Securing Ad hoc Network By Mitigating Jamming Attack

Neeti Yadav[1] Dr. Vivek Kumar[2]

M-Tech Student[1], Principal[2] & Department of CSE & Delhi College of Technology & Management
Palwal, Haryana, India

***Abstract*—**
MANETs have unique characteristics like dynamic topology, wireless radio medium, limited resources and lack of centralized administration; as a result, they are vulnerable to different types of attacks in different layers of protocol stack. Each node in a MANET is capable of acting as a router. The necessity for a secure MANET 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. In our research work we are improving the performance of mobile ad hoc networks under jamming attack by using an CTS/RTS integrated approach. The proposed work includes a network with high mobility, using IEEE Along g standard with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. FTP and Video conferencing with high data rate are being generated in the network. The performance of network is measured with respect to the QoS parameters like throughput, and delay. OPNET (Optimized Network Engineering Tool) MODELER 16.0 is used for simulation. The results of simulation demonstrate that the overall performance of network with jamming attack has been increased by using the integrated approach.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile nodes and connected in dynamic manner. Nodes forming a temporary/short-lived network without any fixed infrastructure where all nodes are free to move about arbitrarily.

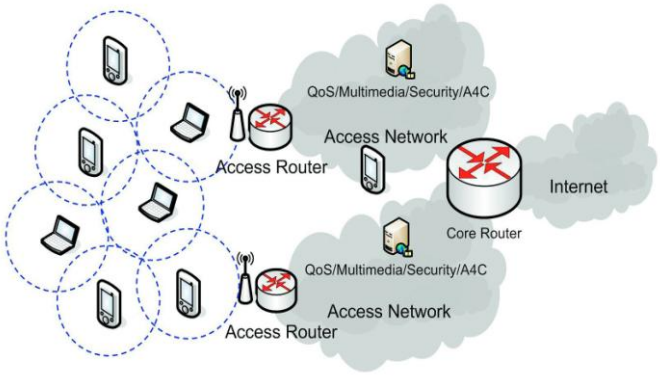

Figure 1.1 Mobile Ad Hoc Networks

Nodes must behave as routers, take part in discovery and maintenance of routes to other nodes in the network [1] Wireless links in MANET are highly error prone and can go down frequently due to mobility of nodes. Stable routing is a very critical task due to highly dynamic environment in Mobile Ad-hoc Network [2].

II. JAMMING ATTACK

Jamming attack is one of the most popular attack models of IEEE 802.11. Ad-Hoc networks are very prone to security threats. Jamming attack is one of the type of Denial Of Service (DoS). Jamming is caused by continuously sending the radio signals in between the transmission which injects the dummy packets thus causing interferences. Since the radio frequency is an open medium, therefore jamming is big problem for wireless networks. Jamming decreases the overall- performance of network by effecting their throughput, network load, end to end delays etc.

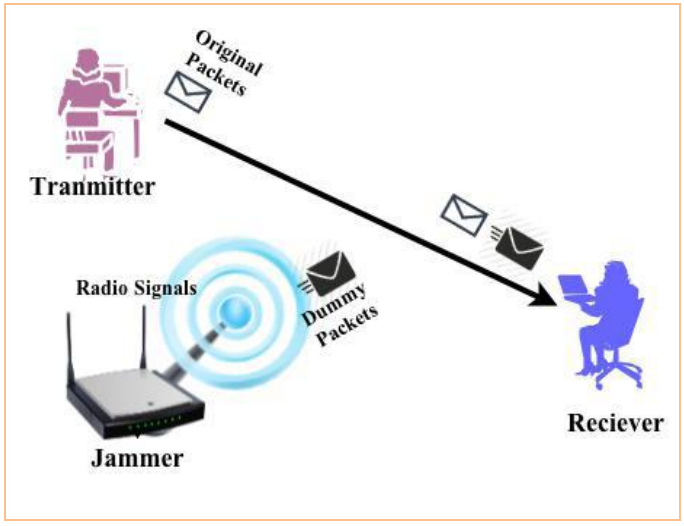

Figure: 2.1 Jamming Attack

III. PROPOSED METHOD

The RTS/CTS mechanism is a handshaking process that minimizes the occurrence of collisions when hidden nodes are operating on the network. The working mechanism of RTS/CTS implementation is shown in figure 1.

ISSN: 2278 – 1323

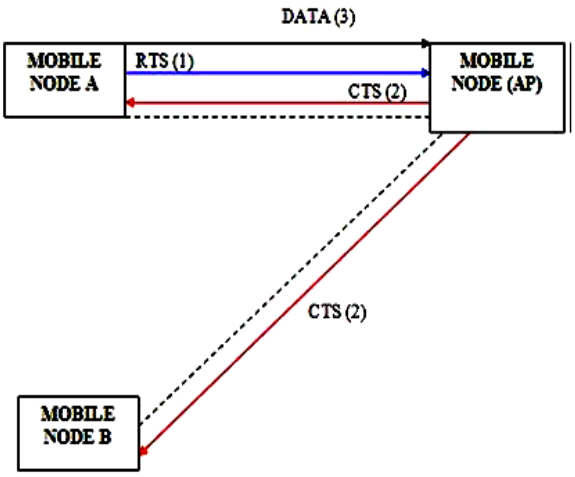

Figure: 3.1 CTS/RTS Mechanism

The AP mobile node receives RTS data from Mobile node A and replies to it with a CTS frame while authenticating it to send data. Meanwhile, the Mobile Node B receives the CTS frame since the Mobile Node A is sending data and the mechanism informs the mobile Node B that the AP is transmitting or receiving data at that time frame. This makes Mobile Node B to wait for a particular time. When a jamming attack is launched on the network, fake RTS frames are sent to the AP mobile node that keeps the medium busy and prevents other nodes from being able to commence with legitimate MAC operations, or introduces packet collisions causing forced and repeated back offs.

The algorithm is as follows:

1. Deploy the nodes.
2. Use RTS & CTS frames for reliable communication.
3. Set the maximum number of packets to be sent by the requesting node/replying node as a Packet_Threshold.
4. Check for each requesting/replying node
{
If
Packet_Sent > Packet_Threshold
then
Declare the node as the attacker node.
Block that node.
}
5. Display the list of blocked nodes in the network. The blocked node will not be able to participate in the further transmissions.

IV. SYSTEM MODEL

In this research we have taken three scenarios. The first scenario describes the network without jammer**.** This scenario consists of 100 mobile nodes deployed randomly in the area of 50*50 k m. The second scenario describes the network with jammers and same parameters. The jammer used here is mobile pulse jammer. The third scenario implements the proposed technique for the detection and prevention of the physical jamming attack.

The scenarios are simulated and analysed on the basis of two parameters- Throughput and Delay.

1. Throughput- Represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to the higher layers in all WLAN nodes of the network.
2. Delay- Represents the end to end delay of all the packets received by the wireless LAN Macs of all the WLAN nodes in the network and forwarded to the higher layers.

The simulation was performed for 300 seconds while the number of seeds used was 300 in order to provide 1 hour simulation performance.

Table 1: 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
Examined Protocols Cases	AODV with 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

ISSN: 2278 – 1323

V. PROPOSED TECHNIQUE

In order to enhance the throughput of the entire network, the presence of the jammer node is very necessary to be stated. Various techniques were opted for the discovery, prevention and mitigation of the jamming attack. In order to enhance the throughput and decrease the delay as compare to the existing approaches, a meliorated detection mechanism is proposed in this dissertation, for the detection of the physical jamming attack.

1. In case, if packet size exceeded to a particular RTS threshold, that packet would have to wait for a particular RTS/CTS interval in order to completely forward that packet to its destination. So, the buffer size is taken as 102400000.
2. Also, high data rate of 54 mbps is taken which were previously 11 mbps during the simple and the attack scenario.
3. The value of the physical characteristics is set to Extended Rate PHY.
4. So, apart from performing the modifications in the data rate and buffer size for the prevention of penalties caused by the drawbacks of the existing techniques and in order to improvise the throughput, improved AODV parameters are also adopted. Here, the active route timeout is taken as 30 seconds.

VI. PERFORMANCE RESULTS

Scenario 1 represents the scenario with no malicious event and normal network state, scenario 2 represents the network that is under the jamming attack and scenario 3 represents the mobile jammers and implementation of the proposed method.

A. Throughput

It is clearly seen that the jamming attack decreases the overall network throughput in comparison to the normal network state. However, the entire network throughput is increased once the proposed unified mechanism is implemented.

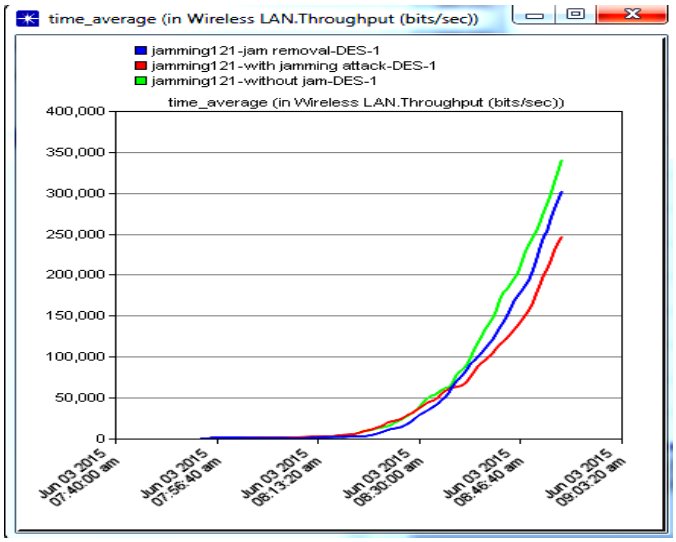

Figure 6.1: Throughput of all three scenarios at 100 nodes

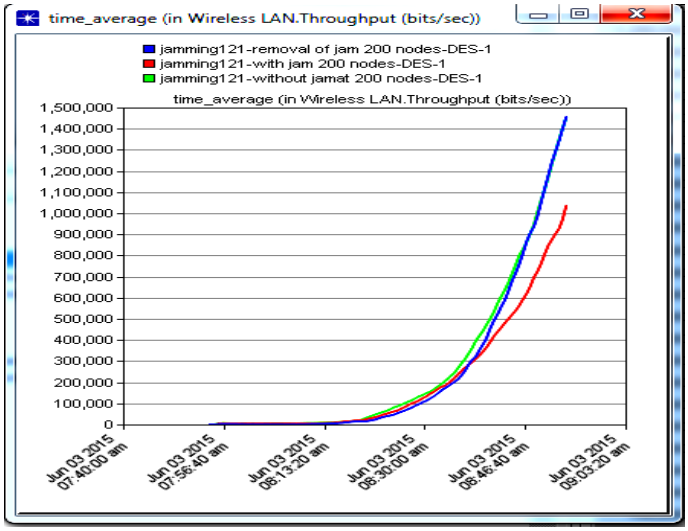

Figure 6.2: Throughput of all three scenarios at 200 nodes

B. End To End Delay

In first scenario of 100 nodes of our experimentation, packets Delay with peak value of approx. 0.010 seconds. In second scenario which is with jamming attack, packets delay Increases to value of approx 0.35 seconds. In first scenario of 200 nodes of our experimentation, packets delay is approx. 0.0020 seconds. In second scenario which is with jamming attack, packets delay increases to value of approx. 0.30 seconds.

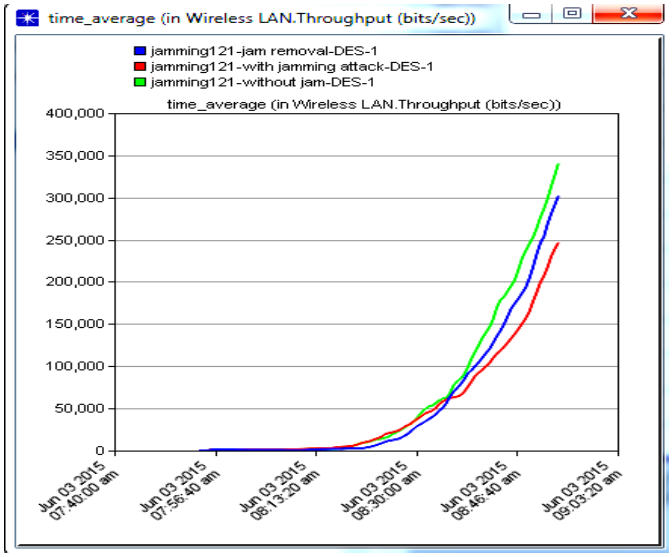

Figure 6.3: Delay of all three scenarios at 100 nodes

The recovery of the end to end delay decreases with our proposed mechanism by elimination of the jamming attack as end to end delay comes to similar to the value 0.000256 seconds. Thus our proposed mechanism eliminates jamming attack in network.

ISSN: 2278 – 1323

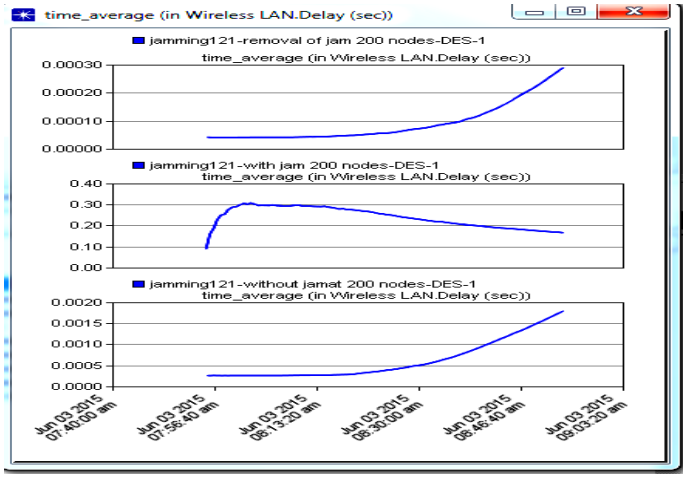

Figure 6.4: Delay of all three scenarios at 200 nodes

VII. CONCLUSION AND FUTURE WORK

The unified mechanism is implemented on the selected nodes on the network and deployed in the specific area. The findings of the research clearly states that, the implementation of such unified mechanisms have a significant impact on the overall network through positively. On the other hand, the implementation of such mechanisms does not only mitigate the jamming attack effects, it also increases the overall performance above the normal state of the network. We consider future research work focused on using real time attacks which is needed to ascertain greater degree of detection of specific vulnerabilities in both Mobile and ad hoc Sensor networks.

REFERENCE

[1] 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

[2] 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

[3] 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

[4] 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

[5] 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

[6] 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.

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

[8] 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.

[9] 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

[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

[14] 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

[15] 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

[16] 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

[17] 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

[18] 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

[19] 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

[20] Nafi, N.S.; Khan, R.H.; Khan, J.Y.; Gregory, M., "A predictive road traffic management system based on vehicular ad-hoc

ISSN: 2278 – 1323

network," Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian , vol., no., pp.135,140, 26-28 Nov. 2014

[21] 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

[22] 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

[23] 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

[24] 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

[25] 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

[26] 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

[26] 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

[27] 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.

[28] 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.

[29] 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.

[30] 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

[31] 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.

[32] 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.

[33] 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

ISSN: 2278 – 1323