AN EFFICIENT APPROACH OF DSR PROTOCOL TO DETECT AND PREVENT BLACK HOLE ATTACK FOR VANET

Tushar Pokar[1], Prof. Shreya Patel[2] & Prof. Rakesh Shah[3]
[1]Student, [2]Asst. Professor, [3]PG Coordinator
[1]Computer Engineering
[1]GMFE, Himmatnagar, India

Received: February 06, 2019 Accepted: March 18, 2019

ABSTRACT: *VANET (Vehicular Ad hoc network) plays an important role in connecting the nodes in the mobility. Here security is a major issue while passing messages from one node (vehicle) to another (vehicle). In wireless network, messages are passed with a wireless router or node. Considering the benefits of VANET, organizing security is a challenging task. Black hole attack is one of the security threats. The black hole attack is a type of a hiding itself as if it has the shortest and the fastest way to the destination node. There can be situations where there can be multiple such nodes which can act as black hole nodes. Our solution is addressing such issues with modified DSR protocol. In the proposed approach, Street side units are put in the crossing point of streets and may acknowledge to exchange bundles when a vehicle experiences an issue of package transmission. The solution protocol differs from AODV that it refreshes the value of sending message flag by taking its neighbourhood nodes into consideration. The results will prove the efficiency of the proposed approach.*

Key Words: *VANET, Routing Protocol, Security Attack, Black Hole, AODV, DSR.*

I. INTRODUCTION

VANET is a self – organized network that allow vehicles to communicate with each other[6]. Each vehicle participating in the network act s as a wireless router or node, allowing vehicles connect and communicate. AODV and DSR is the mainly used routing protocol for VANET. The VANET communication has been classified into two types[2].

1. Vehicle to Vehicle (V2V) Communication: -

Communication takes place in between vehicle to vehicle without the backing of any infrastructure. It is appropriate for communicating with in short range. It is reliable and very quick. Vehicles consist of OBU (On Board Unit), which process data collected from various sensors and is responsible for communicating with other vehicles and infrastructure[2].

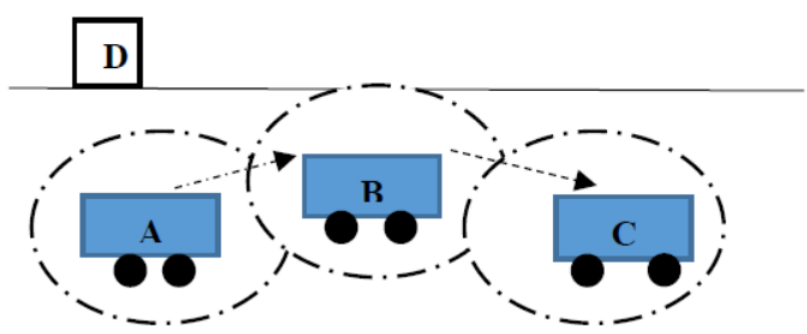


Fig. 1: vehicle to vehicle (v2v) communication

Figure 1 shows vehicle to vehicle communication. A, B and C are vehicles and D is infrastructure. Since all the vehicles are in communicating range, Vehicle A is able to communicate with Vehicle C by means of multi hopping through vehicle B[2].

2. Vehicle to infrastructure Communication: -

Infrastructure act as a static node. They are also termed as Road Side Units. Communication takes place between vehicle and road side units, it is appropriate for long range communications[2].

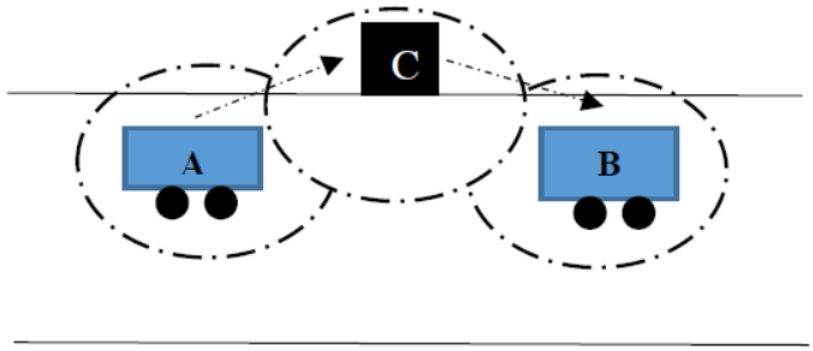


Fig. 2: vehicle to infrastructure communication

Figure 2 shows vehicle to infrastructure communication. A, B are vehicles and C is Infrastructure. Since Vehicle A and Vehicle B are not in the communicating range, they communicate with the help of Road Side Unit (RSU)[2].

II. ROUTING PROTOCOLS:

In this section we will explain the four routing protocols that we study. They are divided into two main categories: Reactive and proactive. Reactive routing protocols, which include AODV and DSR, build the road when they must send a package. To this end, they use different types of query messages that are sent to all nodes of the network. Proactive routing protocols, which include OLSR and DSDV, are those who use a routing table with all the information on predefined routes, which is periodically updated through messages that exchange routing information between the nodes of the network.

A. AODV

AODV belongs to the reactive routing protocols. It uses Route Request (RREQ), Route Reply (RREP), and Route Error (RERR) control messages. It handles source routing and backward learning methods. When a node wants to make a connection with a destination node, the source node broadcasts an RREQ message epidemically. When the final destination receives the RREQ packets, it selects the path with the smallest hop count and delivers it back to the source in an RREP packet. When the information of the path to the destination reaches the source node, this selected path is used to send data [3].

B. DSR

Another notable reactive routing protocol is DSR. It also uses Route Request and Route Reply messages. Route Requests are sent by the source when it is required to send a data packet. Each node that receives the request stores its ID inside the packet, in a route record, and then forwards it until the destination is reached. The destination sends a Route Reply message with a copy of the accumulated route record from the Route Request to the source. The source stores the route in a cache, and it is included in the data packets sent, so nodes use it to forward the message. This is known as source routing mechanism. The protocol also has a Route Maintenance mechanism to report broken links [3].

C. OLSR

OLSR belongs to the proactive routing protocols. It uses two kinds of control messages: HELLO and Topology Control (TC). HELLO messages are broadcast periodically by each node with information about its neighbors. They are received by all one hop neighbors. Based on this information, each node selects its Multipoint Relays (MPR), which is the minimum set of neighbor nodes that allows a node to reach all the other nodes two hops away, reducing the number of retransmitted packets and network resources. On the other hand, the TC message is sent by each node across the entire network; the message carries the information of MPRs' sender node. Using this information, a route from the source to the destination is formed by MPRs of the different nodes in the VANET [3].

D. DSDV

Finally, DSDV is a popular proactive routing protocol. It is based on control packets that are broadcast by each node periodically or when network topology changes are detected, in order to update the routing information of the other nodes. After receiving the Update packet, the node increments the metric by one and retransmits the Update packet to the corresponding neighbors. The process is repeated until all the

nodes in the network have received a copy. The update packet with the smallest metric will be selected and used by each node in its routing table as the path to the message's source [3].

III. ATTACKS IN VANET

There are various types of attacks that can affect the entire system or can mortify the execution of system. These attacks can be marked into subsequent types [6].

1. Impersonation Attack
2. Denial of Service Attack
3. Routing Attack
    a. Worm Hole Attack
    b. Black Hole Attack
    c. Gray Hole Attack
4. Sybil Attack
5. Timing Attack

➢ Black Hole Attack:

In this type of attack, the attackers firstly engage the nodes to transferring the packet through itself. When some malicious users enter into the system's network and stop along messages to next nodes by releases messages are called as black node. When some malicious user enter into the network and stop forwarding messages to next nodes by dropping messages are called as black node[6].

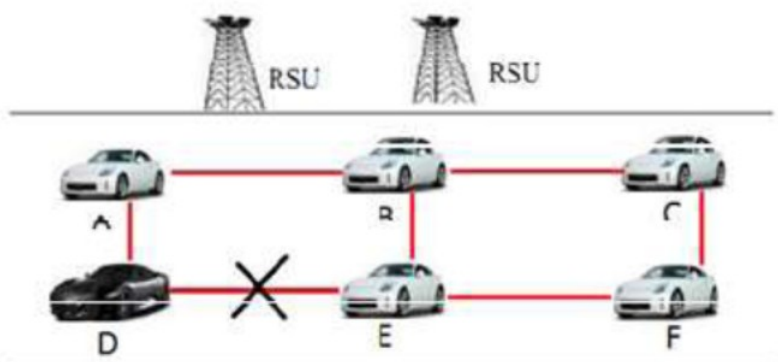


Fig. 3: black hole attack [6]

In figure 3 the vehicle D is doing some malicious activity so, we can say that the vehicle D is a black hole node which was create black hole attack.

➢ Gray Hole attack:

This attack happens if some node dropping 50% of the packets and rest 50% is sending by transferring the message. In this way wrong data is broadcast. A Gray hole is a technique in which the spiteful node just drops the packet from some specific node in the network and forwards all other packets to its destination. This is the addition of black hole attack [6].

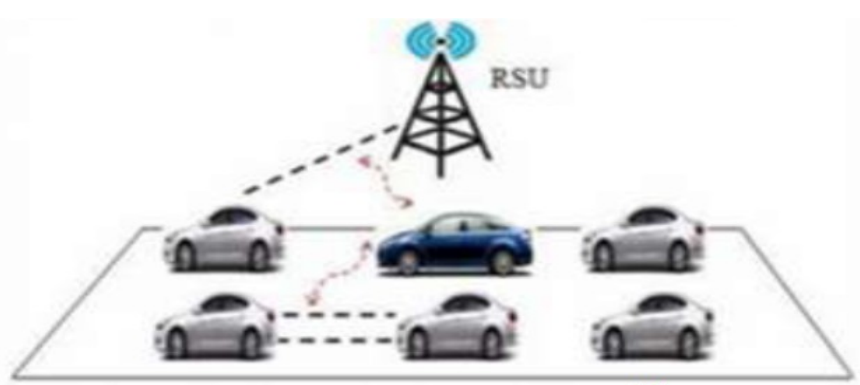


Fig.4: gray hole attack [11]

IV. PROPOSED MECHANISM:

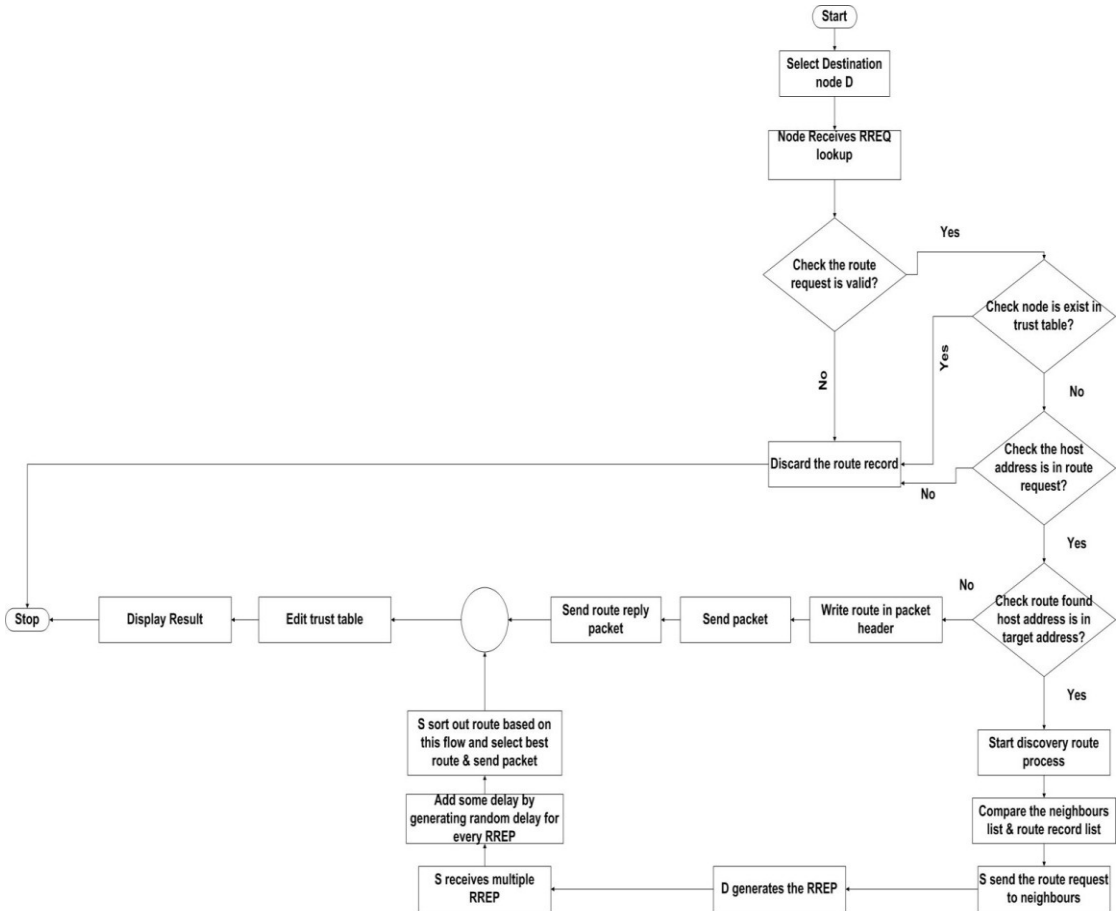


Fig. 5: flow chart of proposed work

- **Algorithm Steps:**
  1. Begin (Start)
  2. Initialize nodes length & breath
  3. Set model
  4. Find coverage set & road side unit
  5. Start transmission
  6. Continue until source has not found
  7. Plot source & destination node
  8. Check RREQ is valid or not
  9. If RREQ is valid than check the node is exist in trust table with flag set or not, and if RREQ is not valid than discard the route record and stop.
  10. If node is exist in trust table with set flag then discard the route record and stop, and if it is not exist in trust table then check for black hole attack
  11. Check black hole attack using route discovery algorithm by DSR
  12. Build PDR & Throughput
  13. Stop

V. SOFTWARE REQUIREMENTS:

Simulation: NS version 2.35
Language: TCL, AWK Script and C++
Operating System: Ubantu 14.04 LTS 64-bit
Road Map and Mobility Generator: VanetMobiSim

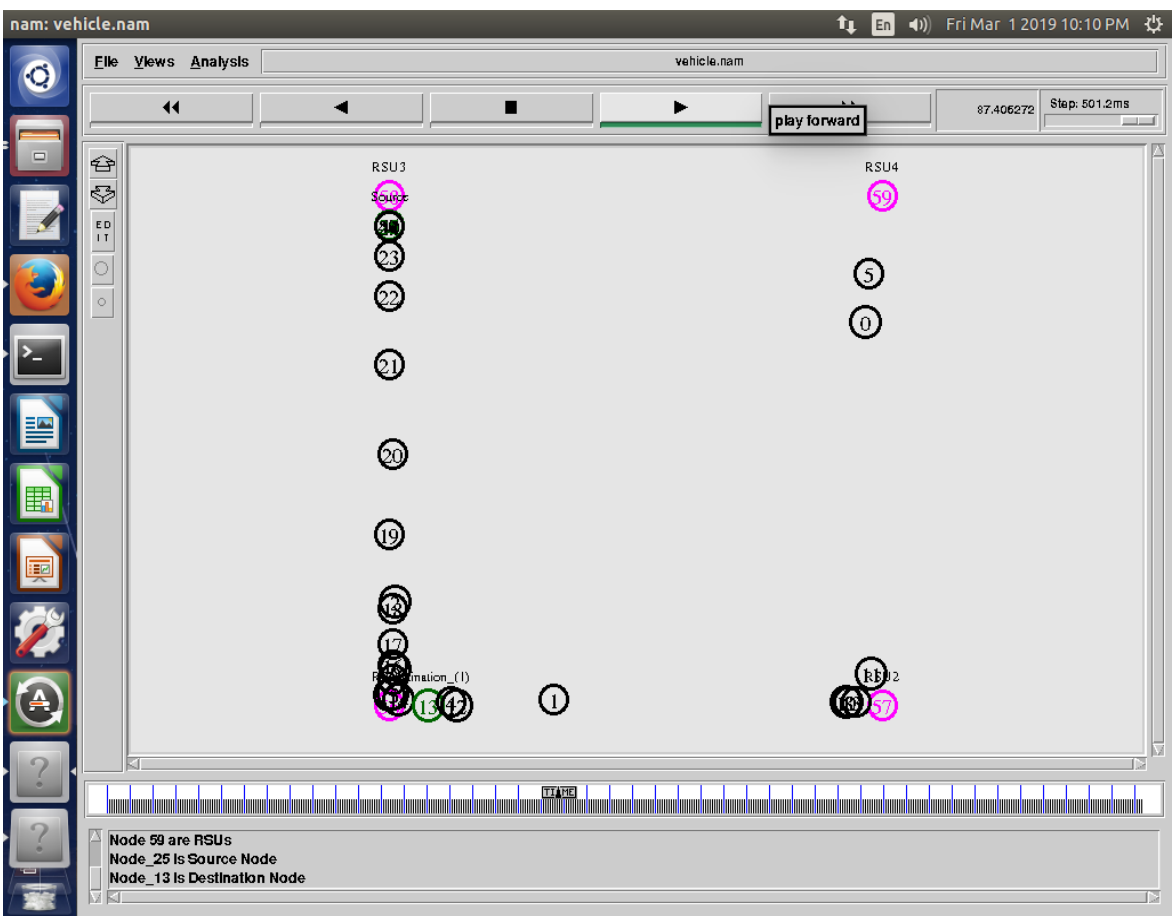
➢ **EXPERIMENTAL SETUP:**

Table 1: simulation parameter

Parameter	Value
Environment Size	2000*2000 meters
Total Number of Nodes	50,100
Node Speed	5m/s, 25m/s, 60m/s, random
Node Type	Highly Mobile Nodes (vehicles)
Packet Type	UDP
Simulation Time	50 s

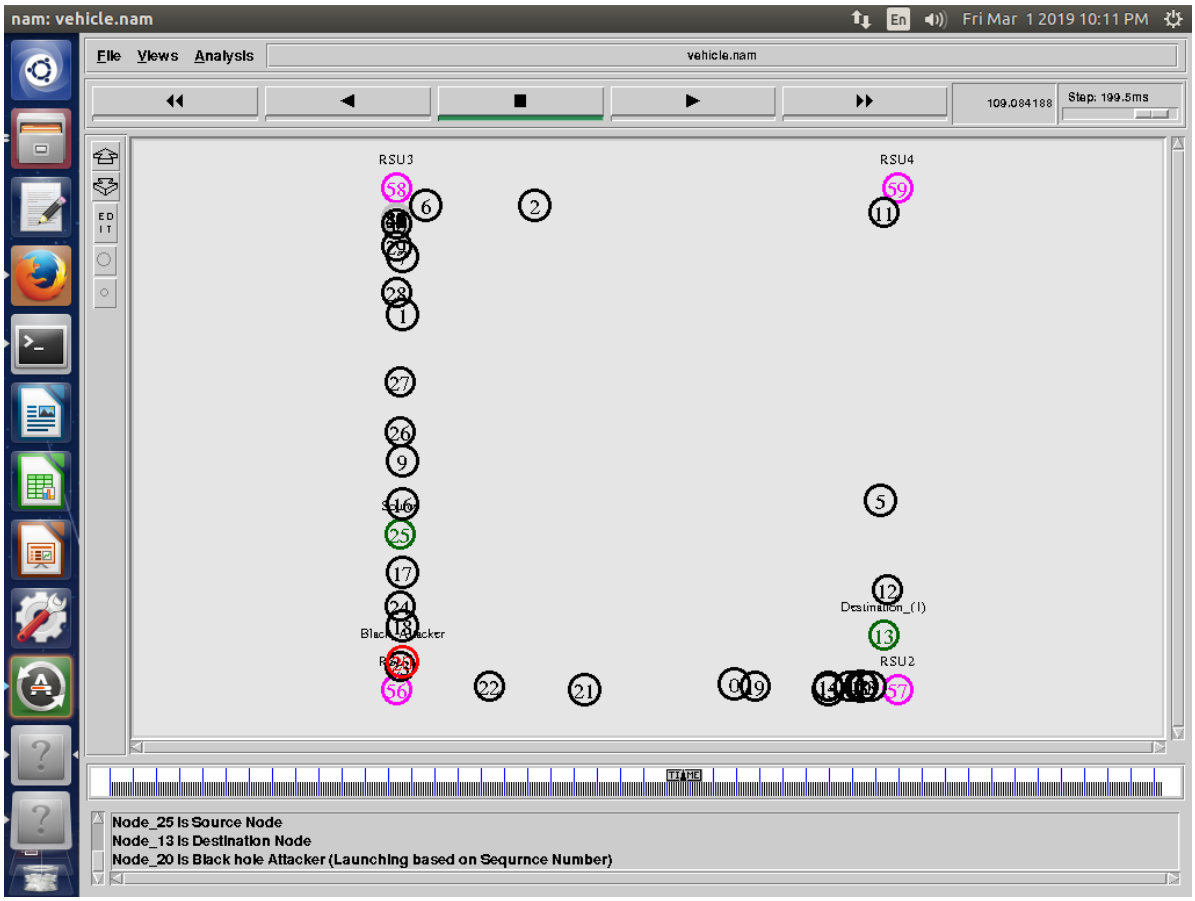
VI. IMPLEMENTATION RESULT:

➢ **Without detection of attacker in DSR**



Attacker node send false route reply that it not contains destination sequence number and also originally it does not contain shortest route. Now source node receives multiple RREP, it accepts false RREP. Now source node send the packets to attacker node and attacker node is drop all the packets.

➢ **Black hole attacker found:**



Node 20 is an attacker node, which node drops the entire packet in the network.

Table 2: result table

	With detection of attacker			Without detection of attacker		
Number of Attacker Nodes	2	4	6	2	4	6
Throughput	0.00103 MB/s	0.00234 MB/s	0.00384 MB/s	0.00057 MB/s	0.00185 MB/s	0.0032MB/s
Packet Delivery Ratio	72.5	76.761	92.063	38.095	63.095	74.603

VII. CONCLUSION

It analyzed possible VANET security threats and mainly focuses on black hole attack .Comparison of reactive routing protocol DSR with or without detection of attacker is carried out. After all experiments in Base Paper, we conclude DSR performance is better than other routing protocols with and without black hole attack. DSR is more scalable than other routing protocols.DSR is better routing protocol to detect & prevent multiple black hole nodes in VANET.

In the future work we will focus on detection of multiple Black hole Attacks using other reactive routing protocols such as AODV and AMODV in VANET.

VIII. ACKNOWLEDGEMENT

I forward my sincere thanks to Prof. Shreya Patel and Prof. Rakesh Shah for there valuable help during the report design of Research Skills. There suggestions were always there whenever I needed it. As supervisor they sparred there valuable time for the in depth discussion on the topics. Also I forward my hearty thanks to other Faculty Members Department of Computer Engineering for their support.

REFERENCES

1. Hanin Almutairi,Samia Chelloug," Anew Black Hole Detection Scheme for Vanets", Copyright © 2014 ACM 978-1-4503- 2767-1/10/10...$10.00.
2. Sai Gautham P, Shanmughasundaram R," Detection and Isolation of Black Hole in VANET ", 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 978-1-5090-6106-8/17/$31.00 ©2017 IEEE
3. Jos´ e Grimaldo, Ramon Marti," Performance comparison of routing protocols in VANETs under black hole attack in Panama City", 978-1-5386-2363 3/18/$31.00 ©2018 IEEE.
4. John Tobin, Christina Thorpe, Liam Murphy, "An Approach to Mitigate Black Hole Attacks on Vehicular Wireless Networks,", University College Dublin, Belfield, Dublin 4, Ireland, 978-1-5090-5932-4/17/$31.00 ©2017 IEEE
5. Afdhal Afdhal, Sayed Muchallil," Black Hole Attacks Analysis for AODV and AOMDV Routing Performance in VANETs", 2017 International Conference on Electrical Engineering and Informatics (ICELTICs 2017)October 18-20, 2017 – Banda Aceh, Indonesia, 978-1-5386-2934-5/17/$31.00 ©2017 IEEE.
6. Arpita Rathod, Prof. Shreya Patel," A Probabilistic Black Hole & Gray Hole Attacks Detection Scheme for Vehicular Ad-Hoc Network", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, DOI: 10.21275/ART20182048
7. Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures," Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)", National Advanced IPv6 Center, Universiti Sains Malaysia Penang, Malaysia,2010 IEEE
8. Ajay N. Upadhyaya, J.S. Shah," Blackhole Attack and its effect on VANET", © 2017, IJCSE.
9. Khattab M. Ali Alheeti , Anna Gruebler, Klaus D. McDonald-Maier ,"An Intrusion Detection System Against Black Hole Attacks on the Communication Network of Self-Driving Cars", 978-1-4673-9799-5/15 $31.00 © 2015 IEEE.
10. Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasubullah, Jamalul-lial bin Ab Manan , "Classes of attacks in VANET", IEEE- 2011.
11. Swati Verma,Bhawna Mallick, Poonam Verma , Impact of Gray Hole Attack in VANET ,IEEE, 2015
12. Sikha Sharma , Er. Shivani Sharma ,"A Review: Analysis of Various Attacks in VANET" ,International Journal of Advance Research in Computer Science, Volume 7 ,No.3 ,May-June 2016.
13. Manjyot Saini , Harijit Singh, "VANET, its Characteristics , Attacks and Routing Techniques: A Survey", International Journal of Science and Research, Volume 5, Issue:5, May 2016.
14. 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.
15. Vinh Hoa LA, Ana CAVALLI ," SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY", International journal on Adhoc Networking Systems, Volume:4, No.2, April 2014.
16. Fiore, M.; Harri, J.; Filali, F.; Bonnet, C. "Vehicular Mobility Simulation for VANETsSimulation" Symposium, 2007. ANSS apos; 07. 40th Annual Volume , Issue , 26 28 March 2007 Page(s):301 – 309