A Novel Delivery Evalution Method for Find Shortest Path and Optimized of VANET Approach

Amandeep Kaur[1], Tanisha Saini[2]
[1]M.tech (Scholar), [2] Assistant Professor
Chandigarh Group of College, Landran

Abstract **-** The VANets (Vehicular Ad Hoc Networks) widely recognized with MANets (Mobile Ad Hoc Networks) and turns into the demanding area of research. In VANET moving vehicles act as the nodes and router to create a mobile network. The information exchanged in vehicles are depend upon the communication modes. The communication is takes part in three ways- vehicle to vehicle, vehicle to infrastructure and hybrid mode. The major goal of VANET is to improve the overall safety of transportation infrastructure that includes - more confortable driving, minimize accidents, local danger warnings, up–to-date traffic information, internet access. Due to the mobility of nodes the issues arises related to security and the attacker attacks to reduce the security. In mostly cases, attack on the availability that unavailable the resources due to Distributed Denial of Service (DDoS) Attack that aims to halt the network. To improve security, detect and prevent attacks in VANet, routing protocol is used. Shortest- Ad hoc on demand distance vector (S-AODV) and Enhanced genetic Algorithm (EGA) are used to improve the security.

Keywords- *VANets (Vehicular Ad hoc Networks), RSU (Road Side Units), B-AODV (Balanced- Ad Hoc ON Demand Distance Vector), S-AODV (Shortest- Ad Hoc On Demand Distance Vector), EGA (Enhanced Genetic Algorithm).*

I. INTRODUCTION

In the new era, internet becomes a necessary part of human needs, as per the need new technologies are introduced day by day to make the life more comfortable and easy. Ad hoc networks are the type of wireless networks that are versatile flat forms which means to move free without any fixed infrastructure. The importance of ad-hoc networks are in military arena, personal area network. industry sector, etc [1]. In today's transportation system safety becomes more important due to the increased number of vehicles [2]. A new kind of ad hoc networks came in transport systems named as VANets to minimize the chances of accidents and to make the driving more interesting and easy..The GPS already exists in vehicles but VANets overcomes the limitations of GPS [3]. VANets are designed for the intelligent transport system. In this networks short range of communication when the vehicles are moved from the particular area the vehicles automatically disconnected [4].

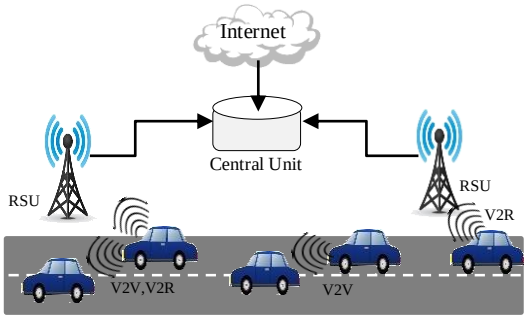

Fig.1 VANet Architecture

VANets are the vehicular ad hoc networks come under the sub class of MANets. In this network the data is transferred by using moving vehicles. The main purpose of VANet is to improve the security and the privacy between the vehicles [5]. In figure 1 the VANet architecture explained with data communication.in above figure1 V2V is vehicle to vehicle communication and V2R is the communication of vehicle with RSU by signals. When nodes communicates the data is stored in RSU and which further sends it to the internet by using central unit. VANets working is based on the RSU and the Routing protocols. The RSU is the road side units and the purpose of RSU is to connect vehicles and communicates by passing broadcast signals. RSU are connected with the main system and store the data [6]. Routing protocols are the important protocols used in VANet to make the communication between vehicles and to prevent the data form attackers. In this paper, Reactive protocols are used in which the data is periodically updated and works on demand. The other protocols are proactive and hybrid [7]. AODV and B-AODV are the reactive on demand protocols that are used to make the communication more secure between the vehicles. In AODV protocols if the data is exchanged then there must be path which refers the discovery phase which increases the vulnerabilities against DDoS attack and overhead the network. To overcome the problems due to DDoS flooding attack B-AODV is discovered. This is balanced–AODV is an enhanced version of AODV protocol. It uses the Balance index in which mean and standard deviation is measured to make the nodes in balanced behavior if there is any node that above the threshold value must be attacker. It increases the bandwidth and reduces the overhead [8]. The characterstics of VANets are highly dynamic topologies, more energy and storage, geographical communication, mobility modelling and frequently network disconnectivity [9]. The applications of VANet are commercial in which internet and web services

are provided to the users for their entertainment and information. In the productive applications the productive benefits are increased, time utilization and fuel saving [10].
The security in the vehicle communication is most important thing to manage. VANets are vulnerable against attacks due to the mobility of vehicles.In this paper is based on the attack on the availability that is DDoS attack. [11].The attacks are categorized in two categories: Passive attacks the attacker only collect the beneficial information and in the Active attacks the attacker collect data modify, injecting, edit and can drop the data [12].

Table 1 Different categories of attacks

Passive attacks	Active attacks
Eavesdropping	Black hole
Location disclosure	Grey hole
Monitoring	DDoS attack
	Sybil attack

DDoS Attack
DDoS attack stands for Distributed Denial of Service Attack. This is the most worrying threat on the network .it simply works within few minutes but very difficult to detect and effect the performance of systems [13]. The attackers are located on different locations at the same time and send the unwanted request which includes artificial messages. This flooding and jamming of unwanted requests make the resources unavailable.

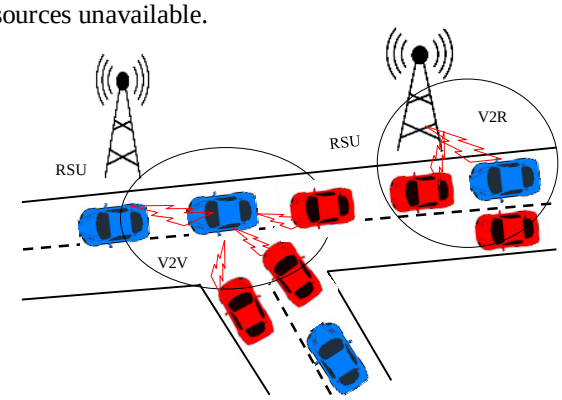

Fig.2. Distributed denial of service attack

It increases the overhead on the network and unavailable resources when they are required. The problems arises during DDoS attacks are – delay increased, packet loss, end to end delay, Accuracy of data decreased, time consuming, overhead increased and throughput decreased [6]. In the figure 3. The distributed denial of service attack is described in which red cars are attackers that send the unwanted requests and blue cars are the moving vehicles. In the above figure the attack on the V2R (vehicle to rsu) and V2V(vehicle to vehicle).

II. RELATED WORK

[8] Mohammad Javad Faghihniya et al., 2016 uses the AODV and B-AODV protocols for detection the denial of service attack and issues are flooding attack, throughput, etc. The B-AODV uses the balance index to balance the behaviour of nodes. The threshold value is set for detection if the nodes are going above the value there is attacker node otherwise data directly sent.
[14] George knight et al., 2016 uses the technique Basic Safety Messages (BSMs) can be bundled composed and relayed as to increase the actual communication range of communicating vehicles. This are designed for the distribution of safety applications.
[15] Wenjia Li et al., 2015 An Attack-Resistant Trust Management Scheme for securing vehicular ad hoc networks. Plan trust management subject to approximates wide range of Vanet appplications to improve traffic safety.
[16] GianmarcoBaldini et al., 2013 used the technique cryptography in particular, signature scheme to provide better security and discretion for VANet. The issues are related to the keys for sending and receiving data.
[17] Irshad Ahmed Sumra et al., 2011 described as, vehicular SMS system to provide VANet facilities to users through SMS system.but needs further research to resolution its trust and privacy issues.

III. RESEARCH WORK

A. *Aim of Research Work*

1) To study the previously used techniques, parameters and their issues. The previous techniques are AODV and the B-AODV protocols in the vehicular ad hoc networks.
2) To create a good and essential algorithm with the help of RSU. S-AODV (shortest ad hoc on demand distance vector) protocol is introduced to overcomes the problems of previous techniques. Flooding attack involved with it to improve the overall performance. S-AODV find out the shortest path on the basis of time not on the range.
3) Implementation of Enhanced Genetic Algorithm which is optimization technique. The purpose of implementing the enhanced genetic algorithm is to find out the best results with the help of fitness function. A best fitness value is selected for the result.
4) To compare the proposed techniques: S-AODV and EGA with the existing techniques: AODV and B-AODV.

B. *Explanation of Research Work*

S-AODV is the shortest ad hoc on demand distance vector which is used to overcome the issues of previous existing work with AODV and B-AODV and to detect the DDoS attack in the VANet. This protocol create route when the data send and received. It send request to the other nodes from the source node and select the route from the node that reply in short time because it is based on the time not like B-AODV i.e based on energy. This technique provide the sequence number numbers to each and every node so the y

become dissimilar and find out the shortest path from source to destination. The sequence 1 start and increment the hop connection. It reduces excess memory. This technique is applicable for large scale .S-AODV increases the throughput, reduces the delay, increase packet delivery rate.

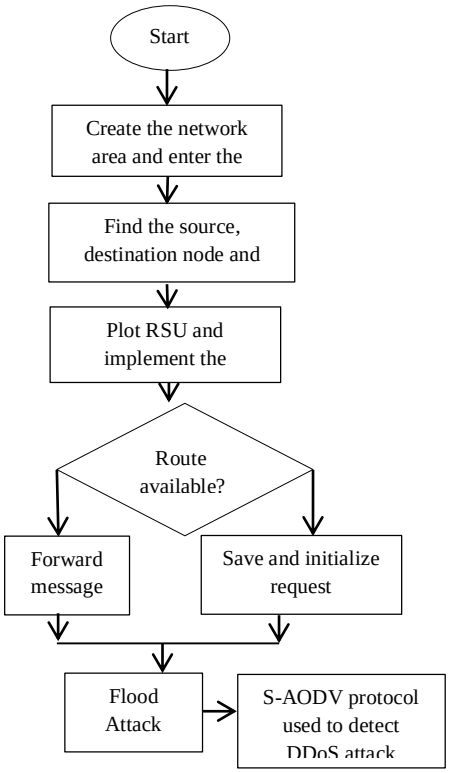

Fig.3 S-AODV Flowchart

Algorithm for S-AODV protocol

Step1. Initialize the VANet to find out the network area and plotting nodes in the network.
Step2. Find source and sink node for sending and receiving data. Find out the coverage set to calculate the distance in range.
Step3. Plot the RSU to manage the data that are send and received by the vehicles in the network. Implement the S-AODV to detect the DDOS attack in the network in which data is sent to the intermediate nodes.
Step4. Check the route availability if yes, data is send otherwise initialize the route request again.
Step5. The flood attack occurs in the network that generates the unwanted requests to the server and increases the overhead and delay.
Step6. Implement the Shortest Ad Hoc on demand distance vector to detect the DDoS effect.
Start from source to destination.
Send requests and select the shortest path
Generates sessions in which unique ids.
If {
values above threshold attacker node.
}
Else
{
Data send directly.
}
Stop

EGA (Enhanced Genetic Algorithm)

This is search and optimization algorithm which is proposed by John Holland in 1970's. Genetic algorithms are used by many fields such as medicines and engineering, space research, etc to find out the best solution to the complex problems like NP hard problems[18]. This algorithm starts first with the population. The population is the number of individuals that are chromosomes. A chromosome is the main part of genetic materials because it is the group of genes used for determining the individual shape and features. The fitness of individual is evaluated. The best solution of problem is given by the fitness functions [19]. The genetic operators are Selection operator in which the chromosomes are selected randomly from the population, Crossover operators in which chromosomes are generated with the combination of two chromosomes, mutation operators in which changes and modification the genes of chromosome. This operator is performed at the end moment when need of modifications [18]. Therefore EGA is used for preventions and recovers the data from the DDoS attack in VANet . After using EGA the performance improved it reduces overhead, increased delivery of more packets, reduced delay and increases the throughput. This approach is chosen from the optimization technique because it checks the code line by line and accuracy is more and decimal coding in it.

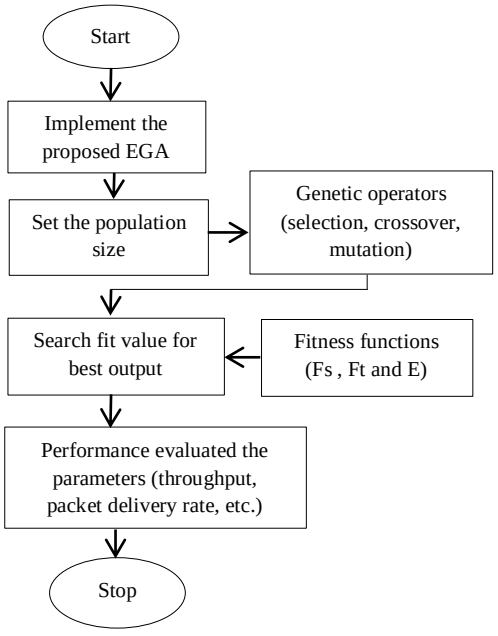

Fig.4 EGA Flowchart

Algorithm for EGA

Step0. Start
Step1. Implement the proposed algorithm used for mitigate the effect of vehicle nodes in the network. we optimize the attacker effect with the help of genetic algorithm with fitness value.
Step2. Set the population size from the problem.
Step3.Apply genetic operators- selection, crossover and the mutation to find out the best results.
Step4. Select the best fit value for the output with the help of fitness fumctions- Fs(intial fitness), Ft(total fitness value) and E(error).
Step5. To evaluate the performance parameters like throughput and packet delivery rate. To reduce the overhead, delay.
Step6. Stop.

IV. RESULT DISCUSSION

A. *Tool Used*

To complete the research work, Matlab is used. Matlab is known as Matrix Laboratory and developed by Math Works. It is high level computing language and is the interactive environment for the algorithm development and data analysis. The wide applications of Matlab is image processing, test and managements, control design and financial modelling and analysis. The Matlab system consists of desktop tools, mathematical function library, language, graphics. Features of Matlab are- high level language, easy to use and learn, provide vast library, built in graphics, etc. Matlab have power to solve all mathematical problems.

B. *Result*

The vehicular ad hoc network is generated to transfer data from node to node. The performance parameters are evaluated with S-AODV and EGA. The comparison of AODV, B-AODV, S-AODV and EGA .

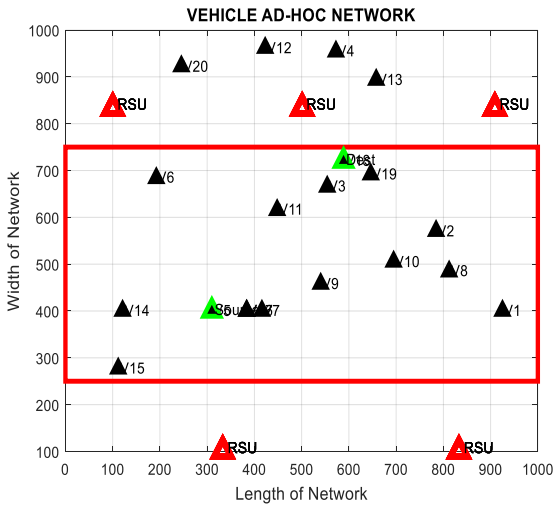

Fig.5 Vehicular ad hoc network

In figure 5 the vehicular ad hoc network is created in which source and destination nodes are selected randomly in the particular range. The red triangles are the RSU, black are the moving nodes and Green colour for the source to destination.

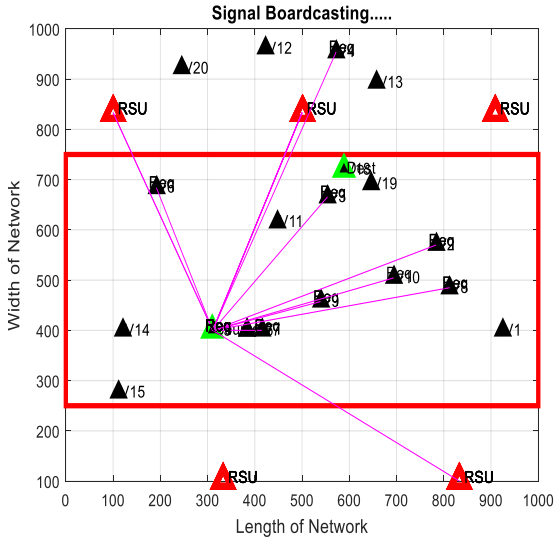

Fig.6 Signal send to the nodes

In figure 6 The souce node send the request to every node and the pink lines used to show the broadcast signal. Then it calculates the time to reach fast at the destination and choose the shortest path and it is measured on the bases on time.

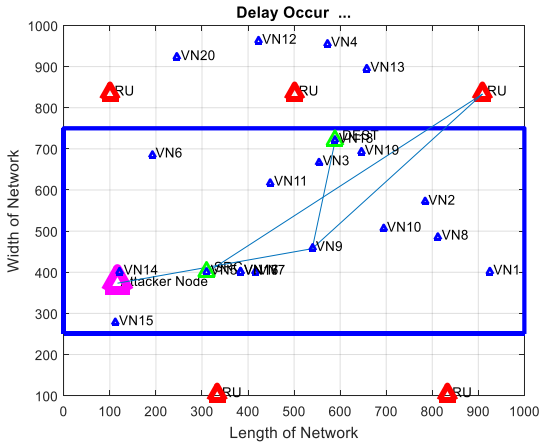

Fig.7 Attack on network

In figure 7 when the data is send from nodes the sessions are created and if the data is greater than threshold value then the attack node shows. The pink node shows the attacker in the network. Otherwise data transferred directly.

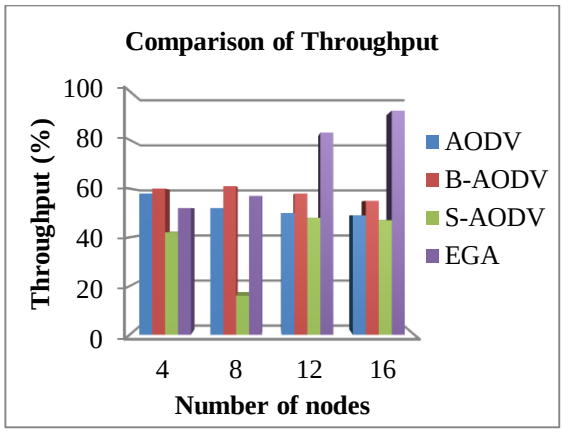

Fig.8 Comparison of throughput with existing and proposed work.

In figure 8 The throughput is compared with AODV, B-AODV, S-AODV and EGA which are the existing and proposed techniques. The throughput is increased maximum by EGA .

Table 2 Comparison between Throughput

Number of nodes	AODV	Balanced AODV	Shortest AODV	EGA
4	58	60	42	52
8	52	61	16	57
12	50	58	48	83
16	49	55	47	92

In table 2 The throughput values are generated from the existing and proposed techniques.

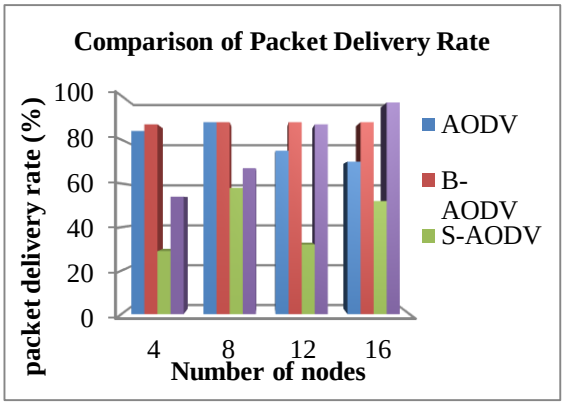

Fig.9 Comparison of packet delivery rate with the existing and proposed work.

In figure 9 the packet delivery rate is compared with the existing and proposed techniques. By getting the result the EGA are the best technique for more packet delivery rate. It detects the attacker that drop the packets and increase the overall packet delivery rate.

Table 3 Comparison between Packet Delivery Rates

Number of nodes	AODV	Balanced AODV	Shortest AODV	EGA
4	84	87	29	54
8	88	88	58	67
12	75	88	32	87
16	70	88	52	97

In the table 3 the result of Packet Delivery Rates values are compared with the existing and proposed techniques.

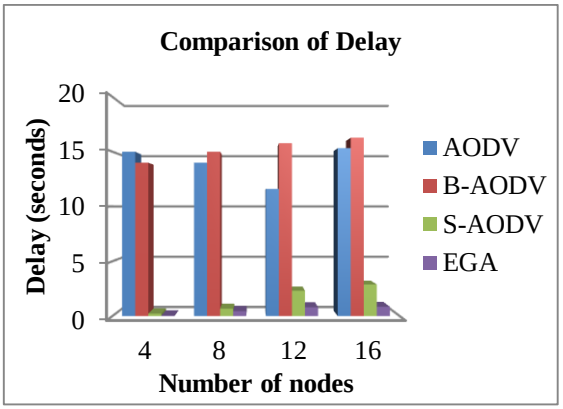

Fig.10 Comparison of delay with existing and proposed work.

In the figure 10 The Delay is increased when the number of nodes increased. To reduce the delay from the network the existing and the proposed techniques compared. By comparing the S_AODV and EGA both reduces the delay and send the data fast in the network. The delay is measured in the seconds which shows how much time takes a node to reach the another node.

Table 4 Comparison between Delay

Number of nodes	AODV	Balanced AODV	Shortest AODV	EGA
4	15	14	0.22	0.0386
8	14	15	0.672	0.4571
12	11.6	15.77	2.31	0.81
16	15.32	16.28	2.88	0.85

In the table 4 the delay is compared with the S-AODV and EGA with the existing techniques AODV and B-AODV. The delay is in the seconds. From the result delay is decreased and minimized in the network by using EGA.

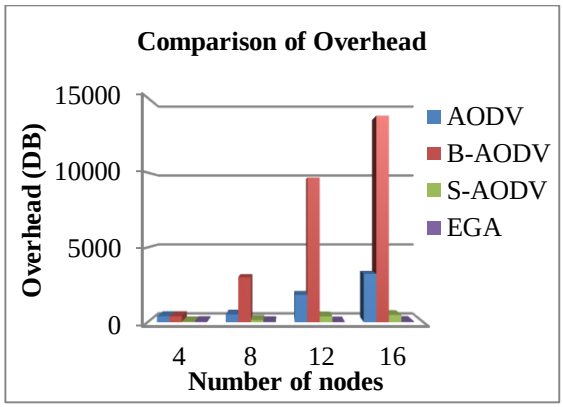

Fig.11 Comparison of overhead with existing and proposed work.

In figure 11 the performance parameters in which overhead is decreased by using the S-AODV and EGA proposed techniques .when the number of nodes increased there is no effect on the performance but in the existing technique AODV and B-AODV is overhead.

Table 5 Comparison between Overhead

Number of nodes	AODV	Balanced AODV	Shortest AODV	EGA
4	402.3	402	38	52
8	514	3005	143	43
12	1827	9666	385	25.59
16	3232	13803	481	59.9

In table 5 The values are generated from the existing and propose techniques which shows that EGA have less overhead than other techniques and the best from the all other nodes.

EGA is the implementation for the performance parameters in which it increases the throughput and packet delivery rate and on the other side it reduces the overhead and delay. By comparison it is right to say EGA is better than other techniques and make the vehicular ad hoc network more secure and for detecting and preventing data from the attacks.

V. CONCLUSION AND FUTURE SCOPE

In this paper, the techniques for detection and prevention of flooding attack that occurs due to the DDoS attack are presented. In VANet security is very essential. The mobility of nodes increases the vulnerabilities against DDoS attack that unavailable the resources. AODV and B-AODV protocols are used to detect the attacker nodes in the network. B-AODV uses the balance index in which mean and standard deviations are calculated to balance the nodes. B-AODV improves the AODV results but the problem is to increase the more throughput, to reduce energy, decrease delay and increasing packet delivery rate. To overcome these problems, S-AODV and EGA and the comparison of results based on new techniques with the existing techniques. S-AODV is the shortest ad hoc on demand distance vector which is used to find out the shortest path from source to destination and is based on time. EGA is enhanced genetic algorithms which used for preventions and it increases the throughput, packet delivery rate, accuracy, and decreases delay, packet loss and overhead.

The VANet future is secure so the usage of VANets increased. The VANet used in administration projects. In India nationwide highways Authority is planning to replace toll system with electronic toll systems within the country. In the upcoming time the VANets are used everywhere to increase the traffic safety, make the driving more comfortable and secure.

VI. REFERANCES

[1]. Helen, D., and D. Arivazhagan. "Applications, advantages and challenges of ad hoc networks." *Journal of Academia and Industrial Research (JAIR)* 2, no. 8 (2014): 453-457.

[2]. Abueh, Yeka Joseph, and Hong Liu. "Message authentication in driverless cars." In *Technologies for Homeland Security (HST), 2016 IEEE Symposium on*, pp. 1-6. IEEE, 2016.

[3]. Boukerche, Azzedine, Horacio ABF Oliveira, Eduardo F. Nakamura, and Antonio AF Loureiro. "Vehicular ad hoc networks: A new challenge for localization-based systems." *Computer communications* 31, no. 12 (2008): 2838-2849.

[4]. Rawat, Priyanka, Kamal Deep Singh, Hakima Chaouchi, and Jean Marie Bonnin. "Wireless sensor networks: a survey on recent developments and potential synergies." *The Journal of supercomputing* 68, no. 1 (2014): 1-48.

[5]. Tyagi, Parul, and Deepak Dembla. "A taxonomy of security attacks and issues in vehicular ad-hoc networks (vanets)." *International Journal of Computer Applications* 91, no. 7 (2014).

[6]. Kaur, Mandeep, and Manish Mahajan. "Protection Against DDOS Using Secure Code Propagation In The VANETs." (2016).

[7]. Kakarla, Jagadeesh, S. Siva Sathya, and B. Govinda Laxmi. "A Survey on Routing Protocols and its Issues in VANET." (2011).

[8]. Faghihniya, Mohammad Javad, Seyed Mojtaba Hosseini, and Maryam Tahmasebi. "Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network." *Wireless Networks*: 1-12.

[9]. Li, Fan, and Yu Wang. "Routing in vehicular ad hoc networks: A survey." *IEEE Vehicular technology magazine* 2, no. 2 (2007).

[10]. Kumar, Vishal, Shailendra Mishra, and Narottam Chand. "Applications of VANETs: present & future." *Communications and Network* 5, no. 01 (2013): 12.

[11]. La Vinh, Hoa, and Ana Rosa Cavalli. "Security attacks and solutions in vehicular ad hoc networks: a survey." *International journal on AdHoc networking systems (IJANS)* 4, no. 2 (2014): 1-20.

[12]. Shrivastava, Satyam, and Sonali Jain. "A brief introduction of different type of security attacks found in mobile Ad-hoc network." *International Journal of Computer Science & Engineering Technology (IJCSET)* 4, no. 3 (2013).

[13]. Kumar, Krishan, R. C. Joshi, and Kuldip Singh. "An integrated approach for defending against distributed denial-of-service (DDoS) attacks." *IRISS-2006* (2006): 1-6.

[14]. Knight, Georgie, Alexander P. Kartun-Giles, Orestis Georgiou, and Carl P. Dettmann. "Counting Geodesic Paths in 1D VANETs." arXiv preprint arXiv:1610.01630 (2016).
[15]. Li, Wenjia, and Houbing Song. "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks." *IEEE Transactions on Intelligent Transportation Systems* 17, no. 4 (2016): 960-969.
[16]. Baldini, Gianmarco, Vincent Mahieu, Igor Nai Fovino, Alberto Trombetta, and Marco Taddeo. "Identity-based security systems for vehicular ad-hoc networks." In *Connected Vehicles and Expo (ICCVE), 2013 International Conference on*, pp. 672-678. IEEE, 2013.
[17]. Wei, Wei, Fengyuan Xu, Chiu C. Tan, and Qun Li. "SybilDefender: a defense mechanism for Sybil attacks in large social networks." *IEEE transactions on parallel and distributed systems* 24, no. 12 (2013): 2492-2502.
[18]. Maheshwari, Ankit, Richa Garg, and Er Naveen Sharma. "A Review Paper on Brief Introduction of Genetic Algorithm." (2016).
[19]. Zhang, Kui, and Lingchen Zhu. "Application of improved genetic algorithm in automatic test paper generation." In *Chinese Automation Congress (CAC), 2015*, pp. 495-499. IEEE, 2015.