ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

VANET TRAFFIC MANAGEMENT AND SECURITY ISSUES

Raghu Kanojia[1] , Rasleen Kaur Deol [2]
[1]M.TECH Research Scholar, GIMET, Amritsar
[2]Assistant Professor, Dept. of CSE, GIMET, Amritsar

Abstract— when data is transferred in VANET from source to destination then either data is successfully delivered or may not show at all. The data which is transferred may contain malicious information. This malicious data may be transferred from node in the VANET. The node transferring malicious data is known as malicious node. The main target of malicious node is to create traffic over the network so that resources required by the nodes on VANET are not accessible. The problems which are caused by malicious node is due to selfish behavior of the nodes. Number of mechanisms is suggested in order to prevent malicious nodes from attacking the VANET. In VANET, route planning and traffic management is very important. In this paper we review the papers dealing with VANET traffic management and malicious node detection.

***Index Terms*— VANET, Traffic, Malicious Nodes.**

I. INTRODUCTION

When data is to be transferred over the network then security will be the prime concern. Also deciding the path and traffic management is important in VANET. In VANET data is exchanged node to node. This will give the chance to malicious node to enter into the VANET. In order to describe our concept we conducted the review involving five papers. The description of all the papers is presented here.

II. RELATED WORK

This paper deals with the detection of misbehaving nodes. The misbehaving node will generate false alert messages and also send falsifying information. The detection of such nodes will be according to consistency of recent messages. Declaring the node is malicious is purely in the hands of receiver. No majority decision is required in this case. In this case prototype will be maintained. Every message which is delivered will be compared against this prototype. If message is valid then it is accepted otherwise it is rejected. In this paper location information is also analyzed. The location information will be important since falsifying information about the location can jam the traffic. Data centric techniques will ensure that focus is set on data and if data is not validated then it will be declared malicious. There exist certification authorities who will give certificate of validation to the sender of information. This certificate will be analyzed in order to accept the information transferred from the source. No action is suggested regarding the node who is transferring the malicious data. So this paper address the issue of misbehaving node without taking any action regarding the blocking the node transferring such information [4].

This paper considers the lack of infrastructure which causes misbehaviors in the VANET. The algorithm considered in this case is improved version of DMV algorithm. Detection of malicious vehicles algorithm is already present on which work has been done. DMN algorithm show better performance as compared to DMV algorithm. The factors which are improved include throughput, end to end packet delay etc. a special term known as verifiers is considered. A verifier will include Load, Distrust value and Distance. All of these factors are considered while deciding whether the node is malicious or not [1].

In this paper end to end communication between nodes will be considered. When this happens chance of malicious data will also come into existence. In this case validation of nodes is considered. Validation of nodes will be a difficult task. In this paper a node has to present the explanation for the data it has collected. This step

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

will be compulsory since malicious node can be present in the VANET. Sensor driven technique that allows nodes to detect the invalid information from node or nodes that are source of malicious data. The node will compare the received data against the model which it maintains. After this validity of data will be presented. Node will be declared malicious if data is invalid [6].

In this paper AODV algorithm is considered. This routing algorithm is generally used in VANET. However this protocol does not detect malicious node. In order to overcome this problem RAODV algorithm is used. This suggested protocol is Robust AODV algorithm used enhanced security mechanisms to prevent malicious entry into the system. The centralized authority will be established in order to ensure security. Whenever data is to be transferred, permission from the centralized server is to taken. If permission is granted then only node is permitted to transfer the data [2].

In this paper entities which are considered are private and public. Security issues are considered in this paper. When large amount of data is injected over the network then traffic will be jammed. This will cause the unavailability of resources to the destination nodes. This paper includes causes and prevention of attacks on VANET. In this paper technique is suggested which will ensure flow of accurate information from source to destination [7].

III. TECHNOLOGICAL COMPARISON

Sr. No	Paper	Category	Description
1	Data-centric Misbehavior Detection in VANETs	VANET	1) We propose a new model of VANET where we assume that most misbehaviors arise out of selfish motives. However, our model can also handle misbehavior from malicious nodes.
			2) We do not revoke misbehaving nodes, but impose fines on them. This reduces the communication and computation costs in calculating, transmitting, and storing certificate revocation lists.
			3) Misbehavior is detected by observing alerts raised by a node and its subsequent action.
			4) Our approach does not rely on voting schemes and group associations. Therefore it is immune to Sybil attacks.
			5) False location information can be detected in addition to detecting false alert messages
2	Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc	VANET	1) A vehicle is considered to show an abnormal behavior if it drops or duplicate the packets received to it so as to create congestion in the network, misguide other vehicular nodes or destroy crucial messages for their selfish motives.
	Networks		2) An honest vehicle forwards the messages received to it correctly to other nodes in the network or creates right messages for transmission.
			3) A vehicle will be tagged as a malicious vehicle, if the vehicle repeats abnormal behavior such that its distrust value, DV exceeds the threshold value.
3	Detecting and Correcting Malicious Data in VANETs	VANET	1) Distance between the nodes is being considered
			2) Range of sensors will be considered
4	Detecting malicious vehicle in a VANET scenario by incorporating	VANET	1) Protocol AODV is considered.
			2) Improvement to AODV protocol is suggested.
	security in AODV protocol"		3) Improvement is known as RAODV protocol.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

5	Malicious Data Detection in VANET	VANET	1) To Develop a Simulated Environment of VANET
			2)To Develop a Threshold based Intrusion Detection based system for anomaly detection
			3) To Evaluate the Impact of Malicious, fabricated And fake message attack.

IV. CONCLUSION

In the existing work although falsifying information is detected and alerts are generated however nodes are not blocked. Which means they are allowed to transmit falsifying information in the future also. The existing scheme of work is listed below:

1) In the analyzed papers, Nodes are considered in VANET where it is assumed that most misbehavior arise out of selfish motives. However, given model can also handle misbehavior from malicious nodes.

2) Existing Work do not revoke misbehaving nodes, but impose fines on them. This reduces the communication and computation costs in calculating, transmitting, and storing certificate revocation lists.

3) Misbehavior is detected by observing alerts raised by a node and its subsequent action.

4) Existing approach does not rely on voting schemes and group associations. Therefore it is immune to Sybil attacks.

5) False location information can be detected in addition to detecting false alert messages.

REFERENCES

[1] U. Khan, S. Agrawal, and S. Silakari, "Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks," Procedia Comput. Sci., vol. 46, no. Icict 2014, pp. 965–972, 2015.

[2] G. Singh, "Malicious Data Detection in VANET," vol. 1, no. 7, pp. 535–538, 2012.

[3] R. S. Raw, M. Kumar, and N. Singh, "Security Challenges, Issues and Their Solutions for VANET," Int. J. Netw. Secur. Its Appl., vol. 5, no. 5, pp. 95–105, 2013.

[4] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On Data-Centric Misbehavior Detection in VANETs," 2011 IEEE Veh. Technol. Conf. VTC Fall, vol. 35, no. 2, pp. 1–5, 2011.

[5] R. Baumann, "Vehicular Ad hoc Networks (VANET)," Ad Hoc Networks, p. 128, 2004.

[6] V. L. Praba and A. Ranichitra, "DETECTING MALICIOUS VEHICLE IN A VANET SCENARIO BY INCORPORATING SECURITY IN AODV PROTOCOL," pp. 594–598.

[7] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," Proc. first ACM Work. Veh. ad hoc networks VANET 04, vol. pp, no. NLE-PR-2006–19, pp. 29–37, 2004.