Performance Enhance of Dynamic Source Protocol in Vanets under Bha in Urban Areas

Kompal Kour Saini[1], Rasneet kaur[2]
[1]*Research Scholar,* [2]*Assistant professor*
[12]*Department of Computer Science Engineering*
[12]*Shaheedudham Singh College of engineering and technology*

Abstract- In the recent world of advanced technology, VANET has a way to the development in the field of automotive, transportation, sensing, computing, wireless communication, and networking technologies. Vehicular ad hoc networks (VANET) have paved the way to the Internet of vehicles (IOV). The internet of vehicles has been used in the variety of the applications such as traffic management, collision avoidance, multimedia streaming, infotainment, and e-health where all the applications depend on the VANET. Though there is a lot of advancement in the various aspects still VANET is challenging issue where communication is difficult from source to destination. The communication problem may be due to change in frequent topology and due to high-speed mobility, sparse network. The requirement of the quality of service is the most challenging issue in the VANET applications. This challenging issue based on the single layer track. In the existing research, multi-hop path for packet delivery is required in the quality of service for decision-based routing protocol. In the existing research, a protocol that describes the physical layer in decision making during the traffic load at the network layer. The data variants are used for highways and urban environments. Implemented cross-layered routing multi-hop named PHY-MAC layer protocol for multiple layer networks. The comprehensive analyses, issue related to quality of service solutions in routing protocols in the urban areas in VANET. In the proposed work, developed a routing protocol is a dynamic routing protocol (DSR) and G–BFOA algorithms. The enhancement is done such as throughput and packet delivery ratio rate is increased and reduced the delay in the VANET.

Keywords- Vehicular Ad-hoc network, DSR (Dynamic Source Routing protocol), G-BFOA (genetic-Bacterial Foraging Optimization) method and PHY-MAC layer.

I. INTRODUCTION

Generally, the ad hoc network is the wireless network which simply transmits the data from source node to destination through wireless links. MANET (Mobile Ad Hoc Networks) is the category of ad hoc network which is composed of mobile nodes. VANET stands for vehicular ad hoc networks [1]. It is relied on the principals of MANET.

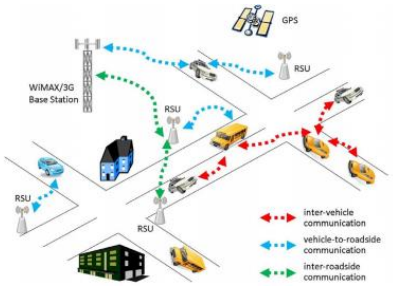


Fig.1: Vehicular Ad-hoc network

In figure 1. RSU utilized as the road side units that collect the information and processed for sending it to the destination. Communication Modes in the vehicular ad hoc networks are takes place into two ways as V2V (vehicle to vehicle) and V2I (vehicle to infrastructure/ RSU). The third communication mode is the hybrid mode [3] [4]. In V2V, the moving vehicles or the sensor nodes are directly linked to each other through wireless signals and begin to send and receive the data packets. In V2I, the moving vehicles are sending data to the road side units for the further processing. At last, the hybrid communication mode is the combination of both vehicle to vehicle and vehicle to infrastructure mode [5].

Security plays an essential role in vehicular ad hoc network. The rate of cybercrime has been increased gradually due to maximum usage of the internet. Though, information is transferred from one vehicle to other some of the threats take place due to weaker network. Hence, intruders gather the essential data and misuse it for some purpose [6]. Therefore, security of the network becomes an essential at time of planning vehicular ad hoc network. Routing protocol directs the path in which communication occurs among different objects to interchange the required data in required amount of the time period. The protocols are designed with need to increase the throughput and decrease the loss of packet and data delay. The routing protocols are dependent on the structure of the vehicular network. These protocols utilize the connection data which presents in the network for the transmission of the data packet from sender to receiver.This is categorized as;

- Re-active
- Pro-Active and [7]
- Hybrid protocol.

Table 1: Different Types of Routing Protocols [8,9]

Protocol	Merits	Demerits
Topology-based routing protocol	Appropriate for different communication	Maximum overhead
Position -based routing protocol	Support high dynamic topology	Deadlock at server.
Geocast-based routing protocol	Reliable and Maximum packet delivery ratio	Node at outer are not altered.
Cluster-based routing protocol	Maximum packet delivery ratio	Overhead at cluster

Dynamic source routing protocol is source routing protocol in which the source determine series of the intermediate hop in data packet of the routing table[10]. In this protocol, the header is copied in query packet of the middle hop that is transferred. After that, the receiver retrieves the route from query and utilizes to reply the receiver hop. In case, receiver hop forwards multiple paths, the source hop will get the data and store multiple paths from the receiver hop. The other hops use the similar connection in the present path [11]. Dynamic Source Routing is reactive protocol that depends on source route method. This protocol is mainly reliant on the link state convention in which sender initiates the route request on demand basis. Generally, source node recognizes the path from sender to receiver that contains location of the central node to path. Dynamic source routing is established for multiple node system. Dynamic source routing based on two approaches which are:i) Path Discovery and (ii) maintenance of path. In this method, sender will forward path demand information (PREQ). Every node gets path demand and that again forwarded to neighboring node. If the destination node or receiver gets the route demand that will response back to sender as route reply message (PREP). Source node will get the shortest route and forward data packets towards the specific route. Path Maintenance is accountable for failure of connections. In case middle hop determines path breakages that will forwards and error fault data to source node. This protocol is based on two methods that permit the Route searching and Route management of the source route.

- Route searching
- Route management

In this section, described about the proposed method is combination of the two methods such as Genetic and Bacteria Foraging Optimization Method. Genetic algorithm is searching heuristic approach used in the field of the artificial intelligence. It is related to the group of the evolutionary approach and it started with the resolution that is encoded into population. And then, fitness function is used for evaluation of the fitness value of every individual and then novel generation is established by the method of selection, crossover and mutation. Then, after the removal of the genetic algorithm is an optimal output is received. If termination does not occur then it will continue with novel population [13].

It is an evolutionary algorithm which computes the cost function after every selective stage of the software design as software execution process and results in best fitness value. The parameters recognize the location of the bacteria. The parameters are given in the desirable range and every group of the separate function recognizes value in space coordinate. After that, one bacterium is located at every point value. Then, in every stage bacteria is situated at every point. At every function the stage of the bacterium moved to novel coordinated function and motion of bacterium is selected by decreased way of cost function. In addition, the bacterium is positioned with highest fitness value [12].

.

II. PRIOR WORK

Kaur, R., Singh, T. P. and Khajuria, V et al.,2018[14] proposed a research on detection of different attacks likes as denial of service, replay attacks through security methods which are cryptographic, hash function and digital signatures. The research determines the transmission region and different facts of vehicular ad hoc network. The detailed of the attacks described in this research are Sybil attack, DOS attack, DDOS attack and timing attack. The various types of attackers and entities are also explained in this research.**Krundyshev, V., Kalinin, M and Zegzhda, P et al., 2018[15]** discussed about data security issues in transmission network in vehicular ad hoc networks. In this research, analyzed the techniques of prevention from routing threats on dynamic system where the attacked node route forward data through the shortest path from source to destination and removal of traffic load from the system. They also proposed a security for vehicular ad hoc networks and other kind of transmission related system utilizing swarm intelligence approach. In an experimental analysis described the swarm intelligence for protection and detection of routing attack. **Shahid, M. A., Jaekel, A., Ezeife, C., Al-Ajmi, Q and Saini, I. et al.,2018 [16]** proposed a research availability, authentication and integrity in vehicular ad hoc networks and comparing kinds of the attacks. Generally, privacy is the main concern for the security concept of the vehicular ad hoc network. In addition, they proposed an identical secure scheme for solving the issue of the unidentified attacks on the system.**Waraich, P. S and Batra, N.et al., 2017[17]** recognized the protection of the DOS attack over the vehicular ad hoc network utilizing quick reply table. In this research, a technique of private routing was established that recognizes and removes the determined security threats. In a DDoS attack, an attacker interrupts the channel and required determined resources. In case, a data loss in any rate, the drop count may get increased automatically and then threshold value was required. In case of route maintenance, a quick reply table was used.**Malathi, A. and Sreenath, N. et al.,2017[18]** focused a research on the detection and

prevention of black hole attack. The minimum probable path to the receiver was searching through a request from sender node (PREQ) to the neighbor node. The middle node transfers the route request to nearest node to search the path from sender to receiver. If the middle node was malicious then the fake route reply was broadcast to sender. The sender will transfer data packets to malicious node that may not transfer to desired destination node and at similar that dispersed through negligence to another route request.

III. RESEARCH METHODOLOGY

In this section, described that the research methodology.(i) To analyze the various previously implemented Vehicular ad hoc network techniques like AODV, DSR and other routing protocols. (ii) To develop a complex algorithm using the Roadside unit, DSR routing protocol and Black Hole Attack together to enhance the current mechanism. (iii) To implement the G-BFOA for Optimization for find best outfit with the help of fitness function.

(iv)Compare the proposed algorithm (DSR and G_BFOA) with the existing algorithm (AODV, OLSR and DSR) on parameters: Delay, Delivery and Network Load.

Description in proposed work:-

1. Developed a vehicular ad hoc network.
2. Area = Network _length *Network_width.
3. Plotting Vehicle Nodes.
4. Assign RSU (Road Side Unit)
5. Searching Continue
   Source and
   Destination
6. Coverage Set
   Coverage Range
   Coverge Area
   Distance for transmission
7. Implement DSR routing protocol
8. Route Discovery
9. Route Maintenance and
10. Chache Memory
11. Unwanted Nodes (BHA)
12. Network Load Increased
13. Time complexity occurs
14. Implement a genetic-BFOA method
15. Set of population
16. Swin and Tumble
17. Elimination and Dispersal
18. Reproduction with Best solution (Fitness Function)
19. Fit Value
20. Performance Metrics
21. Comparison
22. Stop.

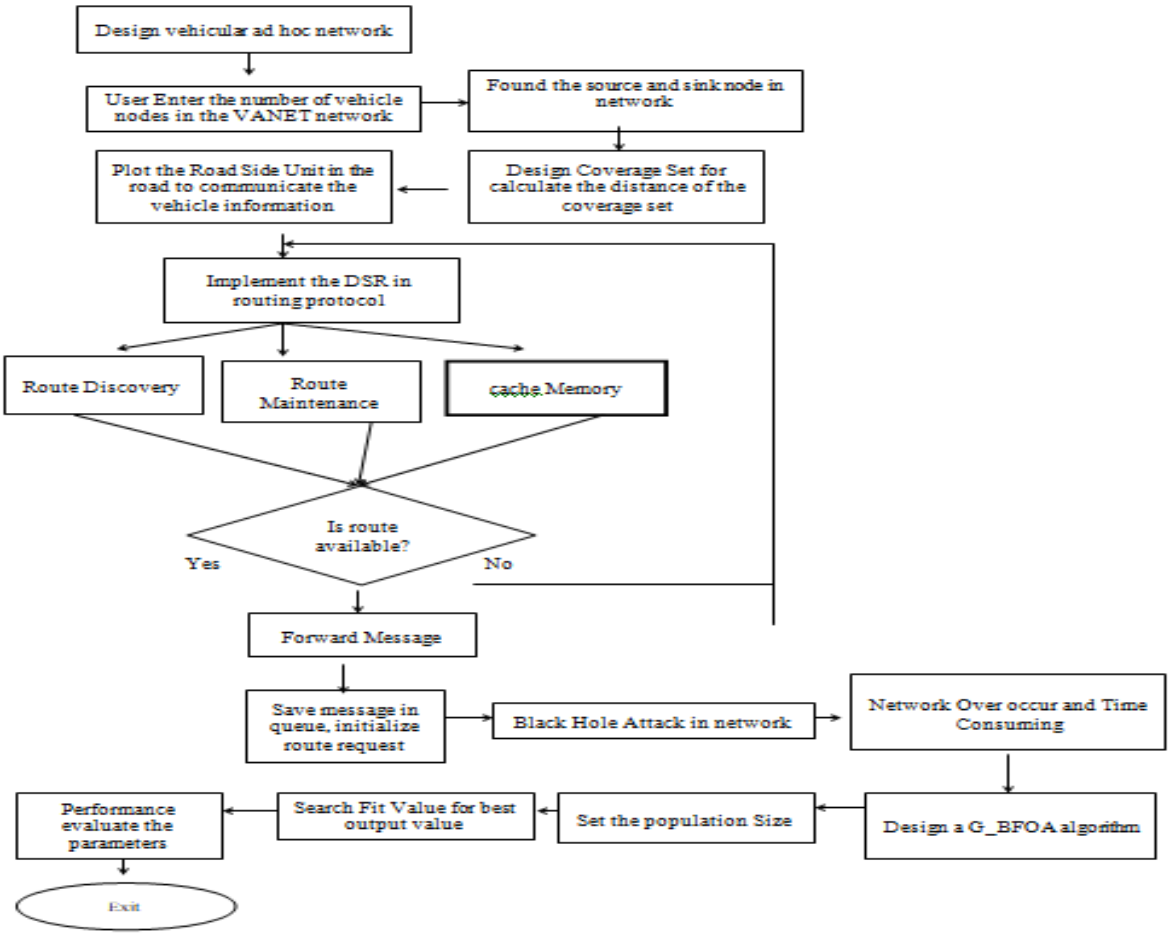


Fig.2: Research Proposal Work

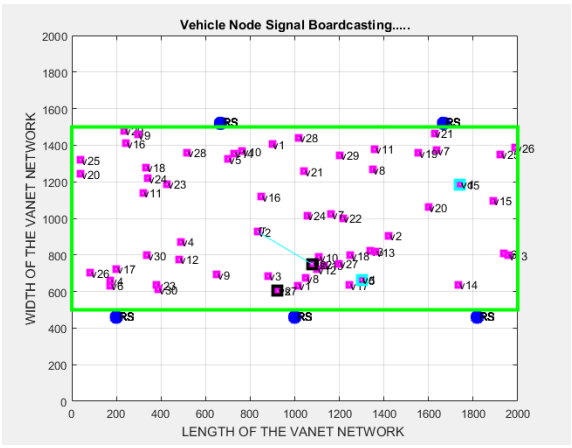
IV. EXPERIMENTAL RESULTS

In this section, it offers the detail description of the network simulation results considered for this research study.

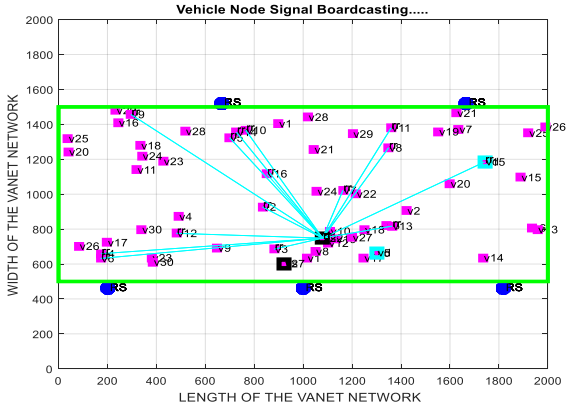
Table 1:- Research Performance Parameters in VANETs

PARAMETERS	VALUES
Area	2000*2000 meters
Number of Vehicles	20,30,40,50….100
Source Vehicle node	5
Destination Vehicle node	8
Coverage Set Area	30*30 vehicle nodes
Cover Set	250 meters
Data Packet Size	1000 bytes
RSU	5
Transmission Limit	500
Language	Matlab Tool and Scripting Languages

Command window, user display the data in the command window and Enter the number or vehicle nodes and calculate the area i.e. length and width. RSU (road side unit) is plotted in the x-axis and y-axis plane. It used the wait base i.e called processed bar to load enter the number of vehicular nodes. Deploy the number of vehicle nodes in the network. (i) Search the source vehicle node in the network and (ii) search the destination vehicle node in the network. Both vehicle nodes are randomly searched in the VANET. A coverage set depends on the distance calculation in the Vehicular Ad-Hoc Network. It has own start node, destination node and evaluate the distance and verification based on the vehicle id. In coverage set design, to evaluate the distance and range of the coverage area.



(i)



(ii)

Fig.3: (i) Start Communication and (ii) Vehicle node Signal Broadcasting

Above figure 4 (i) and (ii) shows the signal broadcasting in the Vehicular ad-hoc network. Signal Broadcasting means to transfer the request source node to another node and checking that node is it active or not. If it is active mode then received or signal then forward information to the next node till destination node. In destination node sent the ACK signal to the src node to all information received from the intermediate node.

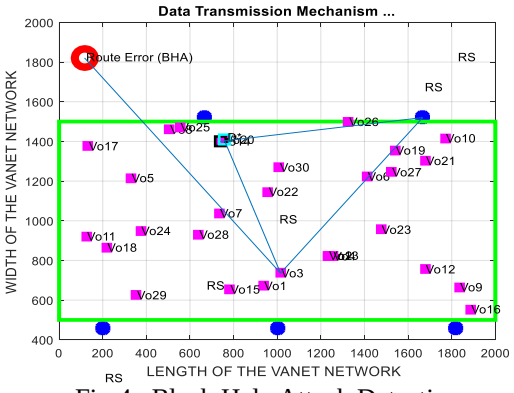


Fig.4: Black Hole Attack Detection

Above figure 4.shows the black hole attack detection process with routing protocol (Dynamic Routing Protocol). In this protocol method are two types such as (i) Route searching and (ii) Route Maintained. In this phase route searching for information transmission one node to another or source to destination node. In route finding faces some issues in the data transmission then load increases, high delay occur and number of request increases and then loss the data packets. In this protocol detect the overload route, time figure out and attack found in the vehicular ad-hoc network.

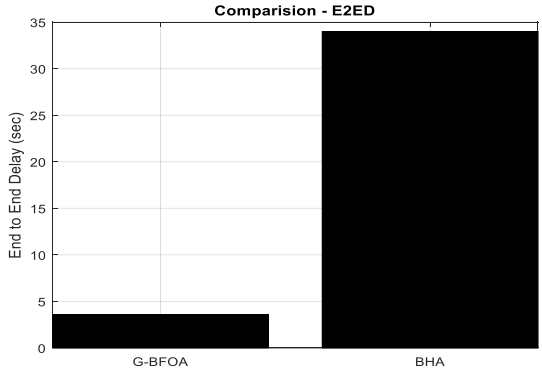


Fig.5: Comparison – End to End Delay

The above figure 5 defines the comparison between proposed and existing methods with end to end delay. In proposed method end to end delay value is reduces as compared to existing method.

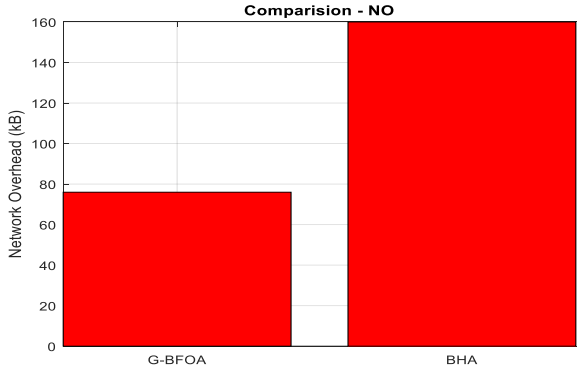


Fig.6: Comparison – Network Overhead

The above figure 6 defines the comparison between proposed and existing methods with network overload . In proposed method network overload value is reduces as compared to existing method.

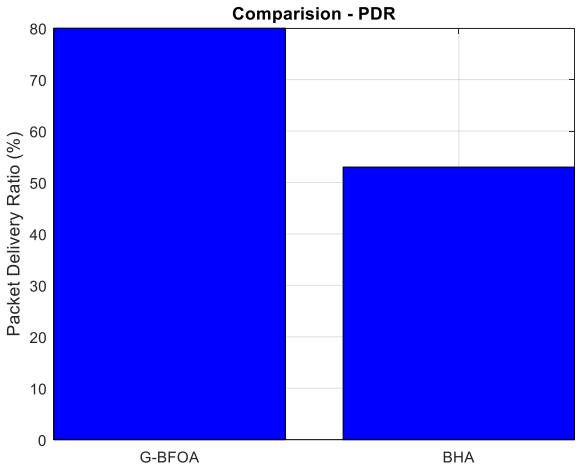


Fig.7: Comparison – Packet Delivery Rate

The above figure 7 defines the comparison between proposed and existing methods with Packet Delivery Rate. In proposed method packet delivery rate value is increases as compared to existing method.

Table 1. Performance Metrics

Parameters	**Packet Delivery Rate**	**End to End Delay**	**Network Overload**
Values	80%	3.55 second	76 kB

Table 1 shows the performance metrics with proposed method using Genetic-Bacterial Foraging optimization method. In Packet Delivery Rate value is 80 % achieved, end to end delay value is achieved 3.55 second and Network overload value is achieved 76Kb.

Table 2. Comparison between Proposed and existing methods

Parameters	**Gene-BFOA method**	**DSR and BHA**
Packet Delivery rate	80%	53%
End to End Delay	3.55 sec	33 sec

Network Overload	76 kB	160 kB

Table 2 shows the comparison analysis with proposed and existing method with PDR, NO and E2D parameters. In Packet Delivery Rate value is 80% improved as compared with 53% , End to End Delay value is 3.55 sec and existing E2D value is 33 sec and Network Overload value is 76 kB value is achieved as compared to existing method and parameters.

V. CONCLUSION AND FUTUREV SCOPE

VANET concluded and self-configuring vehicle network formed simultaneously, that gives direct data communication between vehicles to inter-change data in real time. In BHA (Black Hole Attack), where an attacker node eliminates data packers from the network, are easy to evaluate and vehicle networks are very vulnerable to them, the mainly due to the characteristics of these data communication. However, the network impact of the BHA attack may vary depending on the routing method and the Model used based on mobility. Various researches has been completed to Vehicular ad-hoc networks, but no prior about the influence of BHAs on routing protocols in real time scenarios can be searched. The real time used mobility model modifies the simulation consequences considerably, since it has searched notable difference in the consequences among the surveyed carried out with the mobility model such as random deployment and route searching with mobility model in VANET using URBAN AREAS. In this reason, it considers that the real time scenarios should be used for Vehicular ad hoc network simulations. In existing research work, they have studied the impact of BHAs on 4 routing method such as DSR, DSDV, AODV and OLSR routing protocol in URBAN areas in regards or three performance metrics such as PDR, E2D and NO (network overload). The result analysis with BHA and DSR routing protocol suffers from main impact of attacks. In PDR (packet delivery rate) , it losses the data packets as compared to the routing methods. Attacker nodes come into the network and loss the data packets and increase the network overload and end to end delay. In research method has implemented using gene-BFOA method to find the attack node and mitigate the effect with the help of fitness function. In proposed methods has improved the delivery rate as compared to existing routing methods and reduce the effect of the end to end delay and network overload.

In this section, it can present some of the further lines to continue the research in these research methods. It can implement over URBAN areas mobility structure. In further work can implement an encryption and cryptography methods to improve the security factors and performance metrics such as throughput and packet loss. It research method to avoid and mitigate the attacks effects that can be execute over these 4 routing methods can also be predicted.

VI. REFERENCES

[1]. Tonguz, O., Wisitpongphan, N., Bait, F., Mudaliget, P and Sadekart, V. (2007), " *Broadcasting in VANET*,In *2007 mobile networking for vehicular environments* , vol.2(3),pp. 7-12. IEEE.

[2]. Karnadi, F. K., Mo, Z. H., and Lan, K. C. (2007), " *Rapid generation of realistic mobility models for VANET"* , In *2007 IEEE wireless communications and networking conference* ,vol2(1),pp. 2506-2511, IEEE.

[3]. Grassi, G., Pesavento, D., Pau, G., Vuyyuru, R., Wakikawa, R. and Zhang, L. (2014), April), " *VANET via named data networking*" , In *2014 IEEE conference on computer communications workshops (INFOCOM WKSHPS)* , vol 3(2), pp. 410-415,IEEE.

[4]. Nzouonta, J., Rajgure, N., Wang, G. and Borcea, C. (2009) , " *VANET routing on city roads using real-time vehicular traffic information*" , *IEEE Transactions on Vehicular technology*, vol. *58*(7), pp 3609-3626.

[5]. Fazio, P., De Rango, F. and Sottile, C. (2011), " *A new interference aware on demand routing protocol for vehicular networks*" , In *2011 International Symposium on Performance Evaluation of Computer & Telecommunication Systems* , vol. 2(1), pp. 98-103, IEEE.

[6]. Engoulou, R. G., Bellaïche, M., Pierre, S and Quintero, A. (2014), " *VANET security surveys*" ,*Computer Communications*, vol 3(2),pp. *44*, 1-13.

[7]. Mejri, M. N., Ben-Othman, J. and Hamdi, M. (2014)., "*Survey on VANET security challenges and possible cryptographic solutions*" , *Vehicular Communications*, vol*1*(2),pp. 53-66.

[8]. Chen, L., Tang, H. and Wang, J. (2013), " *Analysis of VANET security based on routing protocol information" ,* In *2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP)* ,vol 2(1), pp. 134-138, IEEE.

[9]. Singh, A., Kumar, M., Rishi, R and Madan, D. K. (2011), " *A relative study of MANET and VANET: Its applications, broadcasting approaches and challenging issues"* ,In *International Conference on Computer Science and Information Technology* ,vol3(1), pp. 627-632, Springer, Berlin, Heidelberg.

[10]. Kumar, V., Mishra, S. and Chand, N. (2013), "*Applications of VANETs: present & future*" , *Communications and Network*, vol. 5(01), pp.12.

[11]. Liang, W., Li, Z., Zhang, H., Wang, S and Bie, R. (2015), " *Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends*" , *International Journal of Distributed Sensor Networks*, vol*11*(8), pp. 745303.

[12]. Yousefi, S., Mousavi, M. S. and Fathy, M. (2006), " *Vehicular ad hoc networks (VANETs): challenges and perspectives*", In *2006 6th International Conference on ITS Telecommunications* ,vol 2(1),pp. 761-766). IEEE.

[13]. Bengag, A and El Boukhari, M. (2018), " *Classification and comparison of routing protocols in VANETs*" , In *2018 International Conference on Intelligent Systems and Computer Vision (ISCV)* , vol 3(2), pp. 1-8, IEEE.

[14]. Kaur, R., Singh, T. P and Khajuria, V. (2018), " *Security issues in vehicular ad-hoc network (VANET)*" , In *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)* ,vol 2(2), pp. 884-889,IEEE.

[15]. Krundyshev, V., Kalinin, M and Zegzhda, P. (2018), " *Artificial swarm algorithm for VANET protection against routing attacks*"

, In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)* , vol 2(2),,pp. 795-800, IEEE.

[16]. Shahid, M. A., Jaekel, A., Ezeife, C., Al-Ajmi, Q and Saini, I. (2018), " *Review of potential security attacks in VANET" ,* In *2018 Majan International Conference (MIC)* , vol 2(3),pp. 1-4, IEEE.

[17]. Waraich, P. S. and Batra, N. (2017), " *Prevention of denial of service attack over vehicle ad hoc networks using quick response table*" ,In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC,* vol 2(1) , pp. 586-591, IEEE.

[18]. Malathi, A. and Sreenath, N. (2017), " *Black Hole Attack Prevention and Detection in VANET using Modified DSR Protocol*." ,*International Journal of Computer Applications,* vol. *168*(7).