

# Machine learning algorithms for privacy preserving in vehicular ad hoc network

Shazia Sulthana, Byppanahalli Narayana Reddy Manjunatha Reddy

Department of Electronics and Communication, Global Academy of Technology, Visvesvaraya Technological University, Belagavi, India

## Article Info

### Article history:

Received Jul 2, 2022

Revised Nov 7, 2022

Accepted Nov 18, 2022

### Keywords:

Black widow optimization

Deep neural network

Privacy

Trusted authority

Vehicular ad hoc networks

## ABSTRACT

Machine learning (ML) will improve the outcomes through the use of methods that categorize the information into the predetermined set. This work is to present an estimation and assessment of machine learning techniques for achieving privacy preservation in vehicular ad hoc networks (VANETs). This method generates two distinct group keys for prime and secondary users. Road side units (RSUs) are deployed to broadcast one group key from the trusted authority (TA) to the primary users, and secondary users are utilized to transmit the other group key. The main aim of this network is developed to avoid vulnerable attacks and to enhance the privacy of this network, Naïve Bayesian classifier (BC), support vector machine (SVM), K-nearest neighbor (KNN), artificial neural networks (ANN), Bayesian network (BN) methods are utilized in correlation with the proposed deep neural networks (DNN) with the black widow optimization (BWO) for protection preserving. These learning characterization procedures are assessed concerning delay, network lifetime, throughput, delivery ratio, and drop and this proposed calculation (DNN-BWO) shows improved results than the current methodologies.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Shazia Sulthana

Department of Electronics and Communication, Global Academy of Technology

Visvesvaraya Technological University

Belagavi, Karnataka, India

Email: shaziasulthana14@gmail.com

## 1. INTRODUCTION

Vehicular ad hoc networks (VANET) plays a major key role in intelligent transportation systems (ITS), as information is generated and exchanged wirelessly through vehicles and other devices. There are various communication occurs from one unit to another unit. The VANET architecture is shown in Figure 1. In vehicle communications that receive internal system data or vehicle operation, one determines factors such as driver fatigue, and drowsiness. Determination of those factors as well as their quality is critical to public safety and driver safety. As technological development is changing, the world experiencing today is touching in most areas, particularly in the field of communication. Since open-space technology has advanced, the issues with traffic congestion and accidents on the roads have been only partially resolved. Researchers started working with this technology that communicates vehicle to vehicle to develop direct or indirect links between them and to be dedicated to anticipated critical problems such as forthcoming incidents or traffic congestion in order to alleviate privacy issues. Deep neural networks which is a machine learning technique have become an essential tool for an extensive range of applications such as the classification of images, pattern recognition, or user language conversion. These techniques have molded extremely high accuracy of prediction in comparison with human performance. Techniques for interpreting and perceptive of the model have become a key ingredient of a strong corroboration method. Safety, infotainment, and multimedia data are tiled in an open-

access environment through the VANET. Serious traffic accidents could result from a malicious vehicle interfering with a network or from data transmission errors. To provide the privacy of data transmission in an open environment, the authentication of vehicles is primary in VANET. The objective of the work:

- In this work, a message authentication method is recommended for use in verifying the validity of the authenticated vehicle.
- In our proposed method, learning of the network is by the use of a deep neural network for intrusion detection and weight optimization are achieved with the black widow optimization (BWO) algorithm.
- The success of the proposed work is assessed by parameters like message delay, delivery ratio, throughput, network lifetime, and message, drop.

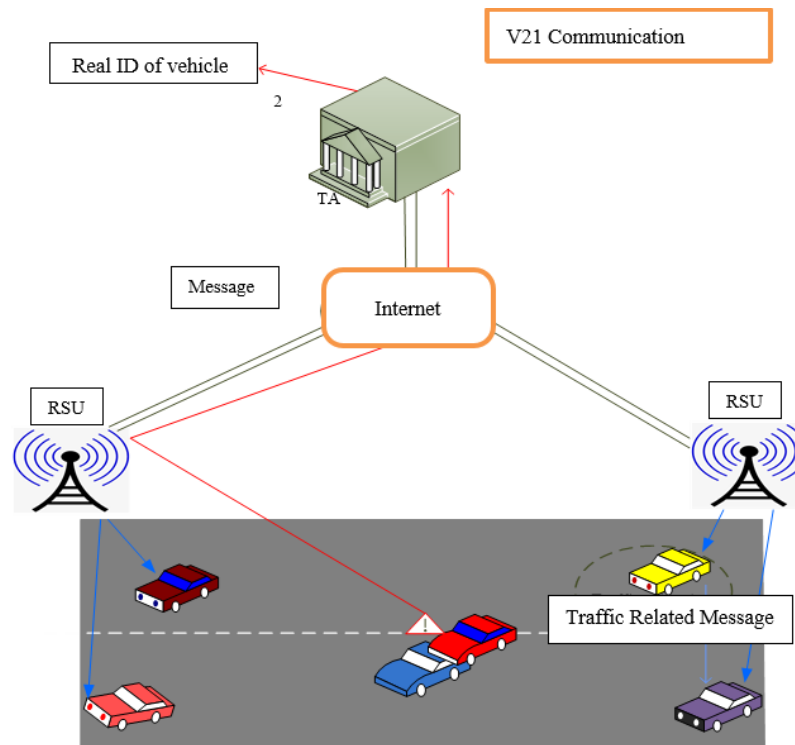


Figure 1. VANET architecture

Wang *et al.* [1] have introduced a scheme that is used for the diffusion of emergency communication in urban areas. Dropping the delay in transferring the trauma communication and reducing communication idleness, this technique has updated forwarding and selection method, which uses recurring segregation, small slots, and bursts to select the isolated neighbor nodes, through asynchronous transmission, efficiently selects a single loop by avoiding the traffic overload between them. Then two-way transmission, much directional broadcasting was designed in terms of the location of transmitters for emergency communication. Through bidirectional or multidirectional broadcasting selects the forwarding node at different directions simultaneously and an efficient forwarding node is selected at each path.

Tian *et al.* [2] have presented an improved location-based protocol for spreading communication between wide vehicular networks. Primarily to identify by using a standard protocol, communication data is transmitted within the coverage area, and sending the message again in terms of the payload included on the message that was arrived. Wu *et al.* [3] have introduced diffusion rules depending on the multiplexed path and invalid information Moving nodes by the use of multi-channel may be able to broadcast and discover information on the diverse path at a similar interval depending on the information from multi-channel. Compared to previous black burst-based techniques, black type burst and multi-hopping diffusion shorten the recurring process for finding the best possible segment. Reinforcement nodes may be chosen quickly to get the finest collision segment, single direction, and many direction broadcasting for instant intersection respectively.

Lyu *et al.* [4] have introduced a capable broadcasting authentication method for securing against computational-depend denial of service (DoS), rather than resisting packet drop through the dynamic nature of

vehicles. This was an advanced and lightweight technique, as trusted mainly on the symmetric algorithm. Furthermore, port block allocation (PBA) saves compressed and re-encrypted message authentication codes (MAC) of signatures without jeopardising security in order to counter DoS attacks based on blocking memory. Rajput *et al.* [5] have introduced an authentication technique that preserves the privacy of nodes in the network. Its combined technique found pseudonym and clustering based on signature gains the advantage over other techniques. This method gives the light weight mechanism by avoiding certified revocation and controlling of the cluster. This scheme uses well-organized authentication with light weight pseudonym conditional anonymity.

Saeed *et al.* [6] have introduced one and many-lane models as a road segment for utilizing the efficient probabilistic flooding method of VANET. The planned systematic structure offers a novel tool covering all counting lanes, ranging in transmitting vehicle as well as strength. This model was evaluated simulation that practically signifies complete congestion and traffic and system features were engaged as standard for intending two propagation approaches using probabilistic floods. This process was analyzed by modeling and establishes to conquer significant operations matched with blind flood relating to attained accessibility, delay from one point to another, and a number of retransmissions, similar to performing optimal flooding and getting through brute force. Krishnamoorthy *et al.* [7] suggested a competent scheme in which the algorithm was utilized to solve the traffic overloading based on the matrix-based routing to obtain optimum results and improved packet delivery ratio along with reduced overhead. This method significantly improved the accurateness the s to attain the traffic pattern on a network as recommended through the experiment.

Vadivel and Bhaskaran [8] proposed an amendable, reliable protocol for networks. The short-distance routing existed to be efficient communication between the several paths. The link capacity is identified as the congestion mechanism, not by the node. Other than the scheme was to some extent not easy the proving the system’s performance when compared to the proposed methods. Kumar *et al.* [9] introduce an adaptable routing protocol for balancing entities in a network to reduce the delay, overhead in routing path, traffic overload, and superior network life. Each mobility in the system considers the latest congestion and conserved predictable records in the transmit table called the vicinity table. This network shows better performance in terms of efficiency, delay, packet drop, jitter, and packet delivery ratio and normalizes overhead onto the network. This algorithm shows better performance compared to the existing techniques, although this algorithm was incompetent to avoid the jamming of the network.

Gowtami and Subramaniam [10] offered a cross-section layer model in the system. The uniqueness of this work was localization in packet recoverable, no randomness, capability to swap efficiency and peer-to-peer improvement. This scheme is reliable; any loss or corruption of packets could be performed through the retransmission of duplicate packets. Alhosainy and Kunz [11] proposed an optimum routing with the congestion avoidance protocol for VANET. A split factor was used by the system to find the linear mechanism for each session with the multipath toward the optimization framework. The new inconsistent, appropriate conversion with the usage of ohm’s law leads to an arched and uncoupled optimization framework so as to create the finest resolution in a scattered outline.

## 2. METHOD

Over the past two decades, wireless networks changed the lifestyle and permitted for exchange of information. It contains dual kinds of ad hoc networks in transportable conversations, known as mobile ad hoc networks (MANET) and vehicular ad hoc networks (VANET). Among these, VANET is an increased advantage because of its dynamicity and high mobility. Communications exist from vehicle to vehicle and the disaster communion is transferred by using cautionary messages [12]. The concealment of these vehicles is optimally fixed by means of the black widow optimization algorithm. The goal of this method is to communicate the information without delay, with more throughput in less and high-density traffic.

### 2.1. Method of implementation

This method mimics the spider’s different movement for counter ship mating which starts with an initial spider population shown in (1):

$$R_{N,d} = \begin{bmatrix} r_{1,1} & r_{1,2} & r_{1,3} \cdots & \cdots & r_{1,d} \\ r_{2,1} & r_{2,2} & r_{2,3} \cdots & \cdots & r_{2,d} \\ r_{N,1} & r_{N,2} & r_{N,3} \cdots & \cdots & r_{N,d} \end{bmatrix} \tag{1}$$

$$lb \leq X_i \leq ub$$

where, the spider population is represented as  $R_{N,d}$  in BWO, the decision variable numeral is represented by  $d$ , the total number population is denoted by  $N$ , the lower band of this population is denoted as  $lb$  and the upper band of the population is denoted by  $ub$  [13]-[15].

The  $R_{N,d}$  is used for the objective function represented in (2);

$$\text{objective function} = R_{N,d} \quad (2)$$

the flow chart of the BWO algorithm is explained in Figure 2.

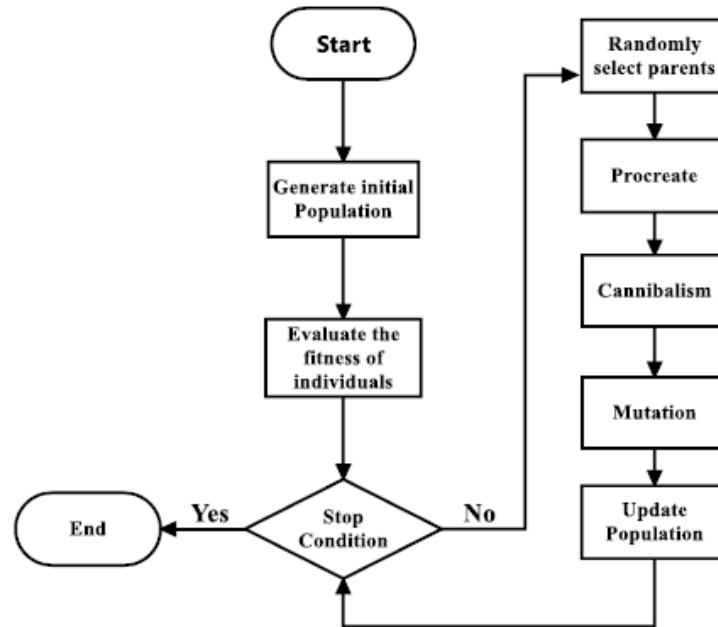


Figure 2. Flowchart for the BWO algorithm

a. Procreate

The spider pair doesn't rely on one another, thus it begins to reproduce independently of other spiders for new inventions connected to this pair. After mating, there are 1000 offspring, but only the strongest ones will survive. The following equation, in which  $x_1$ ,  $x_2$  stand in for the parents, is used to create offspring after reproducing using a group of random numbers known as the widow array.

Where  $y_1$  and  $y_2$  are the young spiders from reproduction and  $\mu$  is the random number between 0 and 1 which is expressed in (3) and (4).

$$y_1 = \mu \times x_1 + (1 - \mu) \times x_2 \quad (3)$$

$$y_2 = \mu \times x_2 + (1 - \mu) \times x_1 \quad (4)$$

b. Cannibalism

In this phase, the optimal fitness value is used to separate males and females, and the cannibalism rate is calculated based on the number of survivors. In the third type of cannibalism, the strong young spider in the quantity of phase eats their mother [16]. The optimal fitness value is used to determine whether spiders are strong or weak.

c. Mutation

The procedure of mutations begins by randomly selecting a number of solutions (widows) from the pop1 population which will be mutated individually. Two cells from each selected solution (widow) are randomly exchanged, and the new mutation solutions will be kept in pop3. The population is created by selecting mute pop numbers at random, and each of the chosen solutions randomly swaps out any two elements from an array. The multi-pop is computed using the mutation rate [17].

d. Convergence

Three components make up the first algorithms: i) iterations that have already been predetermined and characterized [18], ii) observing that the best widow's fitness value has remained constant after several iterations, and iii) attaining the exact precision point.

**2.2. Proposed algorithm: deep neural networks with the BWO**

The main goal of this algorithm is to prevent vulnerable attacks and to improve the privacy of this network. Naïve Bayesian classifier (BC), support vector machine (SVM), K-nearest neighbor (KNN), artificial neural networks (ANN), and Bayesian networks (BN) are used to compare with the proposed deep neural networks (DNN) with the black widow optimization (BWO) for privacy-preserving. The proposed algorithm is shown in Figure 3.

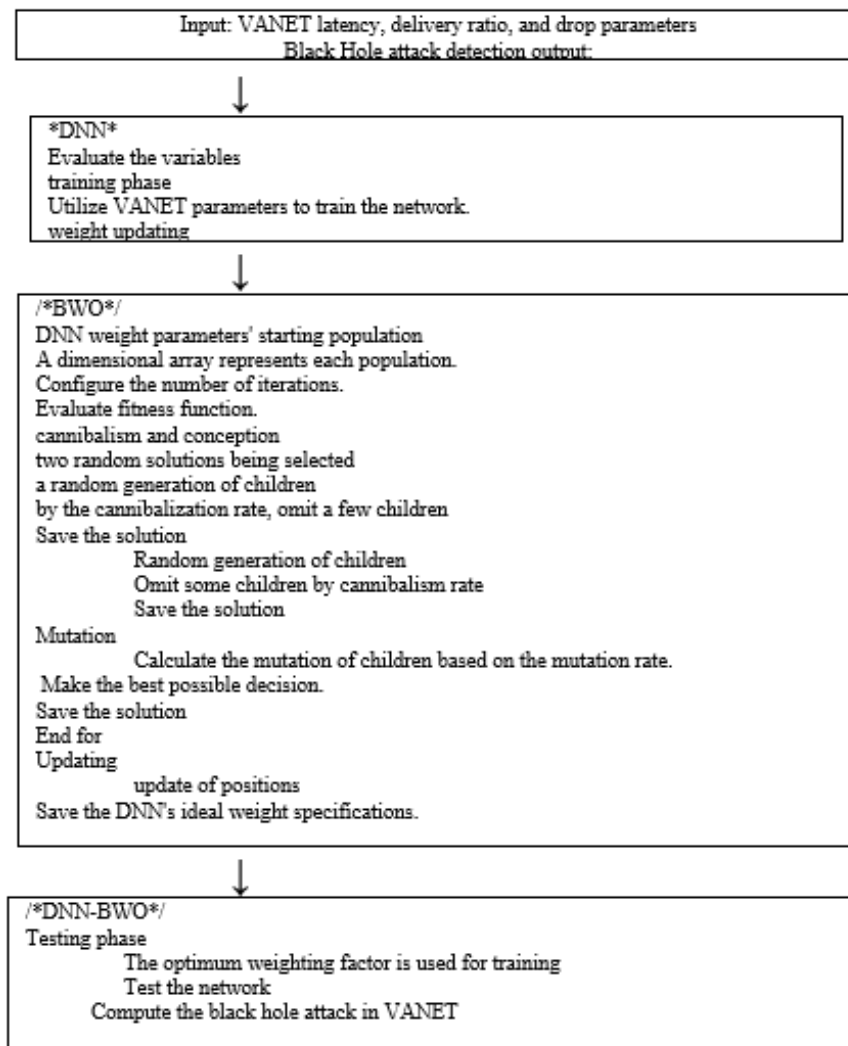


Figure 3. Proposed algorithm

**3. RESULTS AND DISCUSSION**

The proposed DNN-BWO technique's performance validation is examined in this part. Below is a description of the network parameters:

- a. Delay: the latency of a bit to move from starting point to the ending point across the communication network.
- b. Drop: the loss of packet bits arriving at their destination. The drop may due to congestion, noisy channel
- c. Delivery ratio: the delay ratio between the actual and desired response.

- d. Overhead: data packet which is being encapsulated will contain additional information for reliable communication called overhead [18], [19].
- e. Throughput: measurement based on how many successful bits arrived at the destination out of transmitted bits depending on the networks [20], [21]. The simulation setup is explained in Table 1.

To guarantee VANET security and prevent network problems, intrusion detection systems are utilized in VANET (e.g., latency). In order to secure a multi-cluster head anomaly, the SVM technique uses an optimized IDS. KNN proposes an IDS model against spoofing attacks in connected electric vehicles. For the purpose of discovering unidentified intrusions on VANET, Naïve Bayes propose a distributed IDS [22], [23]. Table 2 shows the performance of networks in terms of drop, network lifetime and throughput.

Table 1. Simulation setup

S. No	Parameters	Values
1	Simulator	NS-2
2	Network area	2824*2000
3	Propagation	Two-ray
4	Packet size	500
5	Routing protocol	AODMV
6	Simulation time	100s

Table 2. Shows the performance parameters with drop, delivery ratio and throughput

Number of attack	Drop (in Packets)				
	ANN	KNN	Naïve Bayes	SVM	Proposed
1	50	60	64	54	47
2	49	55	58	52	44
3	45	52	56	48	42
4	42	48	51	43	41
5	39	44	47	40	36
	Delivery Ratio (%)				
1	0.855308	0.742157	0.7042157	0.8042157	0.883298
2	0.872611	0.796864	0.726864	0.826864	0.89688
3	0.88961	0.824161	0.784161	0.854161	0.901602
4	0.896922	0.842294	0.802294	0.872294	0.907729
5	0.904625	0.8768578	0.8568578	0.8968578	0.929818
	Throughput (in Packets)				
1	11054	11038	11030	11044	11056
2	11040	11032	11027	11034	11044
3	11028	11017	11010	11020	11038
4	11010	11005	11000	11008	11017
5	10989	10974	10960	10980	11004

The proposed method is evaluated in comparison to the presently used techniques (ANN, KNN, Naïve Bayes, and SVM). Figures 4 and 5 illustrate the performance characteristics of delay and network lifetime, while Table 2 displays drop, delivery ratio, and throughput, respectively. The performance characteristics with the number of attacks (1 to 5) in the existing approaches and the proposed algorithm are compared in Figures 3 and 4 and Table 2. According to the analysis, the suggested outcomes are superior to the existing methods [24], [25].

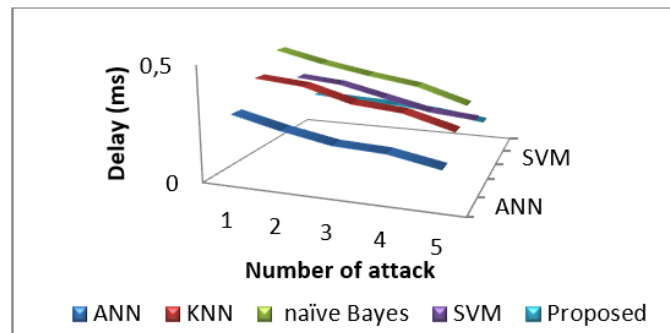


Figure 4. Delay analysis comparing proposed and existing techniques under the blackhole attack

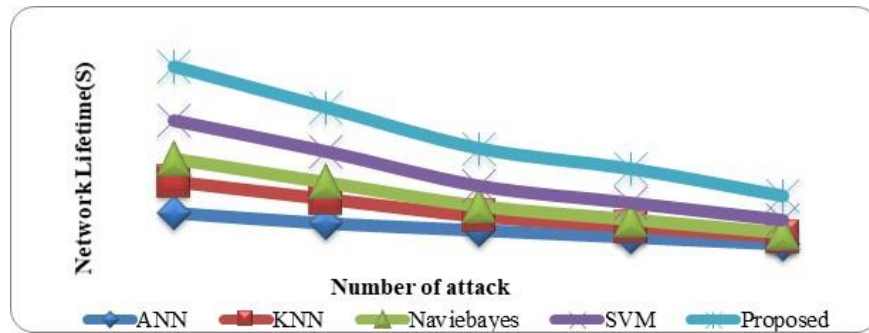


Figure 5. Network lifetime analysis in comparison between proposed and existing method under blackhole attack

#### 4. CONCLUSION

This work is provided on intrusion detection from various attacks by the BWO-DNN technique which gives privacy to data and finds attacks during communication in the VANET environment. For both network intrusion and optimization techniques, the proposed DNN with BWO performs well in mass simulation. The proper training in the DNN system gives secure communication between the trusted authority (TA) and unauthorized users. The attacks labeled using supervised learning for the accurate output separately such as attack and normal output are provided individually so that the TA can easily identify the attacks and produce alerts to the drivers. Thus the security of the DNN-BWO-based technique enhances the security of the VANET system. Then the proposed system has better results as compared with the existing machine learning (ML) techniques such as SVM, ANN, Naïve BC, BN, and KNN.

#### REFERENCES





- [1] Y. Wang, V. Menkovski, I. W.-H. Ho, and M. Pechenizkiy, "VANET meets deep learning: the effect of packet loss on the object detection performance," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, Jun. 2019, pp. 1-5, doi: 10.1109/VTCSpring.2019.8746657.
- [2] D. Tian *et al.*, "A distributed position-based protocol for emergency messages broadcasting in vehicular ad-hoc networks," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1218-1227, 2018, doi: 10.1109/JIOT.2018.2791627.
- [3] L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 13, no. 3, 2017. doi: 10.1177/2F1550147717700899.
- [4] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "PBA: prediction-based authentication for vehicle-to-vehicle communications," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 71-83, 2016, doi: 10.1109/TDSC.2015.2399297.
- [5] U. Rajput, F. Abbas, H. Eun, and H. Oh, "A hybrid approach for efficient privacy-preserving authentication in VANET," *IEEE Access*, vol. 5, pp. 12014-12030, 2017, doi: 10.1109/ACCESS.2017.2717999.
- [6] T. Saeed, Y. Mylonas, A. Pitsillides, V. Papadopoulou, and M. Lestas, "Modeling probabilistic flooding in VANETs for optimal rebroadcast probabilities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 556-570, 2019, doi: 10.1109/TITS.2018.2828413.
- [7] D. Krishnamoorthy *et al.*, "An effective congestion control scheme for MANET with relative traffic link matrix routing," *Arabian Journal for Science and Engineering*, vol. 45, pp. 1-11, 2020, doi: 10.1007/s13369-020-04511-9.
- [8] R. Vadivel and V. M. Bhaskaran, "Adaptive reliable and congestion control routing protocol for MANET," *Wireless Networks*, vol. 23, no. 3, pp. 819-829, 2017, doi: 10.1007/s11276-015-1137-3.
- [9] J. Kumar, A. Singh, and H. S. Bhadauria, "Congestion control load balancing adaptive routing protocols for random waypoint model in mobile ad-hoc networks," *Journal of Ambient Intelligent and Humanized Computing*, vol. 12, pp. 5479-5487, 2020, doi: 10.1007/s12652-020-02059-y.
- [10] M. S. Gowtham and K. Subramaniam, "Congestion control and packet recovery cross-layer approach in MANET," *Cluster Computing*, vol. 22, no. 5, pp. 12029-12036, 2019, doi: 10.1007/S10586-017-1548-2.
- [11] A. Alhosainy and T. Kunz, "Joint optimal congestion, multipath routing, and contention control for wireless Ad Hoc networks," *IEEE Communications Letters*, vol. 21, no. 12, pp. 2670-2673, 2017, doi: 10.1007/s12053-017-9532-5.
- [12] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Debora, "Dual authentication and key management techniques for secure data transmission in vehicular Ad Hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015-1028, 2015, doi: 10.1109/TITS.2015.2492981.
- [13] S. Kanthimathi and P. JhansiRani, "Optimal routing based load balanced congestion control using AODV in WANET environment," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 3, pp. 403-411, 2021, doi: 10.14569/IJACSA.2021.0120348.
- [14] S. Moghanian, F. B. Saravi, G. Javidi, and E. O. Sheybani, "GOAMLP: network intrusion detection with multilayer perceptron and grasshopper optimization algorithm," *IEEE Access*, vol. 8, pp. 215202-215213, 2020, doi: 10.1109/ACCESS.2020.3040740.
- [15] M. R. Devi, and I. J. S. Jeya, "Black widow optimization algorithm and similarity index based adaptive scheduled partitioning technique for reliable emergency message broadcasting in VANET," *Research square*, 2021, doi: 10.21203/rs.3.rs-309575/v1.
- [16] G. Montavona, W. Samekb, and K.-R. Müllera, "Methods for interpreting and understanding deep neural networks," *Digital Signal Processing*, vol. 73, pp. 1-15, 2018, doi: 10.1016/j.dsp.2017.10.011.







- [17] S. Sakr *et al.*, “Comparison of machine learning techniques to predict all-cause mortality using fitness data: the Henry ford exercise testing (FIT) project,” *Medical Informatics and Decision Making*, vol. 17, pp. 174-188, 2017, doi:10.1186/s12911-017-0566-6.
- [18] V. Hayyolalam and A. A. P. Kazem, “Black widow optimization algorithm: a novel meta-heuristic approach for solving engineering optimization problems,” *Engineering Applications of Artificial Intelligence*, vol. 87, 2020, doi: 10.1016/j.engappai.2019.103249.
- [19] M. Selvi and B. Ramakrishnan, “Prioritized and secured data dissemination technique in VANET based on optimal blowfish algorithm and sign crypt ion method,” *International Journal of Computer Networks and Applications (IJCNA)*, vol. 2, no. 4, pp. 165-172, 2015.
- [20] G. S. Li, W. L. Wang, and X. W. Yao, “An adaptive and opportunistic broadcast protocol for vehicular ad-hoc networks,” *International Journal of Automation and Computing*, vol. 9, pp. 378–387, 2012, doi: 10.1007/s11633-012-0658-9.
- [21] M. S. Rayeni, A. Hafid, and P. K. Sahu, “Dynamic spatial partition density-based emergency message dissemination in VANETs,” *Vehicular Communications*, vol. 2, no. 4, pp. 208-222, 2015, doi: 10.1016/j.vehcom.2015.07.002.
- [22] M. S. Sheikh, J. Liang, and W. Wang, “A survey of security services, attacks, and applications for vehicular Ad Hoc networks (VANETs),” *Sensors*, vol. 19, no. 16, 2019, doi: 10.3390/s19163589.
- [23] S. S. Shah, A. W. Malik, A. U. Rahman, S. Iqbal, and S. U. Khan, “Time barrier-based emergency message dissemination in vehicular ad-hoc networks,” *IEEE Access*, vol. 7, pp. 16494-16503, 2019, doi: 10.1109/ACCESS.2019.2895114.
- [24] B. Li and D. Pi, “Learning deep neural networks for node classification,” *Expert Systems with Applications*, vol. 137, pp. 324-334, 2019, doi: 10.1016/j.eswa.2019.07.006.
- [25] S. Mukherjee and N. Sharma, “Intrusion detection using naive bayes classifier with feature reduction,” *Procedia Technology*, vol. 4, pp. 119-128, 2012, doi: 10.1016/j.protcy.2012.05.017.

## BIOGRAPHIES OF AUTHORS



**Shazia Sulthana**     is Assistant Professor at the college of Global Academy of Technology, Visvesvaraya Technological University, Karnataka, India. She is having teaching experience of 15 years, currently perceiving Ph. D degree in the field of Wireless Networks under VTU, Karnataka, India. Her research areas are vehicular ad hoc networks, wireless networks. She has published several papers in refereed International Journals and presented in National and International Conferences. She is a life member of IETE. She has attended several FDPs, conferences and workshops. She can be contacted at email: shaziasulthana14@gmail.com.



**Dr. Bypanahalli Narayana Reddy Manjunatha Reddy**     has joined the Global Academy of Technology in the year 2004 and is currently working as a Professor in the Department of Electronics and Communication Engineering. His research and professional career spans about 23 years. He has completed his Ph.D. degree from VTU in the year 2018. His research interest is in the area of low power VLSI and embedded systems. He has published several papers in refereed International Journals and presented in National and International Conferences. He has also visited many countries like Dubai, China, Thailand, Abu Dhabi and presented his research work. He is a life member of IETE. He has organized/attended several FDPs, conferences and workshops. He also had given several technical talks in many forums. He can be contacted at email: manjunatha\_reddy@gat.ac.in.