

Trust based multi objective honey badger algorithm to secure routing in vehicular ad-hoc networks

Pramod Mutalik, Venkangouda C. Patil

Department of Electronics and Communication, Ballari Institute of Technology and Management, Ballari, India

Article Info

Article history:

Received Nov 29, 2022

Revised Feb 11, 2023

Accepted Mar 9, 2023

Keywords:

Malicious attacks

Packet delivery ratio

Secure route discovery

Trust based multi-objective

honey badger algorithm

Vehicular ad hoc networks

ABSTRACT

A vehicular ad-hoc network (VANET) is a set of intelligent vehicles that interact without any fixed infrastructure. Data transmission between each transmitter/receiver pair is accomplished using routing protocols. However, communication over the VANET is vulnerable to malicious attacks, because of the unavailability of fixed infrastructure and wireless communication. In this paper, the trust based multi objective honey badger algorithm (TMOHBA) is proposed to achieve secure routing over the VANET. The TMOHBA is optimized by incorporating different cost functions, namely, trust, end to end delay (EED), routing overhead, energy, and distance. The developed secure route discovery using the TMOHBA is used to improve the robustness against the malicious attacks, for increasing the data delivery. Moreover, the shortest path discovery is used to minimize the delay while improving the security of VANET. The TMOHBA method is evaluated using the packet delivery ratio (PDR), throughput and EED. Existing researches such as hybrid enhanced glowworm swarm optimization (HEGSO) and ad-hoc on-demand distance vector based secure protocol (AODV-SP) are used to evaluate the TMOHBA method. The PDR of the TMOHBA method for 10 malicious attacks is 90.6446% which is higher when compared to the HEGSO and AODV-SP.

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



Corresponding Author:

Pramod Mutalik

Department of Electronics and Communication, Ballari Institute of Technology and Management

Ballari, India

Email: pramodmutaliker@gmail.com

1. INTRODUCTION

In recent times, vehicular ad hoc networks (VANETs) are considered to be a prominent subclass of the mobile ad hoc networks because of their huge range of applicability. This vehicular communication network is a vital part of the intelligent transportation system (ITS) for offering road safety and traffic efficiency along with the development of wireless communication and embedded technologies [1]–[3]. Vehicles interact with each other and the data is broadcasted with other vehicles as well as road side units (RSUs) using the VANET. The multiple vehicles are linked in an ad-hoc fashion to exchange useful data in VANET [4], [5]. This type of network doesn't have a stationary or fixed base station or other infrastructure support [6], [7]. The data schedule is assisted by RSUs for choosing the transmitter vehicles and/or appropriate data items for transmitting in VANET. The vehicles are installed with the onboard unit to perform calculation and communication processes [8], [9]. VANET has some distinctive features like in mobile adhoc network (MANET) such as dynamic topology, frequent disconnection, communication based on geographical type, mobility modeling, prediction, adequate storage, and energy [10].

VANET minimizes traffic accidents, enhances traffic efficiency and safety, delivers information, entertainment services, and distributes related information [11]. The direct transmission of data is a

challenging task because vehicles are independently and dynamically moving in the network area. Hence, the routing protocol is considered one of the possible solutions for establishing the route in VANET [12]. The reliable message routing of packets to the destination from the source defines the effectiveness of VANET [13]. VANET utilizes wireless media for communication which makes the network susceptible. For instance, the attacker node uses VANET for broadcasting the data to mislead other vehicles. Hence, security is an essential task for identifying malicious attacks in VANET [14]–[16]. Security and truthfulness are essential for creating an effective interaction within the VANET. The capacity of the node is measured by node trust which is used to accomplish an effective data transmission [17], [18].

The related works of secure routing over the VANET are given as: Upadhyay *et al.* [19] presented hybrid enhanced glowworm swarm optimization (HEGSO) to perform the traffic-aware secure routing over the VANET. An average speed and traffic density (TD) were computed using a modified exponential weighted moving averaging approach. These traffic parameters, namely, average speed and TD, were optimized by utilizing the HEGSO. The certificate cancellation of malicious attackers was used to achieve secure data broadcasting in the network. The developed HEGSO was dependent only on the average speed and TD, therefore effective parameters, e.g., trust and energy, were further required to be considered to achieve reliable data transmission. Kumar *et al.* [20] presented the ad hoc on-demand distance vector based secure protocol (AODV-SP) to avoid the blackhole attack. Modified route request (RREQ) packet and route reply (RREP) packets were used by the AODV-SP to perform the secure routing in VANET. The developed AODV-SP discovered the malicious nodes and it was used to mitigate those malicious nodes from the VANET. The behavioral analysis of the node was required, to develop an effective secure routing between the vehicles. Shafi and Ratnam [21] developed the energy and mobility aware routing protocol (EM-ARP) for minimizing energy usage and delay in infotainment services. The mobility and battery power were considered to dynamically select the cooperative relay vehicles (CRV) using the EM-ARP. The selection of CRV was used for balancing the energy distribution, mobility and direction. Further, the trust value was used to evaluate the optimal path and the trust value was computed using the congestion, hop count and link expiration time. The delay was considered during CRV selection to minimize the delay over the VANET.

Hosmani and Mathapati [22] developed robust and reliable secure clustering and data transmission (RRSCDT) to protect the network against malicious vehicles. In RRSCDT, the selection of secure and optimal cluster head (CH) was done based on the weight values. The RRSCDT considered three different values to perform CH selection and those are, density, packet delivery probability, and mobility speed. Further, the nodes were chosen using trust evaluation while transmitting the data. Therefore, the RRSCDT was used to minimize the control overheads using the trust evaluation in VANET. The higher mobility of vehicles caused data loss over the network. Rabiaa *et al.* [23] presented the cross-layer ad-hoc on-demand multipath distance vector (CRAOMDV) routing to perform secure data transmission. In this CRAOMDV, the data was exchanged between the network and medium access control (MAC) layers for identifying and avoiding malicious attackers in VANETs. Each node processed under CRAOMDV stored all data about attackers and the routes with malicious attackers were removed during the routing process. Further, the CRAOMDV is used to select the other path to avoid data loss. Effective cost metrics were essential to achieve optimal route discovery in VANET.

The contributions of this research are concise as follows: i) The secure route via vehicles to a respected destination is generated using the trust based multi objective honey badger algorithm (TMOHBA). The TMOHBA method considers trust as the primary cost value for avoiding malicious attackers in the route that helps to improve the data delivery over the network. Further, the TMOHBA is optimized by using trust, end to end delay (EED), routing overhead, energy and distance. And ii) The EED and distance considered in the TMOHBA are used to minimize the delay during the transmission by selecting the secure route with less traffic and less distance.

The remaining paper is arranged as: section 2 offers the detailed information about the TMOHBA method based secure routing from the sender to receiver in VANET. The outcomes of the TMOHBA method along with its comparative analysis with existing researches are provided in section 3 whereas section 4 provides the conclusion.

2. TMOHBA METHOD

In this research, the secure route discovery using TMOHBA is developed to achieve secure and reliable transmission over the VANET. The generation of a secure route is used to avoid the malicious nodes over the network which is used to enhance the packet delivery of the network. The typical honey badger algorithm (HBA) [24] is converted into TMOHBA to discover the secure route from the transmitter node to the destination node. The HBA generally replicates the activities of the honey badger which either digs and smells or follows the honeyguide bird for discovering the food source. The HBA considered only one cost metric i.e., distance during the optimization process, however, the proposed TMOHBA is optimized using five different cost metrics which are trust, EED, routing overhead, energy and distance. Hence, the

TMOHBA is used to achieve security while minimizing the delay during the data transmission. Figure 1 shows the flowchart of the TMOHBA method.

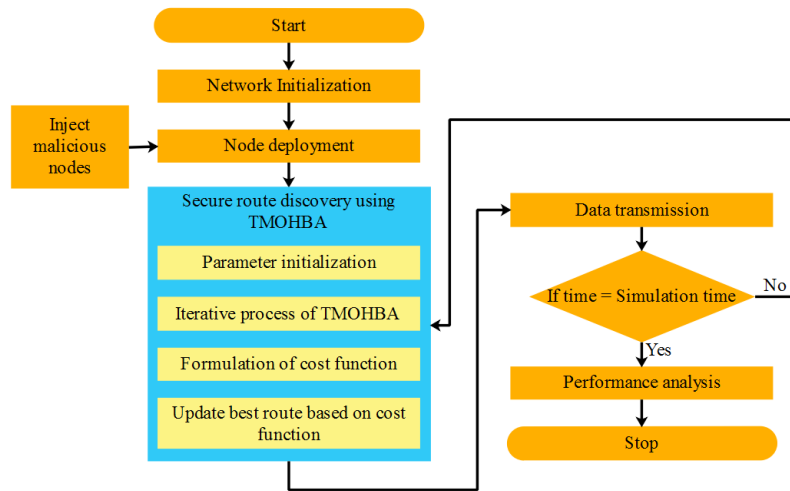


Figure 1. Flowchart of the TMOHBA method

2.1. Network model

VANET is defined as a special kind of network that offers various services to the users such as traffic management, road safety and accident prevention [25]. In the network model, the sensor nodes (i.e., vehicles) are considered as randomly moving along with malicious vehicles (i.e., attackers) in the network area. Hence, it is required to develop secure routing among the vehicles of the VANET. The proposed TMOHBA is used to discover the secure route via vehicles, towards the destination which is explained in the following sections.

2.2. Representation and initialization

At first, each honey badger of TMOHBA represents a route from the transmitter node to base station (BS). The dimension of each solution is equal to the number of nodes that exist in the route. Let, the honey badger i of the TMOHBA be $x_i = (x_{i,1}, x_{i,2}, \dots, x_{i,h})$, where the h defines the honey badger's dimensions which are identical to the amount of nodes that exist in the path. Here, the routes are created randomly while initializing the secure route discovery. The optimal secure route x_{prey} is chosen according to the formulated cost function. The following iterative process of TMOHBA is used to discover the optimal secure route.

2.3. The iterative process of TMOHBA for secure route discovery

The possible routes and best routes obtained from the initialization phase are processed in the iterative process to identify the optimal secure route. The intensity of each honey badger is associated with the concentration strength of prey and the distance between honey badger i and the prey. The prey's smell intensity is denoted as I_i and distance factor is identified according to the x_{prey} that is discovered based on the formulated cost metric. Then this distance factor is used to update the intensity value that is used to enhance the secure route discovery. If there is a higher smell, the movement is fast; Otherwise, there is a slower movement which is provided by the inverse square law as shown in (1).

$$\begin{aligned}
 I_i &= r_2 \times \frac{S}{4\pi d1_i^2} \\
 S &= (x_i - x_{i+1})^2 \\
 d1 &= x_{prey} - x_i
 \end{aligned} \tag{1}$$

where, r_2 is the random number among $[0,1]$; S is concentration strength; $d1$ is the distance between the i^{th} badger and the prey and the position of best prey i.e., the optimal secure route is denoted as x_{prey} . The density factor (α) shown in (2) is used to perform the adaptation from exploration to exploitation wherein, this density factor is utilized for controlling the time-varying randomization. The density factor is minimized along with the iterations to reduce the randomization with time.

$$\alpha = C \times \exp\left(\frac{-t}{t_{max}}\right) \quad (2)$$

where, the constant value $C \geq 1$, and default value is 2; iterations and maximum iterations are denoted as t and t_{max} respectively. The flag F is utilized to alter the foraging direction for obtaining higher chances of scanning the entire search phrase. There are two different processes used in the location update process known as digging and honey phase. The action of the honey badger is similar to Cardioid form in the digging phase whereas Cardioid motion is expressed in (3). The flag utilized to alter the foraging direction is defined in (4). Besides, the honey badger follows the honeyguide bird to discover the beehive that is shown in (5).

$$x_{new} = x_{prey} + F \times \beta \times I \times x_{prey} + F \times r_3 \times \alpha \times d1_i \times |\cos(2\pi r_4) \times [1 - \cos(2\pi r_c)]| \quad (3)$$

$$F = \begin{cases} 1 & \text{if } r_6 \leq 0.5 \\ -1 & \text{else} \end{cases} \quad (4)$$

$$x_{new} = x_{prey} + F \times r_7 \times \alpha \times d1_i \quad (5)$$

where, the honey badger's capacity for getting food is $\beta \geq 1$; random numbers among the $[0,1]$ are r_3, r_4 and r_5 ; random number in the range of $[0,1]$ is denoted as r_6 . The searching ability is mostly based on the smell intensity of prey, distance and density factor. Further, the random number among the $[0,1]$ is denoted as r_7 . The aforementioned (5) is used to discover the possible secure route which is adjacent to the prey's position.

2.4. Formulation of cost function

The unique cost functions considered for discovering the secure route are: Trust (f_1), EED (f_2), routing overhead (f_3), energy (f_4) and distance (f_5). In (6) shows the formulated cost function of the TMOHBA-based secure route discovery. The weighted values $\alpha_1 - \alpha_5$ are assigned to each cost metric. Because each value is non-conflicting, these multiple cost metrics are transformed into a single cost metric.

$$Cost = \alpha_1 \times f_1 + \alpha_2 \times f_2 + \alpha_3 \times f_3 + \alpha_4 \times f_4 + \alpha_5 \times f_5 \quad (6)$$

The primary cost considered in this TMOHBA is the node's trust value which includes two different trust values: direct and indirect trust values. The direct trust (DT) is the ratio between the received packets and broadcasted packets as expressed in (7). Next, the indirect trust (IDT) is computed based on the direct trust from the target node as computed in (8). The final trust computation based on DT and IDT is shown in (9). EED is one of the important costs calculated using traffic prediction. The delay needs to be less, therefore the cost function is efficient while performing the routing. The EED expressed in (10) is measured based on the vehicle's average speed and length of the road segment. The ratio between the number of packets sent and EED is defined as routing overhead which is expressed in (11). If the EED is low, then the traffic over the respective path is also less. In route generation, the node with huge residual energy is chosen for reliable data transmission. Because, the intermediate nodes have to transmit and receive the information from the other nodes. The residual energy computation is expressed in (12). Euclidean distance (f_5) is also considered to discover a secure route with less transmission distance. Because higher distance causes high energy consumption.

$$DT = \frac{R_{a,b}(t)}{S_{a,b}(t)} \quad (7)$$

$$IDT = \frac{1}{NN} \sum_{u=1}^U DT_{u,s} \quad (8)$$

$$f_1 = \sum_{i=1}^P (DT + IDT) / i \quad (9)$$

$$f_2 = \sum_{l=1}^{m_l^d} \frac{l^l d}{AS_l^d(U)} \quad (10)$$

$$f_3 = \frac{\text{Number of packets sent}}{EED} \times 100 \quad (11)$$

$$f_4 = \sum_{j=1}^h E_j \quad (12)$$

where, $R_{a,b}(t)$ and $S_{a,b}(t)$ define the received and broadcasted packets among the nodes a and b ; the amount of neighbor nodes to the node s is denoted as NN ; the total number of participating nodes is denoted as P ; the

length of the road segment Id is denoted as l^{id} ; time is denoted as t ; the total vehicles in the network is denoted as m ; $AS_i^{ld}(U)$ denotes the average predicted speed of vehicle U and E_j defines the residual energy of the j^{th} node.

3. RESULTS AND DISCUSSION

The outcomes of the TMOHBA method are shown and explained in this section. The implementation and simulation of the TMOHBA method are done in MATLAB R2020a. Here, the system is operated with 16 GB RAM and an i7 processor. The TMOHBA method is used to increase the robustness against malicious attackers in the VANET. The network is initialized with 100 nodes deployed in the area of $650 \times 1,000$ m with a mobility of 70 and 100 km/h. Table 1 provides the simulation parameters considered while analyzing the TMOHBA method.

Parameters	Values
Routing method	TMOHBA
Number of nodes	100
Number of malicious attacks	2, 4, 8, and 10
Area	650×1,000 m
Speed range (mobility)	70 and 100 km/h
Simulation time	100 s

3.1. Performance analysis

The performance of the TMOHBA method is evaluated using packet delivery ratio (PDR), throughput and EED. The performances are analyzed in comparison with a conventional optimizer, by name grey wolf optimization (GWO) which uses the default cost function, i.e., distance to perform the route discovery. The results are analyzed by varying the malicious attackers that exist in the network.

3.1.1. Packet delivery ratio

Packet delivery ratio is defined as the ratio between the number of packets received at the destination and the number of packets sent by the transmitter node. The comparison of PDR for TMOHBA with GWO is shown in Figure 2. Figure 2 shows that the TMOHBA achieves better PDR than the GWO method. For example, the PDR of the TMOHBA with 10 malicious nodes is 90.64% which is higher when compared to the GWO. The mitigation of malicious attacks through the implementation of TMOHBA, prevents data loss while broadcasting the data packets. The residual energy considered in the TMOHBA is used to avoid node failure that is additionally used to increase the PDR.

3.1.2. Throughput

Throughput is defined as the number of packers that are successfully received at the destination over the VANET. The throughput comparison for GWO and TMOHBA is shown in Figure 3, Figure 3 shows that the TMOHBA has higher throughput when compared to the GWO. For example, the throughput of the TMOHBA for 10 malicious nodes is 349.022 Mbits/sec which is greater when compared to the GWO. The throughput of TMOHBA is increased because of avoiding malicious attacks on the route. The development of trust based route over the VANET increases the robustness against malicious attacks, which helps to improve the data delivery.

3.1.3. End-to-end delay

EED refers to the amount of time taken to transmit the packet from the source to the destination. The comparison of EED for TMOHBA with GWO is shown in Figure 4. Figure 4 shows that the TMOHBA achieves lesser EED than the GWO method. For example, the EED of the TMOHBA with 10 malicious nodes is 0.0260 s which is less in comparison to the EED of GWO. The EED of TMOHBA is minimized by identifying the path with lesser delay and less transmission distance. Further, the formulated cost function of TMOHBA is used to minimize the routing overhead that is further used to minimize the EED.

3.2. Comparative analysis

The comparative analysis of the TMOHBA is provided in this section wherein, existing researches known as HEGSO [19] and AODV-SP [20] are used to perform the comparison. The comparison among TMOHBA, HEGSO [19] and AODV-SP [20] is provided in Table 2. The graphical comparison of PDR is

shown in Figure 5. From this analysis, it is concluded that the TMOHBA achieves better performance than the HEGSO [19] and AODV-SP [20]. For example, the PDR of the TMOHBA varies from 90.6446% to 93.6396% whereas the HEGSO [19] varies from 78.09% to 93% and the AODV-SP [20] varies from 10.98% to 49%. The trust based secure optimal route using TMOHBA is used to increase the robustness against malicious attacks. The mitigation of malicious attacks is used to improve the data delivery and the shortest path generation is used to minimize the EED.

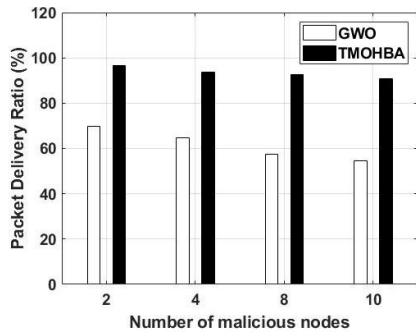


Figure 2. Analysis of PDR

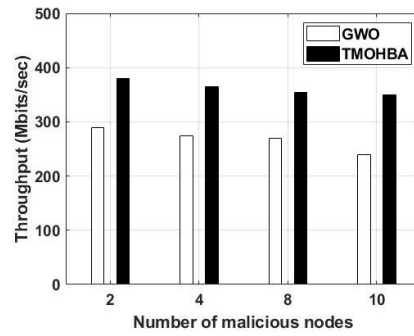


Figure 3. Analysis of throughput

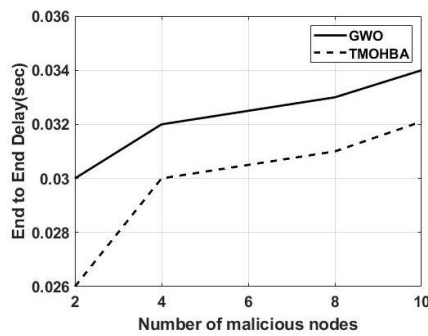


Figure 4. Analysis of EED

Table 2. Comparative analysis of TMOHBA

Performance measures	Methods	Number of malicious nodes			
		2	4	8	10
PDR (%)	HEGSO [19]	93	88	80	78.09
	AODV-SP [20]	49	39.5	28	10.98
	TMOHBA	93.6396	93.6464	92.6426	90.6446
Throughput (Mbits/sec)	AODV-SP [20]	110	78	70	57
	TMOHBA	379.425	364.536	354.074	349.022
	AODV-SP [20]	0.04	0.03	0.048	0.047
EED (s)	TMOHBA	0.020	0.0240	0.0250	0.0260

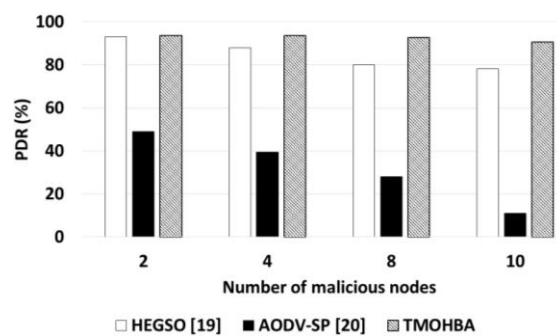


Figure 5. Graphical comparison of PDR

4. CONCLUSION

In this research, the secure route discovery is performed using the TMOHBA over vehicular networks. The TMOHBA is optimized using the trust, EED, routing overhead, energy and distance for achieving a secure and reliable communication. The trust value incorporated in the TMOHBA is used to avoid malicious attacks during route generation which helps to avoid unwanted energy consumption and packet drop. In route discovery, the node failure is avoided using the residual energy whereas the distance and EED are used to identify the route with optimally short distance. The shortest path generation and lesser routing overhead are used to minimize the delay while transmitting the data in VANET. From the results, it is concluded that the TMOHBA method achieves better performance than the HEGSO and AODV-SP. The PDR of the TMOHBA method for 10 malicious attacks is 90.6446% which is high when compared to the HEGSO and AODV-SP. In future, a novel optimization algorithm will be used to develop a secure and energy aware routing for improving the performances of VANET.





REFERENCES

- [1] K. N. Tripathi, A. M. Yadav, and S. C. Sharma, "TREE: trust-based authenticated and secure dissemination of emergency event information for the network of connected vehicles," *Arabian Journal for Science and Engineering*, vol. 47, no. 8, pp. 10689–10717, 2022, doi: 10.1007/s13369-022-06753-1.
- [2] K. A. Awan, I. Ud Din, A. Almogren, M. Guizani, and S. Khan, "StabTrust-a stable and centralized trust-based clustering mechanism for IoT enabled vehicular ad-hoc networks," *IEEE Access*, vol. 8, pp. 21159–21177, 2020, doi: 10.1109/ACCESS.2020.2968948.
- [3] R. Ramamoorthy and M. Thangavelu, "An enhanced distance and residual energy-based congestion aware ant colony optimization routing for vehicular ad hoc networks," *International Journal of Communication Systems*, vol. 35, no. 11, Jul. 2022, doi: 10.1002/dac.5179.
- [4] K. N. Tripathi and S. C. Sharma, "A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETs)," *International Journal of System Assurance Engineering and Management*, vol. 11, no. 2, pp. 426–440, Sep. 2020, doi: 10.1007/s13198-019-00871-0.
- [5] S. S. Sefati and S. G. Tabrizi, "Detecting sybil attack in vehicular ad-hoc networks (VANETs) by using fitness function, signal strength index and throughput," *Wireless Personal Communications*, vol. 123, no. 3, pp. 2699–2719, Apr. 2022, doi: 10.1007/s11277-021-09261-x.
- [6] A. Kumar, N. Sharma, and A. Kumar, "End-to-end authentication based secure communication in vehicular ad hoc networks (VANET)," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 1, pp. 219–229, Jan. 2022, doi: 10.1080/09720529.2021.2014147.
- [7] F. Chbib, L. Khoukhi, W. Fahs, J. Haydar, and R. Khatoun, "A cross-layered scheme for multichannel and reactive routing in vehicular ad hoc networks," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 7, Jul. 2022, doi: 10.1002/ett.4468.
- [8] D. Singh, A. K. Maurya, Ranvijay, and R. S. Yadav, "A trust-based clustering approach to form stable clusters in vehicular ad hoc networks," *Journal of Ambient Intelligence and Humanized Computing*, Apr. 2022, doi: 10.1007/s12652-022-03842-9.
- [9] R. Kolandaisamy *et al.*, "RETRACTED ARTICLE: A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6599–6612, Jun. 2021, doi: 10.1007/s12652-020-02279-2.
- [10] B. Suganthi and P. Ramamoorthy, "An advanced fitness based routing protocol for improving QoS in VANET," *Wireless Personal Communications*, vol. 114, no. 1, pp. 241–263, Jun. 2020, doi: 10.1007/s11277-020-07361-8.
- [11] B. Su, C. Du, and J. Huan, "Trusted opportunistic routing based on node trust model," *IEEE Access*, vol. 8, pp. 163077–163090, 2020, doi: 10.1109/ACCESS.2020.3020129.
- [12] Y. Pramitarini, R. H. Y. Perdana, T.-N. Tran, K. Shim, and B. An, "A hybrid price auction-based secure routing protocol using advanced speed and cosine similarity-based clustering against sinkhole attack in VANETs," *Sensors*, vol. 22, no. 15, 2022, doi: 10.3390/s22155811.
- [13] T. S. Gnanasekar and D. Samiappan, "Optimal routing in VANET using improved meta-heuristic approach: a variant of Jaya," *IET Communications*, vol. 14, no. 16, pp. 2740–2748, 2020, doi: 10.1049/iet-com.2018.6214.
- [14] F. Mirsadeghi, M. K. Rafsanjani, and B. B. Gupta, "A trust infrastructure based authentication method for clustered vehicular ad hoc networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2537–2553, Jul. 2021, doi: 10.1007/s12083-020-01010-4.
- [15] Z. Xu, D. He, N. Kumar, and K.-K. R. Choo, "Efficient certificateless aggregate signature scheme for performing secure routing in VANETs," *Security and Communication Networks*, vol. 2020, pp. 1–12, Feb. 2020, doi: 10.1155/2020/5276813.
- [16] N. S. Divya, V. Bobba, and R. Vatambeti, "An adaptive cluster based vehicular routing protocol for secure communication," *Wireless Personal Communications*, vol. 127, no. 2, pp. 1717–1736, Nov. 2022, doi: 10.1007/s11277-021-08717-4.
- [17] M. Alkhalidy, A. F. Al-Serhan, A. Alsarhan, and B. Igried, "A new scheme for detecting malicious nodes in vehicular ad hoc networks based on monitoring node behavior," *Future Internet*, vol. 14, no. 8, Jul. 2022, doi: 10.3390/fi14080223.
- [18] T. Nandy *et al.*, "An enhanced lightweight and secured authentication protocol for vehicular ad-hoc network," *Computer Communications*, vol. 177, pp. 57–76, Sep. 2021, doi: 10.1016/j.comcom.2021.06.013.
- [19] P. Upadhyay, V. Marriboina, S. Kumar, S. Kumar, and M. A. Shah, "An enhanced hybrid glowworm swarm optimization algorithm for traffic-aware vehicular networks," *IEEE Access*, vol. 10, pp. 110136–110148, 2022, doi: 10.1109/ACCESS.2022.3211653.
- [20] A. Kumar *et al.*, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocessors and Microsystems*, vol. 80, Feb. 2021, doi: 10.1016/j.micpro.2020.103352.
- [21] S. Shafi and D. V. Ratnam, "A trust based energy and mobility aware routing protocol to improve infotainment services in VANETs," *Peer-to-Peer Networking and Applications*, vol. 15, no. 1, pp. 576–591, Jan. 2022, doi: 10.1007/s12083-021-01272-6.





- [22] S. Hosmani and B. Mathapati, "R2SCDT: robust and reliable secure clustering and data transmission in vehicular ad hoc network using weight evaluation," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 3, pp. 2029–2046, Mar. 2023, doi: 10.1007/s12652-021-03414-3.
- [23] N. Rabiaa, A. C. Moussa, and B. H. Sofiane, "A cross-layer method for identifying and isolating the blackhole nodes in vehicular ad-hoc networks," *Information Security Journal: A Global Perspective*, pp. 1–15, 2021, doi: 10.1080/19393555.2021.2007316.
- [24] F. A. Hashim, E. H. Houssein, K. Hussain, M. S. Mabrouk, and W. Al-Atabany, "Honey badger algorithm: New metaheuristic algorithm for solving optimization problems," *Mathematics and Computers in Simulation*, vol. 192, pp. 84–110, Feb. 2022, doi: 10.1016/j.matcom.2021.08.013.
- [25] H. Fatemidokht and M. K. Rafsanjani, "QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks," *Journal of Systems and Software*, vol. 165, Jul. 2020, doi: 10.1016/j.jss.2020.110561.

BIOGRAPHIES OF AUTHORS



Pramod Mutalik     has more than 07 years of teaching and research experience. His fields of interests include: wireless mobile adhoc networks, Logic design, wireless communication, VANET's, embedded systems and VLSI design. He can be contacted at email: pramodmutalikr@gmail.com.



Venkanagouda C. Patil     is working as Professor in the Department of Electronics and Communication Engineering, Ballari Institute of Technology and Management, Ballari, India. He has more than 27 years of teaching experience in the field of engineering and technology. His research areas include: wireless mobile ad hoc networks and wireless sensor networks. At present he is guiding eight research scholars toward Ph.D. under Visvesvaraya Technological University, India. He can be contacted at email: patilvc54@gmail.com.