DOS (DENIAL-OF-SERVICE) ATTACKS IN IEEE 802.11P VEHICULAR NETWORKS BY USING TIME STAMP PROTOCOL

[1]Ankush Hans , [2]Anurag Sharma, [3]Anshu Sharma
[1]Department of computer science
[1]CT Institute of Technology and Research, Jalandhar, India.

***Abstract*:** The attacker usually sends excessive messages in a DOS, asking the network or server to authenticate requests that have invalid return addresses. This causes the server to wait before closing of the connection. Hence keeps the network or server busy. This work entails the concept of platooning i.e. messages get transferred from vehicle periodically.

***Index Terms* - Denial of service attacks, ad-hoc network/MANET, vehicular traffic, time stamp, VANET, delay, PDR, RSU**.

I. INTRODUCTION

VANET: A Vehicular Ad-Hoc Network (VANET) is a secondary structure of Mobile Ad-Hoc Network (MANET) which is used in vehicles and road-side base stations with an aspiration to provide efficient and safe travelling. A vehicle in VANET is measured to be a smart mobile node competent of communicating with its neighbors and other vehicles in inter-connect. Vehicular Ad Hoc Networks (VANETs) are expertise which enables the capabilities of new innovation wireless networks to vehicles. Between mobile vehicles and wayside units, VANET constructs a tough Ad-Hoc network [9].

Inferring protection associated information and traffic administration, VANET is largely intended. Safety and traffic management requires real time information and constantly influence lives of people travelling on the road. Wellbeing is realized as key characteristic of Vehicular Ad Hoc Network (VANET) system.

VANET transfuse adequate prospective in vehicles to broadcast warnings about environmental hazards, traffic and road conditions and provincial information to further vehicles [11].

VANETs are comprised of following entities:

ACCESS POINT: These are prearranged and related to the internet. Vehicle to vehicle communication is categorized in two types of communications: single hop and multi hop.

VEHICLE: It is node of vehicular network. The wireless communication among vehicles (V2V) and between vehicles and infrastructure access point (V2I) addresses by VANET.

1.1 CHARACTERSTICS OF VANET

- High Mobility
- Rapidly Changing Network Topology
- Not any Power constraints
- Network Size without any bound
- Time Critical
- Changing information frequently
- Communicate wirelessly
- Network density is variable
- High computable

1.2 COMPONENT OF VANET

- Vehicles
- Infrastructure
- Communication channels

1.3 COMMUNICATION IN VANET

- Vehicle to vehicle
- .Vehicle to infrastructure
- Cluster to cluster

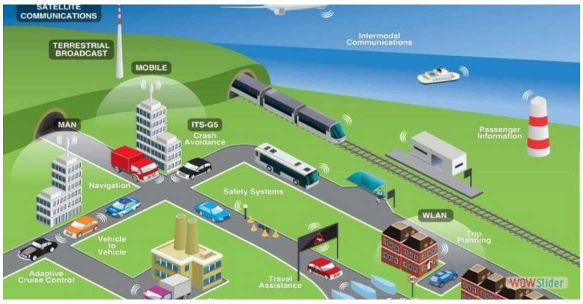


Fig.1: Communication in VANET

II. DOS ATTACK

In a Denial of Service attack, the aggressor generally transmits disproportionately large count of messages seeking the network or server to validate requests with invalid return addresses [10].

The server fails to find the return address of the invader while transmitting the validation consent, rendering the server to halt before finishing the connection.

When the connection ends by the server, the attacker transmits the supplementary verification messages with invalid and void return addresses. Thereby, the course of authentication and server begins again begins to wait, maintaining the network or server's occupancy.

2.1 The fundamental DOS attacks include:

- to avert legitimate network traffic, flooding the network .
- Distracting the connections between two machines, hence avoiding access to a service.
- Shielding an exacting entity from accessing a service.

In 5.9 GHz frequency band, IEEE 802.11p is an international standard for short-range inter-vehicle communication.

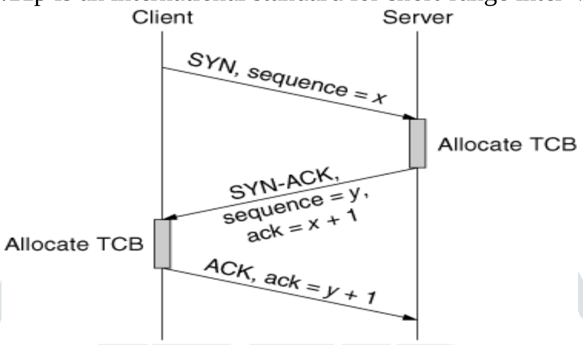


Fig.2: Client-server communication in DOS

This is a work for an adhoc network which includes the type of VANET (Vehicular Adhoc Network). The execution is completed with setup of implicit imitation using Java Socket Programming where client server architecture is deployed by bearing in mind that server is a middleware station to evidently scribe the communication among various nodes of VANET. The client is here a node or known to be virtual vehicle where the packet transmission take place includes the vehicle speed, distance with neighbor vehicle in the network and fuel left for the vehicle running.

III. LITERATURE REVIEW

Anal Patel, Nimisha Patel, Rajan Patel [2015] have reviewed the paper for defending against worm hole attacks in wireless sensor networks. This type of attack majorly affects the network layer of network [2]. This literature deals with detection of worm hole attack and an approach for prevention is proposed. Hash based compression function (HCF) approach was used which uses any secure hash function to calculate a value of hash field for RREQ packet.

Lyamin N.et al. [2014] has reviewed a Denial-of Service (DoS) attacks in IEEE 802.11p. In this paper vehicular ad-hoc networks (VANETs) is proposed. Their work entails the "jamming" of periodic spot messages (beacons) exchanged by vehicles in a platoon. Probabilities of assault recognition and forged apprehension are predictable for two different attacker models [1].

Campolo C.et al.[2013] have reviewed the main open issues related to the use of multiple channels in vehicular networks. The analysis starts from the consideration that several design challenges unique to the vehicular environment need to be addressed in order to make decisions on the adoption and improvement of the multichannel architecture proposed by standardization bodies. [4].

Bergenhem C.et al.[2012] have reviewed that the project vision is to develop and integrate solutions that allow vehicles to drive in platoons with more fuel efficiency, improvement in driver's safety and increased the driver's convenience. A platoon according to SARTRE is a manually controlled lead vehicle with a number of automatically controlled (both longitudinally and laterally) following vehicles [5].

Sapna Gambhir, et.al [2012] have reviewed on PPN: Prime product number based malicious node detection scheme for MANETs[3]. One of the main routing protocols is AODV used in MANETs. The defense of an AODV protocol is persuaded by malicious node attack. In this attack, a malicious node injects a false route reply claiming to have the shortest and spotless route to the destination. However, when the data packets arrive the malicious node discards them.

Pelechrinis K.et al. [2011] mentioned that reviewing of Jamming techniques differs from simple ones with respect to the recurring transmission of interference signals, to more complicated attacks aspiring exploitation vulnerabilities of the specific protocol deployed. In this literature, they have presented a detailed up-to-date discussion on the jamming attacks recorded in the literature [6].

B Mustafa. et al. [2010] reviewed the investigation of diverse ad hoc routing protocols for VANET. Their main objective was to recognize the ad hoc routing method that has better performance in highly mobile environment of VANET. They considered two different scenarios i.e. city and highway, for the measurement of performance of routing protocols in VANET. After carrying out literature review, routing protocols were chosen suspiciously. The chosen protocols were later tested through simulation in conditions of performance metrics i.e. throughput and packet drop [7].

P. Papadimitratos. et al. [2008] have reviewed the problem within the SeVeCom project, having developed a security architecture that provides a comprehensive and practical solution. The researcher analyzed threats and types of adversaries, identified security and privacy requirements and presented a spectrum of mechanisms to secure VC systems V [8].

IV. PROBLEM FORMULATION

In the current paper the probabilistic DOS attack detection is to be done using platooning in which messages get transferred from vehicle periodically. This estimation DOS attack detection cause the problems of false alarm generation which may cause a vehicle get black listed through actually that is not.

V. OBJECTIVES

1. To Simulate VANET by using Net beans in terms of various parameters.
2. To Analyze & Detect DOS attack on VANET by using time stamp protocol.
3. To compare the results of Designed system with Conventional system in terms of delay, PDR, throughput etc.

VI. METHODOLOGY

Our aim is to use research methodology in that manner which produces new knowledge, and here is the form of research methods.

It develops solutions to a problem. Here we will divide our work into two models theoretical model and simulation model.

In the theoretical model we will study different security issues and their solutions.

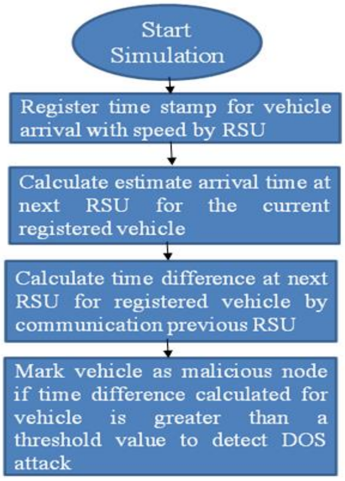
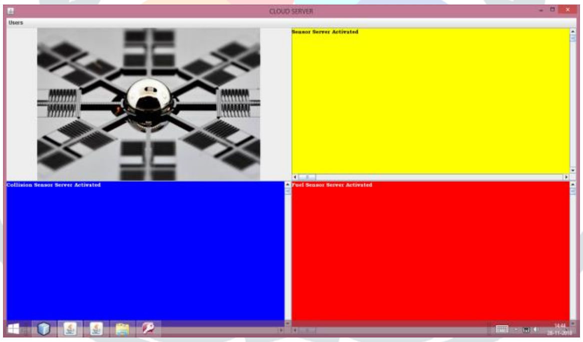

Start Simulation
Register time stamp for vehicle arrival with speed by RSU
Calculate estimate arrival time at next RSU for the current registered vehicle
Calculate time difference at next RSU for registered vehicle by communication previous RSU
Mark vehicle as malicious node if time difference calculated for vehicle is greater than a threshold value to detect DOS attack

Fig.3: Graphical layout of Methodology adopted.

In the simulation model we will run simulation with VEHICULAR AD HOC NETWORK configuration and try to learn mechanisms which will help us to enforce security in Vehicular Ad Hoc Networks.

VII. RESULTS



Sensor Server Activated

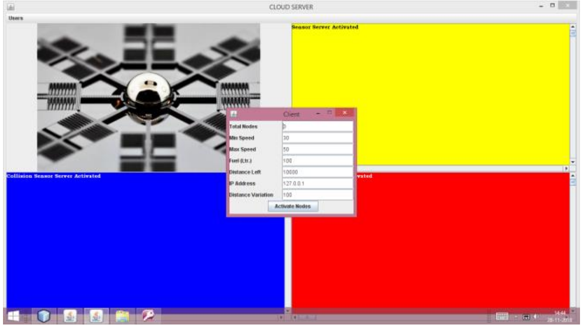
Collision Sensor Server Activated

Fuel Sensor Server Activated

Fig.4: Simulation of VANET after fuel sensor and collision sensor activation.

Figure 4 illustrates the Simulation of VANET by using Net beans in terms of its important parameters.

Fig. 5 illustrates the Simulation of VANET by using Net beans in terms of its important parameters i.e. Total Number of nodes, minimum speed, maximum speed, fuel in ltr., distance left, IP address of the requesting node and distance variation. In a typical exemplary test these values are given to be: Number of nodes=3, minimum speed= 30, maximum speed=50, fuel in ltr.=100, distance left=10000, IP address of the requesting node=127.0.0.1 and distance variation=100 and the nodes are activated.



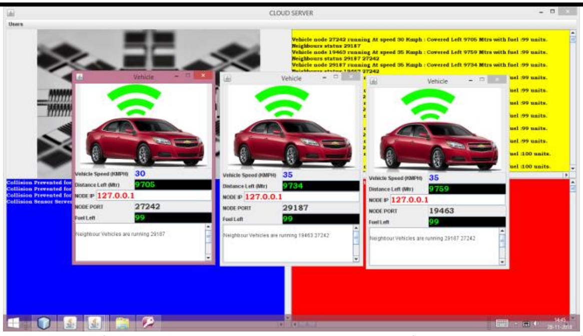
Sensor Server Activated

Collision Sensor Server Activated

Total Nodes: 3
Min Speed: 30
Max Speed: 50
Fuel (Ltr.): 100
Distance Left: 10000
IP Address: 127.0.0.1
Distance Variation: 100

Fig. 5: Simulation of VANET by using Net beans in terms of Total Number of nodes, minimum speed, maximum speed, fuel in ltr., distance left, IP address of the requesting node and distance variation.

Figure 6 gives the output from the cloud server in terms of vehicular speed, distance left(in mtr.), IP of the node, port of the activated node, fuel left and running of neighbor vehicles



```
Vehicle node 27242 running At speed 30 Kmph : Covered Left 9705 Mtrs with fuel :99 units.
Neighbours status 29187
Vehicle node 19463 running At speed 35 Kmph : Covered Left 9759 Mtrs with fuel :99 units.
Neighbours status 29187 27242
Vehicle node 29187 running At speed 35 Kmph : Covered Left 9734 Mtrs with fuel :99 units.
Neighbours status 19463 27242
```

```
Collision Prevented for
Collision Prevented for
Collision Prevented for
Collision Sensor Server
```

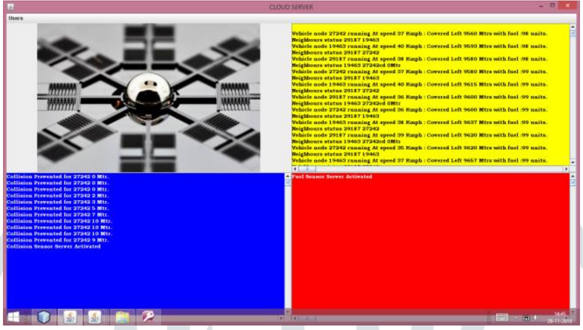
Vehicle Speed (KMPH) 30
Distance Left (Mtr) 9705
NODE IP 127.0.0.1
NODE PORT 27242
Fuel Left 99
Neighbour Vehicles are running 29187

Vehicle Speed (KMPH) 35
Distance Left (Mtr) 9734
NODE IP 127.0.0.1
NODE PORT 29187
Fuel Left 99
Neighbour Vehicles are running 19463 27242

Vehicle Speed (KMPH) 35
Distance Left (Mtr) 9759
NODE IP 127.0.0.1
NODE PORT 19463
Fuel Left 99
Neighbour Vehicles are running 29187 27242

Fig.6: Output from the cloud server in terms of vehicular speed, distance left (in mtr.), IP of the node, port of the activated node, fuel left and running of neighbor vehicles.

The following figure fig.7 is in continuation of fig. 6. It clearly infers the collisions that have been prevented at specific distance.



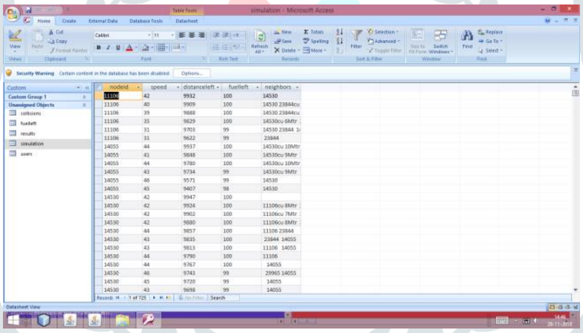
```
Vehicle node 27242 running At speed 37 Kmph : Covered Left 9560 Mtrs with fuel :98 units.
Neighbours status 29187 19463
Vehicle node 19463 running At speed 40 Kmph : Covered Left 9593 Mtrs with fuel :98 units.
Neighbours status 29187 27242
Vehicle node 29187 running At speed 38 Kmph : Covered Left 9580 Mtrs with fuel :98 units.
Neighbours status 19463 27242cd 0Mtr
Vehicle node 27242 running At speed 37 Kmph : Covered Left 9580 Mtrs with fuel :99 units.
Neighbours status 29187 19463
Vehicle node 19463 running At speed 40 Kmph : Covered Left 9615 Mtrs with fuel :99 units.
Neighbours status 29187 27242
Vehicle node 29187 running At speed 36 Kmph : Covered Left 9600 Mtrs with fuel :99 units.
Neighbours status 19463 27242cd 0Mtr
Vehicle node 27242 running At speed 36 Kmph : Covered Left 9600 Mtrs with fuel :99 units.
Neighbours status 29187 19463
Vehicle node 19463 running At speed 38 Kmph : Covered Left 9637 Mtrs with fuel :99 units.
Neighbours status 29187 27242
Vehicle node 29187 running At speed 39 Kmph : Covered Left 9620 Mtrs with fuel :99 units.
Neighbours status 19463 27242cd 0Mtr
Vehicle node 27242 running At speed 35 Kmph : Covered Left 9620 Mtrs with fuel :99 units.
Neighbours status 29187 19463
Vehicle node 19463 running At speed 37 Kmph : Covered Left 9657 Mtrs with fuel :99 units.
```

```
Collision Prevented for 27242 0 Mtr.
Collision Prevented for 27242 0 Mtr.
Collision Prevented for 27242 0 Mtr.
Collision Prevented for 27242 2 Mtr.
Collision Prevented for 27242 3 Mtr.
Collision Prevented for 27242 5 Mtr.
Collision Prevented for 27242 7 Mtr.
Collision Prevented for 27242 10 Mtr.
Collision Prevented for 27242 10 Mtr.
Collision Prevented for 27242 10 Mtr.
Collision Prevented for 27242 9 Mtr.
Collision Sensor Server Activated
```

```
Fuel Sensor Server Activated
```

Fig.7: Result after execution for prevention of collision

All the results from the database have been depicted in the figure below fig. 8.It openly states the id prescribed to various participating activated nodes along with their corresponding speed during the course of execution, distance left ahead of probable collision, fuel left in the corresponding vehicle and identification of its neighboring nodes.

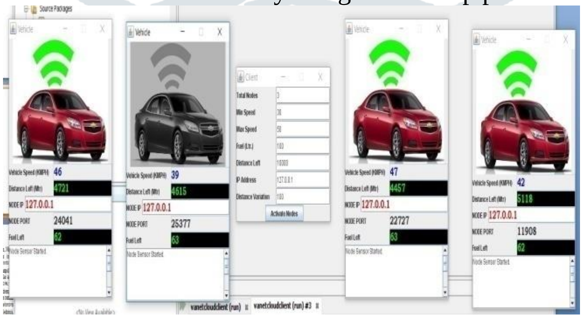


nodeid	speed	distanceleft	fuelleft	neighbors
11106	42	9932	100	14530
11106	40	9909	100	14530 23844cu
11106	39	9888	100	14530 23844cu
11106	35	9829	100	14530cu 6Mtr
11106	31	9703	99	14530 23844 1
11106	31	9622	99	23844
14055	44	9937	100	14530cu 10Mtr
14055	41	9848	100	14530cu 9Mtr
14055	44	9780	100	14530cu 10Mtr
14055	43	9734	99	14530cu 9Mtr
14055	46	9571	99	14530
14055	45	9407	98	14530
14530	42	9947	100	
14530	42	9924	100	11106cu 8Mtr
14530	42	9902	100	11106cu 7Mtr
14530	42	9880	100	11106cu 8Mtr
14530	44	9857	100	11106 23844
14530	43	9835	100	23844 14055
14530	43	9813	100	11106 14055
14530	44	9790	100	11106
14530	44	9767	100	14055
14530	46	9743	99	29965 14055
14530	45	9720	99	14055
14530	43	9698	99	14055

Record: 1 of 725 No Filter Search

Fig.8: results as stored in database after execution.

The analyzed result after detection of DOS attack on VANET by using time stamp protocol is scribed in the following image fig.9



Vehicle Speed (KMPH) 46
Distance Left (Mtr) 4721
NODE IP 127.0.0.1
NODE PORT 24041
Fuel Left 62
Node Sensor Started.

Vehicle Speed (KMPH) 39
Distance Left (Mtr) 4615
NODE IP 127.0.0.1
NODE PORT 25377
Fuel Left 63
Node Sensor Started.

Total Nodes 3
Min Speed 30
Max Speed 50
Fuel (Ltr.) 100
Distance Left 10000
IP Address 127.0.0.1
Distance Variation 100

Vehicle Speed (KMPH) 47
Distance Left (Mtr) 4457
NODE IP 127.0.0.1
NODE PORT 22727
Fuel Left 63
Node Sensor Started.

Vehicle Speed (KMPH) 42
Distance Left (Mtr) 5118
NODE IP 127.0.0.1
NODE PORT 11908
Fuel Left 62
Node Sensor Started.

Fig. 9: Detection of DOS attack on VANET using time stamp protocol.

VIII. CONCLUSION

A vehicle in VANET is embossed as an intelligent mobile node competent of communicating with its neighboring nodes and other vehicles in the network. Protection is considered to be chief aspect of Vehicular Ad Hoc Network (VANET) system. Taking into account that server is a middleware station to records the communication between a variety of nodes of VANET collisions can be averted.

REFERENCES

[1] Lyamin, Nikita, et al. "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11 p Vehicular Networks." IEEE Communications letters 18.1 (2014): 110-113.

[2] Patel, Anal, Nimisha Patel, and Rajan Patel. "Defending against wormhole attack in MANET." 2015 Fifth International Conference on Communication Systems and Network Technologies. IEEE, 2015.

[3] Gambhir, Sapna, and Saurabh Sharma. "PPN: Prime product number based malicious node detection scheme for MANETs." 2013 3rd IEEE International Advance Computing Conference (IACC). IEEE, 2013.

[4] C. Campolo, A. Molinaro, Multichannel communications in vehicular ad hoc networks: a survey // IEEE Communications Magazine, vol. 51, no. 5, pp. 158–169, 2013.

[5] Bergenhem, Carl, Erik Hedin, and Daniel Skarin. "Vehicle-to-vehicle communication for a platooning system." Procedia-Social and Behavioral Sciences 48 (2012): 1222-1233.

[6] K. Pelechrinis, M. Iliofotou, S.V. Krishnamurthy, Denial of service attacks in wireless networks: the case of jammers // IEEE Communications Surveys and Tutorials, vol. 13, no. 2, pp. 245–257, 2011.

[7] Mustafa, Bilal. Issues of Routing in VANET. Diss. Blekinge Institute of Technology, 2010.

[8] Papadimitratos, Panagiotis, et al. "Secure vehicular communication systems: design and architecture." IEEE Communications Magazine 46.11 (2008): 100-109.

[9] Divya Chadha, et al. “Vehicular Ad hoc Network (VANETs): AReview”. International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 3, March 2015

[10] Sheetal P.Desai et al. “Denial of Service Attack Defense Techniques”, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 10 Oct -2017.

[11] Dr. Pankaj Dadhich et al. “Vehicular Ad Hoc Network (VANETs): A Brief Overview”, Journal of Advanced Computing and Communication Technologies, Volume No.5 Issue No.3, June 2017.