MALICIOUS NODE DETECTION THROUGH AODV IN VANET

Taskeen Zaidi, Shubhang Giri, Shivam Chaurasia, Pragya Srivastava and Rishabh Kapoor

Department of Computer Science and Engg.
Shri Ramswaroop Memorial University, Deva road, Lucknow

ABSTRACT

VANET is a subset of MANET which offers communication between the nodes. VANET is a collection of various dynamic nodes that can change it and configure itself on the network. In Vanet, various routing protocols may be implemented to route the packet and Ad-hoc On-Demand Distance Vector (AODV) is one of the protocol that floods the packets to discover route. In Ad hoc On Demand Vector (AODV) routing protocol for VANET, malicious nodes may distrupt the network and make it difficult for the nodes to communicate. In this paper, AODV Routing Protocol is analysed in vanet with and without malicious attack. The malicious node disrupts the limit and floods the network with false packets. Malicious node will affect the performance of the entire network as it consumes more bandwidth and drops packets which in turn reduce the performance of AODV routing protocol and vanet.

KEYWORDS

VANET, RSU, OBU, ITS, AODV

1. INTRODUCTION AND RELATED WORK

Adhoc network are temporary network in which topology of the network changes dynamically. Various protocols are implemented to study the performance of vanet and to detect the malicious node in a network. Vanets are of high level research interest as it provide reliable and multihop communication dynamically. Security is one of the concerned areas of research because communication is affected due to security. It is a big challenge to secure vanet.

Authors[1] describe about Vehicular Adhoc Network(VANET) and explore the issues related to security and challenges which have to be faced by vehicles due to increasing population. The applications of VANET[2] are Vehicle-to-vehicle(V2V) communication , vehicle-to-infrastructure(V2I) and vehicle-to-pedestrian(V2P). And also explains about the technical solution, policy and legal issues related to vehicle-to-vehicle (V2V) communication. Vehicular Adhoc networks (VANETs) and challenges are well explained[3]. A brief description of CCM-MAC, and its use in wireless networks is well explained in[4]. Authors in [5][12] discussed about the security and issues related to VANET, that how VANET gained the attention of research communities. It has also been discussed about the set of solution for the challenges and problems faced by driver and manufacture in achieving safety of life. Authors [7][8][9] discussed about the

DOI:10.5121/ijasuc.2018.9203

performance of AODV routing protocol and packets loss in the network due to Sink Hole attack and Grey hole attack and techniques to detect both the attacks. A brief overview of Vehicular Ad-hoc networks (VANET)[13] and its routing protocols is discussed. And it is also discussed that how with the help of VANET there may be an intelligent communication among the vehicles and roadside infrastructures. The vehicular networking and its applications that work on the projects related to vehicular networking architectures and protocols used are well described in [15]. The method for realistic time detection of Denial of service attacks in IEEE 802.11 with VANET is well explained in [16]. The main study was about the "jamming" of vehicles and attack detection due to false call. The wireless network and its categories i.e Mobile Ad-hoc Network (MANET), Vehicular Ad-hoc Network (VANET) and Static Adhoc Network (SANET) are well characterised [17]. This paper also explains about performance of routing protocol in the existence of Sybil attack. In paper [18] author describes the whole range of implementation for different types of network that are setup in the various regions. VANET has become an active topic for research and development as it has many scope to improve the road safety and traffic architecture. There is need of scalability, robustness and security in VANET architecture and services. In paper [19][21][29] author describe about the VANET which is the key component of Intelligent Transportation system(ITS) and Internet of Things(IOT). In this paper mathematical approach is also implemented to detect the malicious vehicle and route in VANET using prime approach and remove the waste malicious route. VANET is mainly used for improving the efficiency and safety of transportation [22]. The development of wireless communication in VANET and the attacks in Vanet like Sybil attack which affect the network performance having multiple nodes is well described in [23]. The vehicular network security solution and equipment which are accepted by customers, manufacturers and governments is well discussed in [24]. MANET is a collection of mobile nodes that are formed with ad-hoc network infrastructure. MANET has many routing protocols which are attacked from different attackers. Ad hoc On Demand Vector(AODV) is one of the most suitable protocol for MANET and black hole attack by malicious nodes as described in [25].

Author [27] proposed about the performance analysis of the black hole attack, which is the major problem with the computer networking in VANET and How Ad hoc On Demand Vector (AODV) and Optimized Link State routing work on black hole attack and increase the packet passing. The need of the Vanet in preventing road accidents and providing traffic safety was well described in [28].

Author [30] discussed about the sybil attack that how sybil attack have been appraised as a security threat in ad hoc network. Sybil attack in network lead to steal original identity and multiple dummy identities were created. In paper [33] author discuss how VANET maintained the traffic and self organizing communities of wheeled mobile units which consists of large numbers of trucks, cars and as mall static infrastructure nodes as traffic signals within radio communication range to each other and compared the performance of routing protocol i.e AODV, DSR and Swarm Intelligence. Authors [34][35] describe about VANET as multi-dimensional network in which vehicles are continuously changing their location and tested under a realistic environment including mobility model of vehicles and represents data traffic models.

2. BACKGROUND

2.1 VANET

VANET stands for Vehicular Ad-hoc Network, a system of network which requires no planning. There are two types of vehicle communication system: Vehicle to vehicle (V2V), Vehicle to infrastructure (V2I). Both are “Ad hoc” in nature. This special communication network is called VANET.

Vanet provides information sharing, cooperative driving, internet access, safe, free flow of traffic and having wireless communication between vehicles. Challenges faced are Routing, Security framework and Broadcasting.

Example –

A real life example is giving immediate way for Ambulance, when other vehicles will be there on the road. A notification will be sent to all the vehicles which support Vanet system and accordingly the vehicles will change their way.

2.2 Security attacks in VANET

The connection between nodes is mostly established wirelessly in VANET. This increases the chance of security attacks as every node has the access to other nodes in a network. There are various types of attack that could be incurred in a network. If the security attack would be successful then the connection between the nodes could be disrupted (in many cases) or the nodes would be falsified. It could lead to severe accidents. The types of attacks in VANET are as follows:

1. Sybil attack

In Sybil attack, the attacker node has more than one fake identity which results in getting access to the classified information and disrupting the communication between nodes. In case of VANET, it could lead to fake traffic jams which would cause other nodes to take alternative route.

2. Impersonation Attack

The word “impersonation” means the act to do something by being someone else basically to gain information or to do fraudulent activities. In VANET, node impersonation attack means the attacker node sends the wrong information to another node by changing its identity which can cause accidents and the attacker node can escape away without getting identified.

3. DOS attack

If the DOS attack is implemented in any server then the authentic user cannot access the contents of the targeted system. In VANET, the attacker jams all the medium of communication which results in no availability of network to authentic users.

4. DDOS attack

The aim of the attacker which use Distributed denial of service (DDOS) attack is same as that of DOS attack but the approach is different. In DDOS attack, the attacker attempts to attack from different locations in a distributed manner and the attacker uses different time to send the message.

5. Blackhole attack

Blackhole attack is also known as packet drop attack. As the name suggests, the attacker node attracts other nodes to send the packets through it but it drops the packet instead of forwarding it. Blackhole attack has been demonstrated in this project and has been discussed again in the malicious node[3].

6. Wormhole attack

In wormhole attack, the attacker node captures the packets in a network at a particular location and then tunnels the packets to different location and retransmits. In case of VANET, the shortest route cannot be found out using protocol if wormhole attack is performed in a network.

2.3 Security requirement in Vanet

Message Authentication –

All vehicles and road side units should be properly authenticated for sending notifications to other vehicles.

Traceability –

Ability to obtain vehicle real identity, so that it can be traced and charged for navigation services.

Identity preservation –Real identity of vehicle should be kept private from other vehicles and road side equipment.

Confidentiality –

Information and queries of other vehicles should be kept private; such as navigation results.

Non – Repudiation –

In this scenario, a road side vehicle cannot deny that it has transmitted notification, information must be crucial in it.

Congestion and collision control –

In this case, due to lack of poor communication between vehicles and RSUs (Road side units), a traffic scenario will be created and resulting in accidents, collisions and congestion problem.

2.4 AODV:

AODV stands for Ad-hoc On-demand Distance Vector Routing protocol. It is a routing protocol which is especially used in MANETs and other wireless ad-hoc networks. It is mostly used used where thousands of nodes are present so, suits the best for VANET networks where the number of vehicle nodes will be present in excess amount. The nature of aodv protocol is reactive, that means the route form source to destination is arranged On- demand and it doesn't create any extra traffic for communication along links. The sources (sender and receiver) determine the availability of routes. Sequence numbers are used to ensure the freshness of route. The mechanism of Aodv protocol is such that when a node receives a message and holds a route to a destination node sends a backward message through temporary nodes to the requesting node. The source node that initiated the request follows the route containing least number of hops through other nodes. If the link fails, the routing error is passed back to source node and the process is repeated.

In this project, the demonstration of 6 nodes is shown, starting from 0 to 5. The channel type is wireless and model is radio propagation model. The maximum limit of 50 nodes is maintained. The color of node 0 is blue, 1 is red, 2 is tan, 3 is black, 4 is brown and 5 is blue. The shape of every node is circle. After that, the configuration is done and flow is set up. The animation would be done using the network animator (nam). The delay time is set up at 2.0ms.

2.5 NS2

NS2 is an event simulator which is used to simulate real time network. This tool is used by researchers and scientists for monitoring network performance. NS2 is written in C++, TCL and object oriented TCL is also used in NS2. The NS2 simulator is free and represents complex scenarios. The scenario testing will be easy as it supports various protocols and platforms with modularity. In the current work VANET simulation scenario with and without malicious node is represented through NS2 tool.

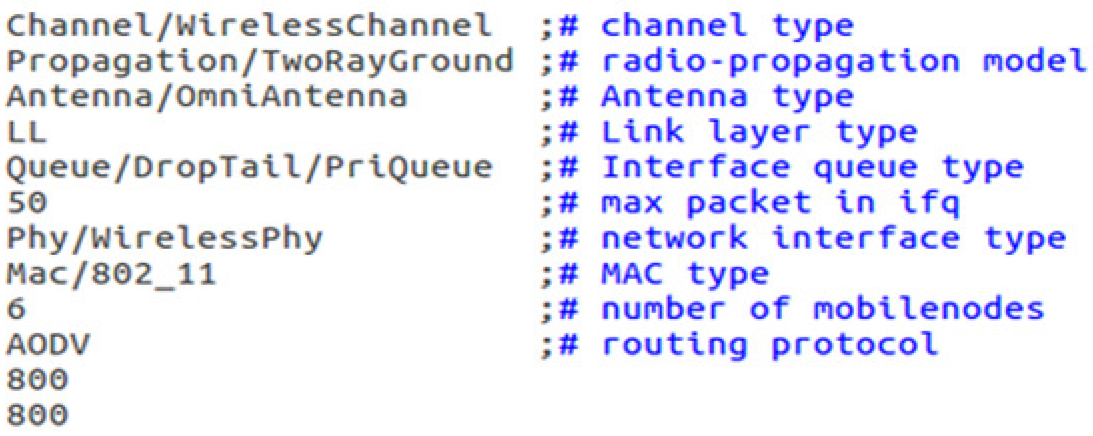
3. MALICIOUS NODE DETECTION IN VANET

As vanet is composed Vehicles and RSU and the vehicles and RSU which is willing to participate in network will be registered with certifying authority and then a unique id is assigned to the vehicle. RSU is maintained by any trusted party or government organizations. If any malicious or illegal node is detected, it will be detected by AODV protocol.

To detect malicious node Certifying authority receives vehicle entry form the RSU and Certifying authority verifies the information and assign a vehicle id to the vehicle. The RSU and vehicle communicate with each other. If any vehicle id does not match with the registered id then Certifying authority will detect it as malicious node.

4. EXPERIMENTAL RESULTS

We used Network Simulator-2.34 to simulate our proposed scheme.



```
Channel/WirelessChannel  ;# channel type
Propagation/TwoRayGround ;# radio-propagation model
Antenna/OmniAntenna      ;# Antenna type
LL                       ;# Link layer type
Queue/DropTail/PriQueue  ;# Interface queue type
50                       ;# max packet in ifq
Phy/WirelessPhy          ;# network interface type
Mac/802_11               ;# MAC type
6                        ;# number of mobilenodes
AODV                     ;# routing protocol
800
800
```

Figure 1: Simulation parameters

As shown in figure 1, Area nodes are plotted according to random mobility model. In this model, every node moves randomly within the specified network range. Simulation is performed with a network size of 800m x 800m and 6 nodes.

Pause Time: After the node reaches to its target location and before going to another arbitrary location, the pause time is taken as 2.0 seconds.

Traffic Type: The communication traffic utilized are consistent bit rate (CBR) association with an information rate of 50 pack for every second. We have simulated with selfish nodes in the network.

As the nodes are mobile so for implementation of mobility a routing protocol AODV is used and at the initial the network is protected from selfish node as shown in figure 2 and 3.

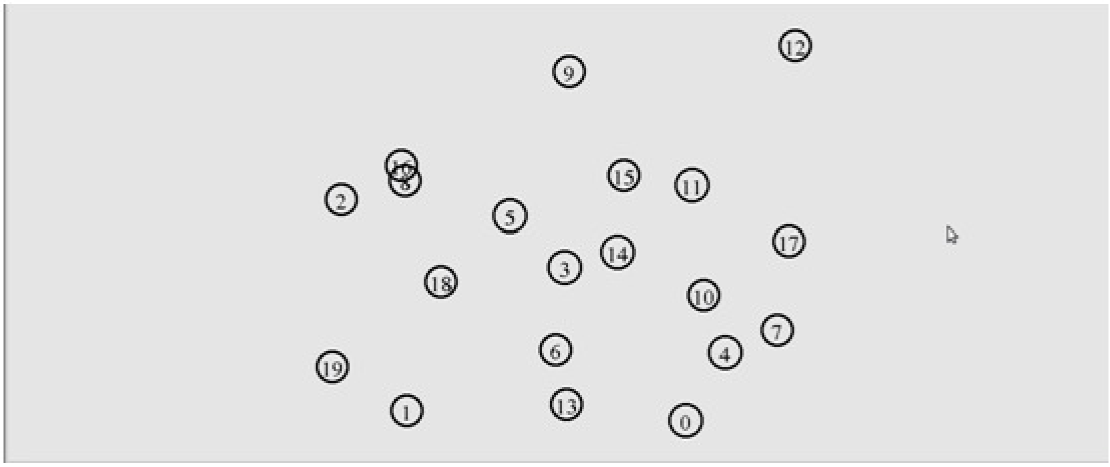
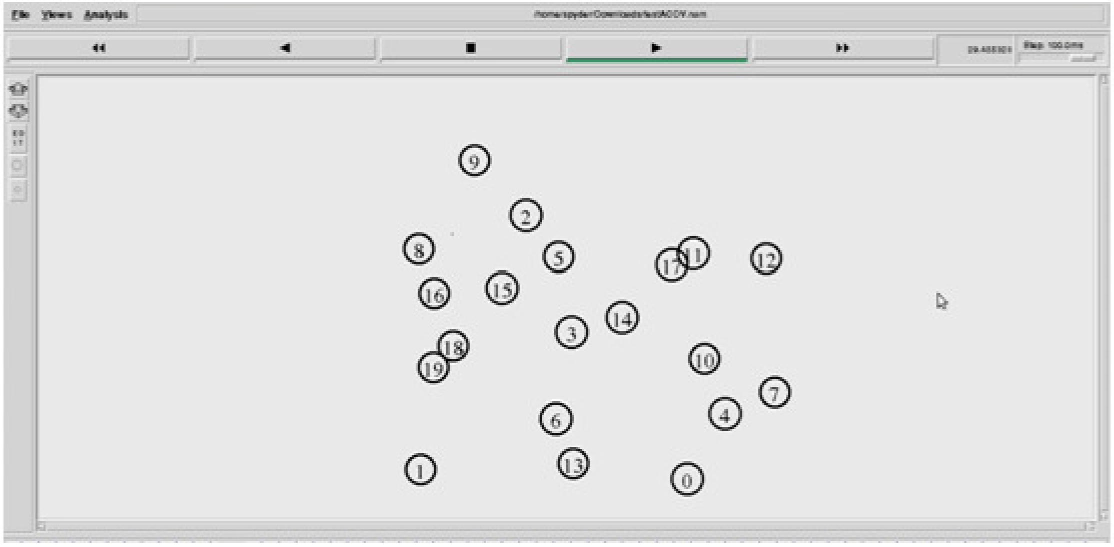


Figure 2: Simulation without malicious node in the network



Firstly the simulation of VANET without malicious node detection is shown in figure 2 and then detects the malicious node as shown in figure 3(a,b,c) and 4.

Node 1 is set as malicious node by following code:

```
$ns at 0.0 "[$n(1) set ragent_] malicious"
```

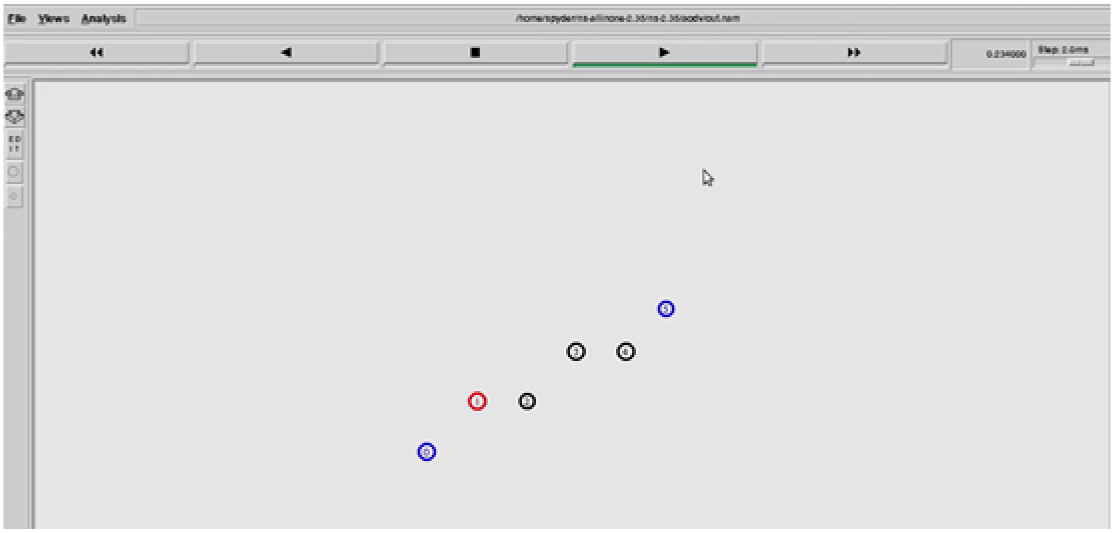


Figure 3(a): Simulation with malicious node in the network

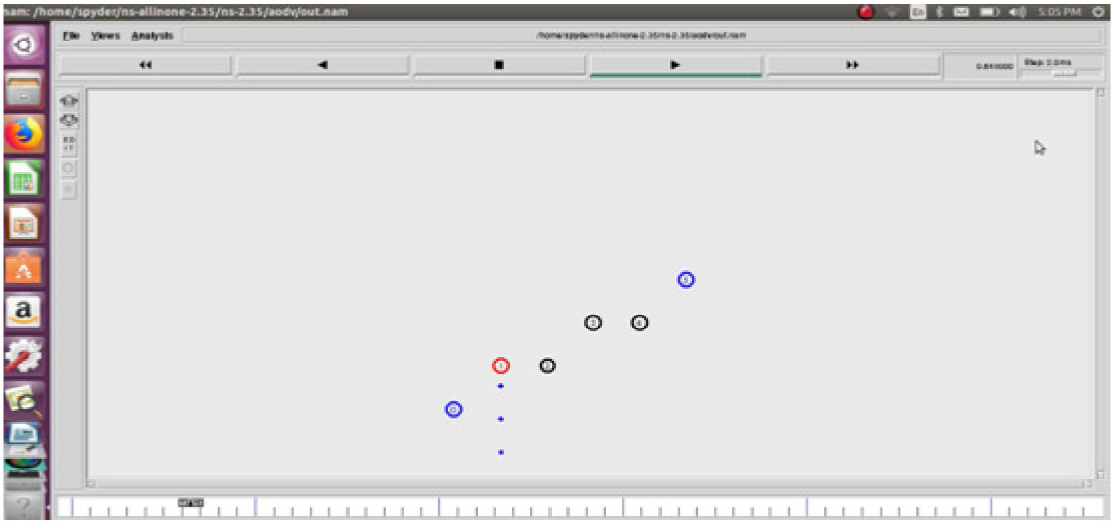


Figure 3(b): Simulation with malicious node in the network

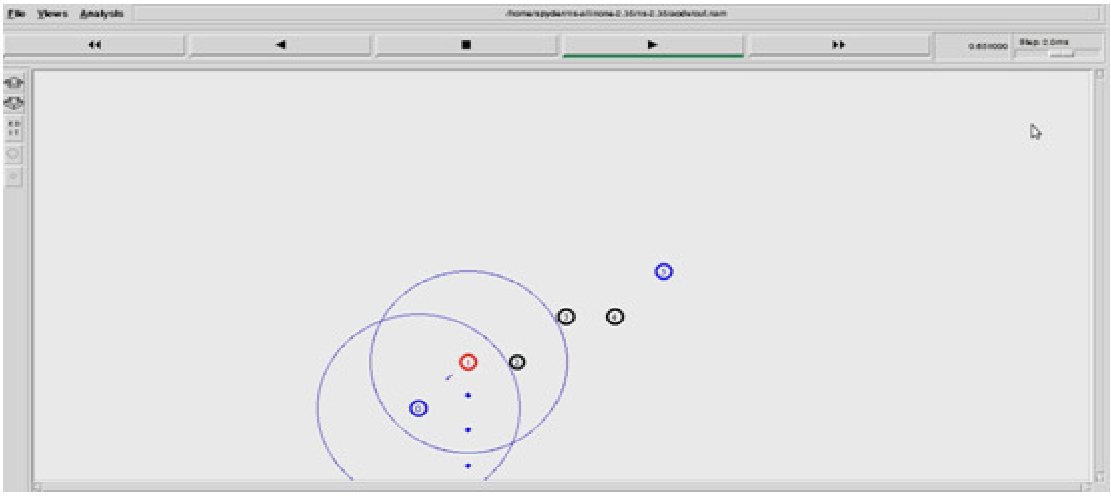


Figure 3(c): Simulation with malicious node in the network

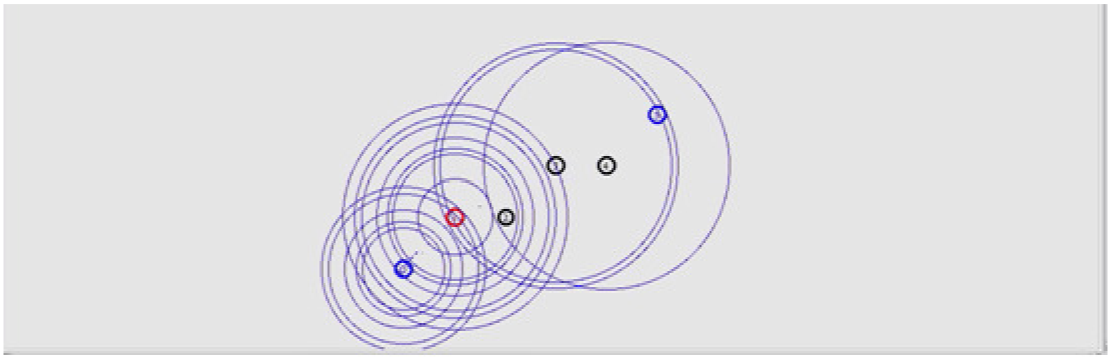


Figure 4.Simulation with malicious node in the network

5. CONCLUSION

In this work aim was to detect malicious node in the network based on the behavior of node. As nodes are mobile in nature so for mobility nodes are implemented with the help of routing protocol AODV .Mac layer and Physical layer follows IEEE 802.11 standards. As malicious node is the main security threat that affect the performance of the AODV routing protocol. In the proposed work, we easily recognized vanet with malicious node and in future we will extend our work in he performance estimation of vanet with and without malicious node and we will also evaluate network performance by considering parameters like bandwith, delay, packet dropped , throughput etc. In the future work we will test this network with different mobility parametrs to secure our network from threats as well as we will identify different kinds of attacks on our network to increase the performance.

REFERENCES

[1] Samara and Al-Salihy,"Security issues and challenges of vehicular ad hoc networks(VANET),Proceedings of the 4th International Conference on New Trends in Information Science and Service Science(NISS '10),May 2010 Gyeongju-si, Republic of Korea 3933982-s2.0-77957823974 Google Scholar.

[2] W. Zeng, H. Yu and C. Lin. (2013, Dec 19),"Readiness of V2V Technology for Application"[online] Available:www.nhtsa.gov.

[3] J. Harri, F. Filali and C. Bonnet, "Mobility models for vehicular ad hoc networks: a survey and taxonomy", IEEE Communications Surveys and Tutorials, vol. 11, no. 4, pp. 19-41, 2009.

[4] A. Nasipuri,J. Zhuang and S. R. Das,"A Multichannel CSMA MAC Protocol for Multihop Wireless Networks", Proc. of IEEE Wireless Communications and Networking Conference (WCNC), September 1999.

[5] Ghassan Samara, wafaa. A.H, Al-Salihy and R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks(VANET)", IEEExplore.

[6] Priya Sharma and Amarpreet singh,"Enhanced attacked packet detection algorithm used for detecting attack in Vanet",IRF International Conference, 27th September 2015, Pune, India.

[7] Avinash P. Jadhao and Dr. D.N. Chaudhari, "Security Aware Adhoc on Demand Distance Vector Routing Protocol in Vehicular Adhoc Network",in International journal for Engineering applications and Technology, Vol. 2, Issue 12, December 2015.

[8] Rauki Yadav, Naveen Hemrajani, Dinesh Goyal and Savita Shivani, "Vulnerabilities, Attacks and their Detection Techniques in Ad hoc Network", in International Journal of Computer Applications, Volume 2, Issue 11, December 2011.

[9] Naresh kumar, R.Mustary, R.P. Chander and Moghal Nisar Ahmed Baig, "performance evaluation of VANET for intelligent transportation system", in World Journal of Science and Technology, Volume 2 Issue 10, January 2013.

[10] Charles Harsch, Andreas Festag and Panos Papaimitratos,"Secure Position-Based Routing for VANETs", in IEEE, Vol.2, Issue 12, November 2007.

[11] Eichler and Stephan, "Strategies for Context-Adaptive Message Dissemination in Vehicular Ad Hoc Networks", in 3rd Annual International Conference on Mobile and Ubiquitous Systems. 2006.

[12] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and JP Hubaux,"Eviction of Misbehaving and Faulty Nodes in Vehicular Networks", IEEE Magazine, vol. 10, October 2007.

[13] V. Namboodiri and L. Gao,"Prediction-based routing for vehicular ad hoc networks", IEEE Trans. Vehicular Tech.,vol. 56, no. 4, pp. 23322345, 2007.

[14] Spaho E., lkeda M., Barolli L., and Xhafa F."Performance Evaluation of OLSR and AODV protocols in a VANET", crossroad scenario in proceeding of the IEEE 27th Advanced Information Networking and Application (AINA) Conference pp. 577- 582, 25-28 March 2013.

[15] Karagiannis, Georgios, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan, Kenneth Lin, and Timothy Weil," Vehicular networking", A survey and tutorial on requirements, architectures, challenges, standards and solutions, IEEE Communications Surveys & Tutorials, 2011.

[16] Lyamin, N. Vinel, A. Jonsson and M. Loo, "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks", Communications Letters, IEEE , vol.18, no.1, pp.110,113, January 2014.

[17] Li He and Wen Tao Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs", Computer Science and Automation Engineering (CSAE),2012 IEEE International Conference on , vol.3, no., pp.261,265, 25-27 May 2012.

[18] Harsch,C.Festag, and Papadimitratos P.," Secure position-based routing for VANETs", In Proceedings of IEEE 66th vehicular technology conference (VTC-2007), Fall 2007 (pp. 26-30), September 2007.

[19] Jinyuan, S. Chi, Z. and Yuguang. F.,"An ID-based framework achieving privacy and non-repudiation", In Proceedings of IEEE vehicular ad hoc networks, military communications conference (MILCOM 2007) (pp. 1±7), October 2007.

[20] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin and Aamir Hassan,"Vehicular Ad Hoc Networks (VANETs)", Status, Results, and Challenges ,in Telecommunication Systems, Volume 50,Issue 4, pp 217-241, 2012.

[21] J.T. Isaac, S. Zeadally and J.S. Cmara,"Security attacks and solutions for vehicular ad hoc networks", in IET Communications, pp. 894-903, 2009.

[22] IAhmed Soomro, H.B.Hasbullah and J.lb.Ab Manan,"Denial of Service (DOS) Attack and Its Possible Solutions in VANET", in WASET, issue 65, 2010 ISSN 2070-3724.

[23] Gilles Guette and Bertrand Ducourthial, "On the Sybil attack detection in VANET", in IEEE International Conference on Mobile Ad hoc and Sensor Systems, 2007, pp. 1-6.

[24] B. Parno and A. Perrig,"Challenges in Securing Vehicular Networks", in Hot Topics in Networks (HotNets-IV), 2005.

[25] H Fussler, S Schnaufer, M Transier and W.Effelsberg,"Vehicular Ad-Hoc Networks: From Vision to Reality and Back", Proc. Of IEEE Wireless on Demand Network Systems and Services, 2007.

[26] R.A. Raja Mahmood andA.I. Khan, "A Survey on Detecting Black Hole Attack in AODV-based Mobile AdHoc Networks", in International Symposium on High Capacity Optical Networks and Enabling technologies, pp. 1-6,2007.

[27] Vimal Bibhu, Kumar Roshan, Kumar Balwant Singh and Dhirendra Kumar Singh, "Performance Analysis of Black Hole Attack in Vanet", in Computer Network and Information Security, pp.47-54,2012.

[28] Adil Mudasir Malla and Ravi Kant Sahu, "Security Attacks with an Effective Solution for DOS Attacks in VANET", in International Journal of Computer Applications, March 2013, Volume 66 - Number 22.

[29] Yun-Wei Lin1, Yuh-Shyan Chen and Sing-Ling Lee ,"Routing Protocols in Vehicular Ad Hoc Networks", A Survey and Future Perspectives, in 2010.

[30] Kumud Dixit, Krishna Kumar Joshi and Neelam Joshi "A Novel Approach Of Trust Based Routing To Select Trusted Location In AODV Based VANET", A Survey in 2015.

[31] Xia Feng1, Chun-yan Li2, De-xin Chen3 and Jin Tang1,"A method for defensing against multi-source Sybil attacks in VANET", in January 2016.

[32] Manjunatha T. N, Sushma M. D and Shivakumar K. M,"Security Concepts and Sybil Attack Detection in Wireless Sensor Networks", in april 2013.

[33] S.S.Manvi, Kakkasageri, M.S.Mahapurush and C.V., "Performance Analysis of AODV, DSR, and Swarm Intelligence Routing Protocols In Vehicular Ad hoc Network Environment", In International conference on future Computer and Communication., pp. 21-25, April. 2009.

[34] Wex p Breuer, J. Held, A. Leinmuller and T. Delgrossi, "Trust Issues for Vehicular Ad Hoc Networks", IEEE,VTC Spring 2008., pp. 2800-2804, May.2008.

[35] F. Karnadi and Z. Mo, "Rapid Generation of Realistic Mobility Models for VANET", in a proc. IEEE Wireless Communications and Networking Conference, 2007.