PREVENTION OF DENIAL OF SERVICE ATTACK ON DYNAMIC SOURCE ROUTINGVANET PROTOCOL

Komal Rani[1], **Meenakshi**[2]
[1]*M.Tech Scholar, Central University of Punjab*
er.komrani@gmail.com
[2]*Centre for computer science and Technology, Central University, Bathinda*

Abstract:

Vehicular Ad Hoc Network (VANET) is a kind of Wireless Ad hoc Network in which node has high mobility, and thus the topology of the network is highly dynamic. VANET has thepotential to increase road safety, improve traffic efficiency as well as comfort to both drivers and passengers. There are different types of attacks possible on VANET. In this paper, implementation and prevention of DOS attack is done on topology based protocol- Dynamic Source Routing (DSR). The performance of DSR protocol is evaluated under different scenarios using Network Simulator (NS2), Simulation of Urban Mobility (SUMO) simulator and Mobility model generator for Vehicular networks(MOVE). The prevention scheme Queue Limiting Algorithm (QLA) proposed by Sinha & Mishra is implemented to prevent Denial of Service attack. The results show that DSR has high throughput and packet delivery ratio at low density of nodes and the value of these parameters become low at high density of nodes. The prevention scheme is capable to prevent DOS attack.

Keywords: *VANET, DSR, OBU, QLA, DOS*

--***--

I. INTRODUCTION

A Vehicular Ad hoc Network (VANET) is a type of Mobile Ad hoc Network (MANET) in which vehicle communicate with nearby vehicles and roadside equipment. In this type of network, vehicles are considered as communication nodes and belongs to a self-organizing network i.e. without prior screening or knowledge of each other's presence, they can communicate with each other. Its architecture consists of three components: On-Board Units (OBUs) which are radio devices installed in vehicles used for exchanging information, Application Unit (AU) is a dedicated device which is located within the OBU or can be connected to the OBU through a wired or wireless connection. . It communicates with the network using Onboard Unit (OBU)and Road Side Units (RSUs) are devices placed along the road and constitute the network infrastructure.VANETs differ from MANETs in many ways: high node mobility, thelarge scale of networks, a high dynamic topology, unreliable channel conditions, and frequent network fragmentation [2]. It has been observed that most of thepeople die and injured due to road accidents. Therefore to prevent all these mishappenings, VANET came into existence.VANET provides a wide range of both safety and non-safety applications [3].

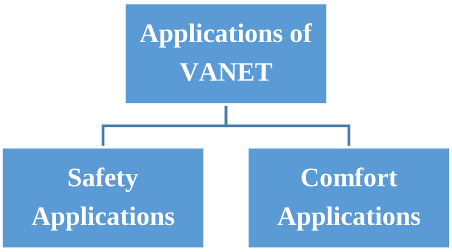


Figure1. Applications of VANET

Safety application provides safety to the passengers such as lane change warning, collision detection, traffic jam, etc. While non-safety application provides comfort and commercial applications to the road users such as audio/video exchanging, electronic payments, route guidance, weather information, internet access,etc [3].

Besides this, there are many challenges that need to be addressed when creating a vehicular ad hoc network are Dynamic topology and Signal fading.The wireless communication in VANETs suffers from issues like noise, path loss and interference as in MANETs.

II. VANET ROUTING PROTOCOLS

A routing protocol governs the way to exchange an information between sender and receiver; it includes the procedure in establishing a route, decision to forward the packets, and maintaining the route or recovering from routing failure. A large number of routing protocols have been developed to provide fast and secure routing of data. But each protocol is suitable for a different scenario and no protocol is universally accepted to be suitable for all the situations [1]. There are five categories of VANET protocols- Topology based protocols, Position based protocols, Cluster based protocols, Geo cast based protocols and Broadcast based protocols.

The topology based protocols use link's information to forward the packet. It is further categorized into three types: Proactive, Reactive and Hybrid protocols. On the other hand, position based protocol uses the position of nodes to forward the packet to thedestination. Cluster based protocols divide the network into agroup of nodes called clusters according to some characteristics like same speed, same direction, etc. In Geo Cast based protocols, thepacket is delivered from thesource node to only those nodes that are lying within ageographical region called Zone of Relevance. Broadcast based protocols are used for transmitting the packets to all the nodes [4].

III. DYNAMIC SOURCE ROUTING (DSR)

It is topology based reactive routing protocol which maintains routes only when needed. DSR protocol consists of two mechanisms i.e. Route Discovery and Route Maintenance. Route discovery involves the Route Request (RREQ) and Route Reply packets (RREP). Whereas Route Maintenance involves Route Error packets (RERR).Route Discovery and Route Maintenance phases are discussed as follows [7]:

- **DSR Route Discovery:** This mechanism involves the source node to discover a route to reach to destination node. Firstly, source node S sends out a RREQ message with the unique request ID to all of its neighbors. If receiving nodes are not a target, then they add themselves to the route and forward the message to their neighbors. If a receiving node is the destination then it sends a REPLY message containing the full route to sender. The target (or destination) node receives same RREQ packets from different paths, but it chooses thebestroute (based on less number of hops) and sends the REPLY message to the sender along that route. The source and destination node will store this route information in their routing table. The source node uses this route to send packets to destination [4].

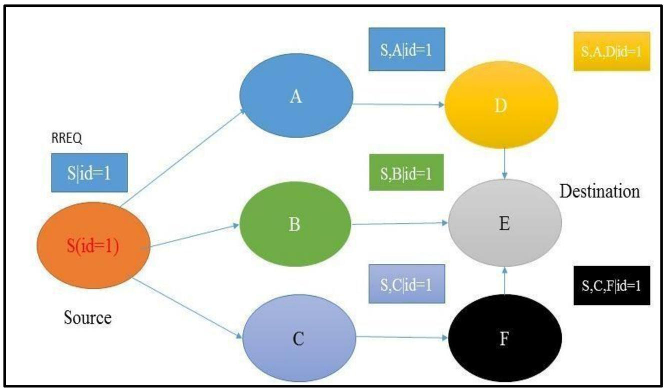


Figure2. Route Request Message

As shown in Figure 2, S is the source node, and E is the destination. Source S has three neighboring nodes named as A, B and C which comes in its transmission range. Node S will broadcast ROUTE REQUEST message whichis received by three neighboring nodes A, B and C. Each ROUTE REQUEST message identifies the initiator by unique request ID and thetarget of the Route Discovery. It also contains a record of each

Intermediate nodes by specifying their names, through which this particular copy of the ROUTE REQUEST message has been forwarded. When the target node E receives three ROUTE REQUEST message, it sends a ROUTE REPLY message along best route to the ROUTE discovery initiator node S with a copy of the accumulated route record from the ROUTE REQUEST. In Figure 2, route along S, B, E is chosen. [7].

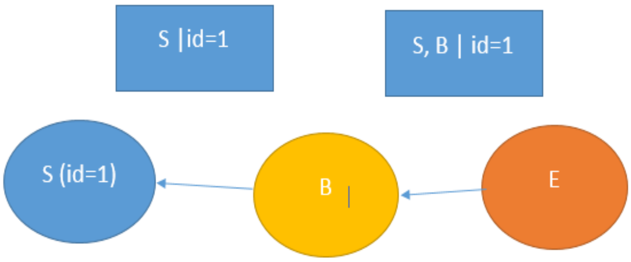


Figure 3. Route Reply message

As shown in Figure 3, destination node E sends route reply message to source S through route E, B and S. The source node uses this route to send subsequent packets to destination E after receiving ROUTE REPLY message.

- **DSR Route Maintenance:** It is the mechanism by which source node is able to detect that source route is broken. This mechanism involves **Link Status Monitoring (LSM)** and **Route Repairing (RR)** phases. LSM is used to check whether the route is active or not. If link breakage is found during LSM, then repairing of routes is the next task to be performed. This phase involves thedissemination of **Route Error (RERR)** message and route rediscovery for brokenroute. After detecting link breakage, the node which has detected a link breakage searches its Route Cache for an alternative route. If it finds an alternative route, then sends data along that route otherwise informs the original sender about broken route through passive acknowledgment. The original sender then searches an alternative route in its route cache. This process is known as Packet Salvaging. In case of unsuccessful Packet Salvaging, source node initiates a new route re-discovery process [4-7].

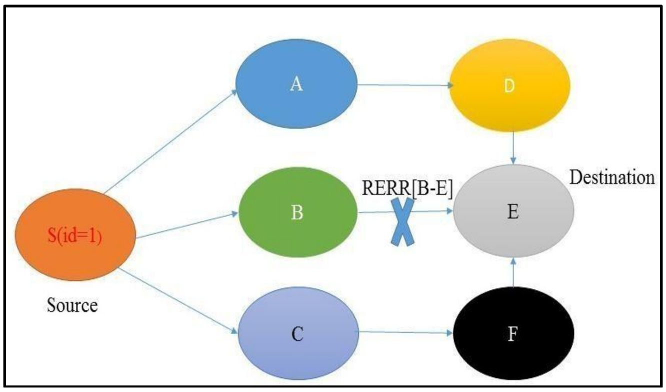


Figure 4. Route Error Message

In Figure 4, node B is unable to send apacket to node E due to link breakage. It then searches for an alternative route in its route cache to reach to node E. If it finds an alternative route in theroute cache, then sends data along that route. Otherwise sends the Route error message (RERR) to thesender (S) to inform about broken link which then searches its route cache to find an alternative route. If it is not found, then sender (S) starts new rediscovery process [4].

IV. ATTACKS ON VEHICULAR AD HOC NETWORK

In VANET, various challenges exist like dynamic topology, open atmosphere and the absence of centralized infrastructure makes it vulnerable to various types of attacks. Attacks are categorized into two types: Passive and active attacks [5].

In apassive attack, an attacker monitors the traffic but does not modify it. For example Eavesdropping, Traffic analysis.

In active attack, the attacker replay old messages, modify messages in transit, or delete selected messages. For example: Black hole attack, Denial of Service,etc**.**

V. DENIAL OF SERVICE (DOS) ATTACK

In this type of attack, the attacker prevents the availability of thenetwork by jamming the channel or to create some problems for the nodes in accessing the network. The main objective of the attacker is to degrade the performance of a network by preventing a legitimate user from accessing the network services and the network resources [8].

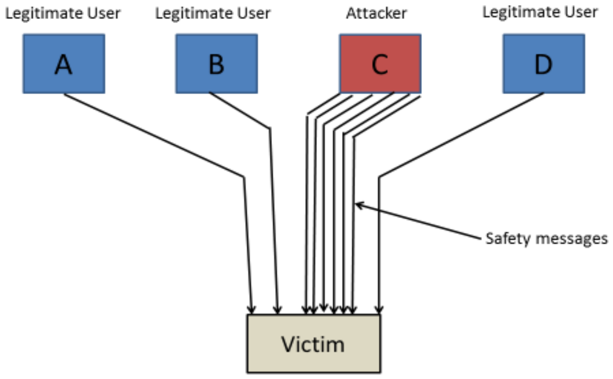


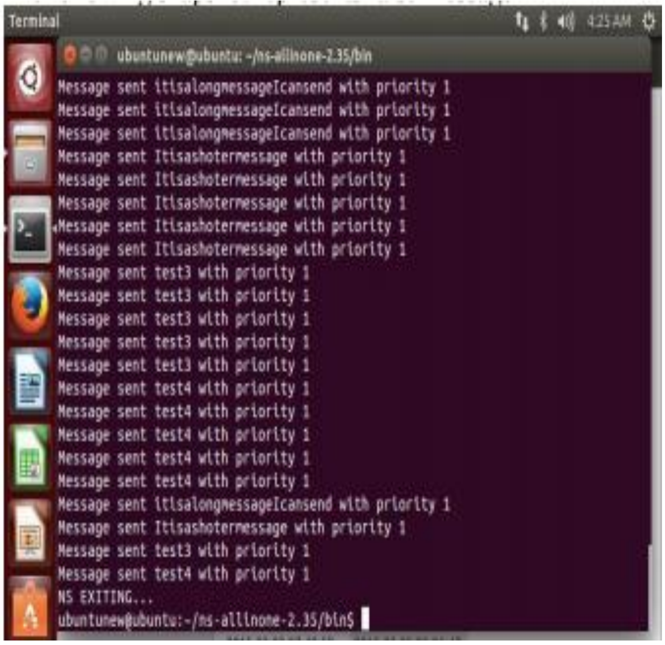
Figure 5. DOS attack

The above figure shows three legitimate users A, B and D. C is an attacker. Attacker sends a large number of safety messages as compared to thelegitimate users. As safety messages has higher priority over other messages. So, most ofbandwidth of thevictim is consumed by attacker that makes victim node unable to respond to legitimate packets. As a result, DOS attack occurs.

VI. IMPLEMENTATION OF DOS ATTACK

As safety messages have high priority over other messages. DOS attack is performed by sendinga multiple number of false safety messages to the victim node which keeps the victim node busy in processing these messages and thus the victim node will be unable to respond the legitimate packets. As a result, denial of service occurs.

The following snapshot represents false message



```
Message sent itisalongmessageIcansend with priority 1
Message sent itisalongmessageIcansend with priority 1
Message sent itisalongmessageIcansend with priority 1
Message sent Itisashotermessage with priority 1
Message sent Itisashotermessage with priority 1
Message sent Itisashotermessage with priority 1
Message sent Itisashotermessage with priority 1
Message sent Itisashotermessage with priority 1
Message sent test3 with priority 1
Message sent test3 with priority 1
Message sent test3 with priority 1
Message sent test3 with priority 1
Message sent test3 with priority 1
Message sent test4 with priority 1
Message sent test4 with priority 1
Message sent test4 with priority 1
Message sent test4 with priority 1
Message sent test4 with priority 1
Message sent itisalongmessageIcansend with priority 1
Message sent Itisashotermessage with priority 1
Message sent test3 with priority 1
Message sent test4 with priority 1
NS EXITING...
ubuntunew@ubuntu:~/ns-allinone-2.35/bin$
```

Figure 6. DOS attack implementation

The above snapshot (Figure 6) represents the false priority messages “Message sent it is along message I can send with priority1”, “Message sent test3 with priority1” and “Message sent test4 with priority1”.These messages have given high priority over other traffic packets by making changes in priority_packet.cc. So, these messagesmake receiver busy in processing these messages due to its high priority.

VII. IMPLEMENTATION OF PREVENTION SCHEME

Queue Limiting Algorithm (QLA) has been implemented proposed by Sinha & Mishra, 2014 to prevent DOS attack on DSR protocol.

In QLA, thelimit on receiving the safety messages is imposed on victim node. After that limitis crossed, the safety messages will be lost because that is not accepted by victim node. In this way, victim node can easily communicate and respond to legitimate packets. Thus, the denial of service is prevented. Detail of QLA is given in [15].

VIII. SIMULATION ENVIRONMENT:

The simulation was performed using ns2.35and SUMO, and MOVE on Linux Ubuntu 12.04 operating system or Intel Core-i7 processor.

In this paper, DSR protocol is evaluated in three conditions: normal condition (without DOS attack), under DOS attackand after applying prevention scheme w.r.t. performance metrics such as Throughput, Packet Delivery Ratio, End to End Delay and Goodput by taking 16,24 and 50 nodes having speed 40Km/hr.

IX. RESULTS AND ANALYSIS

a) Throughput comparison of DSR without DOS attack, under DOS attack and after prevention scheme

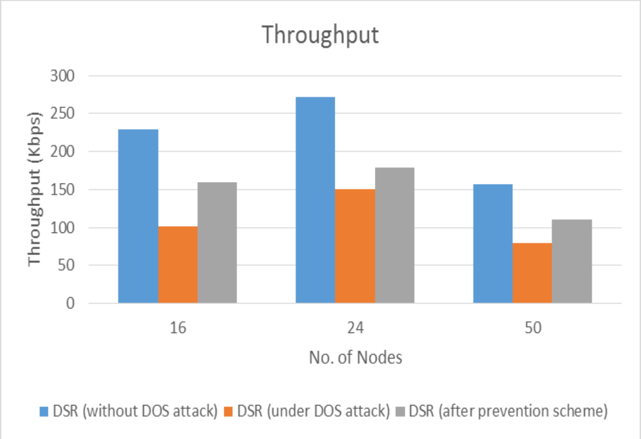


Figure 7. Throughput for different no. of nodes

b) Packet Delivery Ratio comparison of DSR without DOS attack, under DOS attack and after prevention scheme

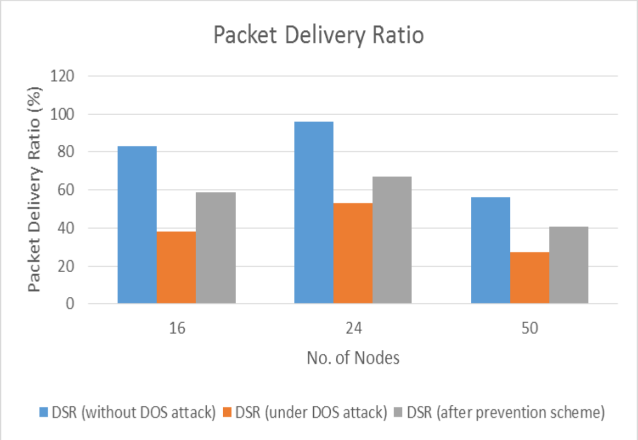


Figure 8. Packet Delivery Ratio for different no. of nodes

c) End to End Delay comparison of DSR without DOS attack, under DOS attack and after prevention-scheme

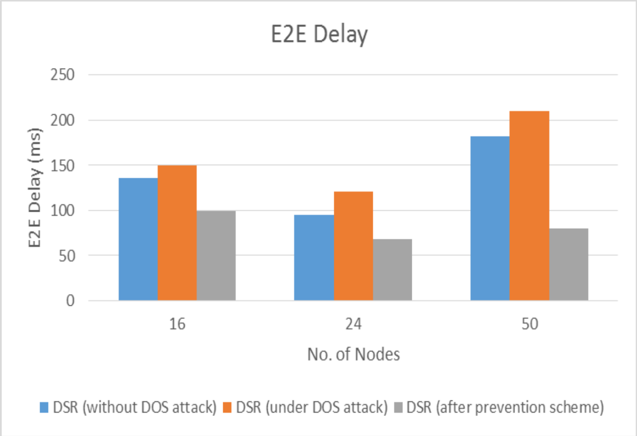


Figure 9. End to End Delay for different no. of nodes

d) Good put comparison of DSR without DOS attack, under DOS attack and after prevention scheme

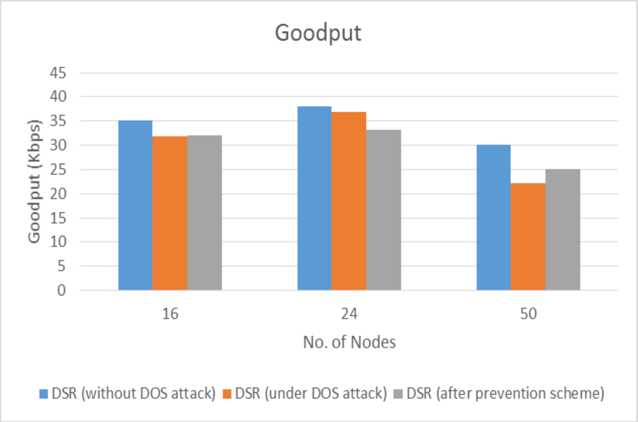


Figure 10. Goodput for different number of nodes

- **Analysis:** Under all three conditions, Throughput increases with increase in number of nodes from 16 to 24 because small increase in number of nodes lead to increase in intermediate nodes which are used to reach the packets to destination in less time.But, throughput decreases at high density (i.e. 50 number of nodes or more) in all three conditions (without DOS attack, under DOS attack and after DOS prevention) because more number of nodes try to access the common medium, thus collision increases thereby increases packet loss and it leads to decrease in Throughput.The throughput of DSR under attack decreases because the false messages sent by the attacker restricts the legitimate packets from reaching the destination. So, Throughput will be degraded.After applying prevention scheme, Throughput increases.
- With asmall increase in thenumber of nodes from 16 to 24, theaverage number of hops used to deliver the packets to destination increases which contribute to transmit the packet successfully.So, PDR increases. PDR decreases at high node density (i.e. 50 number of nodes or more) in DSR because more number of nodes try to access the common medium, thus number of collision increases and thereby increases packet loss and decreasing the delivery of packets to destination.Packet Delivery ratio decreases under attack because as theattack happens, less no. of legitimate packets reach to thedestination. In this way, received packets become less. As a result, PDR decreases. The Packet Delivery Ratio increases after applying prevention scheme because number of legitimate packets reached to destination increases.
- End to End Delay decreases at 24 nodes because a sufficient number of intermediate nodes take less processing time while forwarding the packet to thedestination. In DSR, each node searches a route cache to forward the packet. So, as the number of nodes increases, total time to reach the packet to destination increases. As a result, End to End Delay increases at high node density (50 or more). End to End Delay increases under DOS attack because as theattack

happens, legitimate packets get lost. The sender initiates route rediscovery process again and again to send the packet which increases end to end delay. After applying prevention scheme, End to End Delay decreases.

- Good put value depends on original data excluding route informationGoodput also decreases under DOS attack and increases after applying prevention scheme.

CONCLUSION

DSR is topology based protocol where each node maintains a route cache and it searches a route cache to forward the packet. As the number of nodes increases, thetime taken to reach the packets to destination increases. As a result, Throughput and Packet Delivery Ratio decreases at high density. The simulation results show that DSR is more affected under DOS attack. The prevention scheme Queue limiting Algorithm proposed by Sinha & Mishra has been implemented and it is found that it is capable to prevent VANET from DOS attack. In future, other categories of protocols such as cluster based protocols, Geo cast based protocols, etc. can be analyzed under three different conditions by applying the prevention scheme i.e. Queue Limiting Algorithm (QLA).

REFERENCES

[1] K. C. Lee, U. Lee, and M. Gerla, “Survey of Routing Proto-cols in Vehicular Ad Hoc Networks,” in Advances in Vehicular Ad-Hoc Networks: Developments and Challenges, M. Watfa. IGI Global, 2010, ch. 8, pp. 149–170.

[2] F. Li and W. Yu, “Routing in Vehicular Ad Hoc Networks: A Survey,” Vehicular Technology Magazine, IEEE, vol. 2, no. 2, pp. 12–22, 2007.

[3] Venkatesh, A. Indra and R. Murali, “Vehicular Adhoc Networks (VANETs): Issues and Applications”, Journal of Analysis and computation, Vol. 8, No. 1, 2012, pp.31-46.

[4] D. B. Johnson, D. A Maltz, J. Broch, DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, Ad Hoc networking 2001; Vol 5, pp. 139-172, 2001.

[5] M. Raya, J. Pierre, Hubaux, ”Securing vehicular ad hoc Networks ”Journal of Computer Security, Vol.15, Issue 1, January 2007, pp. 39-68.

[6] N. Chandel, M. V. Gupta, “Review of Routing Protocols for VANET” IJRIT International Journal of Research in Information Technology, Volume 2, Issue 4, pp. 625- 632, April 2014.

[7] M. A. Rahman, F. Anwar, J. Naeemand and M. S. M. Abedin, “Simulation Based Performance Comparison of Routing Protocol on Mobile Ad-hoc Network (Proactive, Rective and Hybrid)”, International Conference on Computer and Communication Engineering (ICCCE 2010), 11-13 May 2010, Kuala Lumpur, Malaysia.

[8] A. M. Malla and R. K.Sahu, “Security Attacks with an Effective Solution for DOS Attacks in VANET”, in International Journal of Computer Applications, March 2013, Volume 66 -Number 22.

[9] K. Verma, H. Hasbullah and A. Kumar, “Prevention of DoS Attacks in VANET”, in Wireless Personal Communications, November 2013, Volume 73, Issue 1, pp 95-126.

[10] I. A. Soomro, H. Hasbullah and J. L. A Manan, “Denial of Service (DOS) Attack and Its Possible Solutions in VANET”, in WASET, issue 65, 2010 ISSN 2070-3724.

[11] M. S. A. kahtani,, “Survey on security attacks in Vehicular Ad hoc Networks (VANETs)”, in 6th International Conference on Signal Processing and Communication Systems (ICSPCS), pp 1 - 9, 2012.

[12] Global Health Observatory (GHO) data, WHO|Reports[online]2013,www.who.int(gho)publications/en/(Accessed:13 April 2015) .

[13] T. Issariyakul and E. Hossain,”An Introduction to NS2 simultor” *International Journal of Computer Applications*. vol. 66 , pp.45-49, March 2012.

[14] S. A. Sultan, M. M. A. Doori, A. H. A. Bayatti and H. Zedan, "A comprehensive survey on vehicular Ad hoc network", *Journal of Network and Computer Applications*, pp.1-13, Feb. 2013.

[15] A. Sinha, & S. K. Mishra, “Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DoS) Attack.” International Journal of Computer Applications, vol. 8 , 2014, pp. 14-17.