ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Impact of Jamming Attack in Vehicular Ad hoc Networks

Rohini Rawat[1], Dr. Deepti Sharma[2]

M-Tech Student, Department of CSE, Advance Institute of Technology and Mgt, Palwal, Haryana, India[1]

HOD, Department of CSE, Advance Institute of Technology and Mgt. Palwal, Haryana, India[2]

Abstract: Vehicular Ad Hoc Networks (VANET) has attracted today's research efforts. Despite the attention that VANET research got, current solutions to attain secure VANET still undergoing to protect the network from oppose and attacks. The necessity for a secure VANET networks is powerfully tied to the security and privacy features. This Jamming attacks are one of them. These occur by transmitting continuous radio ways to inhibit the transmission among sender and receiver. These attacks affect the network by decreasing the network performance. Previously there had been considerable research in the field of increasing the performance of network by using routing protocols. In this paper we are analysing the performance of Vehicular ad hoc networks under jamming attack. This work includes a network with high mobility, using IEEE Along g standard with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. Video conferencing and FTP with high data rate are being generated in the network. For the Simulation purpose we employed OPNET (Optimized Network Engineering Tool) MODELER 14.5 is used for simulation. The performance of network is measured with respect to the QoS parameters like, network load, retransmission attempts, media access delay and. Throughput.

Keywords: AODV, FTP, MANET, VANET, OPNET

I. INTRODUCTION

In today's prospective the sheer volume of road traffic affects the safety and effectiveness of traffic environment. Millions of people are killed around the globe every year in the road accidents. It's been a challenge to stop these accidents and deliver safety of people. Safety applications are vital in nature and sprightly associated to users and their lives. One promising way is to offer the traffic statistics to the vehicles so that they can use them to scrutinize the traffic situation. That can be accomplished by switching the information of traffic situation among vehicles. With the progress of microelectronics, it becomes possible to integrate node and network device into single unit and wireless interconnection VANET is an exciting application of mobile ad-hoc network (MANETs). VANET is the influential technology that can deliver realistic vehicle to vehicle (V2V) and vehicle to roadside infrastructure (V2I) communication. VANETs are self-configuring system where nodes are vehicle and WIFI technologies are used to form these networks. VANETs are permitted to build intelligent transportation system (ITS) that emphases on road safety, traveller wellbeing and traffic efficiency. The accomplishment of VANETs relies on the crucial element such as statistics routing amid nodes and the entrance to the internet. Deprived of any powerful routing methodology, the power of VANETs will be constrained.

Vehicular Networks (also known as VANETs) are a foundation of the projected Intelligent Transportation Systems (ITS). By enabling vehicles to communicate with each other via Inter-Vehicle Communication (IVC) as well as with roadside base stations via Roadside-to-Vehicle Communication (RVC), vehicular networks will contribute to safer and more effective roads by providing appropriate statistics to drivers and concerned authorities. The stimulating research area of Vehicular Networks is where ad hoc systems can be brought to their full potential

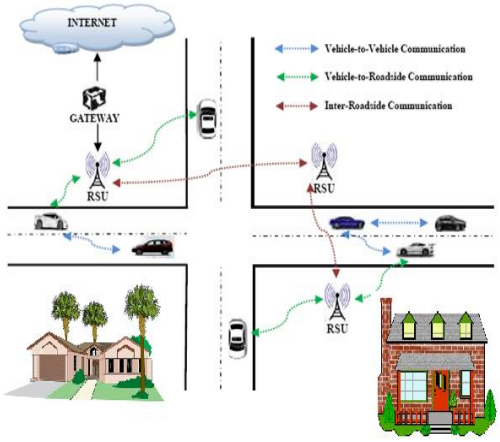

Figure1. Vehicular Ad hoc Network

VANET can be used for a broad range of Safety and Non-Safety applications. It includes sharing of multimedia information and traffic control. When applied to the traffic control, it is helpful in avoiding accidents by distributing information about the road situation, such as traffic accidents and road congestion. Therefore, it can effectively manage city traffic, reduce accidents and improve safety with high efficiency.].

II. JAMMING ATTACK

Jamming attack deliberately transmits of radio signals to disrupt the whole communications by decreasing the signal-to-noise ratio. The term jamming is used to

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

differentiate it from unintentional jamming which called interference. In VANET Jamming is a serious threat to its security. Jammers constantly send repeated signals (in affected area) to interfere with the communication between nodes in the network. The victim feels that the state of the channel is still busy. Therefore, it cannot send or receive packets in the jammed area. When jamming is enabled, the sender may successfully send packets; the receiver cannot receive all the packets sent by the sender. Hence, its packet delivery ratio (PDR) is low. These packets can be carrying important information (life threatening) such as, road conditions, weather, accidents, etc. and failure to receive or disseminate these packets can lead to fatalities.

Challenges: Due to the high mobility of VANET and the rapid change of its topology, defending VANET against jammers has been a hard problem. That because jammers don't have to comply with any protocols and their mobility is not limited. A jammer can be standing on feet or driving randomly down the roads. Moreover, adversaries have full control of when to start jamming and when to go into a sleep mode to hide its existence. All these reasons have made jamming problem a challenge to solve and detect.

III. METHODOLOGY

This section describes the simulation tool used along with the proposed method.

A. Simulation tool used:

OPNET modeler v14.5 is extensive and a very powerful simulation tool with wide variety of possibilities. The entire heterogeneous networks with various routing protocols can be simulated using OPNET. High level of user interface is used in OPNET which is constructed from C and C++ source code blocks.

B. Simulation Setup:

The simulation work focuses on analysing the performance of VANET under jamming attack. Therefore an Integrated approach is used to analyse the network performance under jamming attack. This approach includes:

- High data rate of 54mbps by using IEEE 802.11g standard [9]
- Network with high mobility [2]
- Improved parameter of AODV routing protocol
- Generation of high resolution video conferencing and FTP traffic

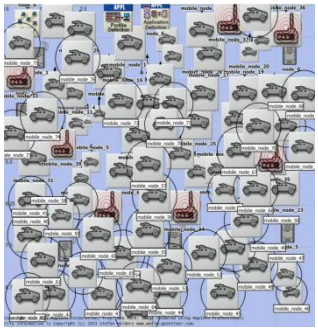

Figure 2: VANET Jamming Attack Scenario

Table I: VANET Simulation Parameters

Examined Protocols Cases	AODV without Jamming Attack
Number of Nodes	100 and 200
Types of Nodes	Mobile
Simulation Area	50*50 km
Simulation Time	3600 seconds
Mobility	Uniform(10-100) m/s
Pause Time	200 seconds
Performance Parameters	Throughput, Delay, Network load
Trajectory	VECTOR
Long Retry Limit	4
Max Receive Lifetime(seconds)	0.5
Buffer Size(bits)	25600
Mobility model used	Random waypoint
Data Type	Constant Bit Rate (CBR)
Packet Size	512 bytes
Traffic type	FTP, Http
Active Route Timeout(sec)	4
Hello interval(sec)	1,2
Hello Loss	3
Timeout Buffer	2
Physical Characteristics	IEEE 802.11g (OFDM)
Data Rates(bps)	54 Mbps
Transmit Power	0.005
RTS Threshold	1024
Packet-Reception Threshold	-95

Table II: VANET Simulation Parameters for Jammer

Examined Protocols Cases	AODV without Jamming Attack
Number of Nodes	100 and 200
Types of Nodes	Mobile
Simulation Area	50*50 km
Simulation Time	3600 seconds
Mobility	Uniform(10-100) m/s
Pause Time	200 seconds
Performance Parameters	Throughput, Delay, Network load
No. of Jammers	10
Jammer Bandwidth	100,000
Jammer band base frequency	2,402
Jammer Transmitter Power	0.001
Trajectory	VECTOR
Data Type	Constant Bit Rate (CBR)
Packet Size	512 bytes
Traffic type	FTP, Http
Active Route Timeout(sec)	4

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Hello interval(sec)	1,2
Hello Loss	3
Timeout Buffer	2
Physical Characteristics	IEEE 802.11g (OFDM)
Data Rates(bps)	54 Mbps
Transmit Power	0.005
RTS Threshold	1024
Packet-Reception Threshold	-95
Performance Parameters	Throughput, Delay, Network load
Trajectory	VECTOR
Long Retry Limit	4
Max Receive Lifetime (seconds)	0.5
Buffer Size(bits)	25600

IV. RESULTS

Number of results was collected in terms of many parameters:

A. Delay: Represents the end to end delay of all the packets received by the wireless LAN MACs of all VANET nodes in the network and forwarded to the higher layer. Jammers would affect the performance of system by increasing the delay as shown in the Fig.3 and 4.

B. Data dropped: Total higher layer data traffic (in bits/sec) dropped by the all the WLAN MACs in the network as a result of consistently failing retransmissions. Jammers could affect the network by increasing Data dropped of network as shown in Fig. 5 and 6.

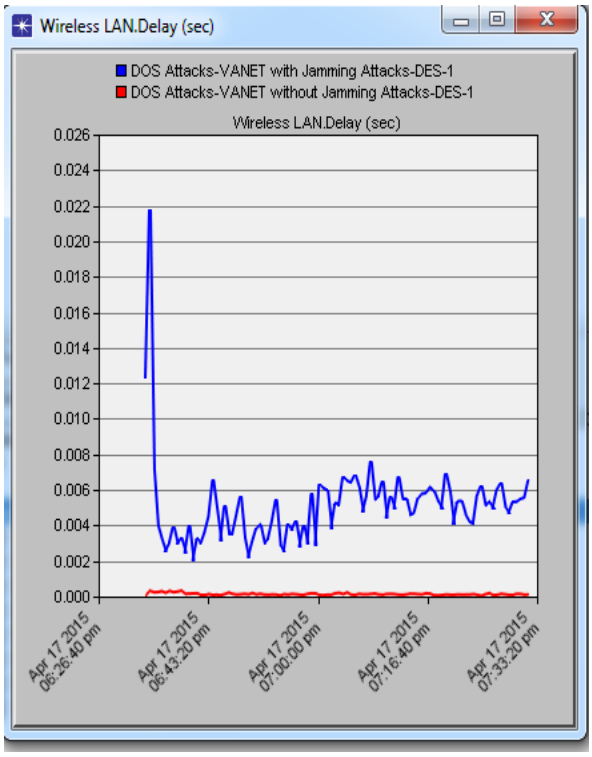

Figure 3: Average Delay of 100 Nodes

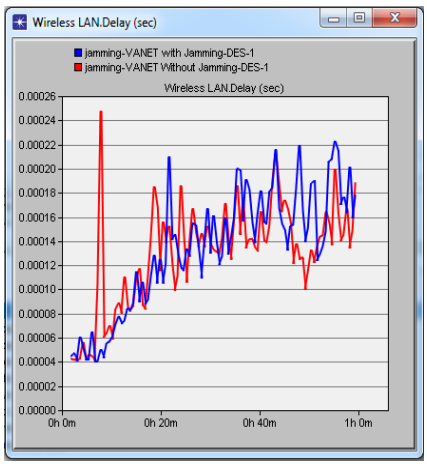

Figure 4: Average Delay of 200 Nodes

C. Network Load: Figure 7 and 8 shows that the network load of the normal network is noted as 22,340 bits/sec and with the jamming nodes in the network it is noted as 25840 bits/sec. The jamming attacker nodes drop the packets and not forwarding the packets for the other nodes.

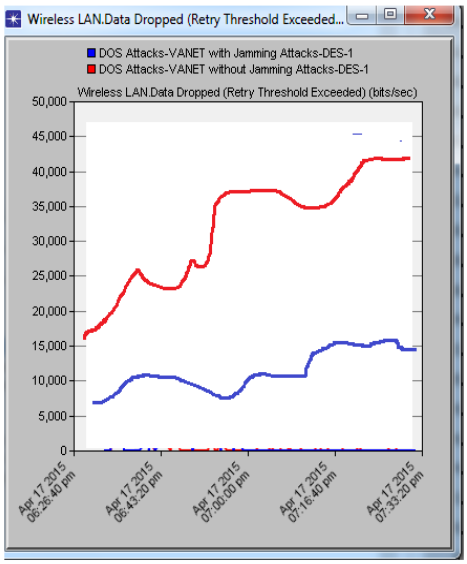

Figure 5: Average Data dropped of 100 Nodes

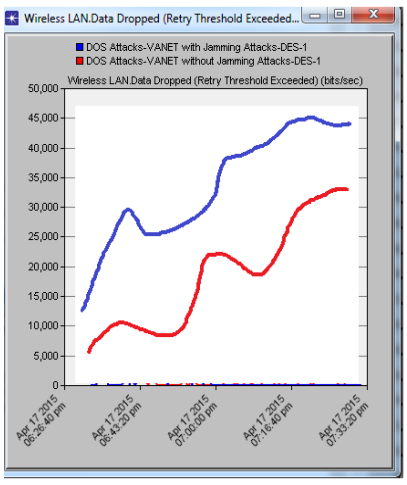

Figure 6: Average Data dropped of 200 Nodes

DOI 10.17148/IJARCCE.2015.44105

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

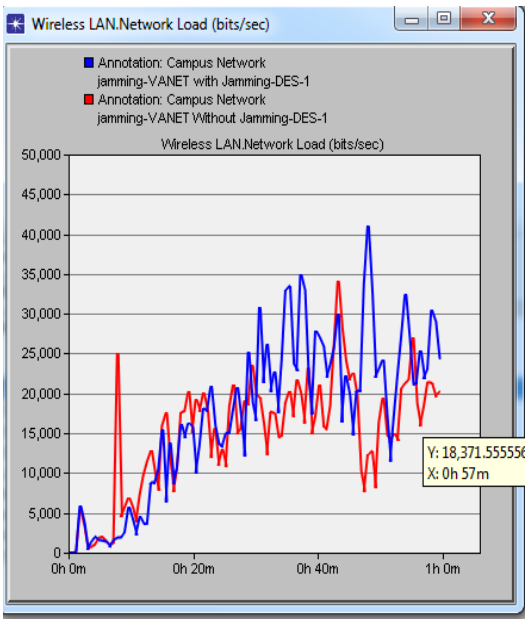

Figure 7: Average Network load of 100 Nodes

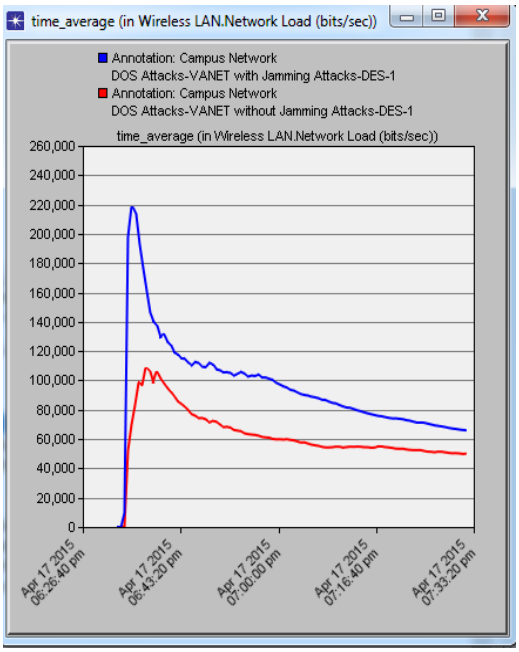

Figure 8: Average Network load of 200 Nodes

CONCLUSION

Jammers attacks will have an effect on network's performance as a result of the jammers interferes with the traditional operation of the network. The effect of attackers studied in this paper was by increasing delay, data dropped traffic received and sent and decreasing packer drop ratio of the network. In this research work, the network performance under jamming attack is analysing by applying integrated approach. This approach includes a network with high mobility, IEEE 802.11g standard with max data rate, heavy traffic like FTP and video conferencing, improved AODV parameters and increased buffer size. In our paper, it was shown that jamming attack reduces the network throughput, retransmission attempts and increases the media access delay.

REFERENCES

[1]. Harri, J.; Filali, F.; Bonnet, C., "Mobility Models for vehicular ad hoc networks: a survay and taxonomy," Communications Surveys & Tutorials, IEEE , vol.11, no.4, pp.19,41, Fourth Quarter 2009

[2]. Sun Xi; Xia-Miao Li, "Study of the Feasibility of VANET and its Routing Protocols," Wireless communication, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on , vol., no., pp.1,4, 12-14 Oct. 2008.

[3]. Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen,Angela Irwin, Aamir Hassan," Vehicular Ad hoc Networks(VANET):Status, Results, Challenges". Springer Science, Business Media.2010

[4]. Samara, Wafaa A.H. Al-Salihy, R.sures, "Ghassan Security Analysis of Vehicular Ad hoc Networks"2010 International Conference on Network Applications,Protocols and Services.

[5]. Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," Advance Computing Conference (IACC), 2013 IEEE 3rd International , vol., no., pp.550,555, 22-23 Feb. 2013

[6]. Grzybek, A.; Seredynski, M.; Danoy, G.; Bouvry, P., "Aspects and trends in realistic VANET simulations, Wireless, Mobile and Multimedia Network, 2012 IEEE International Symposium on a , vol., no., pp.1,6, 25-28 June 2012

[7]. Jie Li, Huang Lu, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs" , IEEE Transactions on Parallel and Distributed Systems, 2012

[8]. Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K., "VSPN: VANET-Based Secure and Privacy-Preserving Navigation," Computers, IEEE Transactions on , vol.63, no.2, pp.510,524, Feb. 2014

[9]. Yen-Wen Lin; Guo-Tang Huang, "Optimal next hop selection for VANET routing," Communications and Networking in China (CHINACOM), 2012 7th International ICST Conference on , vol., no., pp.611,615, 8-10 Aug. 2012

[10]. Performance Comparison Of AODV and DSDV Routing Protocols in Mobile Ad Hoc Networks, Aditi Sharma,Sonal Rana, Leena Kalia, International Journal of Emerging Research in Management and Technology, ISSN:2278-9359 Volume-3, Issue-7, July 2014.

[11]. Ait Ali, K.; Baala, O.; Caminada, A., "Routing Mechanisms Analysis in Vehicular City Environment," Vehicular Technology Conference, 2011 IEEE 73rd , vol., no., pp.1,5, 15-18 May 2011

[12]. Bhoi, S.K.; Khilar, P.M., "A secure routing protocol for Vehicular Ad Hoc Network to provide ITS services," Communications and Signal Processing (ICCSP), 2013 International Conference on , vol., no., pp.1170,1174, 3-5 April 2013

[13]. Pathre, A.; Agrawal, C.; Jain, A., "A novel defense scheme against DDOS attack in VANET," Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on , vol., no., pp.1,5, 26-28 July 2013

[14]. Hamieh, A.; Ben-othman, J.; Mokdad, L., "Detection of Radio Interference Attacks in VANET," Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE , vol., no., pp.1,5, Nov. 30 2009-Dec. 4 2009

[15]. Lyamin, N.; Vinel, A.; Jonsson, M.; Loo, J., "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

[16]. Yeongkwun Kim; Injoo Kim; Shim, C.Y., "A taxonomy for DOS attacks in VANET," Communications and Information Technologies (ISCIT), 2014 14th International Symposium on , vol., no., pp.26,27, 24-26 Sept. 2014

[17]. Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," Advance Computing Conference (IACC), 2013 IEEE 3rd International , vol., no., pp.550,555, 22-23 Feb. 2013

[18]. Li He; 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

[19]. Pooja, B.; Manohara Pai, M.M.; Pai, R.M.; Ajam, N.; Mouzna, J., "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," Computer Aided System Engineering (APCASE), 2014 Asia-Pacific Conference on , vol., no., pp.152,157, 10-12 Feb. 2014

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

[20]. Durech, J.; Franekova, M.; Holecko, P.; Bubenikova, E., "Security analysis of cryptographic constructions used within communications in modern transportation systems on the base of modelling," ELEKTRO, 2014 , vol., no., pp.424,429, 19-20 May 2014
[21]. Nafi, N.S.; Khan, R.H.; Khan, J.Y.; Gregory, M., "A predictive road traffic management system based on vehicular ad-hoc network," Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian , vol., no., pp.135,140, 26-28 Nov. 2014
[22]. Kumar, A.; Sinha, M., "Overview on vehicular ad hoc network and its security issues," Computing for Sustainable Global Development (INDIACom), 2014 International Conference on , vol., no., pp.792,797, 5-7 March 2014
[23]. Mehta, K.; Malik, L.G.; Bajaj, P., "VANET: Challenges, Issues and Solutions," Emerging Trends in Engineering and Technology (ICETET), 2013 6th International Conference on , vol., no., pp.78,79, 16-18 Dec. 2013
[24]. Nafi, N.S.; Khan, J.Y., "A VANET based Intelligent Road Traffic Signalling System," Telecommunication Networks and Applications Conference (ATNAC), 2012 Australasian , vol., no., pp.1,6, 7-9 Nov. 2012
[25]. Shuai Yang; Rongxi He; Ying Wang; Sen Li; Bin Lin, "OPNET-based modeling and simulations on routing protocols in VANETs with IEEE 802.11p," Systems and Informatics (ICSAI), 2014 2nd International Conference on , vol., no., pp.536,541, 15-17 Nov. 2014
[26]. Sadeghi, M.; Yahya, S., "Analysis of Wormhole attack on MANETs using different MANET routing protocols," Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on , vol., no., pp.301,305, 4-6 July 2012
[27]. Jhaveri, Rutvij H.; Patel, Ashish D.; Dangarwala, Kruti J., "Comprehensive Study of various DoS attacks and defense approaches in MANETs," Emerging Trends in Science, Engineering and Technology (INCOSET), 2012 International Conference on , vol., no., pp.25,31, 13-14 Dec. 2012
[28]. C. Sommer, Z. Yao, R. German, and F. Dressler, "On the need for bidirectional coupling of road traffic micro simulation and network simulation," in Mobility Models '08: Proceeding of the 1st ACM SIGMOBILE workshop on Mobility models. New York, NY, USA: ACM, 2008, pp. 41–48
[29]. Zhao and G. Cao, "Vadd: Vehicle-assisted data delivery in vehicular ad hoc networks," Vehicular Technology, IEEE Transactions on, vol. 57, no. 3, pp. 1910 –1922, may 2008.
[30]. Q. Chen, D. Jiang, and L. Delgrossi, "Ieee 1609.4 dsrc multi-channel operations and its implications on vehicle safety communications," in Vehicular Networking Conference (VNC), 2009 IEEE, oct. 2009, pp. 1 –8.
[31]. Y. H. Choi, R. Rajkumar, P. Mudalige, and F. Bai, "Adaptive location division multiple access for reliable safety message dissemination in vanets," in Wireless Communication Systems, 2009. ISWCS 2009. 6th International Symposium on, sept. 2009, pp. 565 –569.
[32]. Biswas, S., & Misic, J to Privacy-preser. (2013). "A Cross-layer Approach ving Authentication in WAVE-enabled VANETs." Vehicular Technology, IEEE Transactions on 62(5): 2182 – 2192
[33]. Pradweap, R. V., & Hansdah, R. C. (2013). A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET. In Information Systems Security (pp. 314-328). Springer Berlin Heidelberg.
[34]. Prado, A., Ruj, S., & Nayak, A. (2013, June). "Enhanced privacy and reliability for secure geocasting in VANET." In Communications (ICC), 2013 IEEE International Conference on (pp. 1599-1603). IEEE.
[35]. Gupta, D.; Kumar, R., "An improved genetic based Routing Protocol for VANETs," Confluence The Next Generation Information Technology Summit, 2014 5th International Conference -, vol., no., pp.347, 353, 25-26 Sept. 2014