Taxonomy of Security in Vehicular Ad hoc Networks",* International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013, pp 1-7

[20] Adil Mudasir Malla, Ravi Kant Sahu, *"Security Attacks with an Effective Solution for DOS Attacks in VANET",* International Journal of Computer Applications, Volume 66– No.22, March 2013, pp 45-49

[21] Swapnil G. Deshpande , *"Classification of Security attack in Vehicular Adhoc network: A survey"*, International journal of emerging trends and technology in computer science, Volume 2, Issue 2, March – April 2013, pp 371-377

[22] Senthil Ganesh N., Ranjani S., *"Security Threats on Vehicular Ad Hoc Networks (VANET): A Review Paper"*, National Conference on Recent Trends in Computer Science and Technology (NCRTCST)-2013, Volume 4, Issue (6) NCRTCST-2013, pp 196-200

[23] Marwa Altayeb , Imad Mahgoub*," A Survey of Vehicular Ad hoc Networks Routing Protocols"*, International Journal of Innovation and Applied Studies, Vol. 3 No. 3 July 2013, pp. 829-846

[24] Sabri M. Hanshi, Mohammad M. Kadhum, *"Geographic Routing Protocol Issues In Vehicular Ad Hoc Networks",* IEEE International Conference on RFID Technologies and Applications, 4 – 5 September, 2013, pp

[25] Sumit A. Khandelwal, Ashwini B Abhale, *"Topology base Routing Attacks in Vehicular Ad hoc Network – Survey*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013, pp 1352-1356

[26] TamilSelvan, Komathy Subramanian, Rajeswari Rajendiran, *"A Holistic Protocol for Secure Data Transmission in VANET"*, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, December 2013, pp 4840-4846

[27] Vinh Hoa LA, Ana CAVALLI, *"Security Attacks And Solutions In Vehicular Ad Hoc Networks: A Survey",* International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014, pp 1-20

[28] 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.04 Jul 2014, pp 210-218

[29] Megha Nema, Prof. Shalini Stalin, Prof. Vijay Lokhande, *"Analysis of Attacks and Challenges in VANET"*, International Journal of Emerging Technology and Advanced Engineering , Volume 4, Issue 7, July 2014, pp 831-835

[30] Vikash Porwal, Rajeev Patel, Dr. R.K.Kapoor, *"Review of Internal Security Attacks in Vehicular Adhoc Networks (VANETs)",* International Journal of Engineering Research & Technology, Vol. 3 Issue 8, August – 2014, pp 633-639

[31] M. Bharat, Dr. K. Santhi Sree, T .Mahesh Kumar, *"Authentication Solution for Security Attacks in VANETs",* International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 8, August 2014, pp 7661-7664

[32] Surmukh Singh, Sunil Agrawal *," VANET Routing Protocols: Issues and Challenges"*, RAECS UIET Panjab University Chandigarh, 06 – 08 March, 2014

[33] Sharaf Malebary, Dr. Wenyuan Xu, *"A Survey on Jamming in VANET",* International Journal of Scientific Research and Innovative Technology, Vol. 2 No. 1; January 2015, pp 142-156

[34] Divya Chadha, Reena, *"Vehicular Ad hoc Network (VANETs): A Review ",* International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 3, March 2015, pp 2339-2346

[35] Ujwal Parmar, Sharanjit Singh, *"Overview of Various Attacks in VANET",* International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015, pp 120-125

[36] Priyanka Soni , Abhilash Sharma, *"Sybil Node Detection and Prevention Approach on Physical Location in VANETS",* International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 7, July 2015, pp 1161-1164

[37] Arif Sari, Onder Onursal, Murat Akkaya, "*Review of the Security Issues in Vehicular Ad Hoc Networks (VANET)"*, Int. J. Communications, Network and System Sciences, 2015,Vol. 8, pp 552-566

[38] Swati Verma, Bhawna Mallick, Poonam Verma, *"Impact of Gray Hole Attack in VANET*", IEEE, 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015, pp 127-130

[39] Yasser Safinejhad, Mehran Abdali, *"Various Types of Attacks in VANETs",* International Journal of Computer & Information Technologies, Volume 3, Issue 04 November 2015, pp 808-813

[40] Khaled Rabieh, Mohamed M. E. A. Mahmoud, Terry N. Guo, and Mohamed Younis, *"Cross-Layer Scheme for Detecting Large-scale Colluding Sybil Attack in VANETs",* Communication and Information Systems Security Symposium, IEEE, 2015 pp 7298-7303

[41] M.Newlin Rajkumar, M.Nithya,P.HemaLatha, *"Overview of Vanet With Its Features And Security Attacks*", International Research Journal of Engineering and Technology, Volume: 03 Issue: 01 Jan 2016, pp 137-142

[42] Sandeep Kad, Kavneet Kaur, *"A Study of Reliable Routing Protocols for Vehicular Adhoc Networks"*, International Journal of Computer Applications, Volume 133 – No.3, January 2016, pp 37-42

[43] Dr. Nirbhay Kumar Chaubey, *"Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study",* International Journal of Security and Its Applications, Vol. 10, No. 5 , 2016 pp.261-274

[44] Preeti Rawat, Shikha Sharma," *Review on Sybil Attack in Vehicular Ad Hoc Network*", International Journal of Science, Engineering and Technology Research, Volume 5, Issue 4, April 2016, pp 1254-1257

[45] Pallvi Minhas, Pallavi Jindal, *"Various Attacks in Vanet: A Review",* International Journal of Advanced Computer Research and Networks, Volume 4, Issue 1, May, 2016

[46] Manpreet kaur , Nitin Bhagat, *"A Review on Various Attacks in VANET* ",International Journal of Computing and Technology, Volume 3, Issue 5, May 2016, pp 292-294

[47] Sandeep Kad, "*A Review on various security techniques in VANETs"*, www.researchgate.net/publication/303973059, 10 September 2016, pp 284-290

[48] Rashmi Mishra, Akhilesh Singh, Rakesh Kumar, *"VANET Security: Issues, Challenges and Solutions",* International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016

[49] Khattab M. Ali Alheeti , Anna Gruebler and Klaus McDonald-Maier, *"Intelligent Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks"*, Computers 2016, pp 1-18

[50] Rejab Hajlaoui, Hervé Guyennet, and Tarek Moulahi, *"A Survey on Heuristic-Based Routing Methods in Vehicular Ad-Hoc Network: Technical Challenges and Future Trends",* IEEE Sensors Journal, Vol. 16, No. 17, September 1, 2016, pp 6782-679.