Secure and Enhanced Vehicular Ad-Hoc Networks Using DSR Protocol and BFOA Algorithm

Mamta Devi
Research Scholar, CSE Department, SECG, Mohali
manhas.sajal@gmail.com

Dr Rakesh Kumar
Professor& Principal, CSE Department, SECG, Mohali
rakesh77kumar@yahoo.com

Er Nidhi Bhatla
Head of Department, CSE Department, SECG, Mohali
engineernidhi@yahoo.com

Abstract The VANETs (Vehicular Ad-Hoc Networks) widely recognized with Manets (Mobile Ad-Hoc Networks) and turns into the demanding area of research. In VANETs moving vehicles act as the nodes and router to create a mobile network. The information exchanged in vehicles are depend upon the communication mode. The communication takes part in three ways vehicle to vehicle, vehicle to infrastructure and hybrid mode. The major goal of VANETs is to improve the overall safety of transportation infrastructure that includes more comfortable driving, minimize accidents, local danger warnings, up–to-date traffic information and internet access. Due to the mobility of nodes the issues arise related to security and the attacker attacks to reduce the security. In most cases, attacks on the availability that unavailable the resources due to a selective forwarding attack that aims to halt the network. Routing protocols is used to improve security, detect and prevent attacks in VANETs. Hybrid approach implementation for prevention and detection using DSR and BFOA are use to improve the security and throughput performance.

Keywords Vehicular Ad-Hoc network (VANETs), DSR (Dynamic Source Routing) Protocol, BFOA+DSR (Optimized Dynamic Source Routing), BFOA (Bacterial Foraging Optimization Algorithm) and Selective Forwarding Attack.

1. INTRODUCTION

Vehicular networks permit vehicles to communicate with each other and with a distinct infrastructure on the road. Organizations can be virtuously Ad-Hoc between cars or facilitated by making use of a substructure. The organization typically consists of a set of so called roadside units that are connected to each other or even to the internet [1]. Otherwise, remaining infrastructure such as cellular networks can be used to resolve.

Vehicular Ad-Hoc Networks have implemented out of the need to provision the growing number of wireless produces that can now be used in vehicles [2]. This process is including remote devices, personal digital supporters, laptops and mobile telephones. As mobile wireless measures and networks developed increasingly important,the demand for Vehicle-to-Vehicle and Vehicle-to-Roadside or Vehicle-to-Infrastructure Communication will remain to grow. VANETs can be subjugated for a broad range of safety and non-safety requests, allow for valuable additional services such as vehicle safety, automatic toll payment, traffic management, improved navigation, location based facilities such as conclusion the closest fuel station, restaurant or travel lodge [3] and infotainment applications such as long as access to the internet. The environment is using to provide a wide-range of information-driven services, adding both safety and non-safety related car applications; Vehicular ad-hoc network has also specific problems on higher layer of the OSI model. Cyber security and information tasks become a novel inter-car communications development.

In vehicular Ad-Hoc networks are several nodes such as vehicles and RSUs(Road Side Units) are normally required with sensing, dispensation and wireless communication abilities. Vehicular to Vehicular and Vehicle to infrastructure communications allow securing requests that give warning message about traffic control, road accident and some other relevant transportation actions. Although, vehicular Ad-Hoc networks threats, due to maximizing reliability on message and manage technologies [4].

The unique privacy and security tasks posed by vehicular ad-hoc networks add trusted data, access control and privacy protection. The applications of VANETs are the Prediction and Traffic Estimation System, which usually gives the predictive information required for pro-active traffic managers and transmit information [5].

An example, in this system could give input to traffic-controllers who manage where and when to travel specific information packet on variable message symbols, called an emission jamming - occur here for modified route or path.

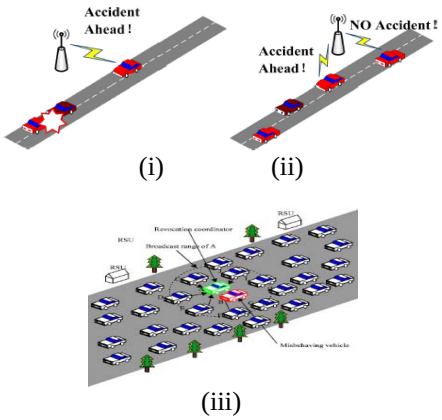


Fig 1. True Alerts v/s False alerts in Vehicular ad-hoc network for traffic monitoring [21]. (i) True Traffic message alert (ii) Contradictory traffic alert message and (iii) Out-side of the false traffic message alerts [6].

The vehicular Ad-Hoc network application defines a roadside unit could be treated as an access-point and a router or even buffer point which could store data and provide information when required. All information on the road-side units are uploaded/downloaded by vehicles [7]. A classification of submissions is also done by Car-to-car traffic submission Car to Infrastructure applications. We are arranging the applications of VANETs into following classes [8]:

- Safety Oriented
- Commercially Oriented
- Convenience Oriented
- Productivity Applications

In section I, described that the overview of the vehicular ad-hoc network. Various challenges and application defines a roadside unit could be treated as an access-point and a router or even buffer point which could store data and provide information when required. In section II, described that the prior studied by the various routing protocols and techniques used in VANET. Section III, discussed with the various routing protocols in VANETs. In section IV, defined that the issues occur in vehicular networks and proposed model defined in section V. In Section VI discussed the proposed work explanation in VANETs networks. Section VII discussed the future scope in VANETs.

2. RELATED WORK

Shiang-Feng Tzeng et al.,2015[10] as in this research the VANETs improves the communication between the vehicles very efficiently to provide traffic safety. The proposed approach is an identity-based batch verification which makes the communication process secure and provides efficient and fast speed between nodes. The proposed approach mainly focuse on the privacy of the networks, transmission along with vehicle information in the network. The author proposed an approach on the basis of various evaluated parameters like delay, overhead, etc. and compare with the existing method to check the performance and capability in real time environment and traffic. Bingyi Liu et al., 2015, [11] in VANETs the communication between nodes and vehicles need to be secure and fast.Various attacks in this field are trying to affect the performance of network communication. VANETs cellular heterogeneous network is a proposed model is used to communicate with the roadside units and vehicles for secure and efficient routing. Existing approaches are mainly based on gateway selection for achieving the security level of routing the message from source to destination. Proposed approach enhanced with Cloud-assisted Message Downlink dissemination which is used to make the communication process more secure. It works with cloud computing, which secures the message passing between cloudserver to roadside units and vehicles. In this approach, the gateway is used as bushes between cellular and VANETs interface. The proposed method compared with various parameters. Chun-Chih Lo et al., 2015 [12]the author worked on traffic-aware routing protocol in VANETs for checking and constructing the source to the destination delivery path. The proposed approach is working on the basis of three different mechanisms which are used to handle their own areas in VANETs. Route construction is the main concept of them to find the correct route for VANETs. Another module is used to collect the traffic information to improve the communication and better management. The third module is road scoring, which is a light weight real-time system used in Van to improve the efficiency of network communication. The performance of the proposed approach is evaluated through end to end delay, packet delivery ratio and overhead. Mahajan, Surabhi, et al., 2010 [13] authors worked on

VANETs IEEE 802.11p to provide secure and efficient routing to communicate with vehicles and roadside units. The inter-vehicular communication, manages the communication and road traffic information to make the communication process more accurate and safe in the network. The proposed approach enhances the VANETs performance with the use of group signature technique. The proposed approach uses encryption during the communication between one to another unit or network node. The proposed approach encryption can only decrypt on authorizing end as in this paper. In the proposed approach, a group communication can also use the encryption and only group members are authorized to read that message. As in performance various parameters are compared to find the best performance of the proposed approach. Rajesh Kumar M, et al.,2016 [14] author did their research in VANETs with optimization technique to enhance the performance of the network. The behavior of the network is dynamic in this paper. Due to this, it's difficult to find the route and communication from one to another node. Lots of techniques are already developed in this field to enhance delay factor, energy efficiency, jitter and throughput of the network. The optimization process in this field is used to find the perfect path for transmission. It also enhance the speed and accuracy of the communication in VANETs. For algorithm efficiency there are various parameters are used for the comparison of delay, packet delivery ratio etc.

3.VARIOUS TYPES OF ROUTING PROTOCOLS

In VANETs, the routing protocols are classified into five categories: Topology based routing protocol, Point based routing protocol, Cluster based routing protocol, Geo cast direction-finding protocol and Program routing protocol. Proactive and Reactive[15]. These protocols are characterized on the basis of area/application where they are most suitable [9]. These routing protocols use links gene that exists in the network to perform packet advancing. They are further divided into following categories:

3.1 **ProactiveProtocol:** Proactive routing protocols are mostly based on shortest path algorithms. They keep evidence of all connected nodes in the form of tables because these procedures are table based. Further more, these tables are shared with their neighbours. Whenever any change transpires in network topology, every node informs its routing table [16].

3.2 **Reactive Protocol:** Reactive routing protocol is called on demand routing because it starts route encounter when a node needs to communicate with extra node thus it reduces network traffic.

Table 1. Comparison between Various types of routing protocol

Protocol Name	**Type**	**Merits**	**Process**
DSR	On-demand reactive	Limited Bandwidth Consumed	Complete path generates the S to D
OLSR	Table driven	Minimize the required no. of CP	Process data in shortening the size of CP
AODV	On demand	Discover the route in less time	Maintained the route are required
DSDV	Table driven	Creates the possible D node	Shortest distance and identifies the address

Table 1 Defines that the comparison between routing protocols. List of Abbreviation's CP-Control Packets, S-Source and D-Destination. DSR-Dynamic Source Routing Protocol, OLSR-Optimized Link State Routing Protocol, AODV-On demand distance vector routing Protocol and DSDV-Destination Sequence Distance Vector Protocol.

Table 2. Protocol Properties in VANETs

Property	DSDV	DSR	AODV	OLSR
Multiple routes	N	Y	N	Y
Un-directed link	Y	Y	Y	Y
Multi-cast	N	N	Y	Y
Periodic Broadcast	Y	N	Y	Y
Route Maintenance	RT	RC	RT	RT

In table 2 defines that the protocol properties of the vehicular Ad-Hoc networks. Some abbreviations are Y-Yes, N-No, RT-Route Table and RC-Route Cache [18].

4. ISSUES IN VANETs

Security in VANETs plays a vital role. VANETs normally refers to a wireless network of mixed sensors or other computing devices that are deployed in vehicles [19]. This type of network enables constant observing and sharing of road conditions and status of the transportation systems. An AODV routing protocol is a sensitive or on-demand routing protocol, which resources if there is data to be sent then the path will create. AODV is normally used in topology based routing procedure for VANETs. Using of broadcast packets in the AODV route discovery phase caused it is tremendously susceptible against DOS and DDOS flooding attacks. Flooding attack is a type of DDoS attack that sources loss of network bandwidth and imposes high overhead to the network.

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 anticipated to be trustworthy since they are normally better protected [20]. 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 VANETs is formed. The adversary can be a stranger located in the wireless range of the vehicles, or the adversary can first cooperation one or more vehicles and behave as an insider later. The adversary is able to eavesdrop, jam, modify, forge, or drop the wireless communication between any devices in range. The Selective Forwarding attack is a type of a denial of facility attack that causes loss of network bandwidth and executes high overhead to the network.

5. PROPOSED WORK

In this proposed work, to analyze vehicular Ad-Hoc network techniques like balanced on-demand distance vector routing protocol. To develop a complex algorithm using road side unit, DSR routing protocol and Selective Forwarding Attack together to enhance the current mechanism. To implement the Enhance Bacteria Foraging for Optimization (BFOA+DSR) for finding best outfit with the help of the fitness function. Compare the proposed algorithm (DSR, RSU and BFOA) with an existing algorithm (B-AODV and RSU) on parameters: Throughput, Overhead, End to End Delay and Packet Delivery Rate.

Step 1: The vehicular Ad-Hoc network in MATLAB 2013 simulation tool used. We use the scripting language to design the VANETs network and deploy the vehicular nodes in VANETs. Search the source and destination node in this network.

Step 2: Assign the vehicular node ids and calculate the each vehicular node energy. We create the coverage set to find the coverage area and distance evaluated.

Step 3: We implement the DSR protocol to communicate the information source to the intermediate node send the request and further data transfer to the destination node.

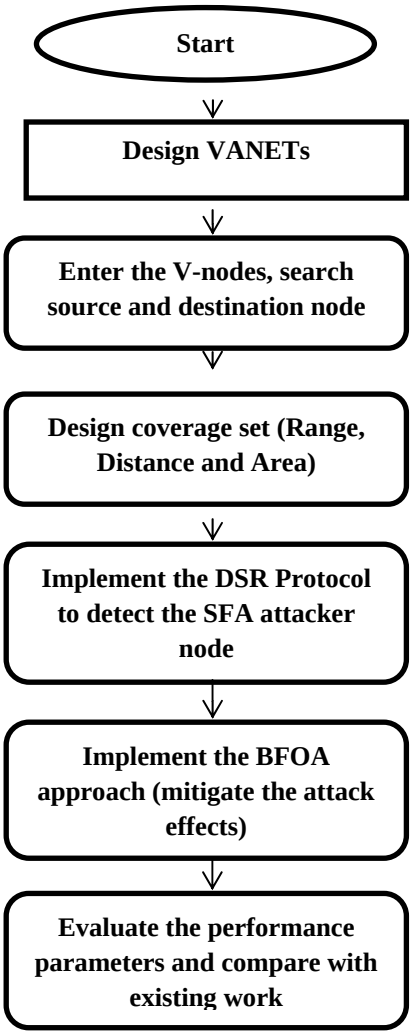


Fig 2. Flow Chart of Proposed Work

Step 4: If route is available then, selective forwarding attack occurs and create the problems like increase the time and decrease the delivery of the packets and throughput in the VANETs.

Step 5: To implement the Enhance Bacteria Foraging for Optimization (BFOA+DSR) for finding best outfit with the help of the fitness function. Compare the proposed algorithm (DSR, RSU and BFOA) with an existing algorithm (B-AODV and RSU) on parameters: Throughput, Overhead, End to End Delay and Packet Delivery Rate.

Step 6: Compared with proposed and existing performance parameters in VANETs.

6. SIMULATION RESULTS

In this section, we discuss the proposed work explanation in VANETs networks. The performance of the proposed BFOA+DSR method is evaluated and the experimental results are presented.

Table 3: Simulation Performance Parameters

Parameter	Value
Network Area	1000*1000m
Number of vehicle nodes	30,50,100
Transmission Range	200m
Node placement	Randomly
Number of Attacker nodes	5,7,10,12,15.16,17,19,20
Speed Mobility	10m/s, 20m/s
Simulation Time	600msec

The simulation framework and table 3 list the parameters used in the simulation scenarios, we use the BFOA+DSR as well as BFOA method when we calculate the performance of the BFOA+DSR method, since the routing technique and optimization technique has been extensively used in several trust management scenarios or structure designed for VANETs such as;

We use the performance parameters to calculate the throughput of the new approach: Precision, Recall, throughput and many more. These are widely used in ML (Machine Learning) and information retrieval to access the throughput of the VANETs.

In this research work, we used the formula in two parameters i.e precision and recall, to calculate accurate results in VANETs.

These binary parameters are defined as follows:

$$\text{Precision} = \frac{\text{No.oftrueatatchernodefound}}{\text{Totalno.ofuntrustworthynodefound}} \ldots\ldots \text{(i)}$$

$$\text{Recall} = \frac{\text{No.oftrueattackernodesfound}}{\text{Totalno.oftruelyattackernodes}} \ldots\ldots\ldots\ldots\ldots \text{(ii)}$$

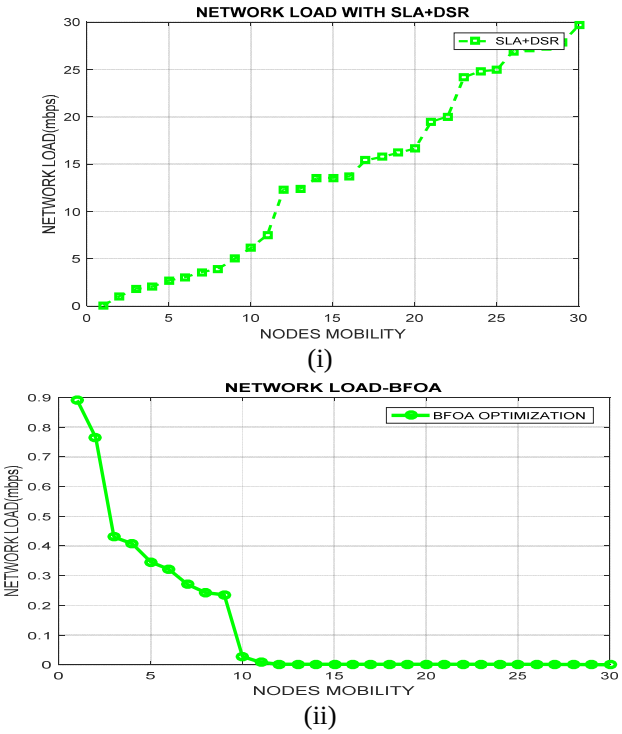
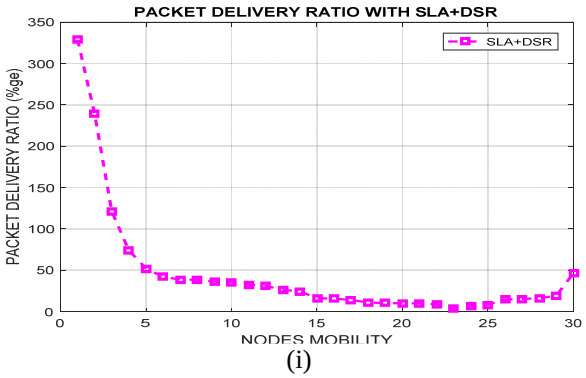
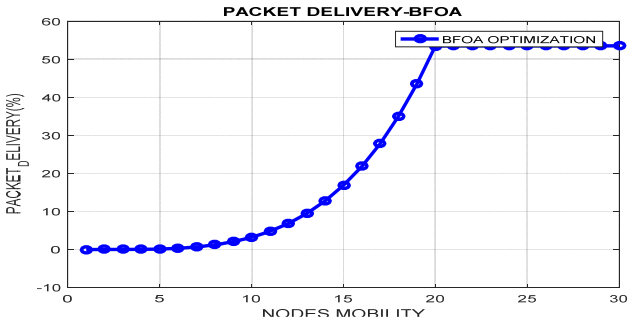


Fig 3. (i) Network Load (attack) and (ii) Network Load (Proposed)

Above figure, 3(i) Shows the network load with SFA attack. The SFA attack takes place where the no of original nodes will be replicated as what happens in the Sybil attack. As the no nodes increase the network load increases, leading to congestion, which will Detroit the network performance. Fig 3(ii) The network load with BFOA as well as BFOA+DSR optimization. It is the ratio of the number of data that are effectively transported to a terminus with the network load associated to the amount of packets that have been sent.

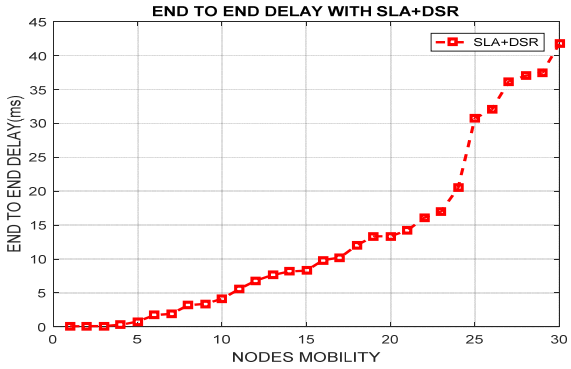




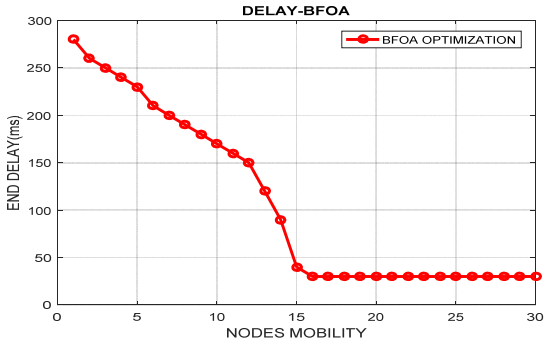
(ii)

Fig 4 (i) Packet Delivery Rate (Attack) and (ii) Packet Delivery (proposed)

The above figure 4(i) shows that the proportion of bits that are positively delivered to an endpoint associated with the quantity of packets that have persisted sent. The above figure shows the distribution ratio with attack nodes has been decreased. The figure shows the delivery ratio with BFOA+DSR optimization. It is a combination of bits that are completely sent to sink associated to the amount of bits that have been referred.



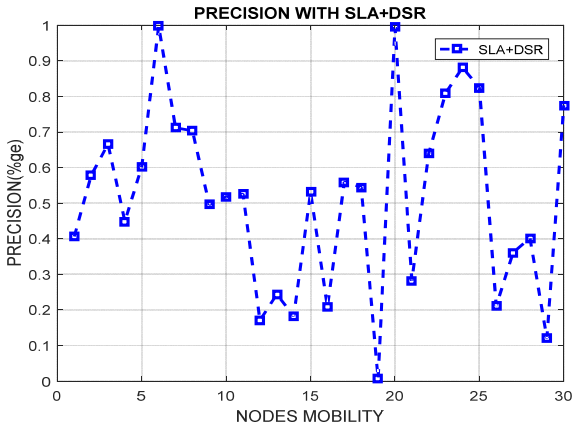
(i)



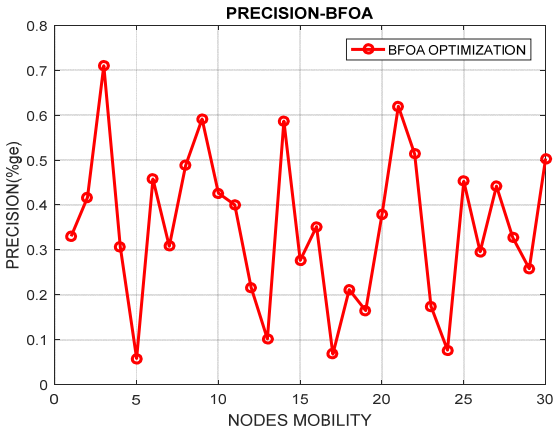
(ii)

Fig 5. (i) Delay (Attack) and Delay (Proposed)

It has also observed that the end delay increases with the SFA attack due to the greater number of identities the number of SFA attackers. Figures show the End to End delay with BFOA+DSR Optimization. The parameter is a significant limitation for assessing a protocol which must be low for good performance.



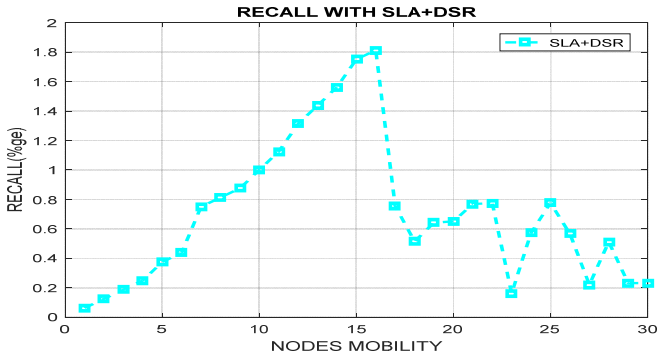
(i)



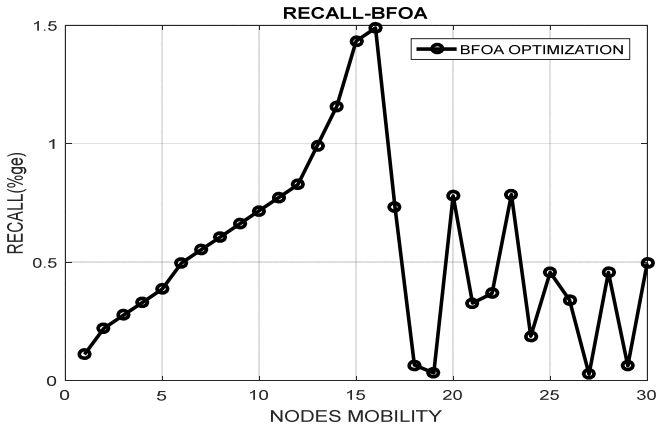
(ii)

Fig 6 (i) Precision (Attack) (ii) Precision (BFOA+DSR)

The above figure shows that, it has also observed that the precision decreases with the SFA attack due to the greater number of identities the number of SFA attackers. The above figure shows that the precision with the BFOA+DSR number of packets, forward lower to higher nodes using optimization technique. Precision belongs to a category of positive data separated by the total number of knobs as belong to the positive category.



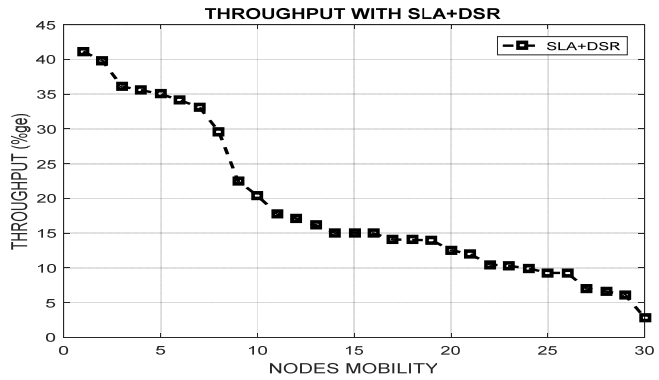
(i)



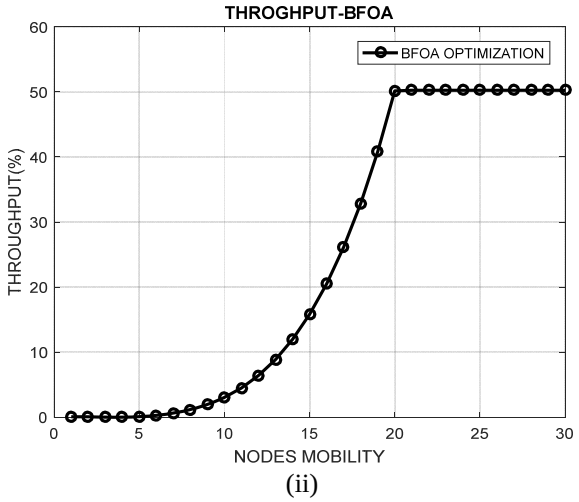
(ii)

Fig 7(i) Recall (Attack) and (ii) Recall (BFOA+DSR)

The above figure 7(i) show that, It has also observed that the recall decreases with the SFA attack due to the greater number of identities the number of SFA attackers. The above figure 7(ii) shows that the recall with optimization techniques low the info transfer because of it's belong to a false negative category.



(i)



(ii)

Fig 8(i) Attack and (ii) BFOA+DSR

In this figure we can see the throughput of the network with SFA attack. The average throughput decreases with the numbers of SFA attacker increases. Fig 8 (ii) The SFA attacker nodes cause a decrease in the throughput of the system. It is because the amount of collisions is more into system and it is optimized using the BFOA+DSR algorithm as shown above.

Table no. 4 Comparison between precision (Proposed and Existing Work)

Number of Vehicle Nodes	Precision [Existing]	Precision[Propsed]
10	0.5	0.45
20	0.59	0.49
30	0.6	0.57

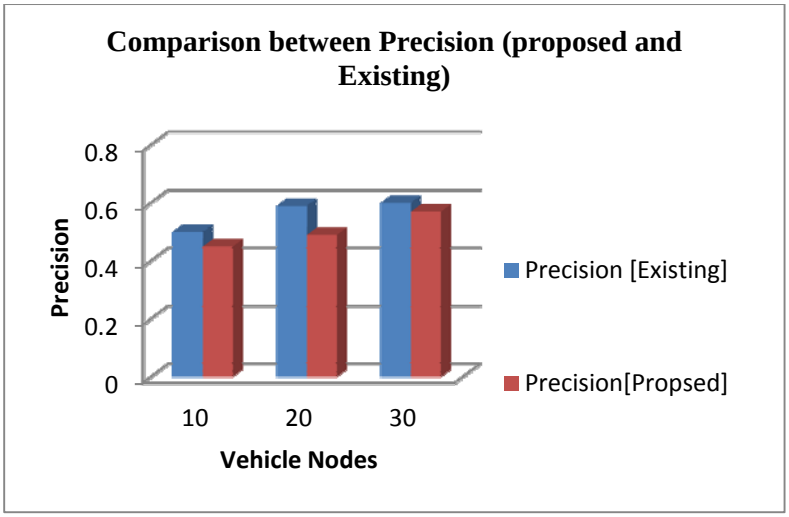


Fig 9 Comparison Between precision (Proposed and existing work)

In this figure define the comparison proposed and existing work; we reduce the precision value as compared to existing one.

Table 5 Comparison between recall (Proposed and Existing Work)

Number of Vehicle Nodes	Recall (Exiting)	Recall (Proposed)
10	1	1.2
20	0.8	0.89
30	0.4	0.5

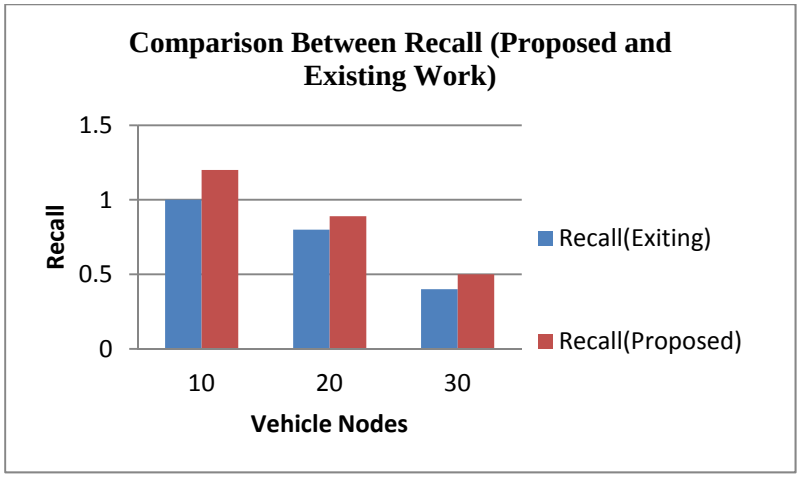


Fig 10. Comparison between Recall (Proposed and existing Work)

In this figure define the comparison proposed and existing work; we improve their call value as compared to existing one.

7. CONCLUSION AND FUTURE SCOPE

In this paper, the techniques for detection and prevention of a selective forwarding attack that occurs due to the SFA attack are presented.In VANETs security is very essential. DSR (Dynamic Source Routing) protocols are used to detect the attacker nodes in the network. DSR uses the shortest index in which mean and standard deviations are calculated to manage the nodes. Existing approaches improve the DSR results, but the problem is to increase the more throughput, to reduce energy, decrease delay and increasing packet delivery rate. To overcome these problems, DSR, BFOA and the comparison of results based on new techniques with the existing techniques. DSR is the dynamic Source routing protocol which is used to find out the smallest path from source to destination and is based on time. BFOA enhances Bacterial Foraging optimization algorithms which used for preventions and it increases the throughput, packet delivery rate, accuracy, and decreases delay, packet loss and overhead.

The VANETs future is secure so the usage of VANETs increased. The VANETs used in administering 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 every where to increase the traffic safety, make the driving more comfortable and secure.

REFERENCES

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

[2] Yu, Bo., and Bin Xiao. (2006) "Detecting selective forwarding attacks in wireless sensor networks." In Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International, pp. 8-pp. IEEE.

[3] Mbarushimana, C., and Alireza S., (2007), "Comparative study of reactive and proactive routing protocols performance in mobile Ad-Hoc networks." In Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, vol. 2, pp. 679-684. IEEE.

[4] Kanitsom, S., and Chotipat, P., (2008), "An effective safety alert broadcast algorithm for VANETs." Communications and Information Technologies, 2008. ISCIT 2008. International Symposium on. IEEE.

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

[6] Chandrasekaran, G., (2008) "VANETs: The networking platform for future vehicular applications." Department of Computer Science, Rutgers Univers3ity.

[7] Mahajan, S., and Jindal, A., "Security and privacy in VANETs to reduce authentication overhead for rapid roaming networks." International Journal of Computer Applications 1, no. 20 (2010): 21-25.

[8] Ade, S. A., and Tijare, P.A., (2010), "Performance comparison of AODV, DSDV, OLSR and DSR routing protocols in mobile Ad-Hoc networks." International journal of information technology and knowledge management 2, no. 2: 545-548.

[9] Kumar, R., and Mayank, D., (2011) "A comparative study of Various Routing Protocols in VANETs." arXiv preprint arXiv:1108.2094.

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

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

[12] Subramaniam, P., Rontala, Kumar, A, T., and ChitraV.,(2011) "QoS for highly dynamic Vehicular Ad-Hoc network optimality."ITS Telecommunications (ITST), 2011 11th International Conference on. IEEE.

[13] Zeadally, S., Ray H., Yuh-Shyan C., Angela I., and Aamir H.,(2012) "Vehicular Ad-Hoc networks (VANETs): status, results, and challenges." Telecommunication Systems 50, no. 4 : 217-241.

[14] Passino, K, M., (2012), "Bacterial foraging optimization." Innovations and Developments of Swarm Intelligence Applications (2012): 219-233.

[15] Horng, Shi-Jinn, Shiang-FengTzeng, Tianrui Li., Xian Wang, Po-Hsian Huang, and Muhammad Khurram Khan. "Enhancing security and privacy for identity-based batch verification scheme in VANETs." IEEE Transactions on Vehicular Technology (2015).

[16] Liu, Bingyi, DongyaoJia, Jianping Wang, Kejie Lu., and Libing Wu., "Cloud-assisted safety message dissemination in VANETs-cellular heterogeneous wireless network." IEEE Systems Journal (2015).

[17] Lo, Chun-Chih, and Yau-Hwang Kuo. "Traffic-Aware Routing Protocol with Cooperative Coverage-Oriented Information Collection Method for VANETs." IET Communications (2016).

[18] Li, Wenjia, and HSong. (2016) "ART: An attack-resistant trust management scheme for securing vehicular Ad-Hoc networks." IEEE Transactions on Intelligent Transportation Systems 17, no. 4 : 960-969.

[19] Kumar, R., and Sudhir K. Routray. "Ant Colony based Dynamic source routing for VANETs." In Applied and Theoretical Computing and Communication Technology (iCATccT), 2016 2nd International Conference on, pp. 279-282. IEEE, 2016.

[20] Rajput, U., Fizza Abbas and Heekuck Oh., (2016) "A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANETs." IEEE Access 4 (2016): 7770-7784.

[21] Harit, S. K., Saini, S. N., Tyagi, and K. K. Mishra. "RSA Threshold signature based node eviction in vehicular ad hoc network." Information Technology Journal 11, no. 8 (2012): 980.