Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 2 – No.3, June 2015 – www.caeaccess.org

EDMVP: Efficient Detection for Malicious Vehicles using AODV Protocol

Mandeep Kaur Saggi
Research Scholar, Dept of CSE
Jalandhar, Punjab

Anshu Joshi
Research Scholar, Dept of CSE
Jalandhar, Punjab

ABSTRACT
The VANETs are a subset of Mobile Ad-hoc NET works (MANETs) in which communication nodes are mainly vehicles. Every vehicle in VANET must be authenticated to establish a reliable and secure network communication. In this paper, a security approach has been proposed in AODV protocol to detect a malicious vehicle. A vehicle can be defined as malicious if it doesn't send acknowledgement to a trusted authority or if it's not registered with the centralized authority. Such malicious vehicles have to be isolated and should not be allowed to participate in the network & further communication is blocked with the malicious vehicles. Sample architecture with centralized control unit, RSUs and some vehicles is illustrated to demonstrate the added security feature. The Proposed protocol was analyzed using the performance metrics Packet Delivery Ratio, Dropped Packets and End to End Delay.

Keywords
MANET, VANET, Malicious node, V2V communication, Attacks.

1. INTRODUCTION
VANET have emerged as an exciting research and application area. Increasingly vehicles are being equipped with embedded sensors, processing and wireless communication capabilities opening a myriad of possibilities for powerful and potential life changing applications on safety, efficiency, comfort, public collaboration and participation while they are on the road The biggest problem regarding the increased use of Private transport is the increasing number of fatalities that occur due to accidents on the roads. Recently, with the advancement in technology more and more vehicles are being embedded with GPS and Wi-Fi devices that are connected in a self organized way, this enables vehicle to vehicle (V2V) communication, forming a Vehicular Ad-hoc Net work (VANET) [1].

A VANET will be a major step toward the realization of intelligent transportation systems. Nowadays, a large number of car manufacturers are supplying vehicles with onboard computing and wireless communication devices, in-car sensors, and navigation systems (e.g., GPS and Galileo) in preparation for the deployment of large-scale vehicular networks. By using different sensors (e.g., road and weather conditions, state of the vehicle, radar and others), cameras, computing and communication capabilities, vehicles can collect and interpret information with the purpose of helping the driver to make a decision, particularly in driver assistance systems. This infrastructure is assumed to be located along the roads and infrastructure can communicate to each other is called as inter roadside or infrastructure-to-infrastructure (I2I) communication. These types of communications infrastructure allow vehicles to share different kinds of information for example protection information for the purpose of post-accident, accident prevention investigation or traffic jams.. Road users employ various applications for safety and efficiency, traffic management, infotainment, warning, comfort, maintenance, music sharing and network gaming. In VANET, vehicles may behave selfishly by not forwarding messages for others in order to save power and bandwidth. The proposed protocol detects all the misbehaving vehicles with help of a Central Authority (CA) and a warning message will be broadcasted to all the trusted vehicles and RSU's in the vicinity. As an initial security measure, the proposed protocol stops communicating with the detected malicious vehicles and drops the packets sent to it and is voids collision between vehicles in order to regulate the traffic.

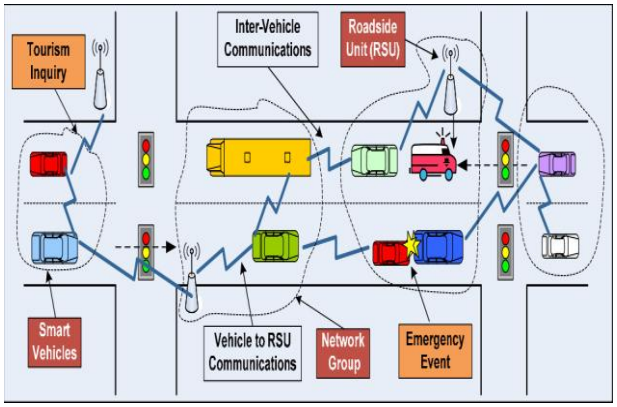

Fig 1: A basic structure of VANETs [2]

This paper is organized as follows. In Section 2, we define the Related Work in VANET. Section 3 present the Major attacks in VANET Section 4 explains the proposed work. Section 5 explains the method used for simulation model & presents factual results. At last, Section 7 concludes the paper.

2. RELATED WORK
In VANET a common security threat of malicious attacks is introduced.

Raza et al [8] 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.. This paper presents a guard node based scheme to identify malicious nodes in Ad hoc On-Demand Distance Vector (AODV) protocol. In this scheme each node calculates trust level of its neighboring nodes for route selection. Performance of the scheme has been evaluated for three different types of malicious attacks (impersonation attack, colluding nodes attack and black hole attack) .

The authors try to solve the problem of Wormhole Attack detection.. The author proposes a scheme in which they use a special packet called Decision Packet. After the route has been set up between a source node and destination node, the former gets the information about all nodes in the path from RREP packet which contains all nodes identity take which has been forming route from source to destination node in recent identified path. If an attacker by somehow changes the hop count value it will result in a change, in hash value of the packet will be consequently discarded [3].

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.

Akhlaq et al [7] 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

3. ATTACKS IN VANET

Attacker's role is important in vehicular network due to launching different type of attacks. The objective of attackers is to create problems for other users of the network by changing the contents type of messages Attackers can be classified according to scope, nature, and behavior of attacks as follow:

3.1 Attacker's Model

To classify the capacities of an attacker, we define four dimensions.

3.1.1 Insider vs. Outsider

The insider is an authenticated member of the network that can communicate with other members. As will be explained later, this means that he possesses a certified public key. The outsider is considered by the network members as an intruder and hence is limited in the diversity of attacks he can mount (especially by misusing network-specific protocols).

3.1.2 Malicious vs. Rational

A malicious attacker seeks no personal benefits from the attacks and aims to harm the members or the functionality of the network. Hence, he may employ any means disregarding corresponding costs and consequences. On the contrary, a rational attacker seeks personal profit and hence is more predictable in terms of the attack means and the attack target.

3.1.3 Active vs. Passive

An active attacker can generate packets or signals, whereas a passive attacker contents himself with eavesdropping on the wireless channel.

3.1.4 Local vs. Extended

An attacker can be limited in scope, even if he controls several entities (vehicles or base stations), which makes him local. An extended attacker controls several entities that are scattered across the network, thus extending his scope. This distinction is especially important.

3.2 Attackers

3.2.1 Selfish Driver

The general idea for trust in Vehicular Network is that all vehicles must be trusted initially, these vehicles are trusted to follow the protocols specified by the application, some drivers try to maximize their profit from the network, regardless the cost for the system by taking advantage of the network resources illegally

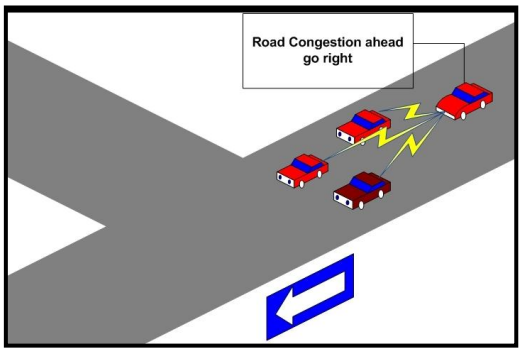

Fig 2: Selfish Driver

3.2.2 Malicious Attacker

This kind of attacker tries to cause damage via the applications available on the vehicular network. In many cases, these attackers will have specific targets and they will have access to the resources of the network [1], [5].

3.2.3 Pranksters:

Include bored people probing for vulnerabilities and hackers seeking to reach fame via their damage [5].For instance, a prankster can convince one vehicle to slow down, and tell the vehicle behind it to increase the speed.

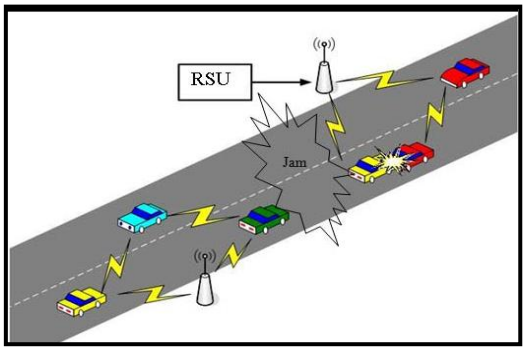

Fig 3: DoS Attack

4. PROPOSED WORK

Proposed scheme localizes the fake identities of malicious vehicles by analyzing the consistent similarity in neighborhood information these fake identities. This module detects various attacks against the control traffic and diagnoses the malicious nodes involved in these attacks. In this work, the new scheme had been proposed which will be based on to detect malicious nodes from the network which are responsible to trigger Sybil attack in the network.

4.1 Assumptions

Architecture has been designed by considering the following characteristics in a VANET scenario. The throughput of the network can be reduced because network resources get wasted. The delay can be raised because packets are routed to

wrong destination or long paths get followed. In this work the techniques which will be proposed are based on some assumptions. These assumptions are:

- 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.

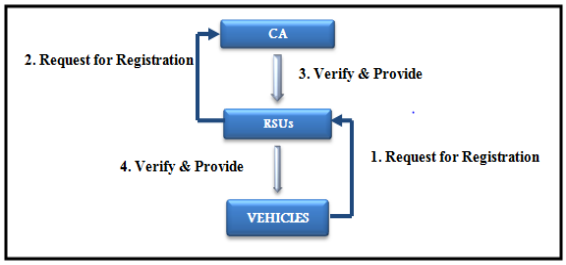

Fig 4: Registration of vehicles and RSUs with CA

4.2 Illustration of Flowchart

Malicious vehicles can change its identity every time and send hello messages to RSU's for network join. The vehicles which are on the network can register it with the server.

The working principle as given in the following algorithm.

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

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 Vi misbehaves after registration, it will be identified by the CA using AODV protocol.

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

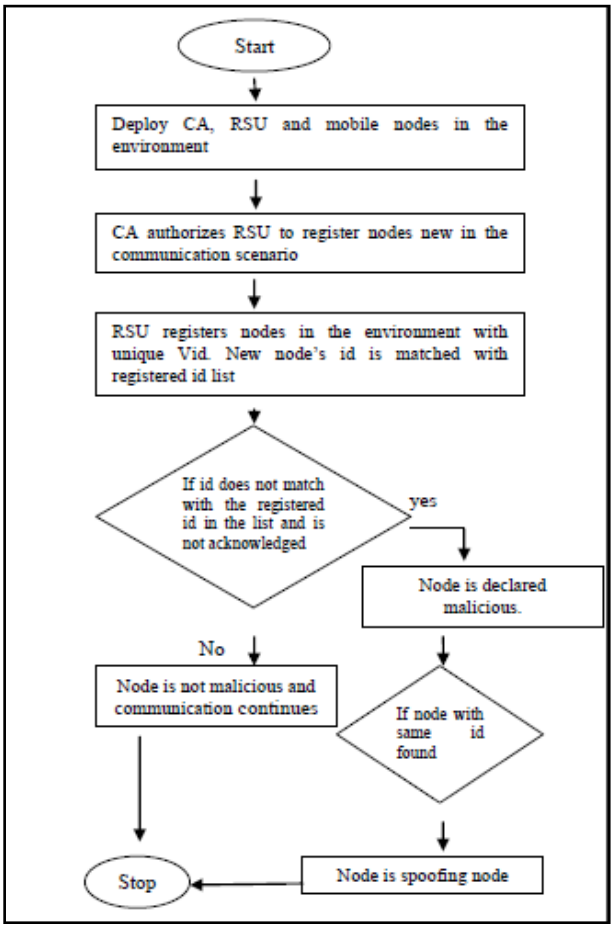

Fig 5: Flowchart of proposed methodology

Detection Algorithm

Input: Let N be an elected Node in the network.
Let R be an RSU
Let CA be the centralized authority

Output: Detection of Malicious and spoofed car

Assumption: CA has complete data of each vehicle

Calculation performed at RSU server. CA registers the vehicles in the environment and allocates ids to RU for further checking.

Registration Process

Start
STEP 1: Registration Process Starts
STEP 2: CA on receiving the information from RSU about new vehicles in environment register the vehicles.
STEP 3: CA verifies the information and registers the vehicle entering the environment with V_id (i).
STEP 4: The vehicles and RSU's communicate with each other.
STEP 5: CA detects the malicious vehicle through RSU by matching the id of the vehicle in the registered list of id's.
STEP 6: IF the id does not matches then node is declared malicious
ELSEIF same id nodes are found
THEN
Node is declared spoofing node
ELSE
Nodes without acknowledgement are also malicious nodes
STEP 7: Stop.

5. EXPERIMENTAL RESULT

Our simulation is based on NS2 is a VANET simulator, which provides a variety of useful models for VANET simulations. In this section, series of analyses are performed to investigate several fundamental issues relating to the proposed detection scheme.

Table 1. Table captions should be placed above the table

Parameters	Values
Simulator	NS-2.34
Area	1000*1000
Number of nodes	7
Vehicles Speed	30m/s
Centralized Authority	1
Routing Protocols	AODV
Packet Size	512kb
RSU	1
Packet Type	Tcp
Movement Model	Random way point

5.1 Simulation Scenarios

NS-2 (Network Simulator-2) has been used for performance evaluation.

5.1.1 Nam and RSU, CA

In the Starting of VANET scenario in which it is showing the Nam Animator.

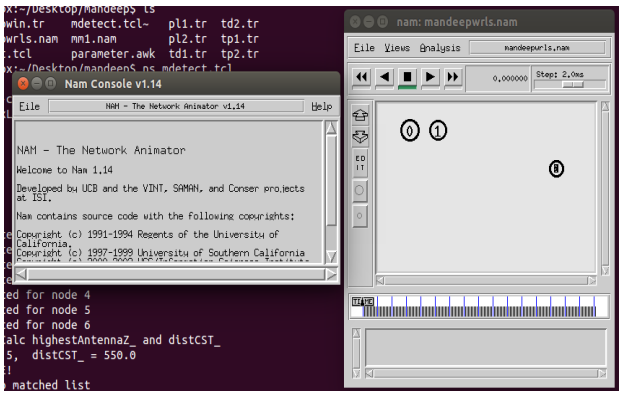

Fig 6: Monitoring Process of malicious nodes

5.1.2 Moving of Nodes

In this scenario it is showing the Randomly Movements of Nodes from Initialized Position.

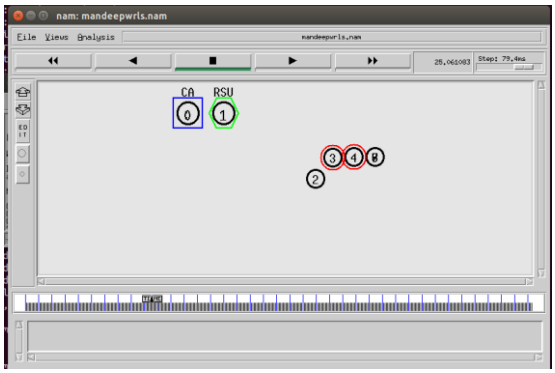

Fig 7: Malicious nodes being detected

5.1.3 Detecting Malicious Nodes

The Detecting the Malicious Nodes through RSU. Spoofing Attack and Malicious Attack.

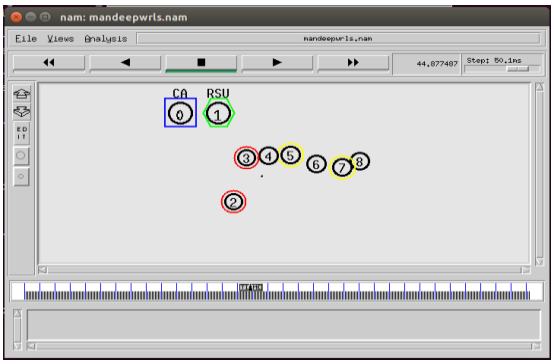

Fig 8: Spoofed node detected

The following are the results generated through computing scenario.

Table 2. Values estimated

No of Nodes	Generated Packets	Received Packets	Packet Delivery Ratio	Average End-End Delay	Average Throughput
9	14265	14106	98.8854	52.6547	608.46

In above TABLE 2, values are estimated from the trace file and generated through AWK Script for throughput, Average end- end delay, packet delivery ratio, received packets and generated packets.

Table 3. Malicious and spoofed nodes detected

CA Registered Node	Current Node	Malicious Nodes	Spoofed Nodes	Not Acknowledged Nodes
109,106,106,110, 101,107,106	0,1,2,3,4,5,6	106,110,101,107	106	106,110,101,107
105,103,109,108,101 109,105	0,1,2,3,4,5,6	103,109,105,101	109	103,109,105,101
108,102,107,110,105, 107,106	0,1,2,3,4,5,6	110,107,106	107	110,107.106

In TABLE 3 illustrates the no of malicious nodes, spoofed and nodes which does not receive acknowledgement in the environment.

5.2 X-graph Results

5.2.1 Packet Delivery Ratio

The no of packets received by total no of packets sent is defined as packet delivery ratio.

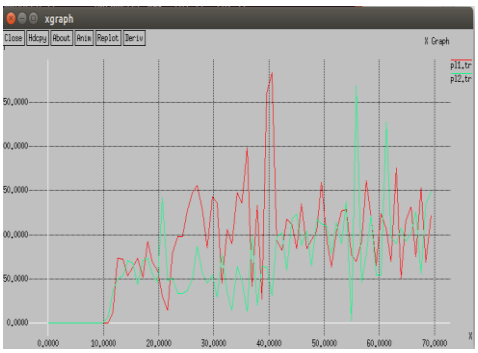

Fig 9. X-graph showing Packet loss during the communication

5.2.2 Dropped Packets

Number of malicious vehicles versus dropped packets is shown in Figure 4. . When the misbehaving vehicles are detected by the protocol, the number of received CBR will decrease, which will increase the number of dropped packets.

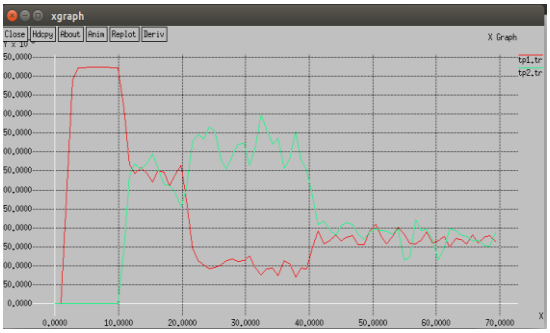

Fig 10. X-graph showing the Throughput achieved during the Communication

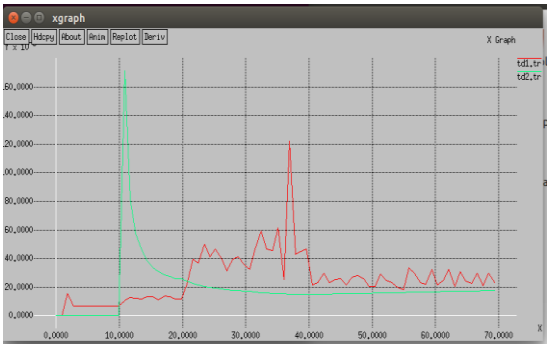

Fig 11. X-graph showing Delay in packets reaching the Destination node

5.2.3 Average End to End Delay

This shows average End to End delay for the various number of CBR traffics. Delay is the time taken to transmit the packet from source to destination.

6. CONCLUSION

In presented architecture of VANET for city traffic scenario and the adversaries that exist in the VANET environment. Vehicles and RSUs in VANET should be registered with the central controller so that every vehicle and RSU in the network will be authorized. City Scenario is considered to analyze the vehicle's behavior. As avoiding collision between vehicles and identifying the misbehaving vehicles plays a significant role in VANET, the existing AODV protocol has been enhanced by suitably incorporating the security features which detects the malicious behavior of the vehicle. Packet Delivery ratio, Dropped Packets and Routing overhead were the performance metrics taken for evaluating the protocol. The obtained results clearly indicate that the protocol identifies the misbehaving vehicle even after proper registration. In similar line additional security feature Our thanks to the experts who have contributed towards development of the template.

7. REFERENCES

[1] Jeong-Ah Jang "A Fixed Sensor-Based Intersection Collision Warning System in Vulnerable Line-of-Sight and/or Traffic-Violation-Prone Environment", IEEE Trans. Intelligent Transportation Systems, vol. no. 13, pp 1880-1890, Dec 2012.

[2] http://www.intechopen.com/ books/ computational-intelligence-and-modern- heuristics/ security-and-privacy- of- intelligent- vanets

[3] Iqbal, S., Chowdhury, S. R., Hyder, C. S., Vasilakos, A. V., & Wang, C. X., "Vehicular communication: protocol design, testbed implementation and performance analysis", In Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, pp. 410-415, June 2009.

[4] Ahmad, A., Doughan, M., Gauthier, V., Mougharbel, I., & Marot, M. ," Hybrid multi-channel multi-hop MAC in VANETs", In Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia" ,pp. 353-357, November 2010.

[5] LIU B., ZHONG Y., ZHANG S.: 'Probabilistic isolation of malicious vehicles in pseudonym changing VANETs'. Seventh Int. Conf. on Computer and Information Technology (CIT 2007), 2007, pp. 967–972

[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] 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.

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