Retraction

Retracted: An Enhanced Hybrid Glowworm Swarm Optimization Algorithm for Traffic-Aware Vehicular Networks

Pratima Upadhyay; Venkatadri Marriboina; Shiv Kumar; Sunil Kumar; Mohd Asif Shah

IEEE Access

10.1109/ACCESS.2022.3211653

Notice of Retraction 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. After careful and considered review of the content of this article by a duly constituted expert committee, this article has been found to have violated IEEE publication principles. Specifically, this article copied portions of content from the following source without appropriate reference: “Development of Energy Efficient Secure Communication Protocols for Vehicular Ad Hoc Networks (VANETs)” Chapter 5–PhD Thesis, March 2020 Therefore, IEEE has retracted the content of this article from Xplore. The authors disagreed with the retraction.

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 24 August 2022, accepted 18 September 2022, date of publication 3 October 2022, date of current version 21 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3211653

RESEARCH ARTICLE

An Enhanced Hybrid Glowworm Swarm Optimization Algorithm for Traffic-Aware Vehicular Networks

PRATIMA UPADHYAY[1], VENKATADRI MARRIBOINA[2], SHIV KUMAR[3], (Senior Member, IEEE), SUNIL KUMAR[4], AND MOHD ASIF SHAH[5]

[1]Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Madhya-Pradesh, Gwalior 474005, India
[2]NITTE Institute of Professional Education, Mangalore, Karnataka 575018, India
[3]Department of Computer Science and Engineering, LNCTE College, Bhopal, Madhya-Pradesh 462021, India
[4]School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India
[5]Department of Economics, Bakhtar University, Kabul 2496300, Afghanistan

Corresponding author: Mohd Asif Shah (ohaasif@bakhtar.edu.af)

ABSTRACT A subclass of a Mobile Adhoc Network (MANET) is a Vehicular Adhoc Network (VANET). It consists of self-configuring moving vehicles which are called nodes. It is an inevitable ingredient of intelligent transportation systems. The vehicular network has some permanent devices called roadside units and moving devices called On Board Units (OBU). Every vehicle traveling on the network must possess the OBU. Safety and non-safety tidings are broadcasted in vehicular networks. Even vehicular network is derived from MANET and its characters are discriminated against the MANET. The various unique characteristics of VANETs are high mobility, changes in network topology, size of the network, long distance between the vehicles, frequently changing vehicle density, and limited time. Because of these special features, the traditional security and routing mechanisms are not suitable for VANETs. Also, the safety messages are modified or discarded by the attacker or any other node and it may lead to the loss of privacy, integrity, confidentiality, and authentication of the data.So to enhance the security of VANETs, it is very much essential to invent a secure communication protocol, to protect the infrastructure of the network and the confidentiality of the data. The simulation results reveal that the secure communication using certificate revocation approach, energy-efficient enhanced secure routing protocol, traffic-aware secure routing for VANETs using Hybrid Enhanced Glowworm Swarm Optimization (HEGSO), and trust model for secure communication in VANETs is ensuring the security in VANETs. When compared to peer existing routing protocols, the proposed scheme significantly reduces the packet failure ratio, response time, and throughput. When compared to ARIOR and I-AREOR, the proposed HEGSO technique diminished delays by 20% and 34%, respectively.

INDEX TERMS VANET, MANET, security, swarm optimization, privacy, data communication.

I. INTRODUCTION

VANETs are simply called as VANETs and it is one of the most important promising networks [1]. Even if it is one of the sub-classes of MANET its characters somewhat differ from ad-hoc networks. VANETs have their own unique features [2]. VANETs permit the vehicle to send and receive the data even when the vehicles are moving. Vehicles can communicate with other vehicles directly or with the help of other vehicles and with the assistance of fixed infrastructures like Road Side Units (RSU) and other communicating devices [3]. Because of these special features of VANETs, it attracts everyone to focus on them. Also, it plays a major role in the government, private sectors, corporations, and companies that take new steps to implement new applications to the VANETs [4]. VANETs consider the moving vehicles as nodes and form MANETs. It permits the vehicles to communicate with each other [5]. When the vehicles are left

The associate editor coordinating the review of this manuscript and approving it for publication was Congduan Li.

from the coverage area or dropped out of the network, other vehicles can join the network and keep the network active. To improve safety it would permit the fire and police vehicles to communicate with each other [6].

Nowadays, since the number of vehicles is increasing, it leads to more traffic and accidents [7]. Also, it is a big problem in most developing countries. So the countries seriously consider the above issues and take so many steps to reduce traffic congestion and improve road safety [8]. For example, the United States of America implemented traffic geometry and which limits the capacity of the lane, to 2200 vehicles per hour, and advised the drivers to maintain the speed limit of 100km/hour. To improve the safety and responsibilities of the driver, warning messages will be broadcasted through a mobile phone or General Packet Radio Services (GPRS) [9]. Cameras are installed on the roadway to assess the vehicle speed and to ensure that the safety belt is properly tightened [10].

VANETs is a new technology that can use the potentialities of current generation wireless networks to vehicular networks [11]. VANETs construct a powerful ad-hoc network between the vehicles and RSU. It creates connections between the nearby nodes (vehicles) and the RSU. VANETs establish successful communication among the vehicles by using the Adhoc network tool IEEE 802.11p [12]. VANET is a motivating network for Intelligent Transportation Systems (ITS) to improve and secure mobility. Normally there are two types of nodes in VANETs namely, OBU and RSU [13]. Here, the vehicles are considered an OBU, so it is a moving node. While the same time RSUs are erected near the roads, so it is considered a fixed node [14]. Also, the vehicles behave as sensor nodes and broadcast information about the traffic and road details like poor road conditions, traffic jams, and vehicle accidents [15].

Vehicular networks have two different types of units namely, OBU and RSU [16]. The OBU helps the vehicle to interact with the other vehicles OBU and RSU. In vehicular networks, vehicles must verify the messages because VANETs maintain a reliable and secure connection [17]. To maintain the authentication, VANETs use key generation mechanisms it permits the transmitter vehicle to create and update the keys in a certain interval for the critical operations [18]. Vehicular networks classified the messages broadcasted between the vehicles OBU and RSU and vice versa into several types, they are explained below,

- **Warning messages:** The messages which carry information about road conditions, accidents, and traffic on roads are called warning messages [19].
- **Emergency Messages:** The messages like the crossing of fire vehicles, VIP vehicles, ambulance vehicles, and police vehicles come under emergency messages. Also, messages broadcasted about the accidents come under this category [20].
- **Personal messages:** Personal communication between the drivers and passengers, details of a driver, vehicle, and passengers are called personal messages [21].
- **Routing messages:** These types of messages hold the information about the various routes like the shortest route, congested route, etc. These types of messages will be depending on the routing protocol used by the algorithm [22].
- **Safety messages:** To enhance secure communication, safety messages are broadcasted on the network. The messages like the speed, present location, direction, and ID of the vehicles come under this category [23].
- **Information messages:** This type of message holds the information about the nearby petrol/diesel/gas/air filling stations, hotels, tourist places, and many more [24].

A. CHARACTERISTICS OF VANETs

VANETs have the following characteristics,

- **High Mobility:** In VANETs, since the nodes are vehicles, they are moving in the network at high speed. So it is very difficult to find the current position of the vehicles [25].
- **Changes in network topology:** As the nodes are moving fast, the location of the vehicles changes often. It leads to the change of the network topology rapidly [26].
- **Size network:** The size of the network is unlimited because it can be applied in one or more villages or cities [27].
- **Broadcasts of information:** In VANETs, the vehicles receive information from the RSU and other vehicles. The nature of the vehicles is to move fast and the nodes broadcast the information very fast [28].
- Wireless medium: In VANETs the information is broadcasted through a wireless medium [29].
- **Time Span:** The information should be broadcasted to the vehicles before the time has expired. Only then the vehicles could take the decision accordingly [30].

The prime aim of VANETs is to provide maximum protection to the broadcasted messages. Vehicular networks enhance safety, decline traffic, broadcast emergency messages and fulfill the needs of the users. Moreover, VANETs propagate warning information between vehicles to reduce energy consumption. To improve the security of VANETs this thesis states the cluster-based secure communication, certificate revocation scheme, establishes the secure path by using enhanced routing & Traffic Density (TD) and calculates the worth of the message which account into consideration.

B. NEED OF SECURITY IN VANETs

Security in VANETs is a crucial one. Usually, in traditional networks, the important security factors are confidentiality, integrity, privacy, availability, etc. Even in VANETs, the above security factors have been considered the prime security is life safety [31]. So the prime information will not be altered or erased by the attacker vehicle or any other vehicle. Also, the details about the vehicles and their drivers will be able to send secretly within the allotted time [32]. If the details are not able to be delivered within a time, it may lead

to loss of the data. Practically it is difficult to implement the traditional security factors in VANETs [33] because in VANETs the nodes are moving at high speed, as well as the entry and exit of the vehicles are frequently changing in nature. Above all, the medium of communication is wireless and the information's exchanged in open, as it is easy to attack [34].

The ad-hoc nature of the network and the wireless communication medium leads the network to attack [35]. If it is a wired medium, the attacker also should be connected in a wired medium. Normal security features such as locked communication, closet, and restricted building access can be implemented to reduce the access of network wires [36]. These types of security features are not available in a wireless network. In VANETs, if the vehicle has suitable equipment, whether it is a legitimate member of the network or not a member, the vehicle can receive and send messages in the network. Even if the attacker is discovered [37], it is difficult to remove him from the network, since they have been freely roaming throughout the wireless region. If it is a wired medium the attacker must use the wired medium to implement the attacks. Normally it is difficult to access a medium like wireless medium [38]. In a wireless medium, an attacker may simply copy or eavesdrop on the information. Since it has no proper infrastructure, it is difficult to distribute the key and provide the digital certificates.

The structure of the VANETs is having the possibility of being unauthorized access, eavesdropping, illicit use, etc. So an implementation of security in VANETs is inevitable [39]. As dynamic topology is one of the particularities of VANETs, implementing security in that type of network is a challenging task [40]. Even if it is challenging, it is very essential, because safety messages generated by the network may be altered, discarded, or delayed due to any attacker vehicle knowingly or unknowingly, which may cause the loss of privacy, integrity, and authentication of the data. Also, consume the resources of the networks. To avoid the above situation, the receivers should ensure the reliability and the worth of the obtained message.

In VANETs, all the nodes are responsible to form the network by themselves. The problem here is that the nodes do not have any clear idea about the other nodes in the network. In VANETs, if the security level is low, it is very easy to be attacked by attackers. Moreover, it carries business-related data, customer-related data, and fun data as it is very essential to provide security.

In VANETs, attacker nodes affects the network performance by altering or injecting wrong data in the network. To make the vehicular network becomes secure it should fulfill the following requirements. They are authentication, confidentiality, accountability, limited credits usage, non-repudiation, revoking the credits, data consistency, privacy, and integrity. The fundamental and prime need for VANET security is authentication. To identify the correct vehicle, authentication is inevitable for VANETs. Especially VANETs involve examining the identification of the vehicle and separating the authorized vehicles and the unauthorized vehicles. Also, it ensures that the received message has come from the authorized vehicle. In any case, if any vehicle executes the message of attacker vehicles it causes serious problems like damaging the network and losing the confidentiality of the data. Also, it may create more problems like road traffic and also affects the journey time of other vehicles. So identifying the correct vehicle is inevitable in VANETs [41].

Confidentiality is also one of the prime security demands in vehicular ad-hoc communication. It ensures that only authorized persons can view the messages. Also, it permits only the particular group members to view the information [42]. If attackers view the message or copy the message it may cause the loss of privacy of the sender and result in some unwanted problems in the networks. The next requirement is accountability. Accountability means the vehicle which has sent the message, will be responsible for that message and that node is required to undertake legal or moral actions. A rule-creating node must be able to detect the attacker's vehicle and list it to punishments. Since safety is a prime application in VANETs, accountability is a critical requirement in VANETs. The next one is the usage of limited credits. It is a badge to achieve authentication and accountability. It is very essential to protect the network from Sybil attacks. So the malicious nodes cannot get the credits of the correct user and affect the networks. The next important requirement is non-repudiation. Here no vehicle should deny the message or part of a message, which they had sent earlier. VANETs attach credits to every vehicle based on their behavior in the network. If any node misuses the credits, the network should be able to revoke those credits. Data consistency is an essential one in VANETs [43]. The network should ensure that all the drivers have received consistent information.

Privacy is an important requirement of VANETs. Each country has its views on privacy. Some nations compelled the drivers to submit their details to avoid fraudulent activities. But at the same time, some nations have implemented their policy to maintain privacy. Whenever the vehicles try to communicate any assistance from the RSU, they expect to maintain their privacy by avoiding informing who are they, from where they have come and where they are going and the purpose of the travel, and so on. On one hand, the network preserves the privacy of the vehicles, but on the other hand, the network is not able to forward the anonymous data, and also it is difficult to identify who has created and injected the data into the network. Since VANETs use wireless mediums, the attackers can easily hack the message and modify the contents of the message. The modified message may create some unnecessary problems in the network. So it is very essential to ensure the integrity of the message [44].

C. PROBLEM STATEMENT

On the one hand, the network preserves the privacy of the vehicles, but on the other hand, the network is not able to forward the anonymous data, and also, it is difficult to identify who has created and injected the data into the network. Since

VANETs use wireless media, attackers can easily hack the message and modify the contents of the message. The modified message may cause some unnecessary problems in the network. So it is very essential to ensure the integrity of the message.

D. MOTIVATION

The main aim of VANETs is to enhance the security between vehicles. But VANETs are suffering from many attacks, such as Denial of Service (DoS), channel jamming, Distributed Denial of Service (DDoS), propagation of tampered messages, spamming messages, etc. The false messages must be instantly controlled to reduce further negative changes on other nodes (vehicles) in VANETs [45]. So it is very much necessary to generate an efficient security system to protect the messages from attackers and consider energy efficiency and other security issues.

The major Contributions of the paper are as follows,

- Proposed a secure communication protocol by revoking the certificates of malicious vehicles.
- Design and study of energy-efficient enhanced secure routing protocols for VANETs.
- Design and study of traffic-aware secure routing using the HEGSO algorithm for VANETs.
- Design and development of a trust model to enhance the secure communication of VANETs.

II. LITERATURE REVIEW

Wireless communication technology was initiated in the 19th century. Nowadays it has become an important and popular medium for transmitting data and information from one device to another. According to this method, data and information are carried out via air without any wire, cable, or other electronic conductors. In wireless technology, the information and data are transmitted as electromagnetic signals such as Radio Frequency (RF), Infrared (IR), and satellite communication. Due to the growth of technologies, nowadays wireless communication is used in many devices like tabs, smartphones, laptops, computers, etc., Wireless technologies have become an increasingly popular alternative in networks. Normally wireless network is not erected entirely without a cable, but it consists of wireless devices that communicate with the existing wired network. In wireless communication, the Access Points (AP) are used for the transfer of data between the wireless device or devices and the wired network. Wireless communications are connected without cables everywhere. Wireless technology is very much essential when wired cables are not suitable. The running and maintaining the cost of radio-based communication is low when compared to wired communication [46].

Wireless communication provides a lot of benefits due to increased accessibility. But, at the same time, it is sensible to a lot of security risks. Since the medium of communication is air, one can easily access the message, when the message is not encrypted by using any powerful algorithm. By using different types of attacks such as DoS attacks, replay attacks, parallel session attacks, nuisance attacks, impersonation attacks, eavesdropping attacks, and location disclosure attacks, the attackers try to attack wireless communication. When the result of these attacks is successful, it will create critical nuisance and security threats. Even if the attack is unsuccessful, it consumes the network resources and affects the authorized user. So it is very essential to provide security to the data traveling on the communication channel. Also, the communication channel can prevent attacks, while it carries data or information from one node to another [47]. The attacker may try to attack the communication medium, decrypt the message, get the plain text and also insert a duplicate message and resend it again. This type of attack may cause various problems, so it is very important to provide security in wireless communication.

In both developed and developing countries [48], the incidents related to traffic are major problems. It leads to a loss of security and confidentiality of the data. To overcome the above issues Intelligent Transportation Systems have been introduced in VANETs for safer infrastructure. It focuses on the security of the transmitted data and reduces traffic. VANETs communication is acquired by exchanging data/messages using Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. In the OBUs, they are assisted and the vehicles communicate with the other vehicles and form the MANET. It permits wireless communication, to communicate in the format of a completely distributed manner when they can connect with the RSU in an infrastructure node. For dedicated short-range communications, the wave protocol is developed based on the IEEE standard 802.11p and it operates in the 5.9GHz frequency range. VANETs should be able to broadcast some critical event information such as road accidents, traffic conditions, road conditions, etc., as early as possible and in a reliable format.

Qu et al. [49] proposed a technique to distribute the Certificate Revocation List (CRL) in a car-to-car infestation manner. In metropolitan areas the number of vehicles is high but the number of RSUs is only limited. So it is a risk to broadcast the updated CRL by using few RSUs. RSUs inspect the certificates of every running vehicle with the latest updated CRL. The node affected by the attacker node may affect other vehicles. So this information regarding the attack may be broadcasted as early as possible by using an infestation manner to reduce the load of the network, consumption of memory, and calculation for distributing, storing, and processing. Also, it is suggested that the incremental updates of a CRL should be shared with all the vehicles.

Gao et al. [50] suggested an efficient and flexible CRL distribution based on the vehicle. Based on this method each vehicle nodes get certificate revocation lists only for its respective region and its trip duration. Also, a piece of fingerprint of CRL is enclosed for the inspection of the CRL piece quickly. To alert about the updated revocation list to all the vehicles belonging to his zone, the RSU broadcasts the part of the fingerprint CRL at a certain interval. After

receiving the updated CRL piece, the vehicles verify it by analyzing the hash value, more than once to be specified by the network. The vehicles check the serial number of the revoked vehicles. This algorithm is very efficient and flexible to identify DoS-related attacks and enhance the privacy and security of vehicle nodes. But it is very complicated and time-consuming.

Umar et al. [51] proposed a simple mechanism to revoke the certificates of the malicious vehicle nodes in vehicular networks. The best method to reduce the size of CRL is compression. To compress the certificate revocation list, certain types of data structures are available. When compared with Adelson-Velskii and Landis (AVL) tree and red-black tree, the bloom filter is double time faster. The computational cost of the bloom filter is ($O(1)$) and also has a probabilistic data structure and a chance for false positives.

Kazi et al. [52] proposed a distributed cluster formation for vehicular networks called D-hop clustering for VANETs (DHCV). The DHCV algorithm creates stable clusters by using mobility information. Every node broadcast its location and speed to its immediate neighbors. Based on this information, clusters are created temporarily, using the distributed method. Since the nodes are moving, the clusters are reconstructed within a certain interval. Based on the relative mobility, every node can select its Cluster Head (CH), within its D-hop nearby vehicles for the construction of multi-hop clusters. D-hop clustering accommodates vehicles into the clusters in a non-overlapping fashion. In DHCV each vehicle is D-hops away from the CH. DHCV improves the lifetime of the cluster member and the head in the cluster.

Zhong et al. [53] introduced a protocol to preserve the security of VANETs. To achieve privacy, authentication, scalability, efficiency, and link-ability this algorithm uses two mechanisms namely Signcryption and group signature at the top of the public key infrastructure. To broadcast information, this system mainly depends on distributed RSU. Signcryption is nothing but encrypting the original message along with the signature. To join a network, the vehicle should need a secret key supplied by the RSU. Whenever vehicles request the secret key, the RSU verifies the details provided by vehicles and distributes the secret key only if it is a licit vehicle. Since it is cluster-based communication, it used group signatures to authenticate the group members. With the help of this algorithm, each node can verify the sender vehicle which exists in the network or is revoked by the CH. To reduce the computation overhead, this algorithm uses the batch verification method.

Jafer et al. [54] proposed a secure communication to broadcast the data in vehicular networks. First, it identified and categorized the various security problems during the time of communication. After that, it used layer-based architecture to avoid the amendment of data. The anonymity layer was used to anonymous the data and the encryption/decryption layer to conserve the authentication of the user. To avoid security leakages, the relay vehicle selection layer was used. The credibility layer was used to preserve the authenticity of the packet information. The transmission layer was used to take care of data transmission. The main drawback of this work is very complicated and not bothered about energy consumption.

Sharma et al. [55] established a secure message communication protocol among vehicles. The Elliptic Curve Cryptographic (ECC) algorithm was used for secure communication. The authentication was performed in two steps: in the first step, the CHs were verified by the certificate authority by exchanging a series of messages and in the second step, the vehicle nodes were verified by the authenticated CHs. Only after the successful authentication, do the CHs permit the vehicles to exchange the information. This scheme is only suited to establish secure communication in smart cities.

Punitha and Martin Leo [56] proposed location-based security in geographic Adhoc routing for vehicular networks. It is a stateless protocol, taking the decision locally by using the next hop and getting the routing path. Usually, the remotest neighbor near the receiver vehicle is selected as the next hop. This scheme assumes that the attacker node spoofs its location as the remotest neighbor vehicle. When the one hop node is selected as the remotest neighbor vehicle, the routing path information's loyal and assured for safety. When the remotest neighbor vehicle is selected as the next hop node, the relative position of the vehicle is enough to achieve the goal. Two directional antennas are used in each vehicle to collect the relative position of the vehicle. The Resource Reservation Protocol (RSVP) combines three rules to detect the attacker node and effectively remove the attacker node and protect the network from injecting malicious information.

Sun et al. [57] analyzed the energy efficiency of parked vehicles to promote connectivity in vehicular networks. The available moving vehicles in the coverage area were grouped into different clusters. The parked vehicles were used as relay nodes and placed among the clusters. The parked vehicles were responsible to guarantee the communication between the vehicles. Some external parameters were used to minimize energy usage. Even though it has reduced energy consumption, it failed to establish secure communication.

A. NEED FOR TRAFFIC-AWARE ROUTING FOR VANETs

The VANETs possess many vehicles and consider them as nodes. Since the escalating nature of technology, the information exchanges are tremendous [58]. Safety and non-safety messages are broadcasted in the vehicular networks. The safety-related messages do not tolerate any delay but the non-safety messages can tolerate minor delays. Whenever safety-related messages are exchanged it is very essential to the availability of a secure and efficient route. It is unable to send the safety messages, on time, without a secure route to the destination vehicle [59]. Most countries are struggling to solve the traffic in urban areas because it consumes a lot of economic resources and leads to a lot of problems. Due to the growth of the population and the intention of the people to live in urban areas the population becomes very high which in turn increases the number of vehicles. When all these

vehicles come to the road, automatically the traffic problems increase. Also, these traffic problems become a barrier to the growth of urban development. So it is very essential to develop the algorithms to select the apt route based on traffic and solve the traffic in urban areas.

III. PROPOSED WORK

The proposed traffic-aware protocol for the urban scenario initially determines two traffic parameters such as explicitly the average speeds and TD. This is trailed by a step in which these parameters are predicted using the 'Enhanced Exponential Weighted Moving Averaging' (EEWMA). This technique predicts the value-centered upon the present in conjunction with the past value of the traffic parameters. Optimization is based on a meta-heuristic algorithm named as Hybrid-EGSO (HEGSO) algorithm. This technique is to select the most optimum routing path between the source to destination.

Let's consider an urban network that contains a 'n' number of vehicle nodes. These vehicle nodes are estimated to travel on a highway road. In the urban area, the road segments are regarded to be distributed randomly. The road structure is considered a 2-way lane. In a 2-way lane, the vehicle nodes can travel on the same side, and in the single-way lane, the vehicles travel on both sides. urban scenario.

A. TRAFFIC PARAMETERS

Let the vehicle on the road be represented as V_i where the value of i is between 1 and n. Let R and I denote the road segment and the intersection point respectively. Consider RI to be the identification of the road segment. The average speed of the road segment's identification is essential, in ascertaining the behavior of the routing protocol. If the road segment's speed is elevated, then the delay in attaining the destination is lessened. The average speed of the road segments, identification at a specific time are given as per the Eq. 1.

$$Av_t = \frac{1}{Nr_t}\sum_{i=1}^{Nr_t} sp_t(V_t) \tag{1}$$

where Av_t implies the average speed of the identification of the road segments at time t, sp_t is the vehicle's speed present at the road segments. The TD in the urban region counts on the vehicles that are present on a road segment at a specific instance of time. The road's TD is determined using the mathematical illustration that is computed as per Eq. 2,

$$Tr_t = \alpha(\frac{V_i \times Nr_t}{L}) + \beta(\frac{d}{L}) \tag{2}$$

where T_r is the TD, α and β are constant values, L represents the length of the road segment, d denotes the average distance between the vehicles, V_i is the vehicle and Nr_t is the 'number of vehicles' at time t on the road.

B. PREDICTION OF TRAFFIC PARAMETERS

The forecast of the TD together with the average speed of the vehicles ascertained the optimal path selection. The road segments which have low TD is considered optimal route. The vehicles' average speed counts on the TD of the vehicles. When the density is found to be high, the vehicle's movement on the road will be low. The path selection of the dense road segment requires a sloppy destination reach by the source vehicle. The prediction permits the preference of the path with less traffic. This prediction process is implemented utilizing the Enhanced Exponential Weighted Moving Average (EEWMA) method.

1) ENHANCED EXPONENTIAL WEIGHTED MOVING AVERAGE(EEWMA)

The EEWMA stands as a statistical method that pertains to a constant factor that is associated with it. The general mathematical expression is shown in Eq. 3.

$$EEWMA(G_{t+1}) = \lambda G_t + (1-\lambda)EEWMA(G_t) + (G_t + G_{t-1}) \tag{3}$$

where, G_t implies the observation at time t and λ is a constant. G_{t-1} implies the observation at time t - 1.

The reason for utilizing the EEWMA is to foresee the average speeds of the vehicles in the road segments. This is essential in deciding the selection of the optimum route. The predicted average speeds are computed as per Eq. 4.

$$EV_{t+1} = \lambda(Av_t + Tr_t) + (1-\lambda)EV_t + (EV_t - EV_{t-1}) \tag{4}$$

where EV_{t+1} is the present predicted average speed of the vehicles and EV_{t-1} is the previous predicted average speed of the vehicles. EV_t is the average speed on the vehicles at time t. The value of the constant λ is chosen to utilize as per Eq. 5.

$$\lambda = 1 - exp(\frac{\Delta T}{\tau}) \tag{5}$$

where ΔT is the sampling time interval and τ is the time constant. At a time denoted as t, the present TD is centered with the road segment that is employed for the prediction of the vehicles' average speed. But for the time t+1, the values of the predicted TD together with the anticipated average speed value are unknown. These can well be computed as per Eq. 6,

$$PT_{r+1} = \lambda Tr_t + (1-\lambda)PTr_t + (PTr_t + PTr_{t-1}) \tag{6}$$

where, PT_{r+1} denotes the predicted TD, PT_{r-1} is the previously predicted TD at time t-1. The vehicle's expected speed is calculated as per Eq. 7,

$$E_{t+1}(V_i) = [Av_t(V_i) + f \times EV_{t+1}] \tag{7}$$

where, the value of f is depicted as per Eq. 8,

$$f = \frac{[Av(V_i) - Av_t]}{[Max(Av(V_i), Av_t)]} \tag{8}$$

where $Av(V_i$ is the average speed of the vehicle V_i at time t. $E_{t+1}(V_i)$ is the vehicle's average speed in the roads segment at time t+1that is predicted by EEWMA. The vehicle's predicted average speed is related to the TD. The selection of

the optimum route is aimed to select the route with minimum traffic and the shortest distance for the vehicle node V_i.

2) OPPORTUNISTIC SELECTION OF THE TRAFFIC AWARE ROUTE

The conception of optimization is introduced here because it is essential for choosing the apt path with minimal TD as well as with elevated average speed. This selection leads to the choice of the optimal route by including the average speeds of the vehicles as the fitness function in the optimization algorithm. The sort of optimization algorithm that is utilized is the HEGSO algorithm.

Hybrid Enhanced Glowworm Swarm Optimization: The traditional GSO algorithm is grounded on the behavior of the glowworm. This is rooted in the natural activities of the glowworm at night. The glowworms exhibit a sort of interaction with the other glowworms in the group based on their luciferin. If the luciferin is more, then the light emitted via the glowworm is more. Consequently, the glowworm goes towards it. There are three distinct phases explicitly luciferin update, movement, and also the neighborhood and update phase.

Algorithm 1 Proposed HEGSO Algorithm

1: **Procedure** HEGSO
2: begin: **Input:** X_i, Q, z, N_{it}, I_o, r_o.
3: Determine fitness function
4: **while** $t < N_{iy}$ **do**
5: **for** each glowworm **do**
6: $l_j(n+1) = (1-\rho)l_j(n) + \beta J_j(n+1)$
7: $x_j(n+1) = x_j(n) + Z(\frac{x_k(n)-x_j(n)}{\|x_k(n)-x_j(n)\|})$
8: $r_d(n+1) = min(r_s, max(0, r_d(n) + B(n_e - |N_j(n)|))$
9: **end for**
10: **end while**
11: Perform the crossover and mutation
12: Return X_{best}
13: **end Procedure**

In Algorithm 1, the luciferin update phase relates to the luciferin production. The quantity of luciferin is directly proportionate to the fitness of its present site on the objective function space. The secondary phase is the movement phase. In this phase, the glowworm chooses the utilization of the probabilistic means to go in the direction of a neighbor who has luciferin value above its own. The subsequent phase copes with the adaptive neighborhood range to perceive the multiple peak presences. The optimization is done by utilizing the HEGSO algorithm. The proposed work uses the hybrid algorithm wherein the HEGSO algorithm is applied furthermore the use of two genetic algorithms namely crossover and also mutation. The optimization process begins after the path is discovered between the starting and ending point of the vehicle node that is present in the road segment. The algorithm for the HEGSO algorithm is displayed as,

Step 1: Initializes the 'Eearch Agents'(EA) that is the individual glowworm X and the size of the population is denoted as Q can be specified as Eq. 9. z Indicates the step size, maximal number of iterations N_{it}, luciferin's initial value I_o, an initial value of the radial gamut of the SA r_o and time instance n are initialized.

$$X = \{x_1, x_2, \ldots .x_Q\} \tag{9}$$

Step 2: Computes the fitness function utilizing the Eq. 10.

$$F = \sum_{t=1}^{n} \frac{L}{EV_t(V_i)} \tag{10}$$

here L indicates the total length of the road segment, the average speed of the vehicles on the road is denoted as EV_t and V_i indicates the vehicle.

Step 3: The subsequent step stands as the luciferin phase. In luciferin phase, each of the new SA is computed utilizing the Eq. 11.

$$l_j(n+1) = (1-\rho)l_j(n) + \beta J_j(n+1) \tag{11}$$

where, $l_j(n)$ implies the luciferins value of the SA at time n, $l_j(n+1)$ implies the luciferins value of the SA at a time $(n+1)$, J_j implies the fitness function and β implies the luciferin decay constant with a value in the gamut [0,1].

Step 4: The objective functions of each new SA are assessed utilizing the same fitness function that is mentioned in step 2.

Step 5: Here, the SA heads for the neighboring glowworm are grounded on the brightness. The movement of the SA is ascertained by the Euclidean distance between the glowworms. In this phase of the movement, the SA heads for the calculated neighborhood grounded on a probabilistic mechanism. The movement of the glowworm is expressed as per Eq. 12.

$$x_j(n+1) = x_j(n) + Z(\frac{x_k(n) - x_j(n)}{\| x_k(n) - x_j(n) \|}) \tag{12}$$

In which, Z is the step size.

Step 6: In this step, the decision range is updated. That is the neighborhood range of the SA is updated. The decision rule is employed in this step as per Eq. 13.

$$r_d(n+1) = min(r_s, max(0, r_d(n) + B(n_e - |N_j(n)|)) \tag{13}$$

where, B implies a constant, r_s denotes the largest sensing radius of the glowworms. n_e is many outstanding SA with high luciferin values in the decision range, $r_d(n+1)$ is the updated value of the neighborhood range and r_d is the previous value of the neighborhood range.

Step 7: Confirm if the stopping norm is satisfied. If the stopping norm is met, then the best solution is obtained. If the terminating criteria are not met, then the two genetic operators explicitly crossover, and also mutation is applied. The 2-point crossover is employed. This is followed by the process of mutation in which there are certain genes. The values that are selected for the crossover operation are mutated and then combined.

IV. SIMULATION AND RESULTS

This section handles the investigation outcomes that were obtained amid the employment of the proposed traffic-aware routing for the urban VANETs system. The simulation parameters are tabulated. Moreover, the performance analysis together with the comparative scrutiny is also detailed.

A. SIMULATION PARAMETERS

The performance analysis of the proposed HEGSO is done by utilizing the Network simulator-2 (NS2). The rationale is stated as ''Comparing with that of NS3 or other simulators, which simulates only Internet models instead of wired or wireless model, is of little use in this scenario. NS3 is not backward compatible to NS2 and is still in infancy''. The road network is simulated with a hundred to five hundred vehicle nodes. The parameters which are considered are the bandwidth, simulation time, number of vehicles, and packet size. These values are given on TABLE 1.

TABLE 1. Simulation parameters used for HEGSO.

Parameter	Value
Simulator	Network Simulator2 (NS-2.34)
Simulation time	50secs
Simulation area	1000m × 1000m
Number of vehicles	500
Packet Size	1024 bytes
Transmit Power	0.660 W
Receiving Power	0.395 W
Initial Energy	50 J
Transmission Range	50 m
MAC	802.11p
Antenna Type	Omni Antenna

B. ALGORITHMS USED FOR COMPARISON

The algorithms AREOR [5], I-AREOR [6], and ARIOR [7] are used to analyze the performance of the proposed traffic-aware routing for urban VANETs. AREOR used an ant colony optimization algorithm to evaluate the quality of the packet. To establish the route, some ants will forward towards the RSU, which is near to the destination and the RSU will send back some ants to the source vehicle. The proactive model is used in VACO to maintain the route. In I-AREOR, multi-point relays are used to curtail the number of packets broadcasted in the network. To find the shortest path, the redundant, direct neighbors and set of links are neglected in this algorithm. The CH is selected based on the link reliability in ARIOR. The vehicle which possesses more link reliability is elected as the head of the cluster. To select the optimized route, the ACO algorithm is used in ARIOR. It is very complex and the E^2 delay is very high than the proposed method.

C. RESULTS AND DISCUSSION

The proposed work is simulated in an urban scenario. The result performance is validated using six metrics explicitly, End-to-End delay (E^2 delay), Packet Delivery Ratio (PDR), Energy Consumption (EC), packet drop, overhead, and throughput. The simulation results proved that the traffic-aware secure routing for VANETs using HEGSO is an effective solution to solve traffic issues in urban areas.

1) COMPARATIVE ANALYSIS

The five metrics that are calculated for the proposed work are evaluated for the other existent techniques such as AREOR, I-AREOR, and ARIOR. The TABLE 2 shows all the values that were obtained.

TABLE 2. Comparison table for the proposed scheme with the existing schemes.

Method	AREOR	I-AREOR	ARIOR	HEGSO
E^2 delay (ms)	4.8	6.72	4.27	3.75
PDR (%)	40.309	45.232	55.107	78.093
EC (mJ)	5.405	5.485	4.995	4.951
Packet drop	299	273	225	101
Overhead (μs)	19783	38840	19783	16366
Throughput (KBPS)	201	227	275	399
Varying average speed of the vehicles 10, 20, 30, 40 and 50Km/h				
Packet Drop	322	297	248	149

The TABLE 2 contrasts the performances shown by the proposed HEGSO and the prevailing VANETs routing protocol such as AREOR, I-AREOR, and ARIOR, in respect of the E^2 delay, PDR, EC, throughput, packet drop, and overhead. Considering the average end-to-end delay which is measured centered on time in seconds, the proposed HEGSO takes very less time of 3.75ms. But the prevailing methods take more time when contrasted with the proposed HEGSO. Similarly, the proposed HEGSO delivered a very good delivery ratio of 78.093% which is higher than the other prevailing methods. The proposed HEGSO also shows very less energy consumption (4.951mJ) than the AREOR, I-AREOR, and ARIOR methods. When compared with the existing method such as AREOR, I-AREOR, and ARIOR, the HEGSO scheme has fewer packet drops (101). The Table also reveals that the overhead of the HEGSO is less when compared with the existing AREOR, I-AREOR, and ARIOR methods. Hence, from the observation, it corroborates that the proposed HEGSO has high-level performance in terms of E^2 delay, PDR, EC, packet drop, and overhead.

2) E^2 DELAY

The average delay is a metric that influences the Trust-Aware Routing Protocol(TARP) performance. This metric is ascertained by employing as per the Eq. 14.

$$E^2 delay = T_s - T_f \tag{14}$$

where T_s denotes the starting time, T_f implies the ending time.

The average delay is ascertained for the HEGSO as well as other prevailing algorithms. The FIGURE 1 illustrates the performance of the proposed HEGSO with the existing AREOR, I-AREOR, and ARIOR. The proposed HEGSO has only a 3.75ms end-to-end delay. But the existing method has

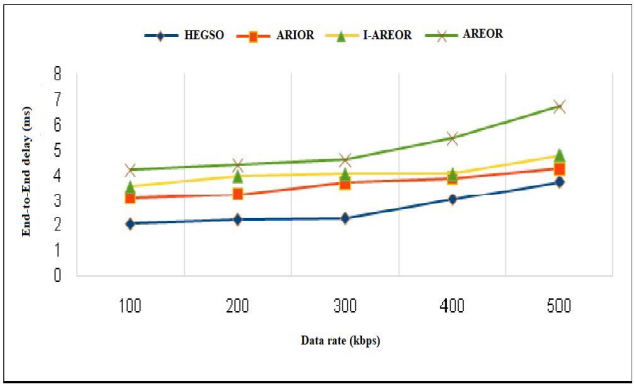


FIGURE 1. Comparison of the E^2 delay.

a high E^2 delay when compared with the proposed method. Hence, the HEGSO effectively predicted the TD, and the packets were transmitted without delay through the apt route, the E^2 delay of the proposed scheme has been declined.

3) DATA RATE VS. PDR

FIGURE 2 shows the data rate Vs. PDR for proposed and existing methods. When the transmission rate is up to 200 kbps, the proposed method delivered 98% of data packets. This is because the proposed method has identified the shortest path between the sender and receiver effectively with the help of search agents. But when the data rate increases and also in the urban scenario have more number of vehicles, the congestion becomes high. Due to this, the PDR is reduced to 78%. But compared with the existing methods, the proposed HEGSO algorithm produces a very good PDR.

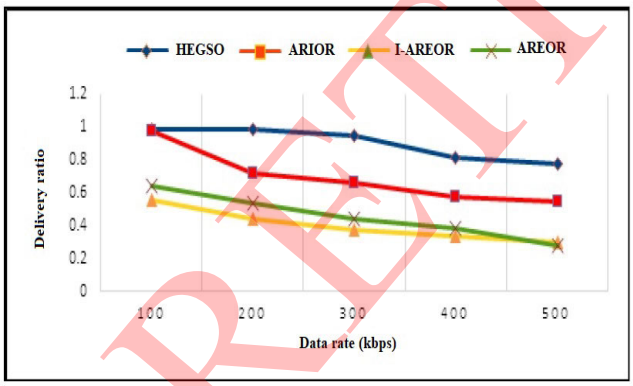


FIGURE 2. Comparison of the data rate Vs. PDR.

4) DATA RATE VS. EC

FIGURE 3 reveals the data rate Vs. EC. Compared with the existing methods AREOR, I-AREOR and ARIOR, the proposed method has less EC. This is because the proposed HEGSO protocol has effectively predicted the TD and selected the apt route for data transmission.

FIGURE 3. Comparison of the data rate Vs. EC.

5) DATA RATE VS. PACKET DROP

The FIGURE 4 shows the data rate Vs packet drop. When compared with the existing AREOR, I-AREOR, and ARIOR methods, the proposed method has a low packet drop. This is because of the optimized selection of the traffic-aware route, of the proposed method. As the packets travel on a traffic-free route the packet drop rate has decreased.

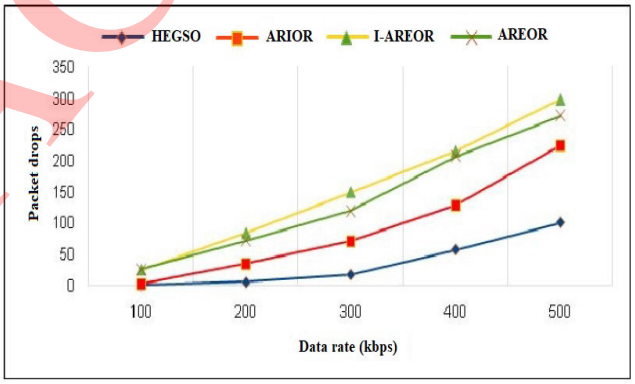


FIGURE 4. Comparison of the data rate Vs. Packet drop.

6) DATA RATE VS. OVERHEAD

The FIGURE 5 compares the performance of the proposed HEGSO with the existing methods based on data rate and overhead. The HEGSO concept is simple and by using the movement of glowworms only, it selected the optimized path between the source and destination vehicle. So compared with the existing algorithms, the proposed method has less overhead.

7) DATA RATE VS. THROUGHPUT

The FIGURE 6 demonstrates the data rate Vs throughput. EEWMA algorithm predicts the TD and average speed of the vehicle effectively to create the apt route. As the data are transmitted via the apt route, the throughput of the proposed system has been increased.

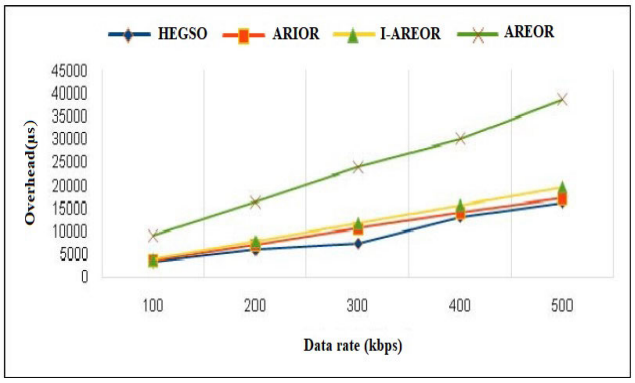


FIGURE 5. Comparison of the data rate Vs. Overhead.

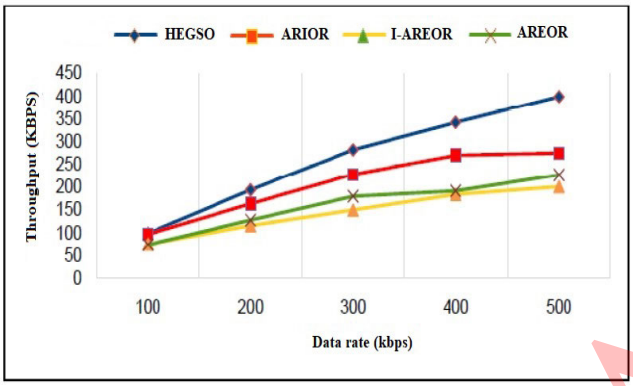


FIGURE 6. Comparison of the data rate Vs. Throughput.

8) AVERAGE SPEED VS. PACKET DROP

FIGURE 7 demonstrates the average speed vs packet drop. When compared with the existing algorithms, the proposed HEGSO method has produced less packet drop. MEWMA algorithm predicts the TD and average speed of the vehicle effectively and these two parameters are very essential to creating the apt route. As the data are transmitted via the apt route, the packet drop has decreased. Thus, it can be concluded that the proposed HEGSO provides better performance than the other methods.

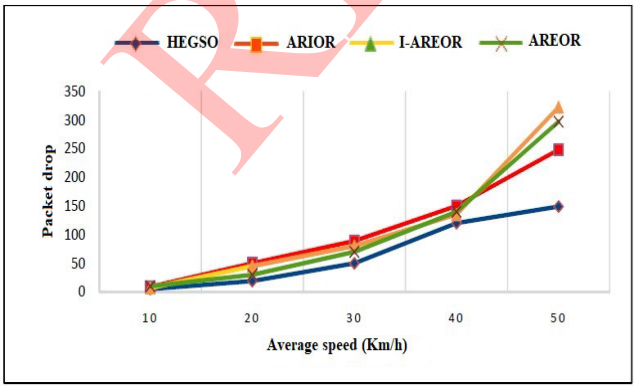


FIGURE 7. Comparison of the average speed Vs. packet drop.

9) PERFORMANCE BASED ON ATTACKERS

The proposed method evaluates HEGSO's key metrics by reducing the number of attacker nodes to 2, 4, 6, 8, and 10. Figures 8–11 show the HEGSO performance evaluation with the ARIOR and I-AREOR.

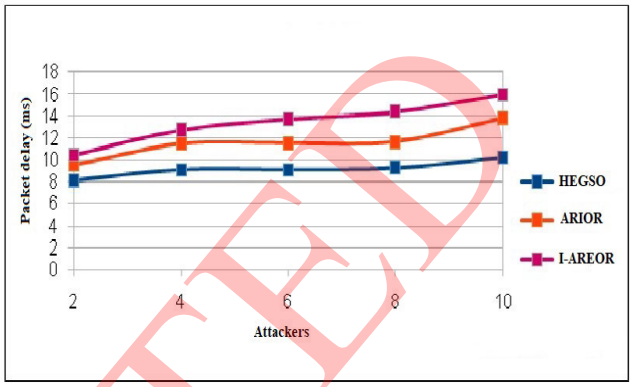


FIGURE 8. Attackers Vs. Packet delay.

Figure 8 compares the end-to-end delay of the HEGSO protocol to peer existing protocols by changing the number of attacker nodes. When compared to ARIOR and I-AREOR, the proposed HEGSO technique diminished delays by 20% and 34%, respectively. Because, the HEGSO technique chose the optimal routes between the source and destination, the packets of data arrived at their time of arrival. However, as the percentage of attackers grows, the delay time also rises.

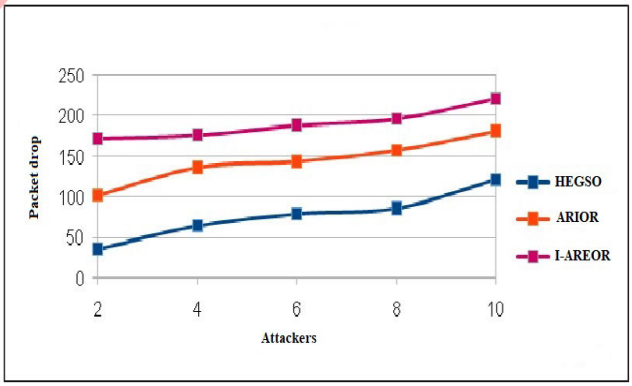


FIGURE 9. Attackers Vs. Packet drop.

Figure 9 depicts a packet drop contrast of the HEGSO technique with the ARIOR and I-AREOR. Due to the use of route discovery, the majority of data packets arrive at their destination. When there are up to six attackers, there is a lower packet delay. However, whenever the percentage of attackers continues to increase to 8–10, the drop rate has risen even more. However, it has a lower packet delay than the ARIOR and I-AREOR.

Figure 10 depicts the attackers versus energy utilization. In the HEGSO technique, the CHs quickly recognized and eliminated malicious vehicles, and they were not allowed to

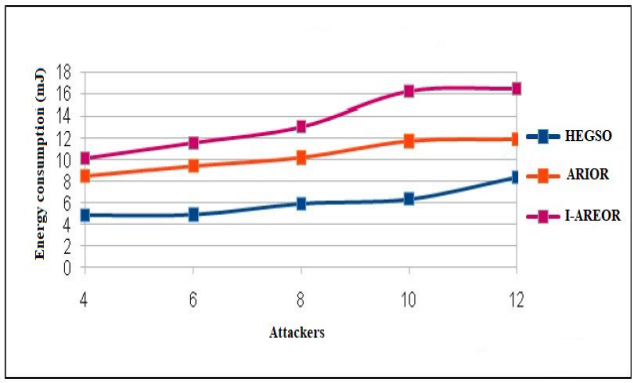


FIGURE 10. Attackers Vs. Energy consumption.

consume network services or energy. As a result, the energy usage is low when contrasted to the peer existing techniques ARIOR and I-AREOR.

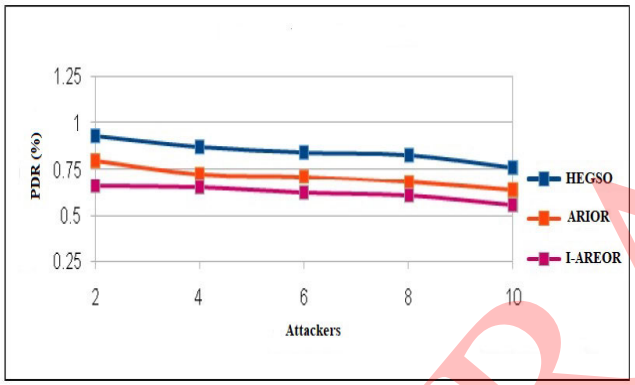


FIGURE 11. Attackers Vs. PDR.

Figure 11 shows the PDR comparison of HEGSO with the ARIOR and I-AREOR for various attacker counts. The proposed approach has a higher PDR than ARIOR and I-AREOR due to optimized path selection and immediate deportation of attackers.

V. CONCLUSION AND FUTURE SCOPE

In this paper, traffic-aware secure routing using HEGSO for urban VANETs has been proposed to establish traffic-aware routing in urban scenarios. The modified exponential weighted moving averaging algorithm effectively predicted the traffic parameters of TD and average speed. Here, the traffic parameters like the average speed along with TD were optimized using the HEGSO algorithm. From the investigation outcomes, it is noticeable that the proposed work yields a lower delay in the urban scenario. The distance and the TD also showed propitious results. This paves a way for better route acquisition and also better connectivity. The proposed one was also compared with the prevailing works. This work can well be additionally enhanced by considering more traffic parameters.

REFERENCES

[1] G. Singh, M. Prateek, S. Kumar, M. Verma, D. Singh, and H. Lee, "Hybrid genetic firefly algorithm-based routing protocol for VANETs," *IEEE Access*, vol. 10, pp. 9142–9151, 2022.
[2] P. Chithaluru, S. Kumar, A. Singh, A. Benslimane, and S. K. Jangir, "An energy-efficient routing scheduling based on fuzzy ranking scheme for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7251–7260, May 2022.
[3] P. Chithaluru, F. Al-Turjman, T. Stephan, M. Kumar, and L. Mostarda, "Energy-efficient blockchain implementation for cognitive wireless communication networks (CWCNs)," *Energy Rep.*, vol. 7, pp. 8277–8286, Nov. 2021.
[4] P. K. Chithaluru, M. S. Khan, M. Kumar, and T. Stephan, "ETH-LEACH: An energy enhanced threshold routing protocol for WSNs," *Int. J. Commun. Syst.*, vol. 34, no. 12, Aug. 2021, Art. no. e4881.
[5] G. D. Singh, S. Kumar, H. Alshazly, S. A. Idris, M. Verma, and S. M. Mostafa, "A novel routing protocol for realistic traffic network scenarios in VANET," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–12, Dec. 2021.
[6] P. Chithaluru, F. Al-Turjman, M. Kumar, and T. Stephan, "I-AREOR: An energy-balanced clustering protocol for implementing green IoT in smart cities," *Sustain. Cities Soc.*, vol. 61, Oct. 2020, Art. no. 102254.
[7] P. Chithaluru, R. Tiwari, and K. Kumar, "ARIOR: Adaptive ranking based improved opportunistic routing in wireless sensor networks," *Wireless Pers. Commun.*, vol. 116, no. 1, pp. 153–176, Jan. 2021.
[8] N. M. S. Kumar, P. K. Pagadala, V. Vijayakumar, and A. Kavinya, "Multi objective glow swarm based situation and quality aware routing in VANET," *Wireless Personal Communications*, vol. 125, pp. 879–895, Mar. 2022.
[9] N. C. Velayudhan, A. Anitha, and M. Madanan, "An optimisation driven deep residual network for Sybil attack detection with reputation and trust-based misbehaviour detection in VANET," *J. Experim. Theor. Artif. Intell.*, pp. 1–24, Aug. 2022.
[10] T. Akhtar, N. G. Haider, and S. M. Khan, "A comparative study of the application of glowworm swarm optimization algorithm with other nature-inspired algorithms in the network load balancing problem," *Eng., Technol. Appl. Sci. Res.*, vol. 12, no. 4, pp. 8777–8784, Aug. 2022.
[11] A. Carie, M. Li, B. Marapelli, P. Reddy, H. Dino, and M. Gohar, "Cognitive radio assisted WSN with interference-aware AODV routing protocol," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 10, pp. 404–4033, 2019.
[12] A. A. Khan, M. H. Rehmani, and A. Rachedi, "Cognitive-radio-based Internet of Things: Applications, architectures, spectrum related functionalities, and future research directions," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 17–25, Jun. 2017.
[13] X. Guo, Y. Chen, L. Cao, D. Zhang, and Y. Jiang, "A receiver-forwarding decision scheme based on Bayesian for NDN-VANET," *China Commun.*, vol. 17, no. 8, pp. 106–120, 2020.
[14] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020.
[15] C. Lu, Z. Wang, W. Ding, G. Li, S. Liu, and L. Cheng, "MARVEL: Multi-agent reinforcement learning for VANET delay minimization," *China Commun.*, vol. 18, no. 6, pp. 1–11, Jun. 2021.
[16] S. A. Chaudhry, "Comments on 'A secure, privacy-preserving, and lightweight authentication scheme for VANETs,'" *IEEE Sensors J.*, vol. 22, no. 13, pp. 13763–13766, Jul. 2022.
[17] J. Chen and Z. Wang, "Coordination game theory-based adaptive topology control for hybrid VLC/RF VANET," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5312–5324, Aug. 2021.
[18] G. Liu, N. Qi, J. Chen, C. Dong, and Z. Huang, "Enhancing clustering stability in VANET: A spectral clustering based approach," *China Commun.*, vol. 17, no. 4, pp. 140–151, 2020.
[19] C.-M. Huang and C.-F. Lai, "The delay-constrained and network-situation-aware V2 V2I VANET data offloading based on the multi-access edge computing (MEC) architecture," *IEEE Open J. Veh. Technol.*, vol. 1, pp. 331–347, 2020.
[20] C.-M. Huang and C.-F. Lai, "The delay-constrained and network-situation-aware V2 V2I VANET data offloading based on the multi-access edge computing (MEC) architecture," *IEEE Open J. Veh. Technol.*, vol. 1, pp. 331–347, 2020.
[21] S. Kumar, "Compartmental modeling of opportunistic signals for energy efficient optimal clustering in WSN," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 173–176, Jan. 2018.

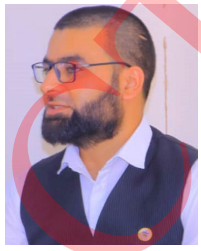
[22] H. Tan and I. Chung, "Secure authentication and key management with blockchain in VANETs," *IEEE Access*, vol. 8, pp. 2482–2498, 2019.
[23] J. Wang, H. Chen, and Z. Sun, "Context-aware quantification for VANET security: A Markov chain-based scheme," *IEEE Access*, vol. 8, pp. 173618–173626, 2020.
[24] L. E. Funderburg, H. Ren, and I.-Y. Lee, "Pairing-free signatures with insider-attack resistance for vehicular ad-hoc networks (VANETs)," *IEEE Access*, vol. 9, pp. 159587–159597, 2021.
[25] S. A. Alfadhli, S. Lu, K. Chen, and M. Sebai, "MFSPV: A multi-factor secured and lightweight privacy-preserving authentication scheme for VANETs," *IEEE Access*, vol. 8, pp. 142858–142874, 2020.
[26] R. Ahmad, R. Wazirali, Q. Bsoul, T. Abu-Ain, and W. Abu-Ain, "Feature-selection and mutual-clustering approaches to improve DoS detection and maintain WSNs' lifetime," *Sensors*, vol. 21, no. 14, p. 4821, Jul. 2021.
[27] K. Selvakumar, M. Karuppiah, L. SaiRamesh, S. H. Islam, M. M. Hassan, G. Fortino, and K.-K.-R. Choo, "Intelligent temporal classification and fuzzy rough set-based feature selection algorithm for intrusion detection system in WSNs," *Inf. Sci.*, vol. 497, pp. 77–90, Sep. 2019.
[28] J. S. Alshudukhi, B. A. Mohammed, and Z. G. Al-Mekhlafi, "Conditional privacy-preserving authentication scheme without using point multiplication operations based on elliptic curve cryptography (ECC)," *IEEE Access*, vol. 8, pp. 222032–222040, 2020.
[29] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors J.*, vol. 21, no. 2, pp. 2422–2433, Jan. 2021.
[30] E. Nisioti and N. Thomos, "Robust coordinated reinforcement learning for MAC design in sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 10, pp. 2211–2224, Oct. 2019.
[31] W. Meng, W. Li, Y. Xiang, and K. K. R. Choo, "A Bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks," *J. Netw. Comput. Appl.*, vol. 78, pp. 162–169, Jan. 2017.
[32] G. A. Ahmed, T. R. Sheltami, A. S. Mahmoud, M. Imran, and M. Shoaib, "A novel collaborative IoD-assisted VANET approach for coverage area maximization," *IEEE Access*, vol. 9, pp. 61211–61223, 2021.
[33] I. U. Din, B. Ahmad, A. Almogren, H. Almajed, I. Mohiuddin, and J. J. P. C. Rodrigues, "Left-right-front caching strategy for vehicular networks in ICN-based Internet of Things," *IEEE Access*, vol. 9, pp. 595–605, 2021.
[34] M. J. N. Mahi, S. Chaki, S. Ahmed, M. Biswas, M. S. Kaiser, M. S. Islam, M. Sookhak, A. Barros, and M. Whaiduzzaman, "A review on VANET research: Perspective of recent emerging technologies," *IEEE Access*, vol. 10, pp. 65760–65783, 2022.
[35] M. Min, W. Wang, L. Xiao, Y. Xiao, and Z. Han, "Reinforcement learning-based sensitive semantic location privacy protection for VANETs," China Communications, vol. 18, no. 6, pp. 244–260, 2021.
[36] H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, and D. Xu, "FADB: A fine-grained access control scheme for VANET data based on blockchain," *IEEE Access*, vol. 8, pp. 85190–85203, 2020.
[37] P. Chithaluru, R. Tiwari, and K. Kumar, "Performance analysis of energy efficient opportunistic routing protocols in wireless sensor network," *Int. J. Sensors, Wireless Commun. Control*, vol. 11, no. 1, pp. 24–41, May 2021.
[38] S. K. Ramakuri, P. Chithaluru, and S. Kumar, "Eyeblink robot control using brain-computer interface for healthcare applications," *Int. J. Mobile Devices, Wearable Technol., Flexible Electron.*, vol. 10, no. 2, pp. 38–50, Jul. 2019.
[39] P. Chithaluru and R. Prakash, "Organization security policies and their after effects," in *Information Security and Optimization*. London, U.K.: Chapman & Hall, 2020, pp. 43–60.
[40] P. Chithaluru, R. Tanwar, and S. Kumar, "Cyber-attacks and their impact on real life: What are real-life cyber-attacks, how do they affect real life and what should we do about them?" in *Information Security and Optimization*. London, U.K.: Chapman & Hall, 2020, pp. 61–77.
[41] P. Chithaluru, K. Singh, and M. K. Sharma, "Cryptocurrency and blockchain," in *Information Security and Optimization*. London, U.K.: Chapman & Hall, 2020, pp. 143–158.
[42] R. Prakash and P. Chithaluru, "Active security by implementing intrusion detection and facial recognition," in *Nanoelectronics, Circuits and Communication Systems*. Singapore: Springer, 2021, pp. 1–7.
[43] R. Prakash, P. Chithaluru, D. Sharma, and P. Srikanth, "Implementation of trapdoor functionality to two-layer encryption and decryption by using RSA-AES cryptography algorithms," in *Nanoelectronics, Circuits and Communication Systems*. Singapore: Springer, 2019, pp. 89–95.
[44] P. Chithaluru, R. Prakash, and S. Srivastava, "WSN structure based on SDN," in *Innovations in Software-Defined Networking and Network Functions Virtualization*. Hershey, PA, USA: IGI Global, 2018, pp. 240–253.
[45] P. Chithaluru and R. Prakash, "Simulation on SDN and NFV models through mininet," in *Innovations in Software-Defined Networking and Network Functions Virtualization*. Hershey, PA, USA: IGI Global, 2018, pp. 149–174.
[46] P. Chithaluru, T. Stephan, M. Kumar, and A. Nayyar, "An enhanced energy-efficient fuzzy-based cognitive radio scheme for IoT," *Neural Comput. Appl.*, pp. 1–23, Jul. 2022.
[47] L. Jena, L. Ammoun, and P. Chithaluru, "Supervised intelligent clinical approach for breast cancer tumor categorization," in *Augmented Intelligence in Healthcare: A Pragmatic and Integrated Analysis*. Singapore: Springer, 2022, pp. 15–40.
[48] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Challenges of future VANET and cloud-based approaches," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–15, May 2018.
[49] X. Qu, E. Liu, R. Wang, and H. Ma, "Complex network analysis of VANET topology with realistic vehicular traces," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4426–4438, Apr. 2020.
[50] Y. Gao, T. Luo, X. He, and Z. Zhang, "Cluster-based interference-free MAC protocol with load aware in software defined VANET," *China Commun.*, vol. 17, no. 12, pp. 217–234, Dec. 2020.
[51] M. Umar, S. H. Islam, K. Mahmood, S. Ahmed, Z. Ghaffar, and M. A. Saleem, "Provable secure identity-based anonymous and privacy-preserving inter-vehicular authentication protocol for VANETS using PUF," *IEEE Trans. Veh. Technol.*, vol. 70, no. 11, pp. 12158–12167, Nov. 2021.
[52] A. K. Kazi, S. M. Khan, and N. G. Haider, "Reliable group of vehicles (RGoV) in VANET," *IEEE Access*, vol. 9, pp. 111407–111416, 2021.
[53] H. Zhong, J. Wen, J. Cui, and S. Zhang, "Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET," *Tsinghua Sci. Technol.*, vol. 21, no. 6, pp. 620–629, 2016.
[54] M. Jafer, M. A. Khan, S. Ur Rehman, and T. A. Zia, "Evolutionary algorithm based optimized relay vehicle selection in vehicular communication," *IEEE Access*, vol. 6, pp. 71524–71539, 2018.
[55] S. Sharma, A. Dua, M. Singh, N. Kumar, and S. Prakash, "Fuzzy rough set based energy management system for self-sustainable smart city," *Renew. Sustain. Energy Rev.*, vol. 82, pp. 3633–3644, Feb. 2018.
[56] A. Punitha and J. M. L. Manickam, "Privacy preservation and authentication on secure geographical routing in VANET," *J. Experim. Theor. Artif. Intell.*, vol. 29, no. 3, pp. 617–628, May 2017.
[57] G. Sun, L. Song, H. Yu, V. Chang, X. Du, and M. Guizani, "V2V routing in a VANET based on the autoregressive integrated moving average model," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 908–992, Jan. 2019.
[58] J. Kang, Y. Elmehdwi, and D. Lin, "Slim: Secure and lightweight identity management in VANETs with minimum infrastructure reliance," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.* Cham, Switzerland: Springer, Oct. 2017, pp. 823–837.
[59] R. Tanwar, S. Balamurugan, R. K. Saini, V. Bharti, and P. Chithaluru, Eds., *Advanced Healthcare Systems: Empowering Physicians with IoT-Enabled Technologies*. Hoboken, NJ, USA: Wiley, 2022.

PRATIMA UPADHYAY is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering, Amity University, Gwalior, Madhya Pradesh, India. Her research interests include addressing data security and privacy in smart infrastructure, machine learning, AI, and the IoT.

VENKATADRI MARRIBOINA is currently working as a Professor and the Head of the Department of Computer Science and Engineering with the Amity School of Engineering and Technology, Amity University, Madhya Pradesh. He published more than 40 research papers in international journals and conferences and published three Indian patents. He served as an Editor for *Communications in Computer and Information Science* (Springer) and *Smart and Innovative Trends in Next Generation Computing* (Vols. 827 and 828, Indexed by Scopus) and a Guest Editor for the SCIE and Scopus-Indexed Journal *Smart and Innovative Trends for NexGen Computing and Communications*. His research interests include machine learning algorithms, data mining, and artificial intelligence.

SHIV KUMAR (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from Banasthali University, Tonk, Rajasthan, in 2012. He is currently working as the Director of the Lattice Science Publication-A Publisher for Periodical Journals, the Chairman of Lattice Science-A Bibliographic Database, and a member of the Elsevier Advisory Panel, since March 2019. He is an editor-in-chief of more than 45 international journals. He has 50 articles in international journals, 19 papers in international conferences, and 13 papers in national conferences. His research interests include voice signal compression, tonality computation of voice signal, and image processing.

SUNIL KUMAR received the B.Tech. degree in CSE from Kurukshetra University, Kurukshetra, in 2006, the M.Tech. degree in CSE from MMU, Ambala, in 2011, and the Ph.D. degree from the University of Petroleum and Energy Studies, Dehradun, India, in 2021. He is currently an Assistant Professor (Selection Grade) in cybernetics cluster with the School of Computer Science, University of Petroleum and Energy Studies (UPES), Dehradun. He has more than 16 years of teaching experience at reputed NAAC accredited universities such as the University of Petroleum and Energy Studies, Dehradun (NAAC accreditation A). He has published more than 20 research articles (including SCOPUS and SCI indexed publications) and the edited/authored various books/book chapters. He served as a reviewer for various journals and conferences. His research interests include WSN, deep learning, the IoT, meta-heuristic optimization, and data mining. He is a Founder Member of the OPEN Community under the University of Petroleum and Energy Studies.



MOHD ASIF SHAH received the B.A., M.A., and Ph.D. degrees with sound teaching and research skills.

He is currently working as an Associate Professor with Bakhtar University (IACBE Accredited), Kabul, Afghanistan. He has been earlier working as an Assistant Professor at the FBS Business School, Bengaluru, Karnataka, India, and Lovely Professional University, Punjab, India (AACSB Accredited). He was served as a Lecturer at the Jamia College of Education and also helped his department with teaching assistance during the Ph.D. He has published more than forty research papers (SCI/WOS/UGC Indexed) with thirty-two citations, the H-index is four (Google Scholar). He has attended more than thirty workshops and faculty development programs sponsored by the Government of India and other agencies. Else than this, he has an excellent grasp of the subject material, with more than five years of using platforms such as CANVAS, LMS, and UMS for online teaching.