An Efficient Way to Prevent DoS Attack in VANET

BarathKumar R[1] , Dr.SivaKumar[2]
M.Tech Student- Dept of CSE -SET- Jain University, Bengaluru, India[1].
Asst.Prof(GUIDE)-Dept of CSE -SET- Jain University, Bengaluru, India[2]

ABSTRACT

Vehicular Ad hoc Networks is a special kind of mobile ad hoc network to provide communication among nearby vehicles and between vehicles and nearby fixed equipments. VANETs are mainly used for improving efficiency and safety of (future) transportation. There are chances of a number of possible attacks in VANET due to open nature of wireless medium. In this paper, we have classified these security attacks and logically organized/represented in a more lucid manner based on the level of effect of a particular security attack on intelligent vehicular traffic. Also, an effective solution is proposed for DoS based attacks which use the Queue limiting mechanism consists of Droptailing as its components. This solution basically adds a level of security to its already existing solutions of using various alternative options like channel-switching, frequency-hopping, communication technology switching and multiple-radio transceivers to counter affect the DoS attacks. Proposed scheme enhances the security in VANETs without any cryptographic implementation.

Keywords:*VANET,Denial of Service,Q Filter,CBR,Droptail,NS-2*

1. Introduction

VANETs is particular, where vehicles and infrastructure at the roadside can keep in touch speak with each. It can self-structure, spread comfortably and cost low with open structures. VANET can pleasure an increasingly significant role in multiple regions: when an event an episode occurs, it sends the procedure message speed to other cars besides the procedure regions that actually help to prevent crashes again; cars catch vehicle velocity, density status of several roads, and they can they are able to take actions ahead of time which facilitates traffic congestion; also, cars can surf the internet via the fixed stations at the roadside.

This can prevent great wastes of time, money and of oil reserves, in addition, governments spend lots of money and destroy the landscape when creating more roads because existing roads do not support the generated traffic. VANETs have weaknesses to various kinds of DoS attacks [8], Blackhole, gray hole and wormhole portion of the region of the safety problems existent in this kind of networks. Nevertheless, an another approach is presented in this paper. The main purpose of this work is to define a proposed approach, a scalable free system for VANETs where users can cooperate via their mobile technology and obtain updated information of interest about the traffic and attacks area in order to choose the best-refreshed path to their goals.

In this paper, we proposed Secure approach (Q-Filter mechanism) is that attacks,for preventing DoS attacks used to commit time. This decreases the overhead for processing and securing the VANET is delayed. This

approach has better special depending Payload,CBR,Time interval and Droptail feature. Therefore, this work proposes a self-managed VANET without any infrastructure, which will serve as an introduction to a more complex VANET, all this with better levels of security. In this paper, we implement the proposed (Q-Filter mechanism) as the solution in NS-2 simulator to test its performance it. In the paper, related works are presented. Afterward, DoSAttack in Vehicular Ad-hoc Network (VANETS), Experimental setup,Final simulation andResults, Finally,Conclusion.

1.1 What is VANET?

A Vehicular Ad-Hoc Network or VANET is a technology that has moving vehicles as nodes in a network for forming a mobile network. VANET turns each and every vehicle into a wireless node, allowing cars to connect to each other which are 100–300 metres apart and, in turn, create a wide range of network. As cars fall out due to signal range and drop out of the present network, other cars can join in to connect vehicles to one another so a mobile Internet can be created. It is assumed to implement systems in which it will be integrated are police and fire vehicles, to communicate with one another to provide safety. It is a term which is used to describe the spontaneous ad hoc network that is formed over vehicles moving on the roads. Vehicular networks are very fast emerging for deploying and developing new and traditional applications. It is characterized by rapidly changing topology, high mobility, and ephemeral, one-time interactions[1]. Both MANETs and VANETs are characterized from the movement and self-organization of the nodes (i.e., in the case of VANETs it is Vehicles).

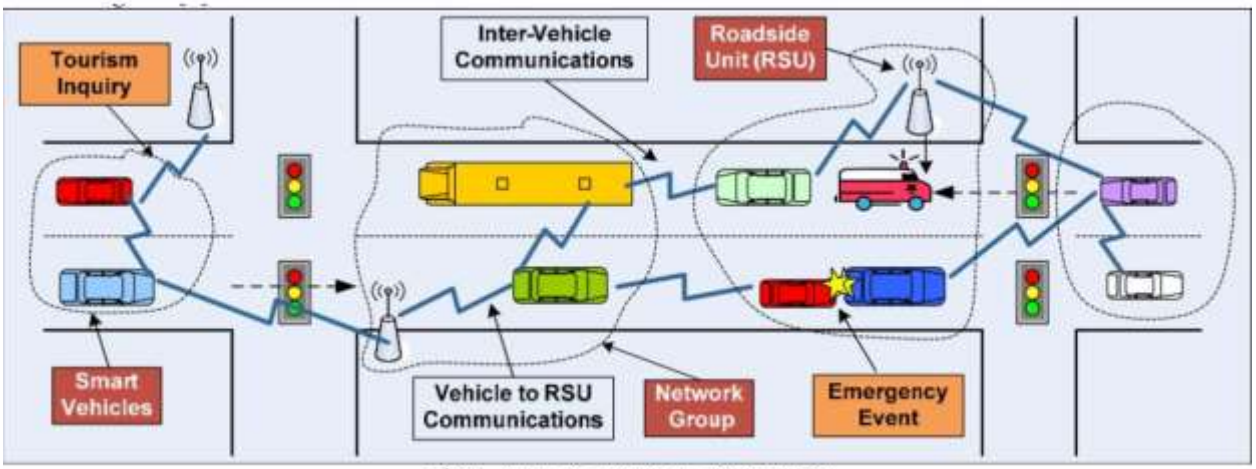

Fig 1. A basic structure of VANETs

1.2 Properties of vehicle for VANET

The moving vehicles are the prior in VANET. These vehicles are known as nodes in VANET. The following properties of vehicles are used for better operation in VANET. They are following.

a) *Sensing:* The different types of sensors are used for sense the Different vehicular and environmental conditions (state of the vehicle, state of road, weather condition, pollution and others).
b) *Processing:* the data or information coming from the different sensors are processed by the vehicles.
c) *Storage:* to store the different type of data and processing results for future uses require a large storage space.
d) *Routing:* The vehicles (nodes) should have the potential to communicate with each other in the VANET (IP or Cellular for example).

1.3 What is smart vehicle?

Vehicles which are equipped with multi-interface cards, sensors and on-board units are called Smart vehicles. The number of vehicles equipped with on-board wireless devices (OBD) and sensors [1] are increasing for efficient transport and management applications are focused on optimizing flows of vehicles by reducing the time taken to travel and avoiding any traffic congestions. As an instance, the sensor presents on on-board could be used to sense traffic congestions and automatically slow the vehicle. In another accident warning system, sensors can be used to determine that a crash can be occurred, so air bags are deployed; this kind of information is then relayed via V2I or V2V within the vehicular network.

It provides different levels of functionality by using number of systems and sensors. The major systems and sensors exploited for intra-vehicle communications we cite: crash sensors, the data recorder, the braking system, the engine control unit, the electronic stability control, the infotainment system, the integrated starter generator, the electronic steering, the tire pressure monitoring system, the power distribution and connectivity, the lighting system, seat belt sensors, etc. For the brake systems, there are also the antilock brake system and the parking brake system. The parking brake is also referred to as an emergency brake; it controls the rear brakes using a series of steel cables. It allows the vehicle to be stopped in the event of a total brake failure[6]. Vehicle-mounted cameras are mainly used to display images on the vehicle console in a smart vehicle.

1.4 Technologies and devices

Commonly, a smart vehicle is equipped with the following technologies and devices:

(i) A wireless transceiver for data transmissions among vehicles (V2V) and from vehicles to RSUs (V2I);
(ii) A Central Processing Unit (CPU) which implements the applications and communication protocols;
(iii) A Global Positioning Service (GPS) receiver for navigation and positioning services;
(iv) An input/output interface for the interaction of human with the system;
(v) Different sensors lying outside and inside the vehicle are used to measure various types of parameters (i.e., acceleration, speed, distance between the neighbouring vehicles, etc. [7]

The basic idea behind smart vehicles is to address safety issues of vehicles, and then with a proper combination of functionalities like communications, control and computing technologies, it will become possible to assist the driver decisions, and will also help to prevent driver's wrong behaviour's.The control functionality is directly added into smart vehicles for connecting it with the vehicle's electronic equipment.

2.VANET Architecture

Communication between vehicles and RSUs is done via wireless technology called as wireless access in vehicular environment (WAVE). The WAVE architecture describes the exchange of security messages, and the WAVE communication ensures the safety of passengers by updating vehicle information and traffic flow. This application ensures the pedestrian and driver safety and also improves the traffic flow and efficiency of the traffic management system. The VANETs comprise several units such as OBUs, RSUs, and TA,Application Unit(AU). Specifically, the RSU typically hosts an application that is used to

communicate with other network devices, and the OBU is mounted on each vehicle to collect the vehicle useful information such as speed, acceleration, and fuel. Then, these data are forwarded to the nearby vehicles through wireless network. All RSUs interconnected with each other are also connected to TA via wired network. Additionally, TA is the head among all components, which is responsible for maintaining the VANETs.

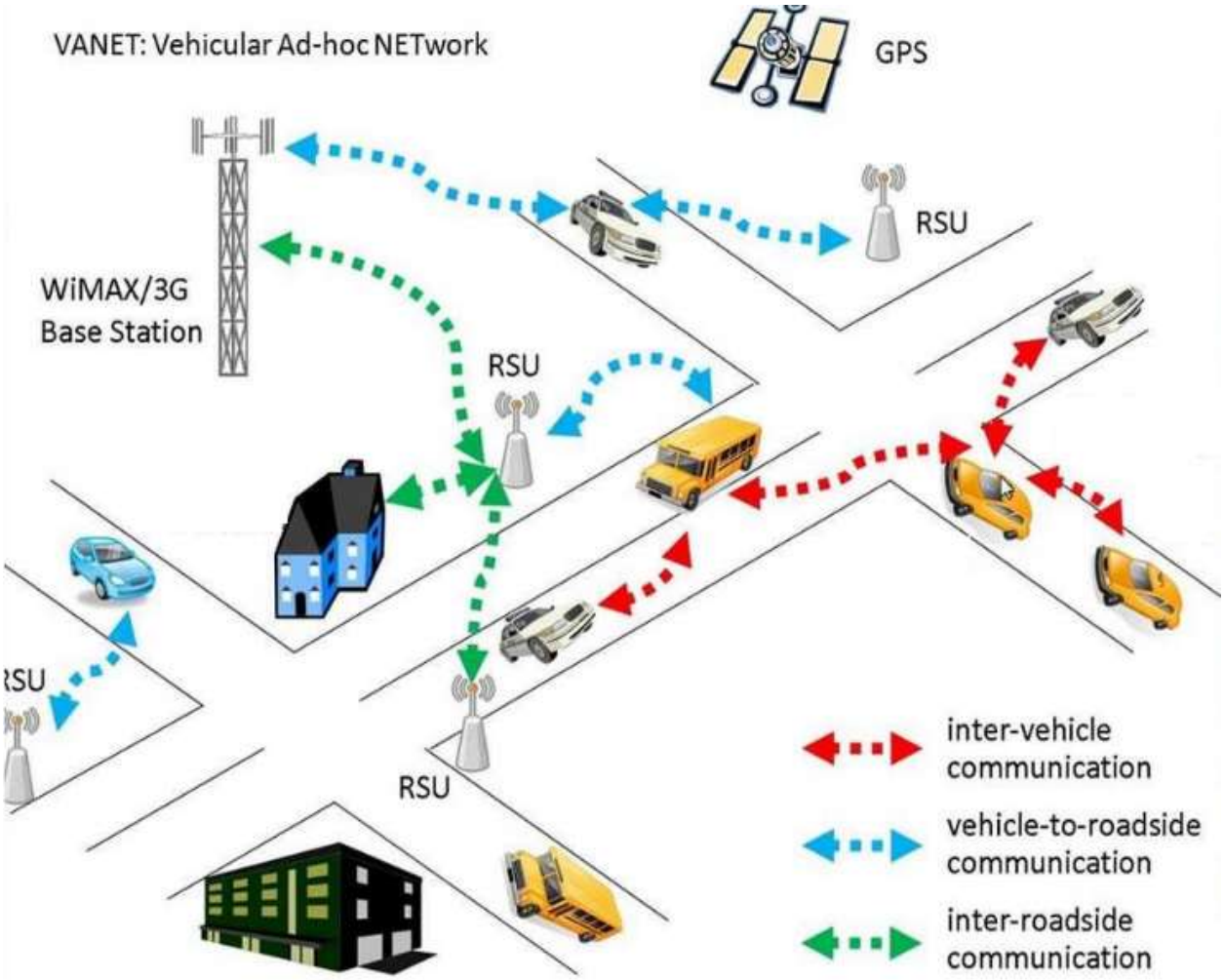

Fig. 2:VANET Architecture.

2.1 Roadside Unit (RSU)

The Roadside Unit is a computing device which is fixed alongside of the road or in specified location such as parking area or at the intersection; it is used to provide local connectivity to the passing vehicles. The RSU consists of network devices for dedicated short-range communication (DSRC) based on IEEE 802.11p radio technology. Specifically, RSUs can also be used to communicate with other network devices within the other infrastructure networks.

2.2 Onboard Unit (OBU)

OBU is a GPS-based tracking device which is usually equipped in every vehicle to share vehicle information to RSUs and other OBUs. OBU consists of many electronic components such as resource command processor (RCP)[2], sensor devices, user interface, and read/write storage for retrieving storage information. The main function of OBU is to connect with RSU or other OBUs through wireless link of IEEE 802.11p and is responsible for communication with other OBUs or RSUs in the form of messages.

Moreover, OBU takes input power from the car battery, and each vehicle consists of sensor type global positioning system (GPS), event data recorder (EDR), and forward and backward sensors which are used to provide input to OBU.

2.3 Trusted Authority (TA)

Trusted Authority is responsible for managing the entire VANET system such as registering the RSUs, OBUs, and the vehicle users. Moreover, it has the responsibility to ensure the security management of VANETs by verifying the vehicle authentication, user ID, and OBU ID in order to avoid harm to any vehicle. The TA utilizes high amount of power with large memory size and also can reveal OBU ID and details in case of any malicious message or suspicious beha2vior [30]. In addition to these, TA has the mechanism to identify the attackers as well.

2.4 Application Units

Application Units (AU) is a device equipped in the vehicle. The connection between AU and OBU may be wired or wireless, in some cases, AU and OBU may couple in a single chip. AU handles the services provided by the provider mostly deals in the safety application and personal digital assistance (PDA).

2.5 Communication in VANET

Communication in VANET is closely categorized into 4 classes.

a) In-Vehicle Communication is more important with respect to driver concern because it provides the information related to vehicle health, performance and driver's fatigue and drowsiness that is essential for driver and public safety.
b) Vehicle-to-Vehicle (V2V) communication provides communication between vehicles, where vehicles can directly communicate with other vehicles, which involves sending and receiving of messages.
c) Vehicle-to-Infrastructure (V2I) communication depicts communication between vehicles and infrastructure such as traffic light or Road Side Units (RSU). RSUs are like routers that are fixed on the roadside and have some horizontal height when it receives some information form any vehicle it transmits that information to the specified destination. RSUs are placed at some fixed distance, this finite distance between RSUs depends on the communication limit of the RSUs devices. For the effective communication, VANET prefers to use the IEEE 802.11 standard.
d) Vehicle to broadband (V2B) communication defines that vehicle might communicate via some wireless broadband communication channel like HSPA(3G) or Long Term Evolution(4G) because those broadband clouds embrace additional traffic information and monitoring data which is helpful in vehicle tracking and active driver assistance[3].

2.6 VANETrouting protocols

High dynamic topology characteristics turn out the efficient VANET routing protocols design to be more hard. The VANET routing protocol can be classified into two categories such as Topology based routing protocols and Position based routing protocols, the most popular sub categories under them is Dynamic Source Routing (DSR), UMB, OLSR, TORA, and Ad Hoc On Demand Distance Vector (AODV) [3]

2.6.1 Topology based routing protocols

Topology based routing protocols use links information to transmit the packets of data between nodes through the VANET. There are two sub categories under this mechanism, the proactive approach which depends on routing techniques related to table driven methodology and the reactive approach which depends on routing techniques related to on demand methodology.

(i) **Proactive routing** protocols are commonly depending on algorithms related to shortest route. They save all the data related to the connected nodes in predefined tables which are the main mechanism in these routing protocols. Also, there data are engaged with the partner nodes. Each routing table is updated by its node when the network topology is changed by any event.

Advantages:

- Real time applications low latency.
- It is not required to have a path discovery.

Disadvantages:

- A huge part of the available bandwidth occupied by unused routes.

(ii) **Reactive routing** protocols are commonly depending on algorithms related to on demand actions. When two nodes want to communicate, they initiate the path discovery and one of its main benefits is the network traffic reduction.

Advantages:

- Flooding is required when it is requested, so it doesn't require proactive overflow in the network.
- It controls the bandwidth as it is Beaconless.

Disadvantages:

- Nodes communication disturbance occurred because of the network exaggerated flooding.
- High latency in path searching.

Geographic based routing protocols are depending on algorithms related to the positioning mechanism using location based applications (For example GPS). Such applications are providing such data for path selection. Also, these protocols are not servicing any tables related to routing data or any information related to the join status with the nearby nodes.

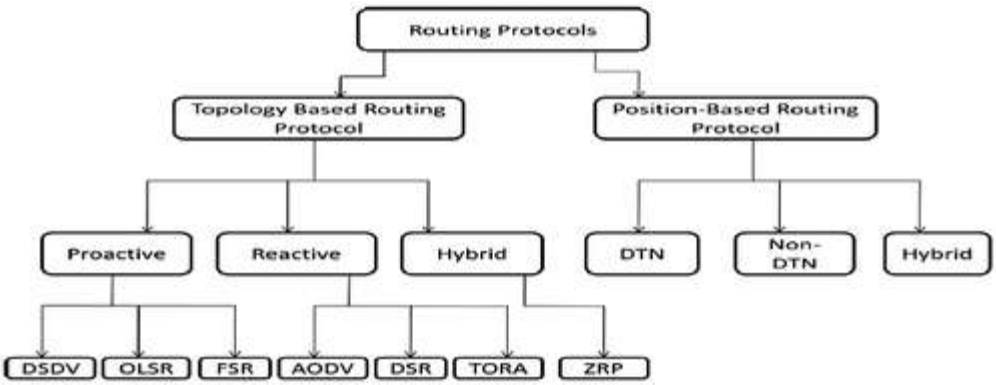

Fig. 3. VANET routing protocols.

2.6.2 AODV

Ad Hoc On Demand Distance Vector routing protocol is depending on a mechanism related to on-demand approach which initiates a path when a VANET node transmits packets of data to another node. The Destination Sequence Number is used by this protocol which is a unique feature not available in similar sub category routing protocols. It can be used in singular and multimode routing.

Like all reactive protocols, the philosophy in AODV, the information is only transmitted between nodes in an on-demand mode. When a node wants to transmit traffic to the host node without a predefined route, it will create a (RREQ) route request message to be flooded to the other nodes in a limited way[5].

AODV uses the below types of control messages for route servicing:

(1) RREQ—When a node is seeking a path to a node, then it transmits the route request message.
(2) RREP—A route reply message is transmitted in a single mode back to the source of a RREQ if the receiver is the node using the required address or it has a functional path to the required address
(3) RERR—In functional paths nodes observes upcoming hops link's status. For reporting technique activation, a "precursor list" is retained by each node, which including its neighbors IP address probably to exercise it as a next hop among each destination node. When the broken link in an active route is detected, other nodes are warned by this message type for the link loss.

Advantages:

- AODV can be used in large VANET networks.
- Any failure in the VANET links is handled in a prompt way by the AODV.
- The route redundancy and excessive memory requirements are minimized.
- Distance Sequence Number is providing recent route to the destination node.

Disadvantages:

- It expends extra bandwidth, because of proactive beaconing _ High control overhead is occurring when many route reply packets for a single path.
- Compared to other approaches, high processing time is required for the connection initiation and the first attempt to set the path.
- Route inconsistency may occurs when old entries are included in intermediate nodes.

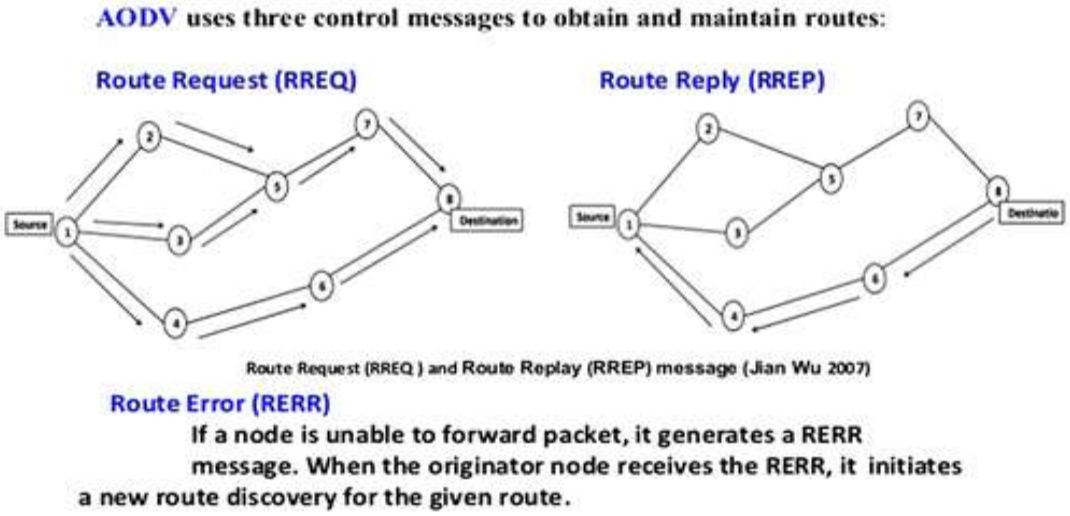

Fig.4. AODV routing protocol.

2.6.3 DSR

The DSR protocol utilizes source routing and maintains functional paths. It consists of route detection and route servicing.

A node requires four essential structures of data that are considered to be conceptual, to be able to engage in the DSR: a Retransmission Buffer, a Send Buffer, a Route Cache and a Route Request Table.

(1) Route Request Table: The route request table is partitioned by the target home address of the route discovery. The Route Request Table is considered of records collection about Route Request packets that were recently forwarded or originated by this node.
(2) Route Cache: In the VANET network every node is servicing its own tables which save the route cache. Route Cache is responsible for storing all requested information related to routing by a new participant node in a VANET network using a DSR routing protocol.
(3) Retransmission Buffer: The Retransmission Buffer of a node is packets queue sent by this node that is expecting for the arrival of an acknowledgment from the next hop in the source path.
(4) Send Buffer: Every packet after being registered in the buffer should be deleted from the send buffer and get rid of it in SEND_BUFFER_TIMEOUT seconds, also is associated with the time it is registered into the buffer.

Advantages:

- No proactive updates are desired in DSR.
- Compared to other approaches, extra overload is occurring on the VANET as it searches for the paths in a reactive approach.
- Beacon less.

Disadvantages:

- Cracked links cant be reformed locally.
- The performance is declining in highly dynamic VANET.
- The VANET is overflowed by superfluous load.
- In high traffic VANET network which is an expected pattern, Byte overhead is occurring by the path data in the header.

2.6.4 OLSR

It means optimized link state routing which means a routing protocol using the proactive mode. In this, whenever any change in the topology occur, MPR (multipoint relay) are responsible to generate and forward the topology information to selected nodes.

It is a proactive protocol based on the table-driven methodology. from its name, the link-state scheme is used by this protocol in an enhanced way to circulate topology information. OLSR is using this mechanism also, but in order to maintain bandwidth the message overflow in OLSR is enhanced as the protocol works in wireless multi-hop scenarios (Jacquet et al., 2003) (Fig. 4).

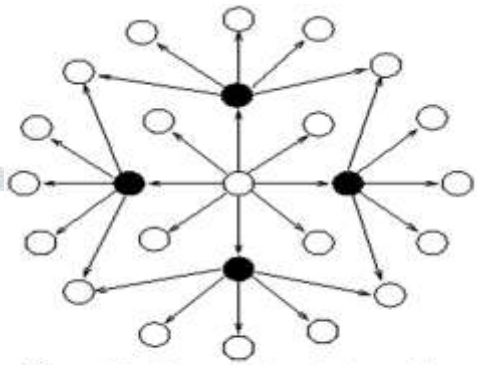

Figure: Flooding a packet in a wireless multihop network from the center node using MPRs(black). The arrows show the way information is passed, *not* all transmissions.

Fig. 5 Flooding packet in wireless Multihop.

As OLSR protocol based on tables, OLSR operation fundamentally consists of servicing and updating information in a set of tables. These tables are including data which is based on received control traffic, and control traffic is produced based on information returned from these tables. the tables are managing the route calculation itself as well (Jacquet et al., 2003).

OLSR uses the below essential control messages types:

(1) Topology Control messages (TC).
(2) HELLO control messages (HELLO).
(3) Multiple Interface Declaration messages (MID).

Advantages:

- In broadcast scenario, reduce the number of retransmission of packets.

Disadvantages;

- •In OLSR, large amount of bandwidth and CPU power is required to compute the optimal path.

2.7 VANET applications

Vehicular applications are classified in the following categories

- Safety oriented
- Commercial oriented

- Convenience oriented
- Productive Applications

2.7.1 Safety Applications

Safety applications include monitoring of the surrounding road, approaching vehicles, surface of the road, road curves etc. [5]. The Road safety applications can be classified as:

i. *Real-time traffic:* The real time traffic data can be stored at the RSU and can be available to the vehicles whenever and wherever needed. This can play an important role in solving the problems such as traffic jams, avoid congestions and in emergency alerts such as accidents etc.

ii. *Co-operative Message Transfer:* Slow/Stopped Vehicle will exchange messages and cooperate to help other vehicles. Though reliability and latency would be of major concern, it may automate things like emergency braking to avoid potential accidents. Similarly, emergency electronic brake-light may be another application.

iii. *Post Crash Notification:* A vehicle involved in an accident would broadcast warning messages about its position to trailing vehicles so that it can take decision with time in hand as well as to the highway patrol for tow away support.

iv. *Road Hazard Control Notification:* Cars notifying other cars about road having landslide or information regarding road feature notification due to road curve, sudden downhill etc.

v. *Cooperative Collision Warning:* Alerts two drivers potentially under crash route so that they can mend their ways.

vi. *Traffic Vigilance:* The cameras can be installed at the RSU that can work as input and act as the latest tool in low or zero tolerance campaign against driving offenses.

2.7.2 Commercial applications

Commercial applications will provide the driver with the entertainment and services as web access, streaming audio and video. The Commercial applications can be classified as:

i. *Remote Vehicle Personalization/Diagnostics:* It helps in downloading of personalized vehicle settings or uploading of vehicle diagnostics from/to infrastructure.

ii. *Internet Access:* Vehicles can access internet through RSU if RSU is working as a router.

iii. *Digital map downloading:* Map of regions can be downloaded by the drivers as per the requirement before travelling to a new area for travel guidance. Also, Content Map Database Download acts as a portal for getting valuable information from mobile hot spots or home stations.

iv. *Real Time Video Relay:* On-demand movie experience will not be confined to the constraints of the home and the driver can ask for real time video relay of his favorite movies.

v. *Value-added advertisement:* This is especially for the service providers, who want to attract customers to their stores. Announcements like petrol pumps, highways restaurants to announce their services to the drivers within communication range. This application can be available even in the absence of the Internet.

2.7.3 Convenience applications

Convenience application mainly deals in traffic management with a goal to enhance traffic efficiency by boosting the degree of convenience for drivers. The Convenience applications can be classified as:

i. *Route Diversions:* Route and trip planning can be made in case of road congestions.

ii. *Electronic Toll Collection:* Payment of the toll can be done electronically through a Toll Collection Point. A Toll collection Point shall be able to read the OBU of the vehicle. OBUs work via GPS and the on-board odometer as a back-up to determine how far the Lorries have travelled by reference to a digital map and 6 GSM to authorize the payment of the toll via a wireless link. TOLL application is beneficial not only to drivers but also to toll operators.

iii. *Parking Availability:* Notifications regarding the availability of parking in the metropolitan cities helps to find the availability of slots in parking lots in a certain geographical area.

iv. *Active Prediction:* It anticipates the upcoming topography of the road, which is expected to optimize fuel usage by adjusting the cruising speed before starting a descent or an ascent. Secondly, driver is also assisted.

2.7.4 Productive applications

We are intentionally calling it productive as this application is additional with the above mentioned applications. The Productive applications can be classified as:

i. *Environmental Benefits:* AERIS research program is to generate and acquire environmentally-relevant real-time transportation data, and use these data to create actionable information that support and facilitate "green" transportation choices by transportation system users and operators. Employing a multi-modal approach, the AERIS program will work in partnership with the vehicle-to-vehicle (V2V) communications research effort to better define how connected vehicle data and applications might contribute to mitigating some of the negative environmental impacts of surface transportation[5].

ii. *Time Utilization:* If a traveller downloads his email, he can transform jam traffic into a productive task and read on-board system and read it himself if traffic stuck. One can browse the Internet when someone is waiting in car for a relative or friend.

iii. *Fuel Saving:* When the TOLL system application for vehicle collects toll at the toll booths without stopping the vehicles, the fuel around 3% is saved, which is consumed when a vehicles as an average waits normally for 2–5 minutes.

3.Problem Description

DoS attack is considered as one of the most severe attacks in VANET. This attack will take down the network to make the service unavailable for the drivers or passengers. This is a vital issue where it may create problem to the drivers on the road and it will particularly be more important if there is life critical information that needs to be transmitted to the drivers. The unavailability of this service or inability to access to it may lead to car accidents [6]. So, this DoS attack issue cannot be neglected and must be taken seriously. DoS attack can also occur in any layer of network communication model. This attack is easy to implement and unavoidable for most of the time. In DoS attack, the attacker controls over the other nodes in network and starts launching attacks. There are 2 possible scenarios that will happen when a DoS attack is launched.

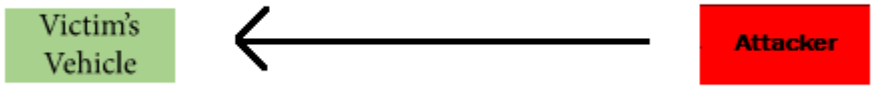

Fig.6. illustrates DoS in Vehicle-to-Vehicle communications.

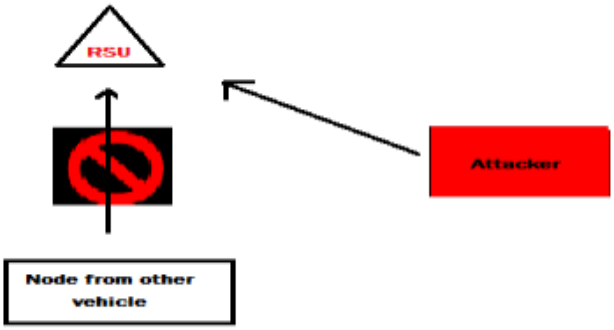

Fig.7.Illustrates DoS in Vehicle-to-Infrastructure communications.

3.1 Literature review

Attacked Packet Detection Algorithm (APDA) provides the DDOS attack detection and prevention, it analysis the packet and communication pattern [18]. The model reduces delay overhead and improves communication. Sniffing attack is prevented by flooding algorithm. Master chock filter method provides the traffic analysis [14]. Mobility model provides the protocol specific evaluation of nodes in network. Sniffing attack is prevented by flooding algorithm. Reference broadcast scheme is achieved by pair wise synchronization to achieve the reliable communication. Enhanced Attacked Packet Detection Algorithm (EAPDA) provides the improved DDOS detection mechanism for VANET [13]. It is work on performance driven measures to reduce the communication delay and attack preserved model was provided the adaptive work solution. It also observed the problem and attack criticality and provides the robust solution. The trust adaptive method is recognizes the bogus message communication and a secure signature specific authentication technique for prevention of DDOS attack**[**11].
Security measures and metrics specification are considered by defensive mechanism. Design of VANET is implemented by channel specific observation and validation. Mobility constraints and environment constraint with resource utilization and integrated security are considered in mobility preserved communication model [10].

UDP spoofing defensive mechanism is used for prevention from DDOS attack in vehicle networkDefensive mechanism isbased upon storage effective tracking of incorporating IPs.Flooding attack defended by resource utilization given bylight weight method. It reduces the computation cost andstorage allocation [15].Protocol tunnelling, unauthorized access, DoS attack problem are identified and solution forthese problem is provided by model. Model applies thetime critical analysis for safe transmission of data over thenetwork and security framework is provided for reducingthe effect of attack on network[16]. S. Roselin Mary et al.proposed an Attacked Packet Detection Algorithm (APDA) which for detecting the DoS (Denial-of- Service) attacks before the verification time. The algorithm detects the invalid requests and attacked packets to avoid the delay that occurs while processing invalid requests and packets. This will not only minimize the overhead delay for processing but also enhances the security in VANET.[18].Aditya Sinha et al. [17] proposed Queue Limiting Algorithm that defines a limited capacity of each vehicle in a network for receiving safety message and defend against DoS attack without posing any security risk. The author classified the messages into four classes and assigned priority to each class for accessing different DSRC channels of communication. An OBU on each vehicle is provided with a scheduler to control internal collision and allow high priority messages to be transmitted before low priority messages but the capacity of messages is decided by the QLA algorithm[19].

3.2 Scope of the Paper

The main aim of this paper is to prevent the Denial of Service attack in VANETand making the service available to the Genuine user.And discarding the attacker send packets from the networks. And by remotely reconfigure of software applications in vehicles automatically and fluently via RSU which in turn access cloud for real time data or information.

3.3 Experiment setup

For this project I utilized the statistical framework in the ns-2 package. It was developed to support simulations that varied parameters and required a standard means of saving data about simulation runs and accessing them later for analysis and visualization.To overcome the issue caused by DoSAttack,I have proposed a mechanism called **Q-Filter** which filters the packet bySize,CBR and Drop tailing.Let us discuss those functionalities in the forthcoming paras.

3.4 Queuing

A queue is used to store traffic until it can be processed or serialized. Both switch and router interfaces have ingress (inbound) queues and egress (outbound) queues. An ingress queue stores packets until the switch or router CPU can forward the data to the appropriate interface. An egress queue stores packets until the switch or router can serialize the data onto the physical wire. Switch ports and router interfaces contain both hardware and software queues.

3.5 Types of queues

Recall that interfaces have both ingress (inbound) queues and egress (outbound) queues. Each interface has one or more **hardware queues** (also known as transmit (TxQ) queues). Traffic is placed into egress hardware queues to be serialized onto the wire.

There are two types of hardware queues. By default, traffic is placed in a **standard queue**, where all traffic is regarded equally. However, interfaces can also support strict priority queues, dedicated for higher-priority traffic.

A Catalyst switch interface may support multiple standard or strict priority queues, depending on the switch model. Cisco notates strict priority queues with a “p”, standard queues with a “q”, and WRED thresholds per queue (explained in a separate guide) with a “t”. If a switch interface supports one strict priority queue, two standard queues, and two WRED thresholds, Cisco would notate this as: 1p2q2t.

3.6 Forms of queuing

The default form of queuing on nearly all interfaces is First-In First-Out (FIFO). This form of queuing requires no configuration, and simply processes and forwards packets in the order that they arrive. If the queue becomes saturated, new packets will be dropped (tail drop). This form of queuing may be insufficient for real-time applications, especially during times of congestion. FIFO will never discriminate or give preference to higher-priority packets. Thus, applications such as VoIP can be starved out during periods of congestion. Hardware queues always process packets using the FIFO method of queuing. In order to provide a preferred level of service for high-priority traffic, some form of software queuing must be used. Software queuing techniques can include:

- First-In First-Out (FIFO) (default)
- Priority Queuing (PQ)
- Custom Queuing (CQ)
- Weighted Fair Queuing (WFQ)
- Class-Based Weighted Fair Queuing (CBWFQ)
- Low-Latency Queuing (LLQ)

3.7 Custom Queuing (CQ)

A less strict form of queuing is Custom Queuing (CQ), which employs a weighed round-robin queuing methodology. Each queue is processed in order, but each queue can have a different weight or size (measured either in bytes, or the number of packets). Each queue processes its entire contents during its turn. CQ supports a maximum of 16 queues.

Each custom queue is identified with a number (1, 2, 3 etc.). Once traffic has been assigned to custom queues, then each queue's parameters must be specified.

Parameters can include:

- A limit – size of the queue, measured in number of packets.
- A byte-count – size of the queue, measured in number of bytes.

Router(config)# queue-list 1 queue 1 limit 15

Router(config)# queue-list 1 queue 2 byte-count 500

Router(config)# queue-list 1 queue 3 limit 25

Router(config)# queue-list 1 queue 4 byte-count 3000

Router(config)# queue-list 1 queue 4 limit 10

3.8 Constant bit rate (CBR)

A stream of data in which the data arrives at a fixed number of bits per second. The term may also imply that there is a guaranteed upper bound on the delay experienced by the data as it is carried. CBR encoding schemes work well when the network bandwidth is known and limited and is quite common in live video sessions where latency must remain low.

As an example, a speech codec generates an 8-bit byte at intervals of 125 microseconds; each byte contains the result of sampling an audio signal, and digitizing it as an 8-bit quantity, and the result is a signal with a bandwidth requirement of 64 Kbps. If during transmission any of the samples are lost or delayed, then the reconstructed speech signal may well be unintelligible as the human ear is very intolerant of gaps in speech.

It is therefore essential to guarantee that the full 64 Kbps can always be carried, and that the transmission delay will be effectively constant.

3.9 Droptail

Droptail is the common algorithm of passive queue management. It drops all the new packets when the buffer is full, and does nothing when buffer still has space. The figure below shows the dropping probability of packets. The only two dropping probabilities are 0 and 1. When the number of packets arrived to the queue larger than the buffer size, the probability of packet dropping is 1. Otherwise, the dropping probability is 0.

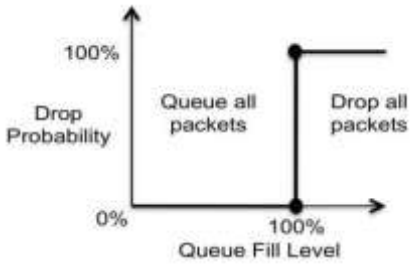

Fig. 8: Drop Probability.

4. Traffic simulation

In this chapter we describe how simulation is done and what the results of the simulation are. The simulation is done in 2 phases and two different simulator have been used One is SUMO(Simulation of Urban Mobility) for road traffic simulation and Veins(Vehicular environment in Network Simulation) for network simulation.

For simulation of road traffic simulator used is SUMO (Simulator for Urban Mobility).

4.1SUMO (Simulation of Urban Mobility)

SUMO is open source and highly portable road traffic simulator, it can handle very large network. It uses microscopic and continuous mobility model. It was developed by Institute of Transportation Systems at the German Aerospace Center [13]. Since SUMO uses microscopic traffic simulation, each vehicle have explicitly defined, each having unique path an indentification. Each vehicle can be further defined by Origin destination metrics (O/D metrics) this metrics contains information about source and destination. Trip file can be generated from O/D metricsusing od2trips. For simulation SUMO need network file to the road network. Now we will discuss how network file is created. Network files define the road map ion which the vehicle runs.

4.2 Network file generation have following phase

4.2.1 Importing map

Although we can manually generate network file by writing route, but this networks are very primitive and it is very difficult to create complex networks.But for the realistic simulation we have to create network file which are present in the real world for that purpose SUMO incorporate by which we can download real world road map Form the openstreetmap.org Fig. 3.2 show map from openstreet.org Fig. 3.2: Map form open street Org The map are downloaded are OSM file, after downloading map from the website the OSM file edited using JOSM Java OpenStreetMap Editor. IN this process all the unwanted route and path are removed to simplify the network file

Fig. 9. Map convert process.

4.2.2 Generation of network file

After editing the OSM file it is ready to create network file. To convert the .osm file to .net.xml file netconvert command line application is provide by SUMO. It takes .osm file as input and gives .net.xml as output file.

4.2.3 Trip file

After creation of network file we have to define route for the vehicle along which vehicle would travel. For this purpose we have to follow two phase one is creation of trip file and using trip file we generate route file for vehicle.

4.2.4 Route file

For simple file we can easily write the route file but for very large network with high density vehicle it is not possible to write routing file manually. So the trips file along with the network file is now used to generate the vehicle routes is created using the Duarouter.exe application which is a part of the SUMO package

4.2.5 Configuration file

Each scenario in sumo has a .sumo.cfg file associated with it which points to the corresponding network and routing files to be used, and also the start and end time of the simulation. This is configuration file.So configuration file is created using combining network file and route file.

4.4Network simulation

After traffic simulation the next phase is to simulate network. Network simulation is used to model computer network configurations before they are deployed in the real world. By using network simulation different network setups are compared, making it possible to recognize and resolve performance problems in network without the need to conduct potentially expensive tests in real world. Many opensouce network simulators available like NS-2, Omnet++, J-SIM. Here in this project, we have used the NS-2 simulator.

4.5 NS-2

Network Simulator (Version 2), widely known as NS2, is simply an event-driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. The simulation NS-2 is controlled by supplying the required modifiable parameters per module that is being used in the simulation using the .cfg file corresponding to the simulation. .cfg file of simulation contains information about size for simulation, launched file for accessing traffic simulation

NS2 consists of two key languages:

C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism (i.e., a backend) of the simulation, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend). The C++ and the OTcl are linked together using TclCL. Mapped to a CCC object, variables in the OTcl domains are sometimes referred to as handles. EEE 802.11p is an amendment from the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE). This protocol is used in physical layer. The source code for mobility lives in the directory src/mobility.

4.6 Final simulation and results

After completing all the above mentioned steps now we can run the simulation in NS-2.The node movement in the network simulation is governed by network file of traffic simulation.This part contains evaluation of Q-Filter compared with CBR,Packet size and Drop tailing. With the help of the NS-2 we were able to prove, ns is simulator project, start 1989 as a different of real. Our networks consist of a heterogeneous traffic sources delivery UDP based and TCP based traffic to the destination. Although all the observations are carried out on UDP based traffic in the presence of TCP traffic, but the results may be used as a ground work for computing more complicated traffic scenarios like TCP based web traffic or UDP based multimedia traffic the simulation setup is done on the Ubuntu 18.04LTS machine running on NS-2.35 and SUMO. It has been observed We run two scenario, one Simulation of Urban Mobility, and Q-filter, we have repeated the experiments by changing the times 0.1 to 0.01. This is clearly shown by the fact that non algorithmic queue management such as Droptail performs better than algorithmic active queue management technique

As we saw in the previous section, DOS attack causes weakness in making the network unsecure and weakening the ordinary approach of the network, in this article we deal with providing a solution for security improvement in car networks against denial-of-service attacks which improves the Throughput of the network by varying between router destination links in 0.5, 1.7, 2.0 Mbps we found throughput for Droptail.

Queuing Method	Bandwidth			
	0.5	1.2	1.7	2
DROPTAIL	501766.78	958105.64	987249.54	1001821.49

1. 1.Fair queuing techniques are resilient to changes in queue limit or queue size i.e.when the queue limit is decreased to half or the link is narrower resources constrain link fair Queuing method do not degrade going from queue size 10 to 5Droptail degrades sharply.

2. 2.The packet loss rate and throughput of the network remains unaffected when queue size is decreased in case of fair queuing method whereas non algorithmicqueuing Techniques are degraded in both performance parameters
3. Finally we conclude that a non-algorithmic queuing method such as Droptail is recommended where security and traffic engineering is not a concern.We perform the calculation of throughput for constant bitrate traffic in the first scenario we calculate However for a bigger sophisticated networks we prefer fair queuing, although it will increase the processing power used in the network thereby reducing the battery life but it the cost that we pay for better traffic engineering.Among the fair queuing methods FQ can be used for high bandwidth networks and SFQ must be used for low resources networks in the term of bandwidth.

5.Conclusion

The results of the paper have been listed in the previous section. The results of the work guide in to the point that network performance is compromised as a level of security in the increased. Enhanced algorithmic and computational loads in the network at routing nodes causes bluishness in the network however implementation of effective queue management is also of paramount importance.We have conducted all the experiments by taking lesser number of nodes but by increasing the number of nodes results may change a bit. In future it is planned to test the solution for more dense and populated network scenarios.

Future work

The result in the paper maybe taken as a reference study for future works the areas where this work might be extrapolated as enlisted below.The experimentation may be done on hard traffic classes like https, DNS etc. may be used.Finally this may be extended to wireless technologies of newer generationslike 4g, LTE etc.

References

[1] I. Ahmad, R. M. Noor, I. Ali, M. Imran, and A. Vasilakos, “Characterizing the role of vehicular cloud computing in road traffic management,” International Journal of Distributed Sensor Networks, vol. 13, no. 5, 2017.

[2] Vinh Hoa La, and Ana Cavalli, “Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey”, Ijans, vol.4, no. 6, pp.48–55, 2014.

[3] Nivraj J.Patel and Rutvij H.Jhaveri, “Trust based approaches for secure routing in VANET: A Survey”, ELSEVIER, vol. 19, no. 71, pp.194–203, 2015.

[4] A. Rahim, F. B. Muhaya, M. Sher, Z. S. Khan, and I. Ahmad, “Performance evaluation of broadcast techniques in VANETs,” Indian Journal of Science and Technology, vol. 2, no. 10, 2009.

[5] T. Yasser, M. Paul,“Vehicle Ad Hoc Networks: Applications and Related Technicalissues”. IEEE Communications Surveys and Tutorials,vol. 10, pp. 74–88, 2008.

[6] A. Rasheed, S. Gillani, S. Ajmal, and A. Qayyum, “Vehicular ad hoc network (VANET): A survey, challenges, and applications,” Advances in Intelligent Systems and Computing, vol. 548, pp. 39–51, 2017.

[7] PathreTyagi and D. Dembla, “Investigating the security threats in VANET Towards security engineering for safer on road transportation,” Advances in communications and Informatics conference New Delhi,2014, pp. 2086–2091.

[8] A. Sinha and S. K. Mishra, “Preventing VANET from DOS & DDoS Attack,” International Journal of Engineering Trends and Technology (IJETT), vol. 4, no. 10, 2013.

[9] Munazza Shabbir, Muazzam A. Khan, Umair Shafiq Khan, and Nazar A. Saqib, "Detection and Prevention of Distributed Denial of Service Attacks in VANETs", IEEE, vol.8, no. 14, pp.123–129, 2016.

[10] VIPIN, Dr.Rajender Singh ChhillarThe DDOS Attack Detection and Prevention inVANET by Group Controlled Analysis Model.

[11]B. Pooja, M.M. Manohara Pai, Radhika M. Pai, Nabil Ajam, and Joseph Mouzna, "Mitigation of the Insider and Outsider DoS attack against the Signature Based Authentication in VANETs", IEEE, vol. 15, no. 2, pp.639–645, 2014.

[12]MohamedNidhal Mejri and Jalel Ben-Othman, "GDVAN: A New Greedy Behavior Attack Detection Algorithm For VANETs", Journal of IEEE Transaction on Mobile Computing, vol. 4, no. 7, pp.53–62, 2015.

[13] Priya Sharma, and Amarpreet Singh, "Enhanced Attacked Packet Detection Algorithm For Detecting Dos Attack In Vanet", International Journal of Advances in Computer Science and Cloud Computing (IJACSCC),vol.3, no. 2, Nov-2015.

[14] S. Abdelsayed, D. Glimsholt, C. Leckie, S. Ryan, and S. Shami,"An efficient filter for denial-of-service bandwidth attacks", inGlobal Telecommunications Conference, 2003. GLOBECOM'03. IEEE 2003 Dec 1 (Vol. 3, pp. 1353–1357). IEEE.

[15] A. John, and T. Sivakumar,"Ddos: Survey of traceback methods", International Journal of Recent Trends in Engineering. vol. 1, no. 2, pp. 241–245, May 2009.

[16] M. Raja and J. P. Hubaux, "Securing Vehicular Ad-Hoc Network", Journal of Computer Security, pp. 40–65, 2007.

[17] A. Sinha and S. K. Mishra, "Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DoS) Attack," International Journal of Computer Applications, vol. 86, no. 8, pp. 14–17, 2014.

[18] S.Roselin Mary, M.Maheshwari, and M.Thamaraiselvan, "Early detection of DOS attacks in VANET using Attacked packet detection algorithm (APDA)", ICICES, pp.237–243, 2013.

[19] Aditya Sinha andSantosh K. Mishra, "Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DoS) Attack", published in International Journal of Computer Applications (0975 – 8887) vol.86,no,8, January 2014.

[20] Amrit ekka, "Simulation of vehicular movement", http://ethesis.nitrkl.ac.in/5250/1/109CS0021.pdf.