MULTICAST ROAD SIDE UNITS FOR FIREFLY OPTIMIZATION TECHNIQUE IN VANET

Ramsharanjit Singh[1], Varun Sanduja[2]
M.Tech (Scholar), Assistant Professor
Department of Electronics and Communication Engineering, CGCTC Technical Campus, Jhangeri

Abstract - The Vehicular Ad Hoc Network (VANET) is an emergent new technology integrating ad hoc network and improves road traffic security. One of the most one challenges in VANET is of searching and maintaining an effective route for transporting data information. At current some types of routing protocols used in VANET Hence, an analysis on routing protocols based on several parameters of. VANET is a essential issue in communication. As one of the most important routing protocols used in Mobile Ad Hoc Networks (MANET), AODV routing protocol is also used in VANET. Vehicular plays an important role in time-to-time world in the area of automobiles. VANETs are the subclass of mobile ad-hoc Networks which have no central arrangement. Nodes are extremely mobile in VANET. VANET is distinguished from MANET by their features, design and applications. A Vehicular Ad hoc Network involves of a set of communicating wireless mobile nodes or devices that do not have any form of secure organization or integrated authority. The security in VANET has become a significant and active topic within the investigation community. This is because of high demand in sharing streaming video and audio in various applications, one VANET could be setup quickly to facilitate communications in a hostile environment such as battlefield or emergency condition likes disaster liberation operation. In spite of the several attacks aimed at specific nodes in VANET that have been discovered, some attacks involving multiple nodes still receive little attention. A reason behind this is because people make use of confidence instruments applicable to wired networks in VANET and overlook the security measures that apply to VANET. Furthermore, it may also have to do with the fact that no survey or taxonomy has been done to explain the features of different multiple node attacks. In the proposed work detect the Sybil attack and prevention of Firefly optimization has been used with fitness function optimization. The whole reproduction will take place in MATLAB environment.

Keywords: Vehicular ad hoc network, Ad-hoc network firefly algorithm and Sybil attack.

I. INTRODUCTION

Vehicular networks permit vehicles to communicate with each other and with a distinct infrastructure on the road. Arrangements can be purely ad hoc amongst cars or facilitated by making use of an infrastructure. The organization usually consists of a set of so known as roadside units that are connected to each other or even to the Internet [1]. Otherwise, remaining infrastructure such as cellular networks can be used for this resolve. Vehicular Ad Hoc Networks have developed out of the need to provision the growing number of wireless produces that can nowadays be used in vehicles [1, 2]. These creates include remote keyless entry devices, personal digital supporters, laptops & mobile telephones. As mobile wireless maneuvers and networks become progressively important, the demand for Vehicle-to-Vehicle & Vehicle- to-Roadside or Vehicle-to-Infrastructure Communiqué will remain to grow [2]. VANETs can be exploited for a broad range of security & non-safety requests, allow for value additional services such as vehicle safety, automatic toll payment, traffic management, improved navigation, location based services such as conclusion the closest fuel station, eatery or portable lodge [3] & infotainment requests such as long as access to the Internet.

VANET is normally part Movable Ad-hoc system. Vehicular Ad-hoc System is mixture of Ad-hoc System& sensing System. In Vanet, automobiles act as sensing’s which container interchange data between each other deprived of any infra-structure System created. Directional mobility& high dynamic of the Automobiles are significant characteristics. In order to contribute in such a system, a vehicle has been prepared with a superior electric instrument which will give ad hoc system connectivity for the automobiles. VANETs are continuously shaped between affecting Automobiles prepared with wireless interfaces that might have dissimilar& same wireless boundary tools, employing less range to intermediate range message system. The best instance of VANET is Transport System of one travel support or any company which is merged internally. This Transport System of an Automobiles are affecting in any parts of city& dissimilar routes to pick or drop client or workers if they are associated together, which make an Ad hoc System& connected wireless[2].

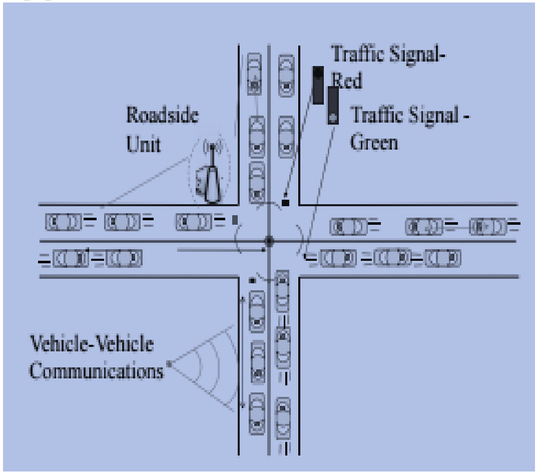


Fig no: 1 Vehicular ad hoc network Architecture

Roadside sensor nodes measure the road condition at several positions on the surface, collective the measured standards & communicate their amassed value to an approaching vehicle. The [4] vehicle generates a cautionary message & dispenses it to all automobiles in a certain geographical region, potentially using wireless multi-hop statement. For post-accident examination, sensor nodes continuously measure the road condition and supply this info within the WSN itself.

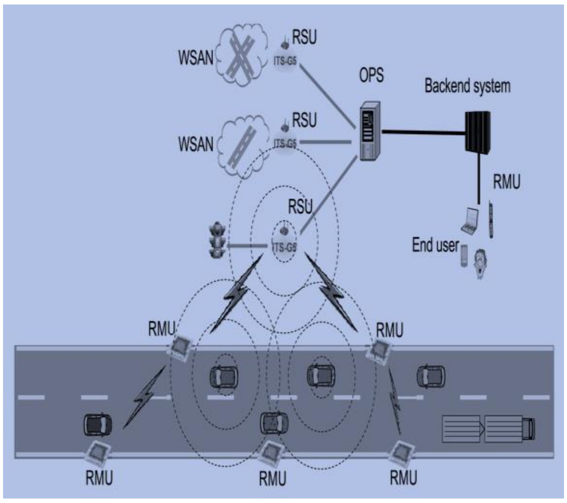


Fig no: 2 Road side unit (RSU) [17]

When a coincidence occurs, road condition data stored over a sufficiently long period can be used for criminal modernization of road accidents. In contrast to the accident prevention service, such an accountability service requirements to be constrained to a well specified group of end-users, e.g. insurance companies or the road patrol [6]. Information stored within the WSN can also be utilized to judge a driver's driving style allowing to the road condition at the instant of an accident.

II. BACKGROUND

A.Intelligent transportation systems

In intelligent transportation systems, each vehicle takes on the role of sender, receiver, and router [4] to transmission info to the vehicular network or transportation activity, which then uses the information to guarantee safe, free-flow of traffic. For communication to occur between vehicles and Roadside Unit vehicles must be prepared with some sort of radio interface or On-board Unit that enables short-range wireless ad hoc networks to be formed [5]. Vehicles must also be formfitting with hardware that permits complete position information such as Global Positioning System or a Difference Global Positioning System receiver. Fixed RSUs, which are associated to the support network, must be in place to simplify communication. The number and circulation of roadside units is dependent on the communiqué protocol is to be used. For example, specific protocols necessitate roadside units to be dispersed evenly throughout the entire road network; particular require roadside units only at connections, while others require roadside units only at section borders. Though it is benign to assume that infrastructure exists to some magnitude and vehicles have access to it irregularly, it is idealistic to require that vehicles always have wireless access to roadside units.

a) Inter-vehicle communication

The inter-vehicle communication conformation uses multi-hop multicast or programmer to transmit traffic linked information over multiple hops to a individual of receivers. In intelligent transportation systems, vehicles requirement only be concerned with movement on the road forward and not behind [6].

There are two types of message systematic in inter-vehicle communications:

(a) Naïve broadcasting and

(b) Intelligent broadcasting.

B. Vehicle-to-roadside communiqué

The vehicle-to-roadside communiqué formation characterizes a single hop broadcast where the roadside unit sends a[7] broadcast message to all prepared vehicles in the vicinity. Vehicle-to-roadside communication formation offers a high bandwidth link between automobiles & roadside units. The roadside units may be placed every kilometer or less, following high data rates to be constant in heavy traffic. For instance, when broadcasting active speed limits, the roadside unit will regulate the appropriate speed limit according to its internal schedule and traffic conditions [8]. The roadside unit will intermittently broadcast a message containing the speed bound and will compare any geographic or reversing limits with vehicle data to regulate if a speed limit warning applies to any of the vehicles in the locality. If a vehicle disturbs the desired speed limit, a broadcast will be delivered to the vehicle in the form of an acoustic or visual warning, requesting that the driver diminish his speed.

C. Routing-based communication

The routing based communication arrangement is a multi-hop unicast where a message is broadcasted in a multi Routing based announcement hop fashion pending the vehicle carrying the anticipated information is reached. When the request is received by a vehicle preserving the desired part of info, the application at that vehicle instantly sends a unicast message containing the information to the automobile it established the application from, which is then exciting with the task of forwarding it towards the query basis.

Table no: 1 Vehicular Adhoc System Attacks

Serial No.	Attack Name	Descriptions
1.	Spoofing	When a malicious knob miss-present his individuality, so this way it can change the idea of sender & sender transform the topology [15].
2.	Worm Hole Attack	Wormhole attack is as well call the tunnel attack. An attacker receives a packet at one point and tunnels it to one more malicious knob in the system. [8]
3.	Denial of services	The aim of malicious node is to be busy to the system knob. This system, if a communication from the certified node will come, then receiver will not receive the message for the reason that he is busy & apprentice has to stay for the handset response [9].
4.	Sybil Attack	Sybil attack refers to the many copies of malicious knobs. It can be occur, if the spiteful node shares its surreptitious key with further spiteful knobs[14]

III. PROBLEM FORMULATION

The survey we have found the problem or research work in which we are going to continue our work of Trust Management in network using the Particle swarm optimization.

VANETs were designated for this study because, among the vehicular networks, the ad-hoc configuration has the greater probable of widespread use:

- It is accessible like compared to cellular communication, lower cost, and offers higher bandwidth. Even though VANETs show great capability, their success is dependent on whether VANET routing protocols are able to satisfy the throughput and delay supplies of applications deployed on these networks [10].
- Most vehicles are restricted in their range of sign, for example by being constrained to follow a covered highway [3].

The study problem that is addressed in this paper will be defined in more details, including the models:

- A VANET normally refers to a wireless network of mixed sensors or other computing devices that are deployed in vehicles [11]. This type of network enables constant monitoring and sharing of road situations and status of the transportation systems.
- Every node in VANETs is equipped with the same wireless communication interface, such as IEEE 802.11p. The nodes are restricted in energy as well as computational and storage competencies.
- The road side units are assumed to be trustworthy since they are frequently better protected [12]. The related vehicles, on the other hand, are commonly more susceptible to various attacks, and they can be co-operated at any time after the VANET is formed [13].

IV. SIMULATION MODEL

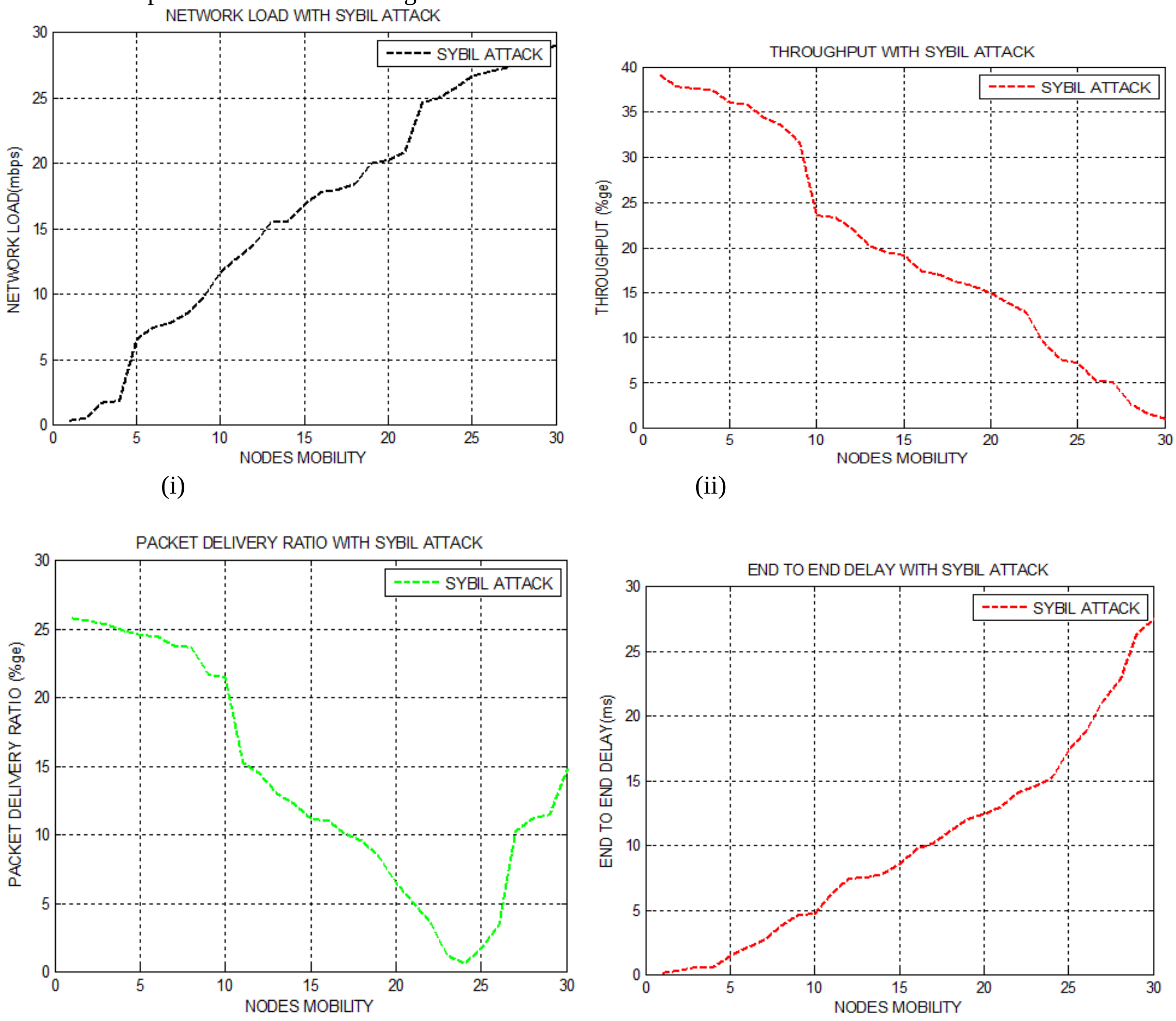
In simulation model, we described that the methodology of the work .Initialize the vehicular ad-hoc network, to create the network focus in data transmission. Sensors are plotting in a particular network to transfer the data one node to another node. To find the source and destination for vehicular ad-hoc network. To generate the coverage set for calculate the distance in particular range. To use the routing protocol for detection. Information Transfer one node to another node attacker will come and loss the information in particular node. Apply optimization technique for prevention and to save the information in particular nodes. Optimization Technique always gives the reduce index and using the fitness function for generates the fit value. To evaluate the performance parameters like throughput, bit error rate and etc. Compare the result in previous parameter.

Performance Parameters

- *A. Throughput* is the rate of production or the rate at which something can be processed.
- *B. Packet Delivery Rate:* The ratio of packets that are successfully delivered to a target compared to the number of packages that have been sent out by the sender.
- *C. End to End Delay* is the summary of Transmitting Delay (at MAC layer), Broadcast Delay and queuing Time of a packet.
- *D. Network Load:* commonly mentioned to as dual-WAN routing or multi-homing is the aptitude to balance traffic across two WAN links without using complex routing protocols.
- *E.Precision* is a description of random errors, a measure of statistical variability.
- *F.Recall* is the fraction of recovered instances that are pertinent, while recall (also known as sensitivity) is the fraction of relevant instances that are retrieved.

V. RESULT AND DISCUSSIONS

In result and discussion we implement the network in MATLAB. The subsequent Development Tools has been used in the expansion of this work. There may also be other tools which can be used in this development as it depends person to person and his interest. The below fig 3(i) described as, the network load with Sybil attack. The Sybil attack takes place where the no of original nodes will be replicated as what happens in the Sybil attack. As the no nodes increases the network load increases leading to congestion which will Detroit the network performance. Fig 3(ii) the networks load with Sybil attack. The Sybil attack takes place where the no of original nodes will be replicated as what happens in the Sybil attack. As the no nodes increases the network load increases leading to congestion which will Detroit the network performance. Fig 3(iii) the proportion of bits that are positively delivered to an endpoint associated to the quantity of packets that have persisted sent. Above figure shows the distribution ratio with Sybil nodes has been decreased. Fig 3(iv) shows that the observed that the end delay increases with the Sybil attack due to greater number of identities the number of Sybil attackers.



(i)

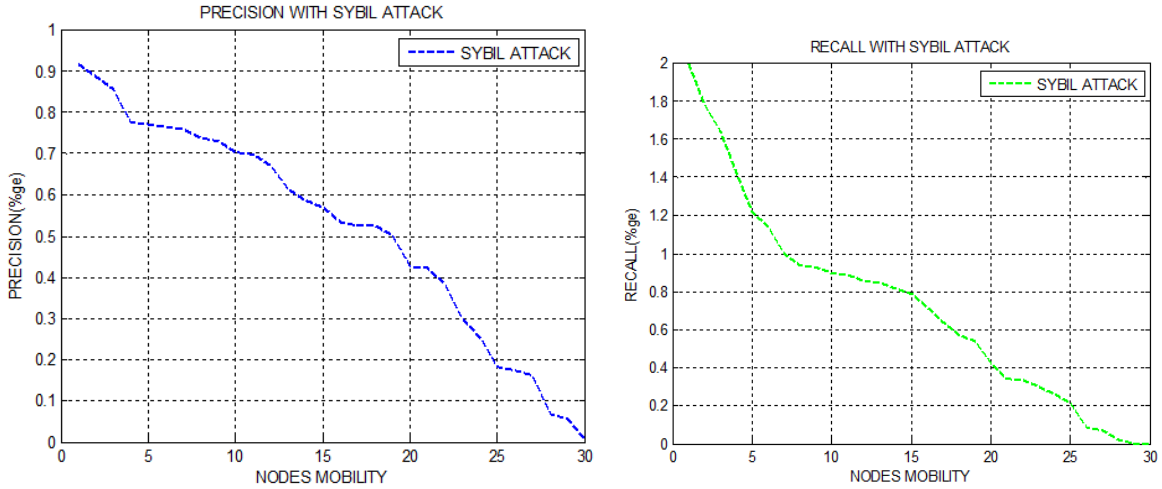
(ii)

(iii)

(iv)

Fig no: 3 In illustration defines that (i) Network Load with Sybil attack (ii) Throughput with Sybil attack (iii) Packet Delivery Rate with Sybil attack and(iv) End to End Delay using Sybil attack

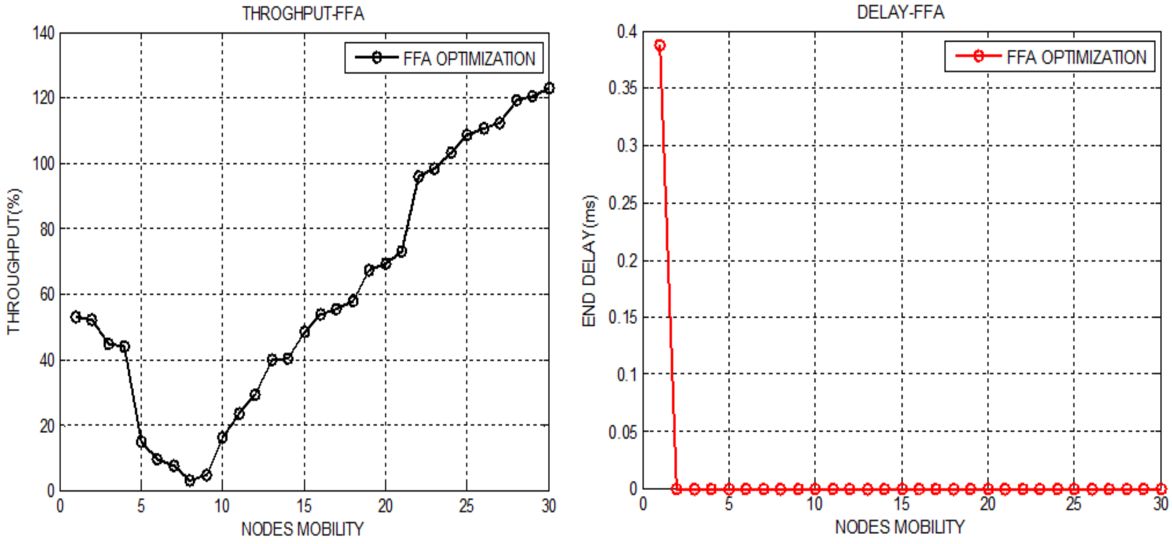
Below fig 4(i) shows that, it has also observed that the precision decreases with the Sybil attack due to greater number of identities the number of Sybil attackers. Fig 4(ii) represents that, It has also observed that the recall decreases with the Sybil attack due to greater number of identities the number of Sybil attackers.



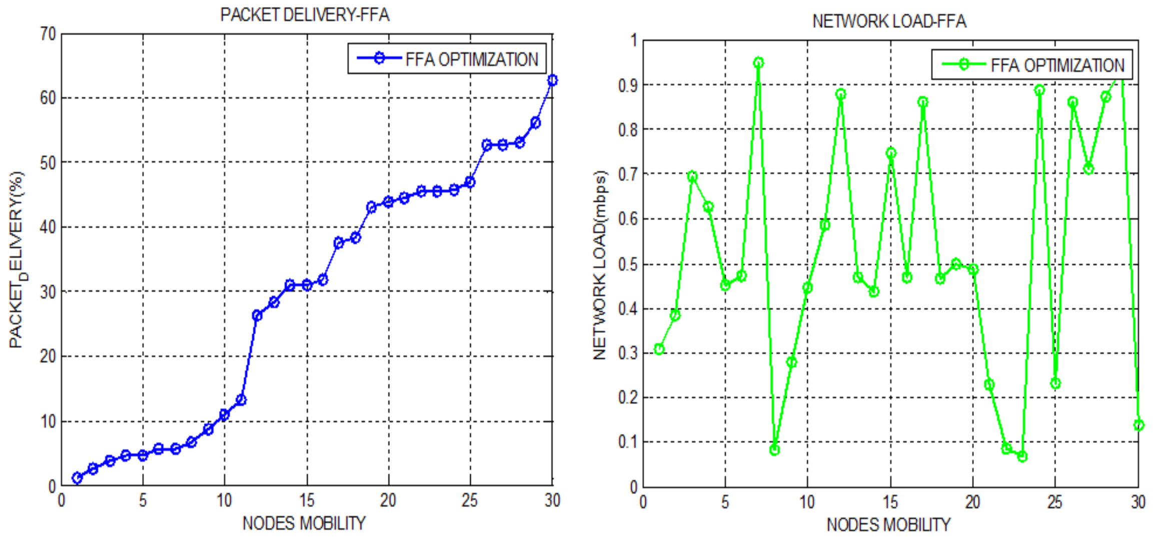
(i) (ii)

Fig no: 4 In illustration defines that the, (i) Precision with Sybil Attack and (ii) Recall with Sybil Attack

Below Fig 5(i) explained as the represents that the, the Sybil attacker nodes cause decrease in the throughput of the system. It is because amount of collisions is more in system and it is optimized using Firefly algorithm as shown above. Fig 5(ii) represents that, the End to End delay with Firefly Optimization. The parameter is a significant limitation for assessing a protocol which must be low for good performance. Fig 5(iii) represents that the delivery ratio with Firefly optimization. It is combination of bits that are completely sent to sink associated to the amount of bits that have been referred. Fig 5(iv) shows the network load with Firefly optimization. It is the ratio of number of data that are effectively transported to a terminus with the network load associated to the amount of packets that have been sent.



(i) (ii)

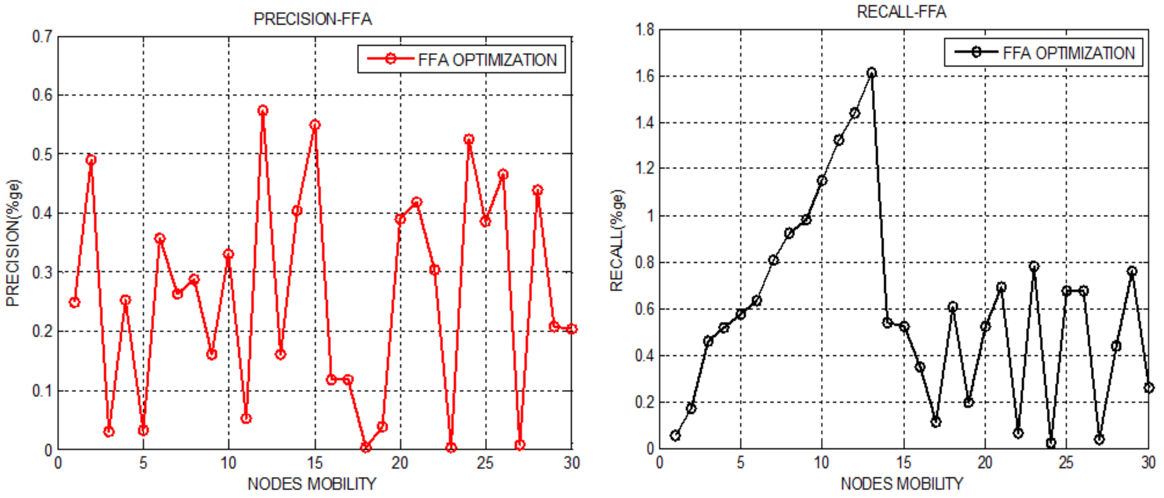


(iii) (iv)

Fig 5(i): In illustration described as the Throughput with FFA (ii)Delay with FFA (iii) Packet Delivery Rate with FFA and (iv) Network Load with FFA.

Below fig 6(i) shows that, It has also observed that the precision increases with the FFA Optimization due to greater number of identities the number of vehicle nodes.

Fig 6(ii) shows that the recall with optimization techniques low the info transfer because of its belong to false negative category.



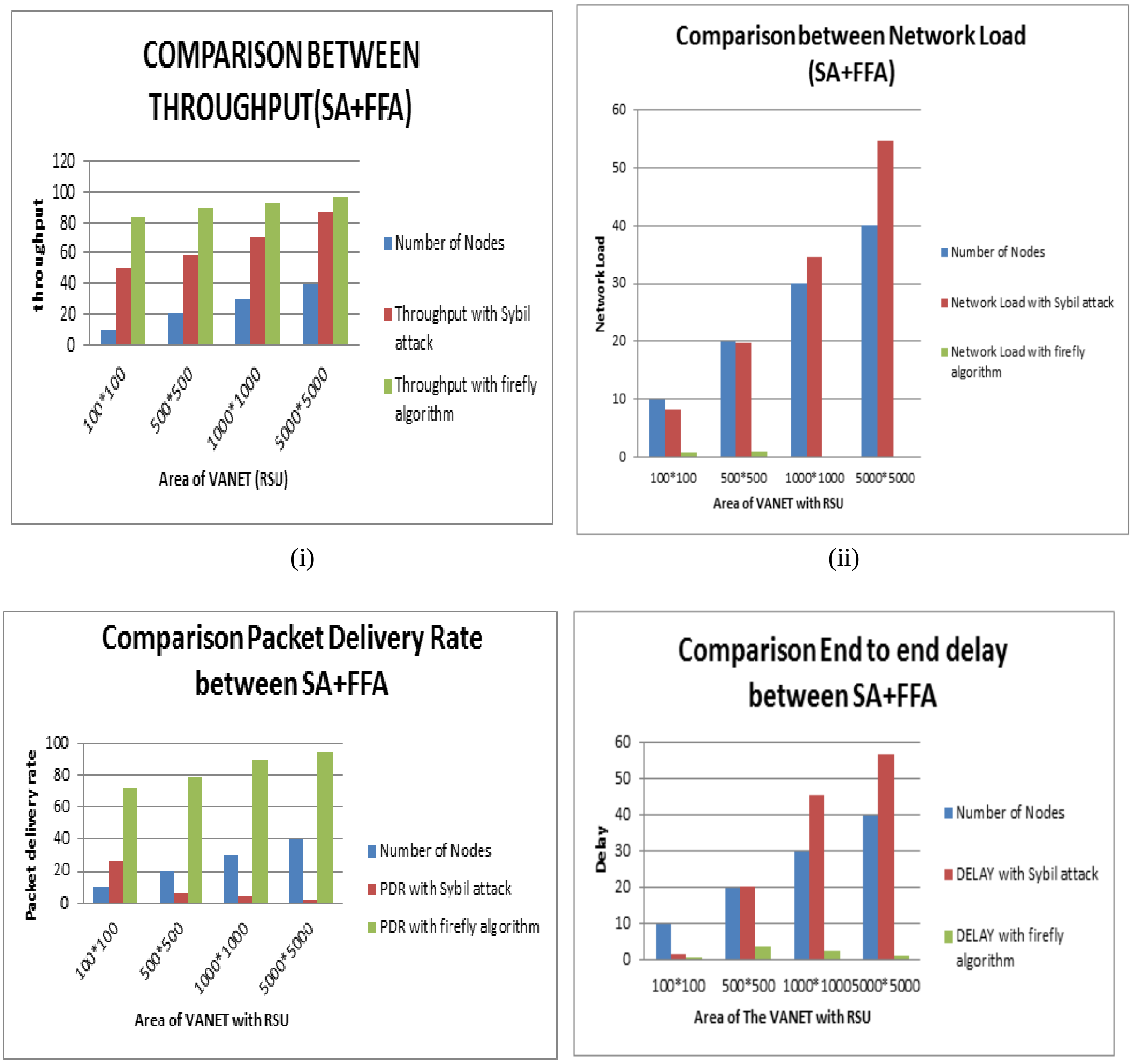
(i) (ii)

Fig 6(i) in illustration described as; (i) Precision with Firefly algorithm and (ii) Recall with Firefly Algorithm.

VI. COMPARISON RESULTS

Below Fig 7(i) here different optimization algorithms like FIREFLY and Sybil Attack with ROAD SIDE UNIT are used to calculate the accuracy of the network. All algorithms take some time to calculate the throughput value of the network which is shown in above figure. From Sybil attack with RSU's rules or management has less accurate network , so that we can say Firefly algorithm calculate accurate value is high. That's why in proposed work Firefly algorithm is used.Fig7(ii) Here different optimization algorithms like FIREFLY and Sybil Attack with ROAD SIDE UNIT are used to calculate the accuracy of the network. All algorithms take some time to calculate the throughput value of the network which is shown in above figure. From Sybil attack with RSU's rules or management has less accurate network , so that we can say Firefly algorithm calculate accurate value is high. That's why in proposed work Firefly algorithm is used. Fig 7(iii) Here different optimization algorithms like FIREFLY and Sybil Attack with ROAD SIDE UNIT are used to calculate the packet delivery rate means eject packet sent of the network. All algorithms take some time to calculate the package deliver value of the system which is shown in above figure. From Sybil attack with RSU's rules or management has less packet deliver , so that we can say Firefly algorithm calculate pdr value is high . That's why in proposed work

Firefly algorithm is used. Fig 7(iv) different optimization algorithms like FIREFLY and Sybil Attack with ROAD SIDE UNIT are used to calculate the packet delivery rate means eject DELAY of the network. All algorithms take some time to calculate the DELAY value of the network which is shown in above figure. From Sybil attack with RSU's rules or management has HIGH DELAY , so that we can say Firefly algorithm calculate DELAY value is minimum . That's why in proposed work Firefly algorithm is used.

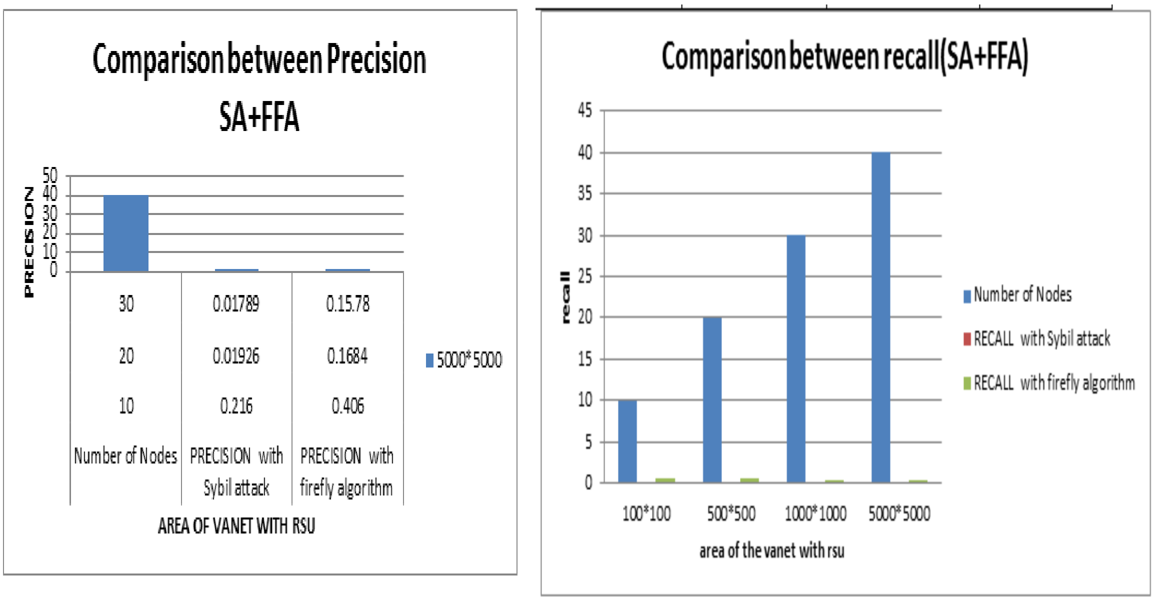


(i) (ii)

(iii) (iv)

Fig 7: (i) In illustration Defined that the comparison between Sybil attack and FFa (throughput) (ii) Comparison between Network Load (Sybil+FFA) (iii) Packet Delivery rate comparison between (Sybil attack and FFA) and (iv) End to end delay comparison between SA+FFA.

Fig 8(i) The different optimization algorithms like FIREFLY and Sybil Attack with ROAD SIDE UNIT are used to calculate the positive data of the network. All algorithms take some time to calculate the positive value of the network which is shown in above figure. From Sybil attack with RSU's rules or management has less precision value , so that we can say Firefly algorithm calculate precision value is maximum . That's why in proposed work Firefly algorithm is used. Fig 8(ii) different optimization algorithms like FIREFLY and Sybil Attack with ROAD SIDE UNIT are used to calculate the negative data of the network. All algorithms take some time to calculate the negative value of the network which is shown in above figure. From Sybil attack with RSU's rules or management has less recall value , so that we can say Firefly algorithm calculate recall value is maximum . That's why in proposed work Firefly algorithm is used.



(i) (ii)

Fig 8(i) an Illustration defined that the comparison Between Sybil attack with FFA in Precision (ii) Recall comparison between Sybil attack and FFA.

VII. CONCLUSION

VANET is no longer an inaccessible feasibility, given that heavy investments are already in the pipeline from several subdivisions including government agencies, vehicle businesses, navigation security and public transport authorities. VANET potentials, areas of submission and prospects are increasing rapidly including several kinds of services with multiple necessities and goals. However, several unique, novel open research contests ranging from wireless network evolution, reliable message broadcasting to event detection are making research in VANETs very attractive. With the wireless technology attractive pervasive and discounted, Vanet is going to turn out to be the networking platform that would support the future vehicular applications. We laid out the some drawbacks including security and performance and several efforts are being undertaken to create Vanet a reality. In upcoming we would like to propose an algorithm that would enhance the performance with the maintenances of safety using a light weight machinery Multiple copies are generated through this attack. It causes traffic congestion, jamming etc. We have formulated our problem and have found a solution to resolve this attack .We have generated an algorithm called Firefly Algorithm which has been applied. After that proposed technique which has been improved my results delay and network load etc. The coming work, mobiles are acquainted and used by us in our day to day life, likewise the future of VANETs is certainly secure.

VIII. REFERENCES

[1]. Suriyapaibonwattana, Kanitsom, and Chotipat Pomavalai. "An effective safety alert broadcast algorithm for VANET." Communications and Information Technologies, 2008. ISCIT 2008. International Symposium on. IEEE, 2008.

[2]. Xi, Sun, and Xia-Miao Li. "Study of the Feasibility of VANET and its Routing Protocols." Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on. IEEE, 2008.

[3]. Merlin, Christophe J., and Wendi B. Heinzelman. "A study of safety applications in vehicular networks." Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on. IEEE, 2005.

[4]. Samara, Ghassan, Wafaa AH Al-Salihy, and R. Sures. "Security issues and challenges of vehicular ad hoc networks (VANET)." New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on. IEEE, 2010

[5]. Vandenberghe, Wim, et al. "Suitability of the wireless testbed w-iLab. t for VANET research." Communications and Vehicular Technology in the Benelux (SCVT), 2011 18th IEEE Symposium on. IEEE, 2011.

[6]. Sumra, Irshad Ahmed, et al. "A novel vehicular SMS system (VSS) approach for Intelligent Transport System (ITS)." ITS Telecommunications (ITST), 2011 11th International Conference on. IEEE, 2011.

[7]. Subramaniam, Prabhakar Rontala, Arunkumar Thangavelu, and Chitra Venugopal. "QoS for highly dynamic Vehicular ad hoc network optimality."ITS Telecommunications (ITST), 2011 11th International Conference on. IEEE, 2011.

[8]. Zheng, Liming, Wanlei Li, and Bo Xie. "Research on Communications over VANET under Different Scenes and Implementation of Vehicle Terminal."Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on. IEEE, 2012.

[9]. Barnwal, Rajesh P., and Soumya K. Ghosh. "Heartbeat message based misbehavior detection scheme for vehicular ad-hoc networks." Connected Vehicles and Expo (ICCVE), 2012 International Conference on. IEEE, 2012.

[10]. Hussain, Rifaqat, et al. "Rethinking vehicular communications: Merging VANET with cloud computing." Cloud Computing

Technology and Science (CloudCom), 2012 IEEE 4th International Conference on. IEEE, 2012.

[11]. Baldini, Gianmarco, et al. "Identity-based security systems for vehicular ad-hoc networks." Connected Vehicles and Expo (ICCVE), 2013 International Conference on. IEEE, 2013.

[12]. Li, Wenjia, and Houbing Song. "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks."IEEE Transaction , 2015.

[13]. Wei, Wei, et al. "SybilDefender: a defense mechanism for Sybil attacks in large social networks." Parallel and Distributed Systems, IEEE Transactions on 24.12 (2013): 2492-2502.

[14]. Zhu, Hongzi, et al. "Impact of traffic influxes: Revealing exponential intercontact time in urban vanets." Parallel and Distributed Systems, IEEE Transactions on 22.8 (2011): 1258-1266.

[15]. Luo, Yuyi, Wei Zhang, and Yangqing Hu. "A new cluster based routing protocol for VANET." Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Transaction on. Vol. 1. IEEE, 2010.