Detecting Malicious Vehicles and Regulating Traffic in VANET using RAODV Protocol

V.Lakshmi Praba,
Govt Arts College for Women, Sivagangai

A.Ranichitra,
Research Scholar of Manonmaniam Sundaranar University, Tirunelveli.

ABSTRACT
Recent developments in wireless communication technologies led to the evolution of Vehicular Ad-hoc Network (VANET). The main goal of VANET is to provide communication between vehicles without compromising security. Controlling the traffic and identifying misbehaving (malicious) vehicles plays an important role in road safety. A vehicle can be defined as malicious if it doesn't send acknowledgement to a trusted authority or if the speed of the vehicle suddenly changes or if its registration renewal time expires. Such malicious vehicles have to be isolated and should not be allowed to participate in the network further.

In this paper, traffic control is achieved by maintaining the distance between the vehicles and the defined malicious vehicles are isolated and further communication is stopped with the malicious vehicle. The existing Ad-hoc On Demand Distance Vector (AODV) protocol has been suitably modified to achieve the above mentioned road safety measures and has been made as Robust AODV protocol (RAODV). RAODV was analyzed using the performance metrics Packet delivery ratio, Dropped packets, average End_to_End delay and Routing Overhead to show that it achieves the goals presented above.

Keywords
VANET, AODV, RAODV, CA, RSU, Malicious

1. INTRODUCTION
Vehicular Ad-hoc networks (VANET) is a new technology that has recently evolved and is widely finding application in areas such as traffic and road safety, payment collection, tourist guiding information and natural hazards. VANET integrates Ad-hoc networks, Sensor networks, Wireless LAN and Cellular networks. In VANET, vehicles act as nodes which can exchange information between each other without any infrastructure network establishment.

All the vehicles in the network has to be equipped with a special electronic device which will provide Ad-hoc connectivity between the vehicles. It is necessary in future for the drivers to be updated with the happenings in and around the moving vehicle. This is possible only with the communication that is established between the participating vehicles of VANET. Moreover, highly dynamic behavior and directional mobility of the vehicles are the important characteristics.

Vehicles in the network can participate in two road scenarios, high way scenario where vehicles will be less and moves very fast and city scenario with more road junctions where the number of vehicles will be high and the vehicles will face many obstacles like pedestrians, other vehicles.

With the significant contributions of various researchers in Vehicular network, securing the VANET plays a vital role. All the messages that are communicated between the participating nodes have to be broadcasted to all the vehicles in the vicinity so that all drivers will be updated with the nearby happenings. The messages transferred between vehicles may be critical that authentication of the sender and a check of message integrity are essential for road safety[1] and an adversary can forge bogus information to mislead other drivers and even cause deliberate traffic accident. Thus data interchanged over VANETs play a vital role in traffic safety. Such data must be accurate as lives may depend on this application[2]. Therefore to achieve anonymous authentication has become a fundamental requirement for securing VANET[3]. Since every participating node in the network may misbehave, this misbehavior has to be identified and isolated from the network. Besides safety applications, VANET also provide comfort applications to the passengers the information like weather information, e-commerce through mobile and internet access [4].

In this paper, Vehicles movement in city traffic was considered. RAODV protocol detects all the misbehaving vehicles with help of a Central Authority (CA) and a warning message will be broadcasted to all the vehicles and RSU's in the vicinity. As an initial security measure, RAODV stops communicating with the detected malicious vehicles and drops the packets sent to the malicious vehicles. Thus the behavior of the vehicles in the city scenario with nine junctions, 16 vehicles and 4 RSUs were studied using various performance metrics.

The organization of paper is as follows; Section 2 overviews the contribution of various researchers in securing VANET. Section 3 presents architecture. Section 4 describes the proposed protocol. The performance evaluation of the vehicles in city scenario has been carried out by increasing the number of malicious vehicles in Section 5 and the paper concludes in Section 6.

2. RELATED WORK
Sanzgiri et al[5] proposed ARAN protocol which is as efficient as AODV in discovering and maintaining routes. The protocol consists of preliminary certification process which is followed by a route instantiation process. It also provides a solution for securing the routing information by incorporating authentication and repudiation services using pre-determined cryptographic certificates.

Li et al[6] presents a secure AODV protocol, SEAR (Secure Efficient Ad-hoc Routing) which identifies authenticators of each node using one way hash function. SEAR is based on symmetric cryptography but asymmetric cryptography is used only for initial keys distribution.

Li et al [7] proposed a Token Routing Protocol (TRP), based on the security enhancement of AODV protocol. TRP generates token using hash-chain algorithm which is used to identify the authenticity of the routing packets and to choose correct route for data packets. As TRP uses hash algorithm, it provides comparable security with a significant reduction in delay and energy consumption.

Shen et al [8] proposed three basic frameworks; a policy based plug-in security framework, multi-layer QoS guided routing and a proportional integral derivative (PID) controller for a distributed dynamic management system. This model aims to maximize QoS and security.

Raza et al [9] proposed a model which identifies malicious nodes in which each node calculates trust level of its neighbors based on the opinions of the other node. If the trust value of a node is lower than a predefined threshold value, then the node is identified as malicious and it is isolated from the path. The scheme has been evaluated for impersonation attack, colliding nodes attack and black hole attack.

Akhlaq et al[10] proposed Classified AODV protocol which includes the routing mechanism and exchange of security parameters in single. In this model, security achieved is based on the utility of digital certificates issued by Certification authority. It was assumed that trust relationship exists between CA and all participating nodes. Authentication is achieved by double encryption of session key and Data confidentiality through data encryption using AES algorithm.

Xu et al[11] proposed a novel scheme which implements ARAN protocol which is more efficient than original ARAN in signature generation and verification by using Hash to Obtain Random Subset(HORS) One-time signature instead of digital signatures. This scheme provides authenticity of mobile nodes and ensures protections using proxy signature for route reply and transitive signature for route aggregation. Token generated contains creator's identity and public key and is signed by the creator.

Bhargava et al [12] proposed a security scheme to prevent internal attacks for AODV protocol. The intrusion detection and response model is presented to identify and remove the attacks. The system shows that the overhead is marginal.

Kravets et al [13] integrated the trust level of a node and the security attributes of a route. SAR protocol uses sequence numbers and timestamps to avoid replay attacks. Trust level key authentication is used to prevent interception and subversion threats. Modification and fabrication of messages can be avoided by verifying the digital signatures of the transmitted packets. Even though the discovered route is not shortest route it will be very secure.

Jain et al[14] modified the AODV protocol by including the source route accumulation feature. TAODV is trusted based protocol which extends the routing table and routing messages of AODV with trust information which can be updated directly through monitoring the neighbor node. TAODV uses the opinion based on the cryptographic schemes that perform signature generation and verification at every routing packet. This system reduces the overhead and the trustworthiness of the routing procedures can be guaranteed as well.

Zapatta[15] proposed is a security extension of the AODV Protocol, based on Public key cryptography. SAODV Routing messages are digitally signed in order to guarantee their integrity and authenticity. The Hop Count field which is to be changed by every node is mutable information. SAODV protects this information and the scheme leverages the idea of hash chains. Each node possesses a key pair that makes use of an asymmetric cipher.

3. ARCHITECTURE FOR VANET

Architecture has been designed by considering the following characteristics in a VANET scenario.

- VANET consists of vehicles and Road Side Units (RSUs) as their nodes.
- All vehicles and the RSUs who want to participate in the network have to be registered with the Centralized Authority (CA) (Figure 1) and will be assigned a unique identification by submitting their original identity.
- RSU will be maintained either by the government or any trusted third party and will not malfunction at any cost.
- After registration the vehicles can participate in the network.

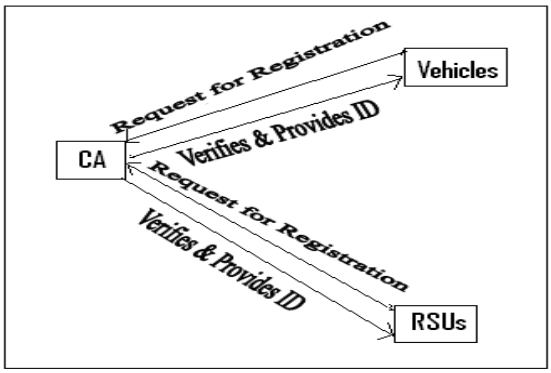

Figure 1: Registration of vehicles and RSUs with CA

The working principle of RAODV is as given in the following algorithm.

Step 1: Vehicles and RSU Initiates the request for registration process.

Step 2: On receiving the request, CA makes a request about their real identity.

Step 3: CA verifies the identity and sends an unique ID for each vehicle and RSUs.

Step 4: The vehicles and the RSUs communicate with each other.

Step 5: If any vehicle V_i misbehaves after registration, it will be identified by the CA using RAODV protocol.

Step 6: The misbehaving vehicle V_i will be isolated from the communicating environment.

This paper considers a city traffic scenario with nine junctions in which every road has two lanes (Figure 2). The vehicle movement will be based on the movement of the other vehicles. If the vehicle moving ahead slows down then the vehicles behind it, have to decelerate. If needed, when there is a traffic jam at the junction, the information will be broadcasted to the approaching vehicles and the crossing vehicle has to wait until all vehicles crosses the junction or switches the lane and then it has to proceed.

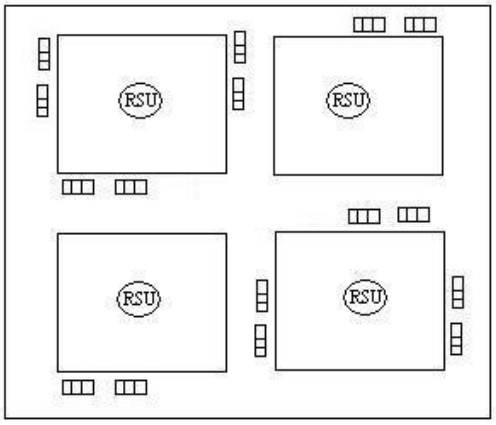

Figure 2: City Scenario

4. RAODV

Ad-hoc On Demand Distance Vector (AODV) [16,17] protocol is a reactive protocol that enables dynamic, self-starting, multihop routing between participating mobile nodes to establish and maintain an Ad-hoc network. AODV can handle low, moderate, and relatively high mobility rates, as well as a variety of data traffic levels. Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are some of the message types defined by AODV. The security feature for detecting malicious node has not been incorporated in AODV protocol [18, 19]. As it is found that AODV is best suited for VANET, it was decided to enhance AODV by adding this security feature.

There is a possibility of a vehicle to misbehave even after proper registration. VWAIT, MDETECT and VSPD are the procedures defined in RAODV protocol to detect the misbehaving vehicles and regulate the traffic. The procedure VWAIT makes the vehicles to wait for few seconds in order to regulate traffic, MDETECT detects the malicious vehicles and VSPD finds the variation in distance between vehicles.

VWAIT decreases the vehicle speed of the particular vehicle and inform the same to the vehicles behind it so as to avoid collision.

If a vehicle is not acknowledging the trusted Vehicle's/ RSU's /CA's RREQs message or if its registration renewal time expires then that vehicle is defined as malicious by the MDETECT procedure in RAODV. In the simulated environment, uniform vehicle speed has been set as 50 m/s which leads to uniform distance between vehicles and the distance between the vehicles is 10 meters.

Vehicle speed detection procedure VSPD finds any variation in distance between the vehicles. If there is any change in the speed of a particular vehicle, then VSPD defines the vehicle as malicious.

The algorithm for the above procedures is as follows.

4.1 Algorithm

```
// initialize all vehicles as trusted vehicles (TV)
var
     number_of_vehicles = n;
     number_of_RSU = r;
     speedlimit = 50; // m/s
    vexpriytime=100; //seconds
begin
  // to regulate traffic//
do
{
   if [DISTANCE (V(i),V(i+1) <=10]
       call  vWait(v(i));
      i=i+1;
} while (i<=n);
// detecting malicious vehicles//
do
{
if not [ (v(i).sentAckTo(TV_k)   ||   (v(i).sentAckTo(RSU_j)) ||
v(i).sentAckTo(CA) ]
        v(i).malicious = true;
elseif [ v(i).expirytime < currenttime]
        v(i).malicious= true;
else
       call VSPD;
endif
i=i+1;
}
while (i<=n);
end;
```

To be precise, avoiding collision between vehicles and isolating malicious vehicles are the two major contribution of this RAODV protocol.

4.2 Performance Metrics

4.2.1 Packet Delivery Ratio

Packet delivery ratio is 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 from the source.

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

4.2.2 Dropped Packets

The total number of packets which fails to reach the destination is defined as the dropped packets.

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

where DPackets –Dropped Packets
SCBR-Sent Constant Bit Ratio
RCBR-Received Constant Bit Ratio

4.2.3 Average End to End Delay

Average End-to-end delay is the time taken for a packet to travel across the network from the source to the destination.

$$EndtoEndDelay = \frac{\sum_{i=1}^{n} CBR_i(RT) - CBR_i(ST)}{Totalno.ofG.P} ms \quad (3)$$

4.2.4 Routing Overhead

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

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

5. PERFORMANCE EVALUATION

5.1 Simulation Environment

NS-2 (Network Simulator-2) [20] 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, at the vehicle speed 50m/sec and uses CBR (Constant Bit Ratio) as a traffic generator. The CBR traffic is varied as 7 and 8 and the performance were analyzed. The simulation parameters are summarized in Table 1.

In the 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 study is performed by varying the number of malicious node in the vicinity area using Packet delivery ratio, Dropped Packets, Average End to End delay and Normalized Routing Load as metrics.

Table 1. Simulation Parameters

Parameter	Value
Simulator	NS-2
Simulation Time	150sec
Centralized Authority (Base Station)	1
No. of Vehicles	16
No. of RSU	4
No. of CBR traffic	7 and 8
Vehicle Speed (m/sec)	50
Packet Size	512 KB
Transmission rate	0.064 Mbps
Protocol	RAODV
Area	1000m x 1000m
Antenna	Omni directional

5.2 Simulation Results

For evaluating the AODV protocol, it was assumed that the vehicles and RSUs are already registered with the central controller and all the vehicles are moving with a uniform speed within the described area.

Once a malicious vehicle is detected by RAODV protocol, packets sent to it will automatically be dropped so that it is isolated from other vehicles and stops further communications to that vehicle. In order to prove that this has been achieved, it is demonstrated using the metrics of Packet delivery ratio, Number of dropped packets, End_to_End delay and Routing Overhead. The performance was analyzed by increasing the number of malicious vehicles using the RAODV protocol.

5.2.1 Packet Delivery Ratio

Figure 3 shows the performance of the RAODV protocol on the basis of PDR for various CBR traffics by increasing the number of malicious vehicles in the communication range. Initially the performances were analyzed by considering all the vehicles as trusted, which gave 69.6213% with number of CBRs 7(Table 3). When vehicles start to misbehave, it will be identified by the central controller and it should not sent packets to the malicious vehicle as an initial measure. When the total number of sent packets decreases with increase in the malicious vehicle obviously the PDR should also decrease irrespective of the number of CBR traffics.

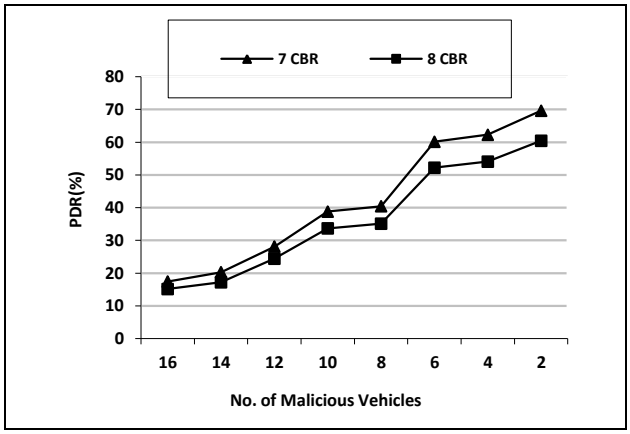

Figure 3: No. of Malicious Vehicles Vs PDR

5.2.2 Dropped packets

Number of vehicles versus dropped packets is shown in Figure 4. When all the vehicles are reliable in the simulated environment the value of received CBR was 9174 irrespective of number of CBR traffic with a few packets being dropped here and there (Table 3).

When the vehicles start to misbehave, the number of received CBR will decrease, which will increase the number of dropped packets with all number of CBR traffics when the malicious vehicle was detected by RAODV.

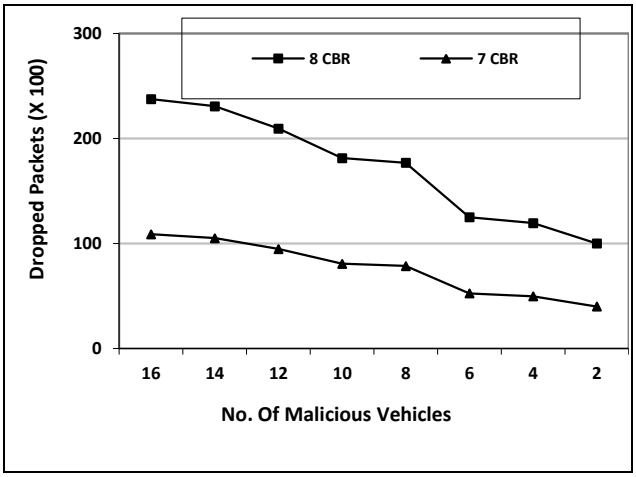

Figure 4: No. of Malicious Vehicle Vs Dropped Packets

5.2.3 Average End to End Delay

Figure 5 shows average End to End delay for the various number of CBR traffics. From the observed results it is clear that when the sent packet decreases, the delay would be less but when all the vehicles are malicious more control messages will be transferred which will increase the delay.

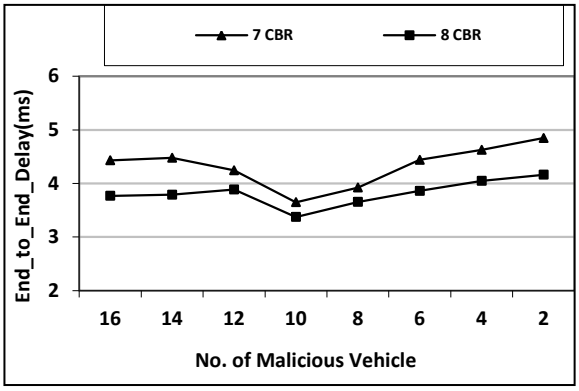

Figure 5: No. of Malicious Vehicle Vs End_to_End Delay

5.2.4 Normalized Routing Overload

Figure 6 shows the performance of RAODV protocol on the basis of routing overhead by varying the number of malicious node. As the number of malicious vehicles increases the number of received packets decreases which in turn increases the control packets. Hence the routing overhead increases gradually with the increase in the number of malicious vehicles.

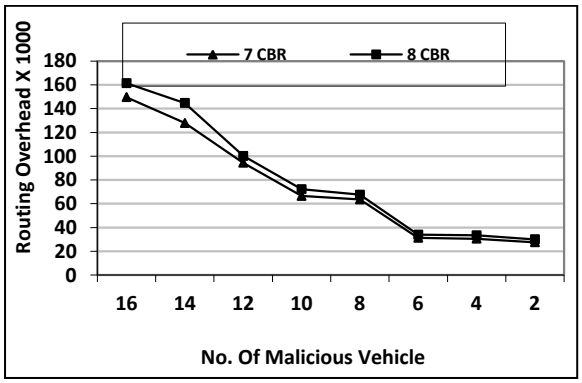

Figure 6: No. of Malicious Vehicle Vs Routing Overhead

Following were the findings from the obtained results

- Increase in number of malicious vehicle will decrease the Packet Delivery Ratio.
- Increase in number of malicious vehicle increases the number of dropped packets.

  From the above findings, it is proved that malicious vehicles were not used for transmitting packets.
- Increase in end to end delay shows that malicious vehicles are not acknowledging the trusted Vehicle's/ RSU's /CA's RREQs message and the packets could not reach the destination.
- Increase in number of malicious vehicle will increase the routing overhead by transmitting more number of control packets rather than data packets. With the obtained data, it is clear that malicious vehicle will not respond to the trusted vehicles/RSUs/CA which increases the control packets.

Table 2 shows the Packet Delivery Ratio (PDR in %) of the city scenario in which all the vehicles become malicious at a given time. At the particular time of 15 sec, PDR was 3.9346% which is obvious because no vehicle will transmit packets from that time. At the time of 135 sec, almost all the packets were transmitted before the vehicles become malicious and the PDR was 87.2262%. PDR values show that RAODV works efficiently in identifying malicious nodes and regulating the traffic.

Table 2: PDR values when all vehicles becomes malicious at the given time

Time	PDR(%)
15	3.9346
30	9.03542
45	16.0109
60	25.0572
75	36.1308
90	48.9155
105	61.6785
120	74.4414
135	87.2262

6. CONCLUSION

This paper focuses the importance of securing VANET. Vehicles and RSUs in VANET should be registered with the central controller so that every vehicle in the network will be authorized. City Scenario is considered to analyze the vehicle's behavior. As regulating the traffic and identifying the misbehaving vehicles plays an important role in VANET, the existing AODV protocol has been enhanced as RAODV by suitably incorporating the security features which detects the malicious behavior of the vehicle. A vehicle can be malicious, if it doesn't respond to the control messages of RAODV or if its renewal time expires or if there is a sudden change in the vehicle speed which may lead to the collision of the vehicles.

Packet Delivery ratio, Dropped Packets, Average End_to_End Delay and Routing overhead were the performance metrics taken for evaluating RAODV protocol. The obtained results clearly indicate that the RAODV protocol identifies the misbehaving vehicle even after proper registration. In this paper, the existing AODV protocol is enhanced with the security suitable for VANET scenario. In similar line additional security feature could be incorporated in AODV protocol as the feature research focus.

7. REFERENCES

[1] H.K Choi, I.H Kim, J.C Yoo, "Secure and Efficient Protocol for Vehicular Ad-hoc Network with Privacy

Preservation", EURASIP Journal on Wireless Communications and Networking", 2011.

[2] Jose Maria de Fuentes, Ana Isabel Gonzaez-Tablas, Arturo Ribagorda, "Overview of Secuirty issues in Vehicular Ad-hoc Networks" 2010.

[3] Yipin Sun, Rongxing Lu,Xiaodong Lin, Xuemin Shen, Jinshu Su," An Efficient Pseudonymous Authentication Scheme with strong Privacy Preservation for Vehicular Communications" IEEE Transactions on Vehicular Technology,2010.

[4] T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato, and Y. Nemoto, "A stable routing protocol to support its services in vanet networks" IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3337–3347, November 2007.

[5] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer," A secure routing protocol for Ad-hoc networks"Proceedings, 10th IEEE International Conference on Network Protocols,Nov 2002,pp 78 – 87.

[6] Qing Li, Meiyuan Zhao,Jesse Walker, Yih-Chun Hu, Adrian Perrig, Wada Trappe, " SEAR: A Secure Efficient Ad-hoc On Demand Routing Protocol for Wireless Networks" ASIACCS'08.

[7] Leiyuan Li , Chunxiao Chigan "Token Routing: A Power Efficient Method for Securing AODV Routing Protocol", Proceedings of the 2006 IEEE International Conference on Networking, sensing and Control, pp 29 - 34.

[8] Zheng Ming Shen , J.P Thomas, "Security and QoS Self-Optimization in Mobile Ad-Hoc Networks" IEEE Transactions on Mobile Computing, vol 7, Issue 9, Sep 2008, pp 1138 – 1151.

[9] Imran Raza, S.A. Hussain,"Identification of malicious nodes in an AODV pure Ad-hoc network through guard nodes" Elsevier Computer Communications vol 31, Issue 9, June 2008, pp 1796–1802.

[10] Monis Akhlaq, M Noman Jafri, Muzammil A Khan, and Baber Aslam, "Addressing Security Concerns of Data Exchange in AODV Protocol", Proceedings of World Academy of Science, Engineering and Technology, vol 16, Nov 2006, pp 29-33. ISSN 1307-6884.

[11] Shidi Xu, yi Mu and Willy Susilo,"Authenticated AODV Routing Protocol Using One-Time Signature and Transitive signature Schemes", Journal of Networks, Vol 1 No. 1, May 2006, pp 47 – 53.

[12] Sonali Bhargava and Dharma P.Agrawal," Secuirty Enhancements in AODV Protocol for Wireless Ad-hoc Networks", 54th IEEE Vehicular Technology Conference 2001,vol 4, **pp** 2143 – 2147

[13] R.Kravets, S.Yi, and P.Naldurg," A Security-Aware Routing Protocol for Wireless Ad-hoc Networks", In ACM Symposium of Mobile Ad-hoc Networking and Computing 2001.

[14] Yogendra Kuamr Jain and Pankaj Sharma," Trust Based Ad-hoc On-demand Distance Vector for MANET",National Conference on Secuirty Issues in Network Technologies (NCSI 2012) .

[15] Manel Guerrero Zapata, "Secure Ad-hoc On-Demand Distance Vector(SAODV) Routing", draft-guerro-manet-saodv-06.txt, September 5,2006.

[16] C.Perkins, E. Belding-Royer, S.Das, "Ad-hoc On-Demand Distance Vector(AODV) routing", RFC 3561,July 2003.

[17] Mubashir Husain Rehmani, Aline Carneiro Viana, Sidney Doria, Reda Senouci, " A Tutorial on the implementation of Ad-hoc on Demand Distance Vector(AODV) Protocol in Network Simulator (NS-2), jun 2009.

[18] Alekha Kumar Mishra, Bibhu Dutta Sahoo, "A Modified Adaptive-SAODV Prototype for Performance Enhancement in MANET",IJ-CA-ETS, vol 1, issue 2, Sep '09, pp 443-447.

[19] Manel Guerrero Zapata, N.Asokan, "Securing Ad-hoc Routing Protocols" ACM 2002.

[20] NS2 Network Simulator http://www.isi,edu/nsnam/ns

APPENDIX

Table 3: Simulation data of various metrics by increasing the number of malicious vehicles

		Number of Malicious Vehicles							
Metrics		**2**	**4**	**6**	**8**	**10**	**12**	**14**	**16**
PDR	**7 CBR**	69.6213	62.2752	60.1351	40.4493	38.7949	28.1248	20.3005	17.4471
	8 CBR	60.4427	54.0651	52.2071	35.1166	33.6803	24.4169	17.2091	15.1469
No. Dropped Packets	**7 CBR**	4003	4971	5253	7847	8065	9471	10502	10878
	8 CBR	6004	6972	7254	9848	10066	11472	12566	12879
End to End delay	**7 CBR**	4.84547	4.62581	4.43859	3.92271	3.6494	4.24321	4.47727	4.43018
	8 CBR	4.16272	4.04716	3.8592	3.65442	3.37363	3.88588	3.78808	3.76795
Routing Overhead	**7 CBR**	0.02758	0.03059	0.03130	0.06360	0.06651	0.09444	0.12785	0.14963
	8 CBR	0.03009	0.03339	0.03395	0.06754	0.07218	0.10011	0.14472	0.16137