DOI: 10.21917/ijct.2012.0084

DETECTING MALICIOUS VEHICLE IN A VANET SCENARIO BY INCORPORATING SECURITY IN AODV PROTOCOL

V. Lakshmi Praba[1] and A. Ranichitra[2]
[1]*Department of Computer Science, Government Arts College for Women, India*
E-mail: vlakshmipraba@rediffmail.com
[2]*Manonmaniam Sundaranar University, India*
E-mail: ranichitra117@gmail.com

Abstract
Vehicular Ad hoc Networks (VANET) has emerged as a recognized advancement in wireless technologies. Each node in the network may be either a vehicle or Road Side Unit (RSU) which has to be equipped with the necessary communication facility. Every vehicle in VANET must be authenticated to establish a reliable and secure network communication. The AODV routing protocol which is normally applied in a VANET scenario does not detect malicious vehicles, if it exist. In this paper, a security mechanism has been incorporated in the AODV protocol to strengthen it as Robust AODV (RAODV) to detect a malicious vehicle. Sample architecture with centralized control unit, RSUs and some vehicles is illustrated to demonstrate the added security feature. AODV routing protocol has been applied in a simulated environment using NS-2 package. Performance metrics such as Packet Delivery Ratio, End to End delay, Routing Overhead and Number of dropped packets, for various vehicle speed were analyzed with the RAODV protocol.

Keywords:
Ad hoc, VANET, RSU, Central Authority, AODV

1. INTRODUCTION

Vehicular Ad hoc Networks (VANET) has emerged as a recognized advancement in wireless technologies. VANET integrates Ad hoc networks, Sensor networks, Wireless LAN and Cellular networks.

To improve the safety and efficiency of the transportation system and to enable new mobile applications and services for travelling, Intelligent Transportation Systems (ITS) have been developed. The field of Inter Vehicle communication, including vehicle to vehicle and Vehicle to Road Side has been recognized as an important component of ITS[1,2].

In VANET, vehicles act as nodes which can exchange information among each other without any infrastructure network establishment. In order to participate in such a network, a vehicle has to be equipped with the necessary radio communication hardware. Since each network node acts as wireless station and mobile router at the same time, distant vehicles can communicate with each other by using intermediate vehicles for packet forwarding [3].

VANET is also a type of MANET however the mobility pattern of VANET nodes is predefined as they move on specific paths and not in random direction. As the mobility pattern of VANET nodes is predictable, the limitation on limited storage capacity and high processing power does not exist [4].

Various Ad hoc routing protocols have been proposed by many researchers which suits VANET scenario. The Ad hoc protocols can be categorized as proactive protocols, reactive protocols and hybrid protocols. These protocols help in exchanging the data between source and destination through the intermediate nodes to forward the packets. Proactive or table driven protocols maintains a fresh lists of destinations and their routes by distributing the routing table information. A Reactive or on-demand protocol finds a route on demand by broadcasting the Route Request packets. A Hybrid routing protocol combines the features of both proactive and reactive protocols.

Large number of researchers has contributed their findings towards securing VANET [5]-[11]. However, detecting malicious behavior of a particular vehicle is yet to be incorporated. In this paper, Reactive AODV routing protocol has been enhanced with security feature, to detect the malicious behavior of the vehicle.

This paper is organized as follows; Section 2 describes the characteristics of VANET. Section 3 describes the VANET's architecture scenario which has been used for demonstrating the incorporated security feature in the AODV protocol. In Section 4 the performance evaluation has been carried out by analyzing RAODV protocol. Section 5 presents the conclusion and future scope.

2. CHARACTERISTICS OF VANET

Vehicular networks have specific characteristics which have to be taken into account while building the architecture. As stated in [13] VANETs comprise of radio-enabled vehicles which act as mobile nodes as well as routers for other nodes. In addition to the similarities to Ad hoc networks, such as short radio transmission range, self-organization, self management, and low bandwidth, VANETs can be distinguished from other kinds of Ad hoc networks as follows,

Highly Dynamic Topology: Due to the rapid changes in the speed of vehicles, the topology of VANET often changes.

Frequently Disconnected Network: Due to the above reason, the connectivity of the VANETs is subjected to change frequently. Especially when the vehicle density is low, it has higher probability that the network will be disconnected with a very short duration of communication.

Sufficient Energy and Storage: A common characteristic of nodes in VANETs is that nodes have ample energy and computing power (both storage and processing), since nodes are vehicles instead of small handheld devices.

Mobility Modeling and Prediction: Due to high movement of vehicles and dynamic topology, mobility model and prediction play an important role in network protocol design for VANETs.

Interaction with On-Board Sensors: The sensors in each vehicle can be used to get the vehicle position, their speed and direction to establish Ad hoc communication.

No Confidentiality for Safety Information: For safety applications, the information contained in a message is of interest for all road users, and hence message is not confident [14].

Central Authority: For the sake of security, each and every vehicle in the network has to be registered with a common Centralized Authority and should be assigned an unique identifier.

Power Consumption: In traditional wireless networks, nodes are power limited and their life depends on their batteries. But Vehicles can provide continuous power to their computing and communication devices [15].

3. ARCHITECTURE FOR VANET WITH CENTRALIZED AUTHORITY

In designing the system model, the following assumptions are brought into consideration. VANET consists of Vehicles and Road Side Unit (RSU) as their nodes. Each and every node has to be registered with the Centralized Authority. Each node will be assigned a unique identification by submitting their original identity like vehicle number. RSU will be maintained by the Government so that RSU will not malfunction at any cost.

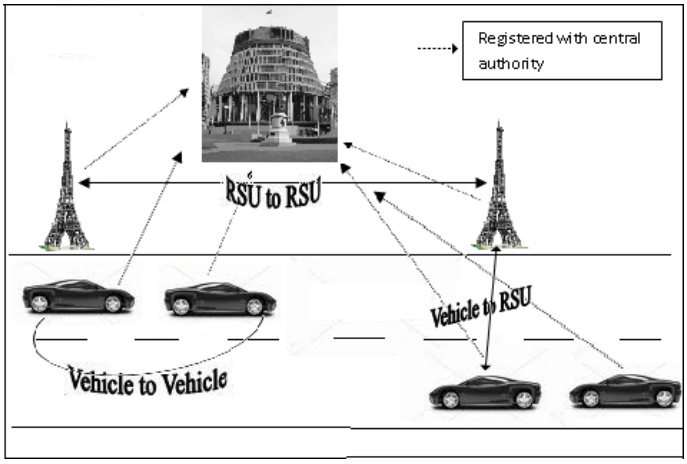

Fig.1. Architecture with Centralized Authority

Sample architecture is shown in Fig.1. In this model, a Centralized Authority with two RSU, and four vehicles, of which two travels in one direction and the other two in the opposite direction with uniform speed has been considered. All the nodes (RSU and vehicles) are registered initially with the base station which acts as a Centralized Authority. Each and every vehicle in the network will be placed with a special electronic device which provides Ad hoc network connectivity for them. Each vehicle equipped with the device will be a node in the network and can receive and relay other's messages through the wireless network. Vehicles in the network can communicate through intermediate vehicles and /or nearby fixed road side unit.

The message is transferred from one vehicle to other through RSU. The vehicle which enters first in each direction will receive the message from the RSU and then it passes it to the other vehicles in the same direction. RSU in the network stores the information like vehicle ID, speed, and type etc., of all the vehicles crossing its area with the help of onsite camera.

In this paper, we present RAODV protocol based on the AODV, which detects the malicious vehicle even after proper registration. Once a malicious vehicle has been detected by a central authority (CA), a warning message will be broadcasted to the nearby RSUs and vehicles in the vicinity area. As an initial measure, the packets will not be sent to the malicious vehicles. During the simulation period, if a vehicle behave maliciously then immediate action of isolating it from other vehicles is handled by RAODV protocol and it is evaluated using the metrics described below.

3.1 PERFORMANCE METRICS

Packet Delivery Ratio: Packet delivery ratio describes the loss rate of the packets. It also affects the maximum throughput. It can be defined as the ratio between the total numbers of the Constant Bit Ratio (CBR) packets delivered to the destination to the total numbers of packets sent by the source.

$$PDR = \frac{\sum_{i=1}^{n} receivedCBR_i}{\sum_{i=1}^{n} sentCBR_i} \times 100 \quad (1)$$

Dropped Packets: In a computer network, packet loss occurs when one or more packets travelling across a computer network fail to reach their destination. The total number of packets dropped during the transmission is calculated as follows,

$$DPackets = \sum_{i=1}^{n} SCBR_i - \sum_{i=1}^{n} RCBR_i \quad (2)$$

where,

DPackets –Dropped Packets

SCBR-Sent Constant Bit Ratio

RCBR-Received Constant Bit Ratio

Average End to End Delay: It includes all delays caused by buffering during route discovery, queuing at the interface, retransmission at the Medium Access Control (MAC), propagation and transfer times. In simpler terms the average End-to-end delay is the time it takes for a packet to travel across the network from source to destination.

$$EndtoEndDelay = \frac{\sum_{i=1}^{n} CBR_i(RT) - CBR_i(ST)}{Total\ no.ofG.P} ms \quad (3)$$

Routing Overhead: The ratio of total numbers of routing packets generated to the total number of data packets received during the simulation time.

$$Routing\ Overhead = \sum_{i=1}^{n} \frac{ControlPacketGenerated_i}{DataPacketreceived_i} \quad (4)$$

4. PERFORMANCE EVALUATION

4.1 SIMULATION ENVIRONMENT

NS-2 (Network Simulator-2) [16] has been used for performance evaluation. Vehicle behavior has been studied in the area of 1000m x 1000m. Each and every vehicle which participates in the network has to be registered with the base station which acts as a Centralized Authority.

The experiment uses fixed number of vehicles with CBR (Constant Bit Rate) as a traffic generator and uses a maximum of four CBR traffic, data transfer rate as 0.064Mbps at the vehicle speed 50, 75, 90, 100, 110 and 120 m/sec. The simulation parameters are summarized in Table.1.

Table.1. Simulation Parameters

Parameter	Value
Simulator	NS-2
Simulation Time	300sec
Centralized Authority (Base Station)	1
No. of Vehicles	4
No. of RSU	2
No. of CBR traffic	4
Vehicle Speed (m/sec)	50,75,90,100,110,120
Packet Size	512 KB
Transmission rate	0.064Mbps
Protocol	AODV
Area	1000m x 1000m
Antenna	Omni directional

In our system, it was assumed that initially all the vehicles including RSU are reliable. Since RSUs are deployed and maintained by trusted parties it is assumed that there is no possibility for the RSU to be compromised even at a later stage. It is assumed that there is a possibility for a vehicle to misbehave even after due registration. The initial screen shot of the vehicle is shown in Fig.2.

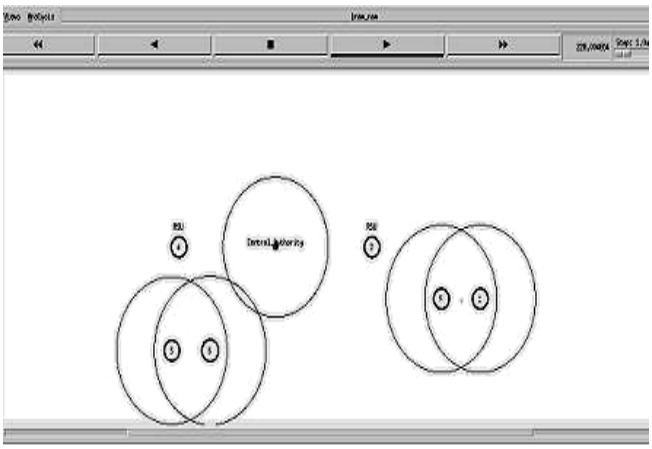

Fig.2. Initial Screen shot after node deployment

4.2 SIMULATION RESULTS

Packet Delivery Ratio, Average End_to_End Delay, Dropped Packets and Routing Overhead are the performance metrics considered. The performance evaluation was carried out considering these metrics using RAODV protocol with and without malicious node.

Packet Delivery Ratio: Fig.3 shows the performance of the RAODV protocol on the basis of PDR for various speeds of the vehicles. Initially the performance was analyzed by considering all the vehicles as trusted, which gave a PDR of 99% in average irrespective of the speed of the vehicles in free attack. When vehicle 4 started misbehaving, it must be identified as malicious either by the CA or RSU and packets should not be send it. When the total number of packets sent to the vehicle decreases obviously the PDR should also decrease. The average PDR of 27% was obtained with a malicious node being detected. The decrease in PDR clearly indicates that RAODV has successfully detected the malicious node.

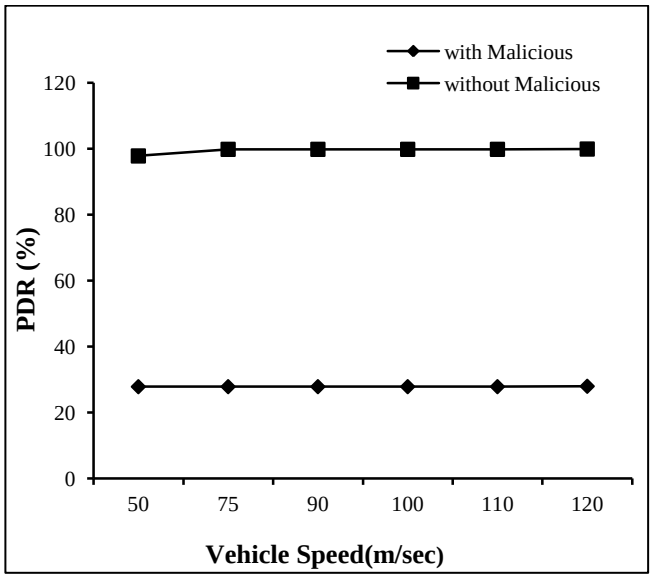

Fig.3. Vehicle Speed Vs PDR

Number of Dropped packets: In this simulated environment the value of the sent CBR was around 16252 uniformly for various vehicle speeds with few packets being dropped here and there when all the vehicles were reliable. When vehicle 4 started misbehaving, it will not receive packets and hence the received CBR was around 4528, so the number of dropped packets was around 11000 irrespective of vehicle speed when the malicious node was detected by the RAODV. Fig.4 shows the number of dropped packets after detecting a malicious vehicle.

Average end to end delay: Fig.5 shows average end to end delay for various vehicle speeds with and without malicious vehicle. Normally, with the volume of packets in the observed results, it is clear that when more number of packets were sent the delay will be more and the lesser the packets, the lesser the delay. The chart clearly indicates that with a malicious vehicle being detected the number of packets being sent is less and hence the delay.

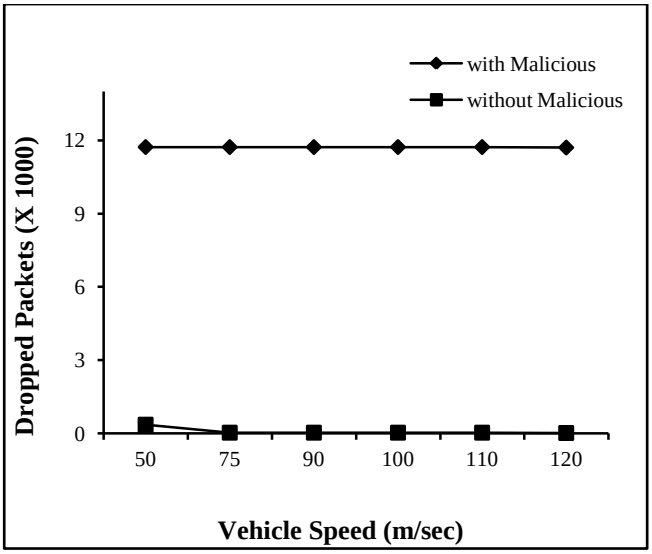

Fig.4. Vehicle Speed Vs No. of dropped packets

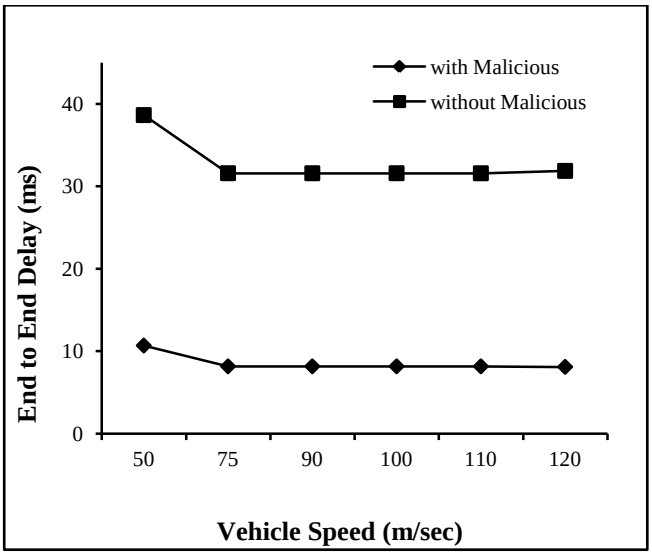

Fig.5. Vehicle Speed Vs End to End delay

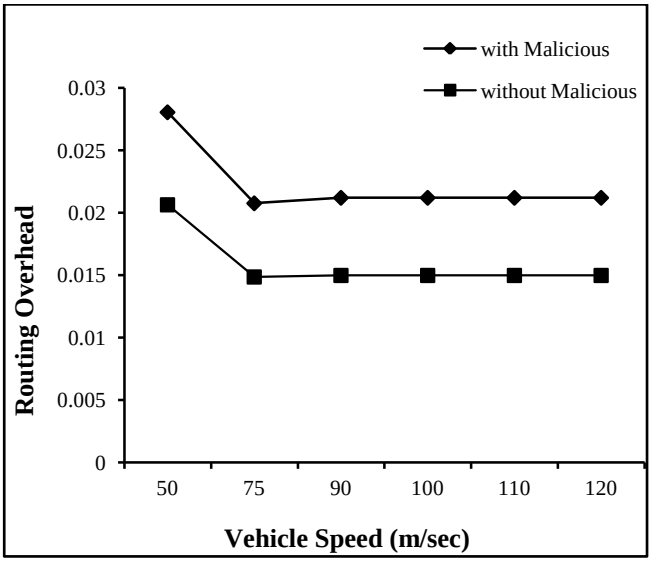

Fig.6. Vehicle Speed Vs Routing Overhead

Routing Overhead: Fig.6 shows the performance of RAODV protocol on the basis of routing overhead by varying the vehicle speed. In the simulated environment the generated packets was around 16252. With one malicious vehicle being detected the number of dropped packets and control packets increases which in turn increases the routing overhead value.

6. CONCLUSION

In this paper, we have presented the important and unique characteristics of VANET. Architecture has been designed with a Centralized Authority to which every vehicle and RSU registers. AODV protocol has been strengthened as RAODV protocol with an added security feature of detecting malicious vehicle. The proposed architecture has been evaluated for the performance metrics of Packet Delivery Ratio, Average End to End Delay, Routing Overhead and Number of dropped packets. The obtained results clearly indicated that the RAODV protocol identifies a misbehaving vehicle even after proper registration. In this paper, an attempt has been made to enhance AODV by incorporating security in to it. In similar line, research can be focused to enhance the protocol for incorporating other security related issues. Other ad hoc protocol can also be enhanced as a feature research scope.

REFERENCES

[1] U.S Department of Transporation, Intelligent Transportation Systems (ITS) Home, 2011, http://www.its.dot.gov/index.htm.

[2] Yi Qian and Nader Moayeri, "Design Secure and Application-Oriented VANET", *Proceedings of the IEEE Conference on Vehicular Technology*, 2008.

[3] Sven Jaap, Marc Bechler and Lars Wolf, "Evaluation of Routing Protocols for Vehicular Ad Hoc Networks in city Traffic Scenarios", *Proceedings of the 11th EUNICE Open European Summer School on Networked Applications*, pp. 584-602, 2005.

[4] Saira Gillani, Imran Khan, Shahid Qureshi and Amir Qayyum, "Vehicular Ad Hoc Network (VANET): Enabling Secure and Efficient Transportation System", *Technical Journal, University of Engineering and Technology, Taxila*, Vol. 13, 2008.

[5] R. Lu, X. Lin, H. Zhu, P. Ho and X. Shen, "ECPP: Efficient conditional Privacy Preservation Protocol for Secure Vehicular Communications", *Proceedings of the IEEE INFOCOM*, pp. 1903- 1911, 2008.

[6] P. Golle, D. Greene and J. Staddon, "Detecting and Correcting malicious data in VANETS", *Proceedings of the ACM VANET*, pp. 29-37, 2004.

[7] J.P. Hubaux, S. Capkun and J. Luo, "The security and privacy of smart vehicles", *IEEE Security and Privacy Magazine*, Vol. 2, No. 3, pp. 49-55, 2004.

[8] C. Zhang, X. Lin, R. Lu and P.H. Ho, "Raise: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks", *IEEE International Conference on Communications*, 2008.

[9] X. Lin, X. Sun, P. Ho and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for Vehicular

Communications", *IEEE Transactions on Vehicular Technology*, Vol. 56, No. 6, pp. 3442-3456, 2007.

[10] M. Lott, R. Halfmann, E. Schultz and M. Radimirsch, "Medium access and radio resource management for ad hoc networks based on UTRATDD", *Proceedings of the ACM MobiHoc*, pp. 76-86, 2001.

[11] Q. Xu, T. Mak, J. Ko and R. Sengupta, "Medium access control protocol design for vehicle-vehicle safety messages", *IEEE Transaction on Vehicular Technology*, Vol. 56, No. 2, pp. 499-518, 2007.

[12] H. Zhu, X. Lin, H. Zhu, P. Ho and X. Shen, "AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks", *IEEE International Conference on Communication*, pp. 1436-1440, 2008.

[13] Fan Li and Yu Wang "Routing in Vehicular Ad Hoc Networks: A Survey", *IEEE Vehicular Technology Magazine*, Vol. 2, No. 2, pp. 12-22, 2007.

[14] Emanuel Fonscca and Andreas Festag, "A Survey of Existing approaches for Secure Ad Hoc Routing and their Applicability to VANETS", *NEC Technical Report, NEC Network Laboratories*, pp. 1-28, 2006.

[15] Ioannis Broustis and Michalis Faloutsos, "Routing in Vehicular Networks: Feasibility, Security and modeling Issues", *International Journal of Vehicular Technology*, Vol. 2008, pp. 1-8, 2008.

[16] NS2 Network Simulator

[17] http://www.isi,edu/nsnam/ns.