ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Performance Evaluation of Vehicular Ad Hoc Networks under Sybil Attack

Shikha Arora, Urvashi Chugh

M.Tech Student, Department of CSE, Manav Rachna International University, Faridabad, Haryana, India [1]

Asst. Professor, Department of CSE, Manav Rachna International University, Faridabad, Haryana, India[2]

ABSTRACT: Reliable message transmission by multi-hoping in wireless network is developing research field. It is very complicated if nodes travel with high speed. A wireless Network can be categorized in three ways Mobile Ad-hoc Network (MANET), Vehicular Ad-hoc network (VANET) and Static Ad-hoc Network (SANET), in this VANET needed enough research. VANET is having a positive technique to achieve better safety and management in road traffic that provides several ranges of valuable facilities. The security and safety of messages is the significant need for vehicular network. Privacy and Security of the messages are the two concerns encouraging strong vehicular network designs. This paper shows routing protocols, and the network attacks that can be reduce the working performance of VANET. This paper also explains comparative performance of routing protocol in existence of Sybil attack.

KEYWORDS: network security, Vehicular ad-hoc networks (VANETs); Sybil attack.

I. INTRODUCTION

Vehicular Ad-hoc Networks (VANETs)[I] is a type of Ad-hoc Networks [1][2] that needed sufficient research and development. The interaction between Vehicle Node to Vehicle Node in VANET is very stimulating because of its fast mobility and frequent system partition. The interactions in VANETs present tougher challenges as compared to other common Ad-hoc networks. Infrastructure free situations and sophisticated active system configuration cause continuous network system partition. Moreover, VANETs are frequently organized by the restriction of roadways where houses, plants and other several obstacles influence the communication medium. There are some organizations that are working on Intelligent Transportation Systems (ITS) development [3]. It is essential to make a VANETs communication system that permits suitable, steady, reasonable circulation of data for better comfort. The convergence of computing, transportation and communication technologies services and wireless that our transportations highways and streets can be utilized for both communication and transportation activities [4]. Vehicular ad hoc network utilizes wireless communication networks that do not need any static infrastructure. Vehicles itself is a communication node and relays information building dynamic vehicular networks with nearer vehicles. Because of huge no. of Vehicle nodes moving on the road and the traffic monitoring and traffic safety is a big problem that's why several communication applications included in VANETs. These applications consists traffic monitoring, traffic safety and unpiloted vehicle applications. These applications depends real-time communication.

In VANETs, highly dynamic vehicle nodes operate without any static server can generate a collision on wireless medium in the communication of vehicle nodes. On the disputation medium, packet losses and delays take place frequently. Thus, it is essential to develop a set of efficient method to communicate sensitive information in real time.

In last some years lot of work has been performed on the development of various vehicular networks protocols with reference to real time based communication for the VANET's. In VANETs, there are two kind of communications: (1) vehicle to vehicle (V2V) and (2) vehicle to infrastructure (V2I). Vehicles have On Board Units (OBUs), which contains processors, Omni directional antennas, GPS unit, and sensors for V2V communications. Vehicles also perform V2I interactions with roadside infrastructures, which are located within a fixed distance of one another based on the communication range of the roadside devices, also called Road Side Units (RSUs). RSUs interacts one another through wireless medium or wired links. They can also be mobile. The V2I communications can be further explored to offer applications i.e. Internet since RSUs can be linked to a network. The V2V communications can be utilized to forward emergency and real-time information i.e. an accident or road traffic information so that other vehicles can take other routes to prevent traffic congestions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

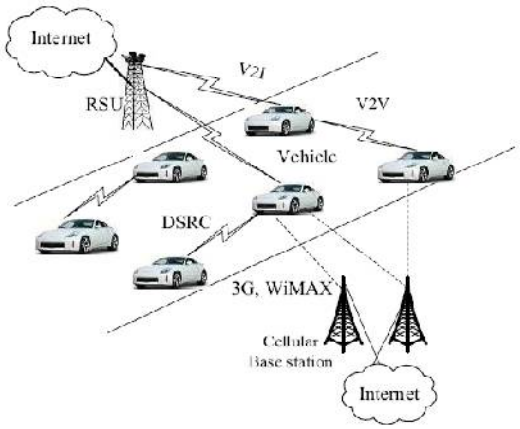


Figure 1: Vehicular Ad hoc Networks (VANETs)

II. ROUTING PROTOCOLS IN VANET

Protocols have set of rules or agreement between two connecting devices in this way the Routing have some rules to categories the work or route distributions. Topology based and geographic routing are the two classes of the Routing protocols (fig. 2).

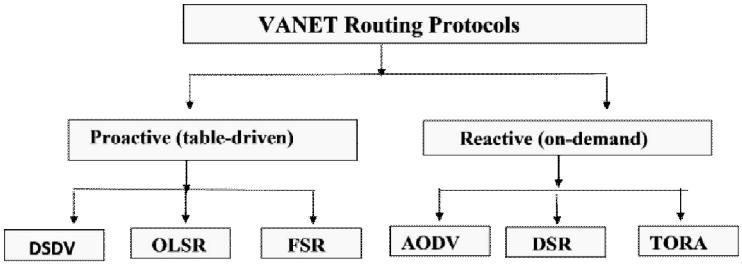


Figure 2: Routing Protocols in V ANET

Topology-based routing is based on the information of connections that present in the network to execute data packet forwarding. Geographic routing is based on the information of neighbour nodes location to achieve packet forwarding. When connection information changes in a regular interval, topology-based routing undergoes from routing route breaks.

Proactive (table-driven) [9, 10]: In this kind of routing routes are static for all communicating nodes.

Fisheye State Routing [2, 3] manages the topology map or guideline for each node and broadcasts the connection updates for only its neighbour nodes rather than entire network. Furthermore, the updated state of connection information may be broadcast in different frequencies for various node entries. That depends on the distance between their hops and the position of current node. The Nodes Entries that are additional away are broadcast with inferior incidence instead of ones that are earlier.

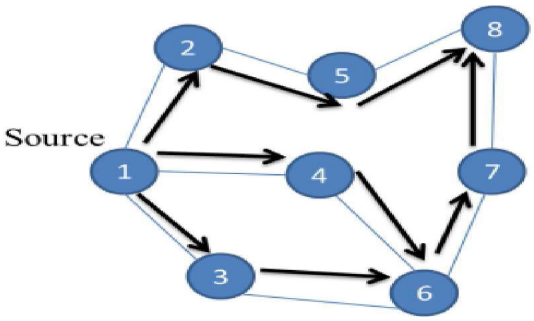
Reactive (On Demand)[9,11]: In this routing built a route only when it is needed for a node to interact with another node. Routes are not static for routing.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

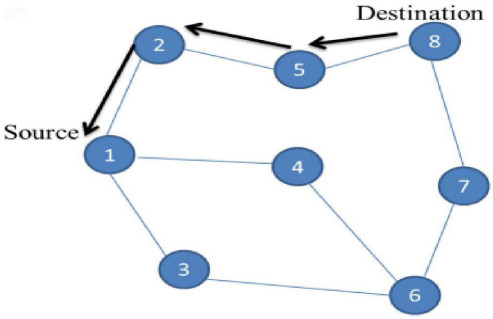
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016



a) RREQ transmission



b) RREQ path to the source

Figure 3. AODV route finding

AODV - Ad-hoc On-demand distance vector [11] in this routing each nodes saves the node address distribution to the route request query (RREQ) in their routing strategy (3a). When the process stored its prior hop these phenomenon is called backward learning. And when the process reached to the target then a reply packet (RREP) is then forwarded by the complete route that is stored by the backward learning to the source (3b). At every stage the nodes travels through the path, the record managed by the node would store its prior hop, which made the forward route from the source. The query flooding and create the response is a full duplex path. After path building, nodes can manage the path as long as the source utilizing it. When connection failure takes place because of any reason the node will be informed to the source and will in rotate fired a different response query process to determine a new route.
Hybrid: Hybrid routing is the combination of the characteristics of reactive and proactive protocols.

III. WORKING OF VEHICULAR NETWORKS

Vehicular Networks consists several nodes, around dimensions of vehicles surpassing more than thousands of million across the world. Today, these vehicles nodes will command an authority to maintain it that is known as local server, every vehicle nodes can get in contact with other vehicle nodes having a dedicated short range radio signals communication [12] with 5.9 GHz frequency in the range of 1 KM. This statement can be a Random communication which the place that the communicated or associated nodes can progress freely, in this procedure there is no requirement of wires needed, this kind of network communication based on ad-hoc network. The router Road Side Unit (RSU) links the vehicle to vehicle (V2V) on the highway and links with other network devices automatically. Every vehicle has On board Unit (OBU)[13], which links the automobile with Road Side Unit through Dedicated short range radio signals communication, along with apparatus is Tamper Proof Apparatus [13],

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

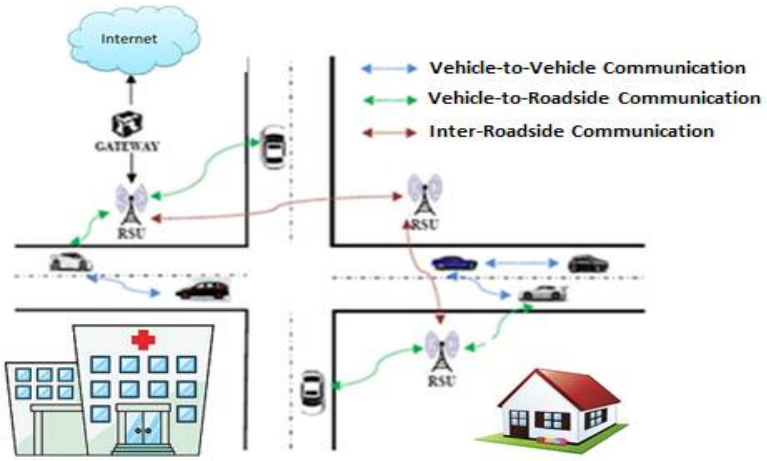


Figure 4: Architecture of VANET

V. EXPERIMENTATION AND RESULTS

This section presents the Sybil attack behaviour within VANET for AODV routing protocol. AODV routing protocol has been selected because it performs better as compared to other routing protocols in all scenarios with availability of attack. All the work related to simulation is performed in OPNET simulator version 14.5 [17]. Initially no. of nodes is 50, and the simulation time is 180 sec. Total 50 nodes were positioned for simulation in the terrain of 1500m X 1500m. All nodes move arbitrarily in the terrain, which is essential for examining vehicle movement. The speed of every node changed from 10mps to 50mps. AODV protocol is utilized for packets routing. Sybil attack was implemented for examining the scenario in existence of attack.

A. Analysis of Sybil attack in VANET

This section gives the effect of the Sybil attacks in AODV protocol.

A. Variation in Pause Time

(a). Throughput for AODV with and without Sybil attack in variation of Pause Time.

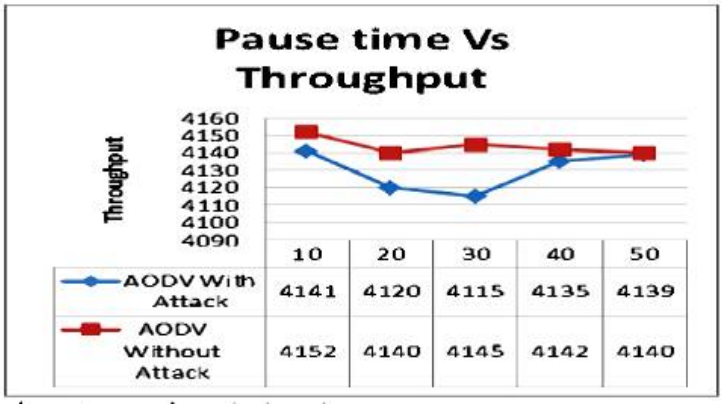


FIgure 5: Pause time Vs Throughput

The above fig 5 illustrates that the AODV performance with and without Sybil attacks when there is no variation in node speed and pause time changes. Routing protocol throughput under Sybil attack is poor when the participating nodes increases from 10 to 50 against the routing protocol which does not witness the Sybil attack.

B. Variation in Node Speed

(a) Throughput for AODV with and without Sybil attack in variation of Node Speed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

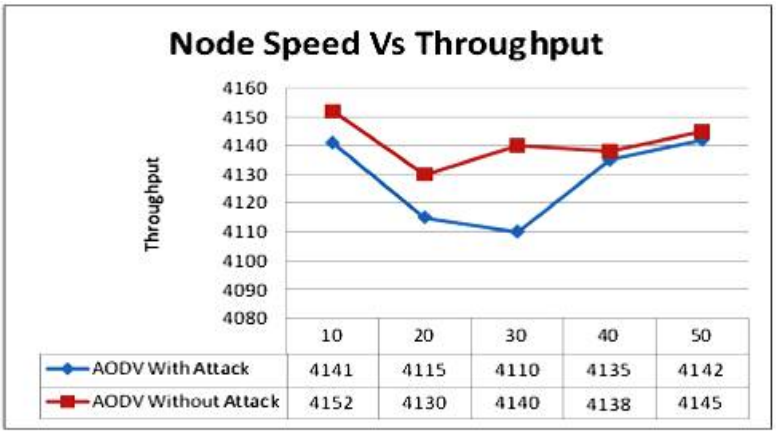


Figure 6: Node speed Vs Throughput

Fig 6 presents that the AODV performance with and sswithout Sybil attack when the pause time is constant and the node speed changes. Then the AODV performance is lesser when it witnesses the Sybil attacks. The throughput of the Sybil affected AODV is continuously poor when the participated nodes in the network is increased from 10 to 50.

VI. CONCLUSION

Vehicular network is a complicated network in which all nodes are mobile and move arbitrarily. The packet transmission is a problem in this network, because the node location is not fixed. Every transmission builds a new route for packet transmission. If attack takes place in this scenario then it spoils all communication. Several Network attack as well as Sybil attack generates major loss in packet transmission in any network. This paper is concentrated to the impact of Sybil attacks on the VANETs communication. There is several routing protocol for communication. After analysis and review it is concluded that AODV routing protocol may perform better in VANET in existence of attack. The vehicular network with AODV routing protocol in existence of attack is examined with support of OPNET simulator. The results are satisfactory. But still enhancement in routing protocol for vehicular network is needed. In future we will implement enhanced version of AODV with characteristic of anti-Sybil attack.

REFERENCES

[1] Anjum A. Mohammed, Gihan Nagib, "Optimal Routing In Ad-Hoc Network Using Genetic Algorithm",Int. J. Advanced Networking and Applications, vol. 03, Issue. 05, pp. 1323-1328, 2012.

[2] Ashutosh Lanjewar, Neelesh Gupta, "Optimizing Cost, Delay, Packet Loss and Network Load in AODV Routing Protocol", *(IJCSIS) International Journal of Computer Science and Information Security,*Vol. 11, No. 4,April2013.

[3] P. Karthikeyan, S. Baskar, A. Alphones, "Improved genetic algorithm using different genetic operator combinations (GOCs) for multicast routing in Ad-hoc networks", Springer, vol-17, pp. 1563-1572, 2013..

[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] Dalbir Singh and Manjot Kaur, "Mitigation of Sybil Attack Using Location Aware Nodes in VANET", International Journal of Science and Research (IJSR), Volume 4 Issue 11, November 2015

[11]Jaydip Kamani and Dhaval Parikh, "A Review on Sybil Attack Detection Techniques", Journal for Research, Volume 01, Issue 01, March 2015

[12] Kewei Sha, Shinan Wang and Weisong Shi, "RD4: Role-Differentiated Cooperative Deceptive Data Detection and Filtering in VANETs", International Journal of Network Security & its Applications(IJNSA), Vol 3, No.6, 2010.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

[13] 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 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]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.
[25] 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
[26] 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
[27] 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