Efficient and Secure communication in Vehicular Ad hoc Network

Kamlesh Namdev
PhD Research Scholar Dr.K.N.Modi University, Newai(Raj)

Prashant Singh, PhD

ABSTRACT
Recent advances in development of Wireless Communication in Vehicular Adhoc Network (VANET) has provided Emerging platform for researchers. VANET are movable & fixed infrastructure. One of the main challenges in VANET is to secure communication. VANET is a open network for all and different types of attacker available for attack to victims node in the network & create problem in communication. Denial of services (DOS) and DDOS are very destructive for security system as well as authentication and Privacy are big challenges, finally we designed DOS prevention algorithm, Which is capable secure communication.

Keywords
Attacker, Attacks, victims node, DOS, DDOS etc.

1. INTRODUCTION
Safety systems are becoming nowadays an attractive topic for the research community with the increase in the number of traffic accidents and the complexity of the roads infrastructure. Vehicular Ad Hoc Network (VANET) is a new class of wireless networks that allows the communications among neighboring vehicles and between vehicles and nearby road-side infrastructure such as traffic lights and command centers. This technology offers a wide set of applications and services ranging from safety applications and traffic management systems to commercial and marketing services.

The basic point in such kind of networks is building efficient and secure communications. The clustering is one of the most important tasks in VANET that is concerned with organizing and optimizing the communications.

VANET require real time message propagation that is able to deliver data in a timely and accurate manner. For example considering the case of safety applications, any delay in the message delivery may entrain dangerous and mortal accidents. So we need a strategy which is helpful, efficient and a secure communication.

During clusters formation, some vehicle's driver may derail the protocol principles and turn them to their advantage. Some others may prefer to save their time and resources by not following the model rules after cluster formation. Numerous contributions have been advanced to cope these misbehaving vehicles.

As a solution, we propose a model that is able to detect misbehaving node.

2. VANET SECURITY REQUIREMENTS IN CITY SCENARIO
A driver at location "A" moving towards location "B" finds a traffic jam and wants to communicate to other nodes trying to help them. The other drivers may take alternative routes or any other suitable action. If such communication is intentionally or unintentionally changed. There may be serious consequences.

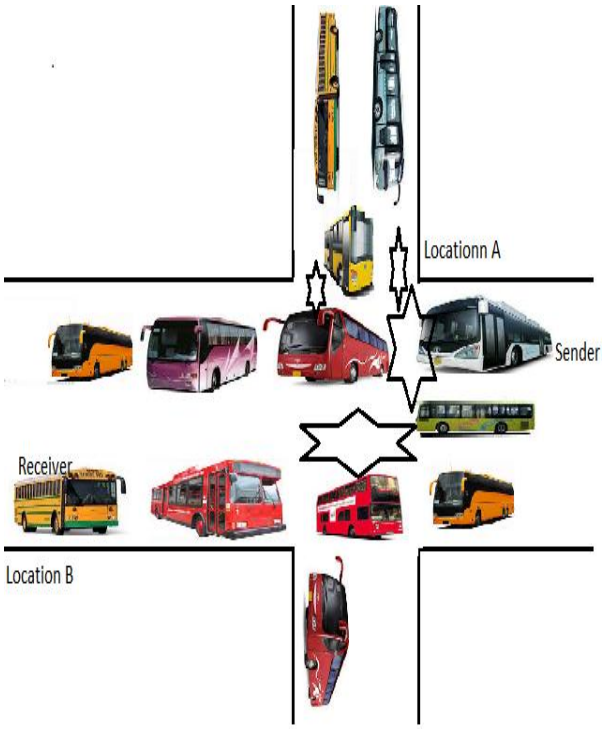

Figure 1 Source destination diagram

Information may be very important for a particular vehicle, or to a vehicle driver, pertaining to traffic problems. In the VANET system the information is forwarded through intermediate vehicle as available in the network. This flow of information can be intentionally disturbed by any mischievous node.

The communication can be attacked by following type:

1) Sending numerous copies of the message or
2) Messages thereby jamming the channel,
3) Delay in passing the information,
4) Dropping the information packet etc.

3. TYPES OF ATTACKERS IN VANET
Different types of attacker in VANET create security problem. Some attackers act in different time during communication and harm the valuable information which may directly affect the vehicles and may lead to jam, accidents etc.

1) Greedy Drivers: Selfish drivers trying to maximize their gain by making believe a congested path to their

destinations, and consequently suppress traffic by attacking the routing mechanisms.

2) Snoops: Drivers attempting to profile drivers and extract their identifying information. Malicious Snoops can even track vehicle locations and determine the identities of drivers by corresponding them to the house or work sites.

3) Pranksters: Drivers trying to disable applications or prevent information from reaching others vehicles. Such attacks are denoted by Denial of service attacks (DoS).

4) Malicious Attackers: Drivers deliberately attempting to make harm via the available applications within the network. Several attacks focus on damaging exchanged data between vehicles such as message fabrication, suppression or alteration. Sybil attack (Masquerade) [1]) belongs also to this category.

5) Industrial Insiders: If vehicle manufacturers are responsible for securing communications within VANETs, employees can reveal confidential data to malicious entities.

4. ATTACKERS PROPERTY

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.

1) **Coverage Area**: Attacker could cover the main area of road, and it depends on the nature of the attacks. Basic level attacker has controlled one DSRC channel 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.

2) **Technical Expertise:** Technical expertise of the attacker makes them stronger for creating attacks in the network. Attacker having ability to extracts the program code and secret keys of the computing platform of OBU and RSU by launching physical attacks.

3) **Resources**: Budget, manpower and tools are the three main key resources and attackers depend on it to achieve their goals.

5. TYPES OF ATTACKS

1) **Jamming**: The jammer deliberately generates interfering transmissions that prevent communication within their reception range. In the VANET scenario, an attacker can relatively easily partition the network, without compromising cryptographic mechanisms and with limited transmission power [2].

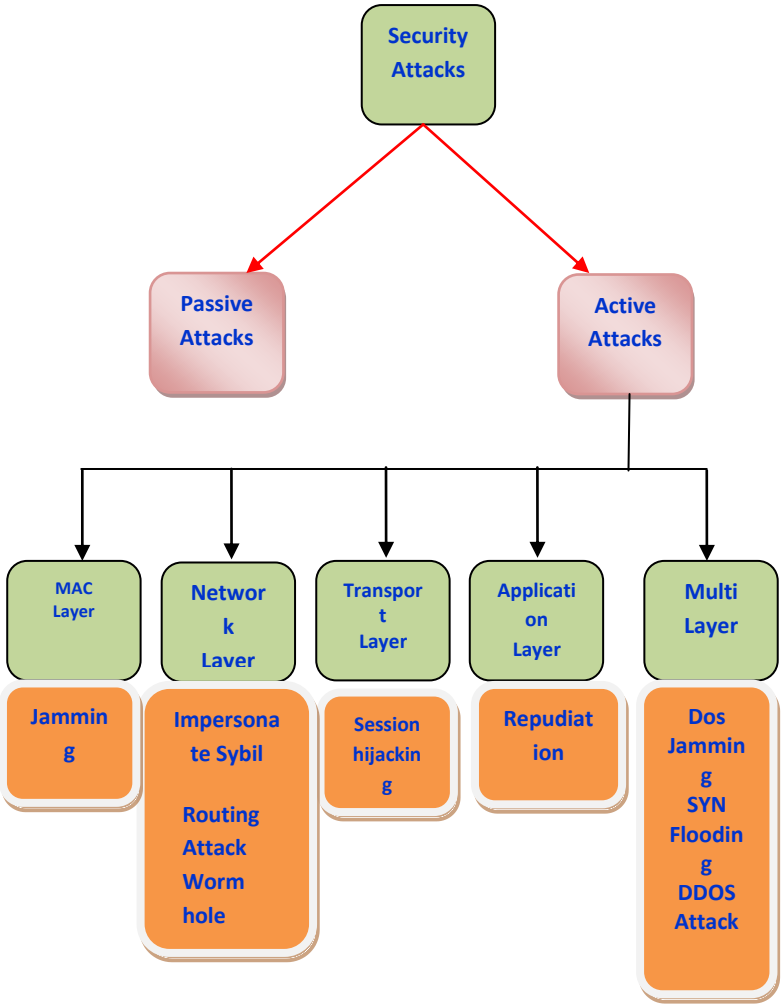

Figure: 2 Classification of attacks based on Layers

2) **Node Impersonation Attack:** Each vehicle has a unique identifier in VANET and it is used to verify the message whenever an accident happens by sending wrong messages to other vehicles [2]. Fig 5.2 explains this scenario in which vehicle A involves in the accident at location Z. When police identify the driver as it is associated with driver's identity, attacker changes his/her identity and simply refuses it[5].

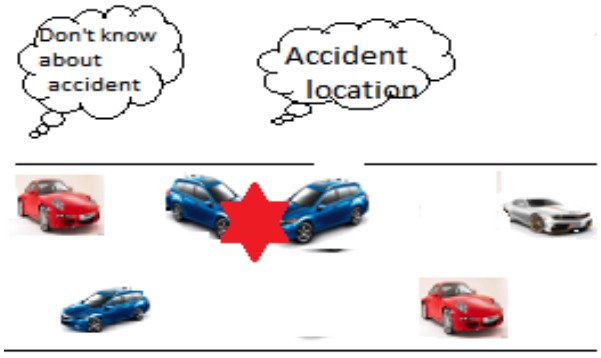

Figure 3 Node Impersonation Attack

3) **Sybil Attack:** Sybil attack [2] so belongs to the first class. In Sybil attack, the attacker sends multiple messages to other vehicles and each message contains different fabricated source identity (ID). It provides illusion to other vehicle by sending some wrong

messages like traffic jam message [2]. Fig 5 explains Sybil attack in which the attacker creates multiple vehicles on the road with same identity. The objective is to enforce other vehicles on the road to leave the road for the benefits of the attacker.

4) **Routing attack**: Routing attacks re the attacks which exploits the vulnerability of network layer routing protocols. 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:

5) **Black Hole attack**: In this type of attack, the attacker firstly attracts the nodes to transmit the packet through itself. It can be done by continuous sending the malicious route reply with fresh route and low hop count. After attracting the node, when the packet is forwarded through this node, it silently drops the packet.

6) **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.

7) **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. This selection can be of two types-one is malicious node can drop the packet of UDP whereas the TCP packet will be forwarded. Another is malicious node can drop the packet on the basis of probabilistic distribution.

8) **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.

9) **Repudiation**: The main threat in repudiation is denial or attempt to denial by a node involved in communication. This is different from the impersonate attack. In this attack two or more entity has common identity hence it is easy to get indistinguishable and hence they can be repudiated.

10) **Denial of Service (DOS)**: DOS attacks are most prominent attack in this category. In this attack attacker prevents the legitimate user to use the service from the victim node. DoS attacks can be carried out in many ways [3].

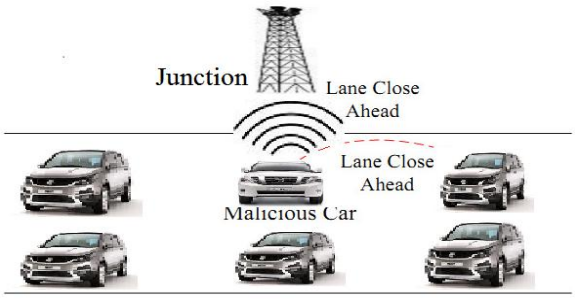

Figure 4 Dos Attack

11) **Jamming**: In this technique the attacker senses the physical channel and gets the information about the frequency at which the receiver receives the signal. Then he transmits the signal on the channel so that channel is jammed.

12) **SYN Flooding**: In this mechanism large no of SYN request is sent to the victim node, spoofing the sender address. The victim node send back the SYN-ACK to the spoofed address but victim node does not get any ACK packet in return. These results too half open connection to handle by a victim node's buffer. As a consequence the legitimate request is discarded.

13) **Distributed DoS attack**: This is another form of Dos attack. In this attack, multiple attackers attack the victim node and prevents legitimate user from accessing the service.

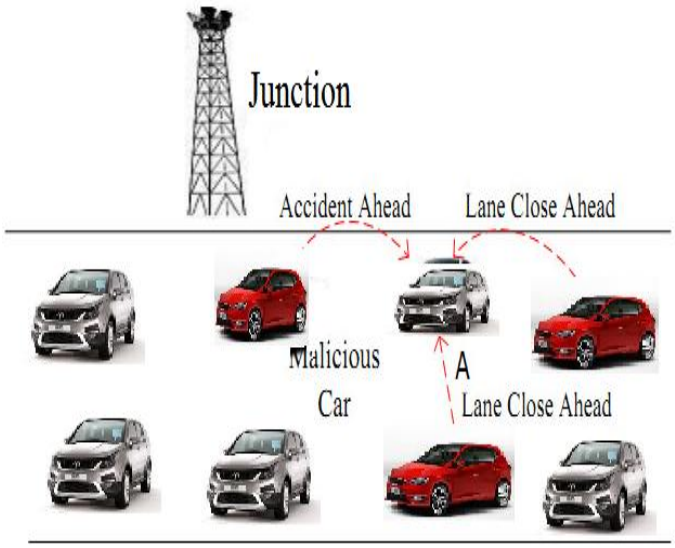

Figure 5 DDos attack

6. DESIGNED ATTACKERS PREVENTION TECHNIQUE

Before presenting the prevention mechanism some introduction is needed about the working of VANETs and how DoS attack will restrain communication between vehicles (Fig. 2). In VANET each vehicle is equipped with OBU and for communication it uses DSRC channels. OBU in vehicle is an intelligent device having sensors, modem, processing unit, and storage capacity [4]. Vehicles can communicate with Junction point as well as other vehicles. Where junctions are available vehicle send their information regarding crash,

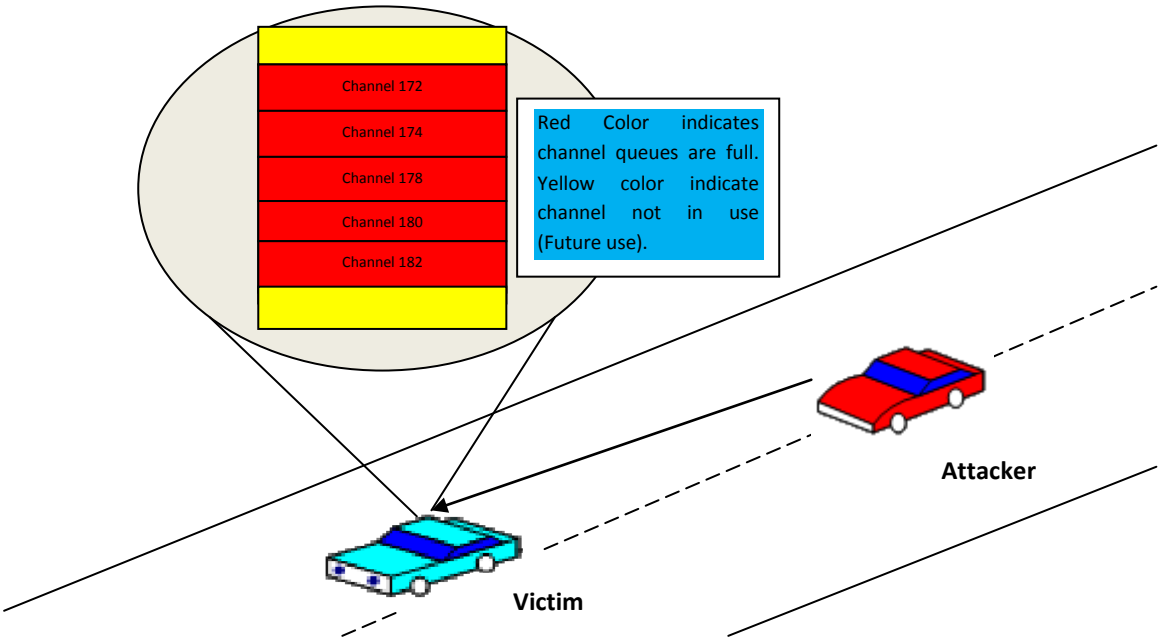

Figure 6 DoS attack, where attacker car sends enormous messages to the victim. Thus; all the channels of victim are filled by the messages. Show in circle

Collision and other information to it and junction forward this information to other vehicle that are intended to go to that place. Some places in city where junction are not available vehicle pass the information to each other. But when attacker comes into frame things will be uncontrolled. Attacker sends enormous amount of (false) safety massages to the victim node. Hence all the channels of DSRC are filled with CLASS 1 messages or high priority massages, thus victim node is unable to communicate with other vehicle and it may be prone to accident or crash.

7. DESIGNED SECURE COMMUNICATION

ALGORITHM

Algorithm: 1 Handling attackers

Attacker sends multiple (false) safety messages to the victim vehicle through DSRC channels. Because safety massages has highest priority over other massages they use all the bandwidth of the victim, thus victim is unable to communicate with other vehicles and denial of service occur. Our protection scheme works on that, in our scheme each vehicle have some upper bar for receiving a limited number of safety massages. Thus, receiving limitation of safety massages will protect the node from DoS attack. When DoS attack happen all the internal queues of OBU are filled with messages and all the resources of OBU are busy in processing of these messages so communication with other vehicle. But if only limited numbers of messages (safety message) are received from sender, OBU will perform its task quite easily.

Algorithm: 2 Control Block Module algorithm

Control Block Module: This module collects the Internet Protocol (IP) address of incoming data and making a table entry of it.

Algorithm: 3 Algorithm for queuing module

Queuing Module: For finding the upper limit of message (safety message) receiving for particular vehicle, vehicle sends a hello packet in the network at regular time interval and wait for its reply. When reply come, OBU counts the number of reply; we assume it "Y". We know that class a safety massage are generated when any event has taken place so at the small time interval if we assume that maximum 10 events have happened (Max probability).

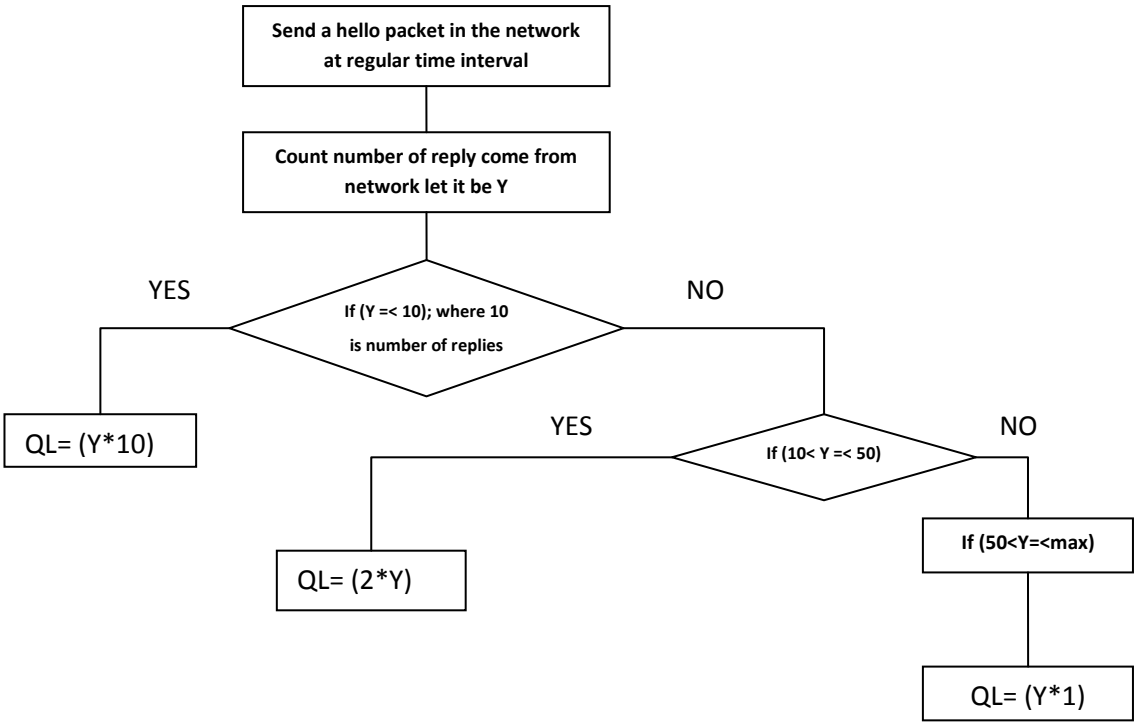

Figure 7 Logic diagram of the designed algorithm

This mechanism is able to protect vehicle from DoS attack

8. SIMULATION AND RESULT ANALYSIS

We have enhanced our previous work "Clustering in Vehicular Ad Hoc Network for Efficient Communication "[6] , where we designed a strategy for efficient communication using clustering but when we talk about the communication, security is must compulsory for that, so we have designed the prevention technique in this paper and inbuilt with AAP[6] protocol , then simulate the newly developed algorithm AAP using NS2 simulator and find out the following results .

	ATTACK ON AODV	ATTACL ON AAP
SEND	9564	9564
RECV	5070	9110
ROUTINGPKTS	418915	1499
PDF	53.01	95.25
NRL	82.63	0.16
No. of dropped data	4494	454
Actual Performance	433549	20173
Efficiency	55.51%	96.30%

Table 1 showing Implemented protocol's result is better than AODV. Here the efficiency is improved by 1.84 % than AODV VANET routing protocol. Dropping packet makes the difference between sending and receiving packets. There are numerous conditions which occur when communication faces the problems those give the losses to communication and dropping packets.

ALL TYPE PACKET DROP ANALYSIS on AODV vs Implemented protocol

Table: 2 Results analysis of (Dropping packets) AAP vs AODV

	AODV		AAP	
Drop from ARP	30	0.14%	22	0.11%
Drop from IFQ	37	0.17%	26	0.13%
Drop from CBK	63	0.29%	30	0.15%
Drop from TOT	0	0.00%	0	0.00%
Drop from NRT	199	0.92%	73	0.35%
Drop from END	7	0.03%	4	0.02%
Drop from DUP	0	0.00%	0	0.00%
Drop from RET	0	0.00%	0	0.00%
Drop from BSY	0	0.00%	0	0.00%
Drop from SAL	0	0.00%	0	0.00%
Drop from ERR	0	0.00%	0	0.00%

Total Drop Via Congestion	440	2.04%	207	1.00%
Total Drop	776	3.60%	362	1.76%

Table 2 showing that dropping packets of AODV & Implemented protocol. It is clear that total dropping packet of AODV rate 3.60% than Advance AODV Protocol (AAP) dropping rate 1.6%

9. CONCLUSION

This paper includes different attacks in VANET which have been classified depending on the special layers. It has been experimental that the categorization.

We have discussed security challenge and security necessities. We have found after review that attacks in multilayer similar to denial of services (DOS) and DDOS are very destructive for security system as well as authentication and Privacy are big challenges, finally we simulate & analysis between AODV & AAP designed DOS prevention algorithm.

The situation is highly satisfactory under security attack condition where our implemented system efficiency is recorded as 96.30% as against 55.51% in AODV. It is also very satisfying to see when individual parameter behavior is compared between the existing system i.e. , AODV and our implemented system, that the performance by our developed system both under "normal" and "security" conditions has shown significantly high level compared to AODV.

Thus we confidently state that the proposed system by us is a highly efficient and secured system.

10. REFERENCES

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

[2] Megha Nema1 , Prof . Shalini Stalin2 , Prof. Vijay Lokhande3 "Analysis of Attacks and Challenges in VANET" Department of Computer Science engineering, BIST, Bhopal- (M.P.), India.

[3] D.Jiang,V.Taliwal, A.Meier, W.Holfelder and R.Herrtwich,"Design of 5.9GHz DSRC based vehicular safety communication", IEEE Wireless Communication Magazine , Vol.13, No.05, Nov 2006, pp:36-43.

[4] Karan Verma, Halabi Hasbullah, Ashok Kumar, "Prevention of DoS Attacks in VANET", in Wireless Personal Communications, November 2013, Volume 73, Issue 1, pp 95-126.

[5] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, M. Zhendong, F. Kargl, A. Kung, J-PHubaux, "Secure vehicular communication system : Design and Architecture Communications" IEEE Magazine, November 2008,vol. 46, pp. 100-109.

[6] Kamlesh Namdev, Dr. Prashant Singh, " Clustering in vehicular Ad Hoc Network for Efficient Communication" , International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 11, April 2015 .

[7] Megha Nema1, Prof. Shalini Stalin2, Prof. Vijay Lokhande3 "Analysis of Attacks and Challenges in VANET" , International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 7, July 2014.

[8] Vehicle Safety Communications Consortium.(n.d.) Vehicle Safety Communications Project: Task 3 Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC, 2005.

[9] 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.

[10] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, "Survey on security challenges in VANET", IJCSN International Journal of Computer Science and Network, Vol 2, Issue 1, 2013