Privacy Preserving Partially Homomorphic Encryption with Optimal Key Generation Technique for VANETs

Tamilarasi G (prithvi6781@gmail.com)
Alagappa University
Rajiv Gandhi K
Alagappa University
Palanisamy V
Alagappa University

Research Article

Keywords: VANETs, Security, Privacy, Homomorphic encryption, Optimal key generation, Levy flight, GOA

Posted Date: August 13th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-743381/v1

Privacy Preserving Partially Homomorphic Encryption with Optimal Key Generation Technique for VANETs

G.Tamilarasi[1,*] Dr.K.Rajiv Gandhi[2] Dr.V.Palanisamy[3]

[1,*]Research Scholar, Department of Computer Applications, Alagappa University, Karaikudi 630004 , Tamilnadu, India

[2]Assistant Professor, Department of Computer Science, Alagappa University Model Constituent College, Paramakkudi - 623707 , Tamilnadu, India

[3]Professor & Head, Department of Computer Applications, Alagappa University ,Karaikudi- 630003 , Tamilnadu, India

[1]prithvi6781@gmail.com [2]dr.krajiv.84@gmail.com [3]vpazhanisamy@yahoo.co.in

*Corresponding Author: **G. Tamilarasi ,** prithvi6781@gmail.com

Abstract

In recent days, vehicular ad hoc networks (VANETs) has gained significant interest in the field of intelligent transportation system (ITS) owing to the safety and preventive measures to the drivers and passengers. Regardless of the merits provided by VANET, it faces several issues, particularly with respect to security and privacy of users/messages. Because of the decentralized structure and dynamic topologies of VANET, it is hard to detect malicious or faulty nodes or users. With this motivation, this paper designs new privacy preserving partially homomorphic encryption with optimal key generation using improved grasshopper optimization algorithm (IGOA-PHE) technique in VANETs. The goal of the proposed IGOA-PHE technique aims to achieve privacy and security in VANET. The proposed IGOA-PHE technique involves two stage processes namely ElGamal public key cryptosystem (EGPKC) for PHE and IGOA based optimal key generation process. In order to improve the security of the EGPKC technique, the keys are optimally chosen using the IGOA. Besides, the IGOA is derived by incorporating the concepts of Gaussian mutation (GM) and Levy flights. The experimental analysis of the proposed IGOA-PHE technique is examined in a wide range of experiments. The resultant outcomes exhibited the maximum performance of the presented IGOA-PHE technique over the recent state of art methods.

Keywords: VANETs, Security, Privacy, Homomorphic encryption, Optimal key generation, Levy flight, GOA

1. Introduction

Vehicle ad hoc networks (VANET) are developed as a part of Mobile Adhoc Network (MANET) [1, 2] applications. VANET is deliberated as a significant method for intelligent transportation systems (ITS) [3]. Recently, VANET was an emphasis of many scientists in the field of wireless mobile transmission. The goal of VANET has to give an inter vehicle transmission and road side unit (RSU) to vehicle transmission for increasing safety of the road and enhance local traffic flow and the performance of road traffic via giving timely and accurate data to road clients [4]. In VANET, vehicle is utilized as network nodes, as shown in Fig. 1. The OBU & RSU in VANET develops a link between itself using dedicated short range communication (DSRC) from the single/multi hop transmission [5]. VANET offers many applications and services to the user, all of them are involved by infotainment, navigational aid, and security of the driver [6].

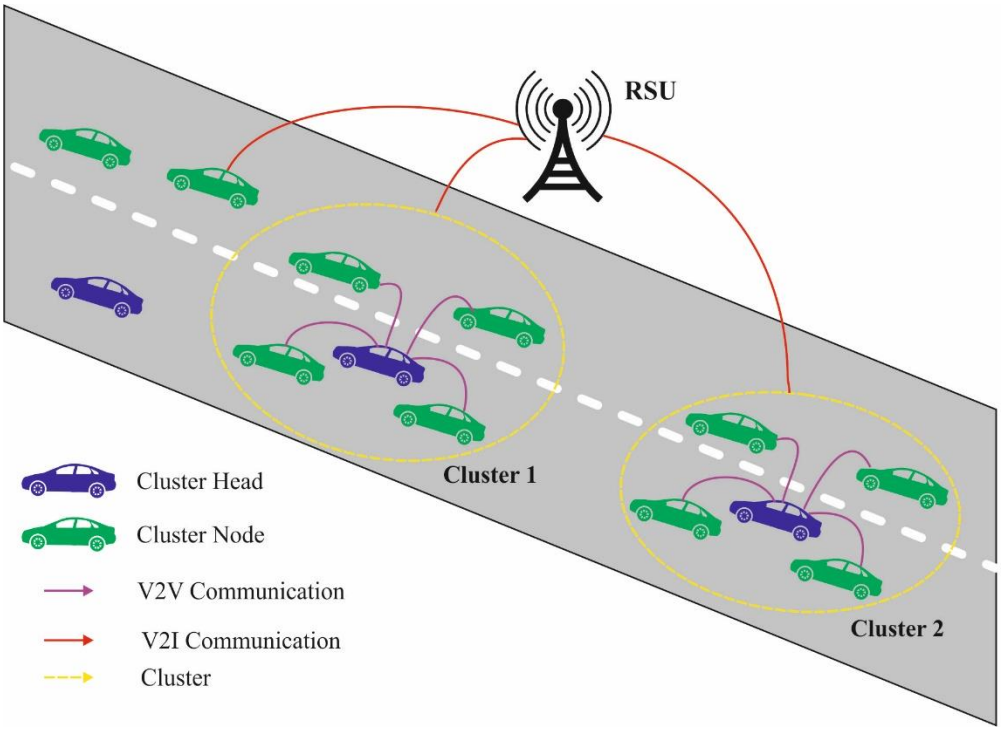

Fig. 1. Structure of VANET

Though the interest around the significant advantages of VANET is developing, the dynamic nature of VANETs (vehicle could leave & join willingly) together a multitude of scheme and application interrelated requirement makes it highly difficult for designing an effective method to ensure vehicle privacy [7]. Privacy represents vehicle privacy (driver) and vehicle position. If a vehicle sends a message, nobody (but appropriate authority) can define the position/identity

of the vehicle from the message a vehicle transmits. Simultaneously, whole messages transmitted by the vehicle must be valid beforehand processed further. Till this problem is resolved to the optimal fulfillment of the user, extensive placement of VANET could not be performed. Verification should be attained at 2 levels, initially at node level, represents node verification, and next at message level represents message verification [8].

The fundamental standard of message authentication could be shortened by signing a message by the sender and later verify the integrity & authenticity of the message at the receiver end. Particular verification needs like scalable and strong authentication, effective and scalable certificate revocation, lower computation overhead should be tackled and resolved for ensuring secure transmission in VANET. Guaranteeing privacy of vehicle (driver) is a major problem in which an effective solution should be made or else an adversary can track vehicles traveling route by analysing and capturing it message [9] and identify the vehicle (driver) might contain serious impact for the drivers.

To tackle this problem, several scientists have projected procedures where vehicles can utilize pseudonym rather than their real identity in transmission simultaneously allowing authorities for extracting the real identity from pseudonyms to punish and trace mischievous vehicles [10]. This protocol is known as conditional privacy-preserving protocol. Allocating pseudonyms to vehicles and modifying them regularly is another approach utilized for ensuring privacy of the vehicle. For maximizing privacy, vehicles should modify pseudonyms more often though the occurrence of these changes remains uncertain. Features like storage size and availability play a significant part in defining the rate whereat the pseudonym must be modified [11]. Most of the studies in the survey tackling privacy, security, and authentication utilize TA to obtain and load OBU & RSU by security variables like pseudonyms, keys, and certificates. Fig. 2 illustrates the secure data transmission in VANET.

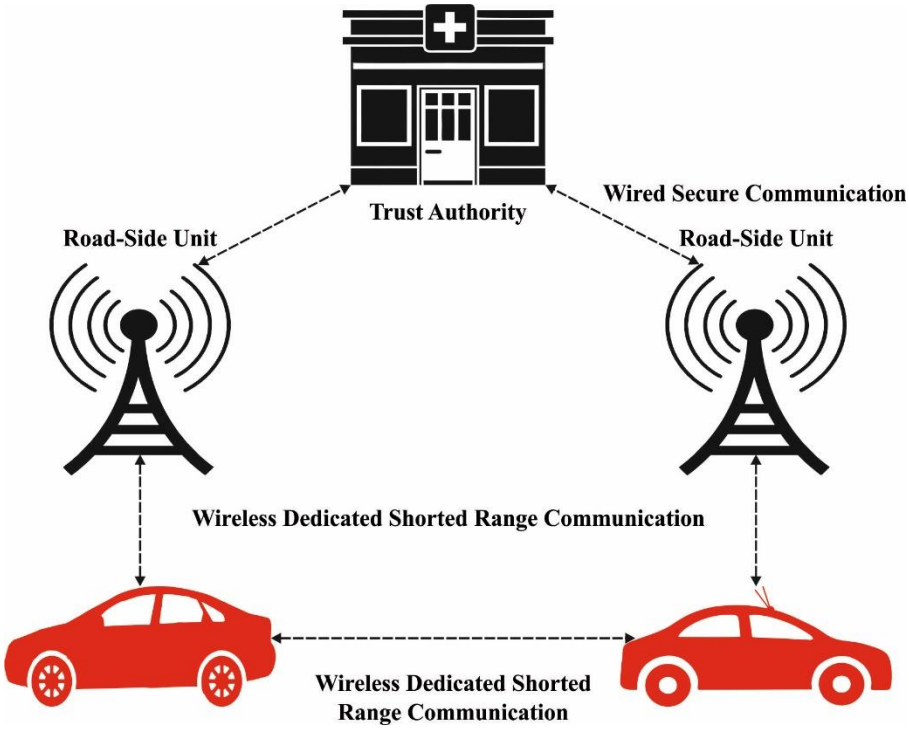

Fig. 2. Secure data transmission in VANET

Conventional methods to authenticate and secure message dissemination, mainly depending upon key management and message encryption, could assure secure message interchange among destination pair and known sources. This method cannot directly be employed in terms of VANET because of the dynamics of VANET. Message dissemination in VANET could be susceptible to insider attacks (viz., attacks from valid VANET members), that might damage the content of disseminated message or transmit malicious message. Therefore, guaranteeing the authenticity & integrity of the transferred message in VANET is a significant problem.

This paper designs new privacy preserving partially homomorphic encryption with optimal key generation using improved grasshopper optimization algorithm (IGOA-PHE) technique in VANETs. The goal of the proposed IGOA-PHE technique aims to achieve privacy and security in VANET. The proposed IGOA-PHE technique involves two stage processes namely ElGamal public key cryptosystem (EGPKC) for PHE and IGOA based optimal key generation process. To improve the security of the EGPKC technique, the keys are optimally chosen using the IGOA. Above and beyond, the IGOA is derived by incorporating the concepts of Gaussian mutation and Levy flights. For assessing the security results of the proposed IGOA-PHE technique, a wide range of simulations were performed and the results are investigated under several measures. The

2. Related works

Al-Shareeda et al. [12] presented a VANET based privacy preserving communication scheme (VPPCS) that meets the requirement for contextual & content privacy. It leverage the elliptic curve cryptography (ECC) as well as identity based encryption system. They have executed comprehensive security analyses (random oracle module, BAN logic, security attribute, and security of proof) to verify and validate the presented system. The analyses have displayed that this system is secure and also displayed to be efficient in a calculation. Cui et al. [13] proposed an effective and privacy preserving data downloading system for VANET, depending upon the edge computing model. In the projected system, an RSU could detect the common data by examining the encrypted request transmit from neighbouring vehicles with no need for sacrificing the privacy of their downloaded request. Additionally, the RSU stores the common data in near qualified vehicle named ECV. When a vehicle needs to upload the current data, it could upload it directly from the adjacent ECV. This technique raises the uploading performance of the scheme.

Alfadhli et al. [14] proposed a light weighted multi factor verification and privacy preserving security solution for VANET. Additionally, it removes the heavyweight dependency on the scheme key through decentralizing the broad area of CA to local areas and attains strong controller of the domain key. Ali and Li [15] proposed an effective ID-CPPA signature system depending upon bilinear map for V2I transmission. This raises the efficacy by signing and authentication of message at the RSU is executed. Moreover, this ID CPPA signature system supports the batch signature authentication technique, that decreases the computation overhead on RSU thus allows it for authenticating a huge amount of traffic interrelated messages in many vehicles in area with higher traffic density.

Wang et al. [16] proposed a novel identity based anonymous authentication system. In this system, the master key of the system won't be directly set up in TPD. For generating private key of the vehicle, further privacy is needed, and this privacy is given using RSU. Thus, revoking a malicious vehicle in VANET is effective, hence the RSU should end making the current privacy for the vehicle. Additionally, the signature authentication method includes no bilinear pairing operation, creating the authentication procedure highly effective. Wang et al. [17] proposed a hybrid CPPA protocol depending upon PKI certificate and identity based signature. In this system approach, the TA allocates the exclusive long term certificate for all the listed nodes. Vehicles with valid certificates could employ the anonymous short term

identity in the present RSU for signing security relevant messages. The identity based signatures avoid CRL checking and the complicated bilinear paring operations.

Moni and Manivannan [18] proposed a privacy preserving authentication, scalable, distributed, low overhead system for VANET. This method utilizes MHT to authenticate RSU and MMPT for verifying the vehicles. In Benarous et al. [19], a novel privacy preserving solution for pseudonym on-road on-demand refilling is presented whereas the vehicle anonymously authenticates itself to the local authority subsidiaries of the central trusted authority for requesting a novel pseudonyms pool. This technique contains challenge based authentication and anonymous ticket. Al-shareeda et al. [20] presented an identity based CPPA system that supports the batch authentication procedure for the concurrent authentication of many messages with every node.

3. The Proposed IGOA-PHE Technique

The overall working principle involved in the proposed IGOA-PHE technique is here. It is stated that the IGOA-PHE technique follows a 2-stage process namely EGPKC for PHE and IGOA based optimal key generation process. These processes are neatly elaborated in the following subsections.

3.1. Design of EGPKC Technique

Generally, it is stated in 1985 using discrete method cause problems to constrained areas (partial HE technique). It has key decryption, generation, and encryption operations. Usually, this technique has private key (an arbitrary amount) $xi \in Zi^{*}_{\mathrm{qi}'}$ by its corresponding public key $yi \equiv (\mathrm{g}i')^{xi}\ mod\ qi$, whereas g$i'$ identify the generator to Gi_1 using prime order qi'. Therefore, the novel involvement, to optimize the corresponding private key with the help of new hybrid method. An optimization handles creation of an optimum key this indeed enhances and states the security emergency. Moreover, an encryption message m$i \in Gi_1$ & public key yi is determined by $ci_1 \equiv (\mathrm{g}i')^{\mathrm{n}}\ mod\ qi$, $ci_2 \equiv yi^{ri}\mathrm{m}i\ mod\ qi$, whereas ri denotes random amount. Likewise, the decryption ciphertext $\{ci_1, ci_2\}$ & private key xi is determined by $mi \equiv ci_2\left(ci_1^{xi}\right)^{-1}\ mod\ qi$.

Most of this technique takes an equivalent ciphertext by selecting a plaintexts attack for every probabilistic polynomial time adversaries Ai. Also, the message encrypting arbitrarily in two

different messages assured by Ai, to identify the elected message is increased to random resolving. For considering, the ElGamal cryptosystem is determined by the game module with the challenger Ci and opponent Ai.

- Initially, Ai elects two separate messages as $\mathrm{m}i_0$, $\mathrm{m}i_1 \in Gi_1$ and forward it to Ci'.
- After, this technique calculates Ci' elects $ai \in \{0,1\}$ and ri_1, $xi \in Zi^*_{qi'}$ arbitrarily and set $yi \equiv (\mathrm{g}i')^{xi}\ mod\ qi$, $ci_1 \equiv (\mathrm{g}i')^{ri} modqi$ and $ci_2 \equiv (\mathrm{g}i')^{rixi}\mathrm{m}i_{ai}\ mod\ qi$. Likewise, Ci' provide Ai as $\mathrm{g}i'$, yi, ci_1, & ci_2.
- The calculated challenge Ci' analyses Ai on ai.
- For calculating a guess as Ai provides ai' and forward it return to Ci'.

Now, Ai becomes a success when $ai' = ai$ otherwise fails.

In Above mentioned game, consider Ai recognizes gi', $(\mathrm{g}i')^{\mathrm{x}i}$, $(\mathrm{g}i')^{ri}$ & $(\mathrm{g}i')^{xiri}\mathrm{m}i_{ai}$ but Ai cannot get right access for xi and ri'. Now, the success possibility of probabilistic polynomial time challenger Ai for achieving ai is high to random guessing as given in Eq. (1):

$$Pi\ [ai' = oi] = \frac{1}{2} + negl \tag{1}$$

In Eq. (2), Pi denotes success possibility and $negl$ represent trivial improvement. Eventually, the ciphertext along with an optimum private key is revealed in MAC.

Generally, the MAC frames are modelled to maintain minimal sophisticated form by a sufficient strength for declaring stable transmission on the noisy channel. Also, each successive protocol layer is added to the frame from layer specific footers & headers. The MAC structure has four frames.

- Initially, the beacon frame, employed with the coordinator to transfer beacons.
- In 2nd, the data frame, utilized to broadcast the whole data.
- In 3rd, the acknowledgment is used for assuring the efficient frame is delivered.
- Laslty, the MAC command frame is utilized for managing the whole MAC peer entity control transmissions.

Now, the data frames transmit the MAC payload and aforementioned procedure is finished in the data frame. MAC payload executes the ciphertext with corresponding transmissions and

private keys. On the recipient side, an equal decoder process takes place and eventually, attains the original data.

3.2. Design of IGOA for Optimal Key Generation

The private key in ElGamal cryptosystem is enhanced to accomplish the accurate ciphertext. A novel technique is developed; where it is implemented to create the ciphertext using numerical values. In general, the proposed ciphertext has numbers (1, 2, 3. . .), alphabets $(\mathrm{a}, \mathrm{A}, \mathrm{b}, \mathrm{D}, \ldots)$ and special characters$(!, @, *, \ldots)$. Based on the penalty is set, (i) once the ciphertext using numeric values are attained, penalty $= 0$ (ii) after the ciphertext is attained with alphabetical and special characters, penalty could reduce in interval. The aim is to achieve a decreased penalty (given in Eq. (2), e.g., the ciphertext should be in numerical values.

$$Ob = Min(penalty) \tag{2}$$

Grasshopper is deliberated as pest depending upon the loss they impose on vegetation and crops. In place of performing separately, grasshopper creates few biggest swarms amongst all living beings. The impact of an individual in a wind, swarm, food source, and gravity affects swarm motion. The GOA is a new SI based metaheuristic method that is stimulated using longer range and sudden movement of adult grasshoppers in a group. Metaheuristic algorithm reasonably separates the search procedure as to exploitation & exploration phases. The longer range and sudden motions of the grasshopper denote exploration stage, and local motions for searching for an optimal food source represent exploitation stage. A numerical module for this behavior is given in Mirjalili [21] can be denoted as:

$$x_i = S_i + G + A, \tag{3}$$

Whereas x_i denotes location of i grasshopper, S_i indicates social interaction in a group, G represents force of gravity performing on i grasshopper, and A signifies wind direction. By extending S_i, G & A in (1), the formula is given by:

$$x_i = \sum_{j=1, j\neq i}^{N} s\left(|x_j - x_i|\right)\frac{x_j - x_i}{d_{ij}} - g\hat{e}_g + u\hat{e}_w, \tag{4}$$

Whereas $s(r) = fe^{-r/l} - e^{-r}$ denotes function stimulate the influence of social interaction and N represents amount of grasshopper. $g\hat{e}_g$ Indicates extended G element, while g signifies gravitational force and $\hat{e}_g$ denotes unit vector directing to the center of earth. $u\hat{e}_w$ Represents

extended A element, let u denotes constant drift and $\hat{e}_w$ indicates unit vector directing in the wind direction. d_{ij} denotes distance among the i & j grasshopper and estimated by [22]:

$$d_{ij} = |x_j - x_j|.$$

Since grasshoppers rapidly detect comfortable zone and show poor convergence, the impacts of wind and gravity are far weaker compared to the relationship among grasshoppers, means numerical module must be altered by:

$$x_i = c\left(\sum_{j=1, j\neq i}^{N} c\frac{\mathrm{ub} - \mathrm{lb}}{2} s\left(|x_j - x_i|\right)\frac{x_j - x_i}{d_{ij}}\right) + \hat{T}_d, \tag{5}$$

Whereas ub & lb represents upper & lower boundaries of the search space, T_d indicates value comparative to the target (optimal solution establish until now), and c denotes reducing coefficient which balance the process of explorations & exploitations can be denoted by:

$$c = c_{\max} - iter\ \frac{c_{\max} - c_{\min}}{\mathrm{Max}_{\mathrm{iter}}}, \tag{6}$$

Whereas $c_{\max}$ denotes maximal value (equivalent to one), $c_{\min}$ represents minimal value (equivalent to 0.00001), iter indicates present iteration, and $\mathrm{Max}_{\mathrm{iter}}$ signifies maximal amount of iterations.

Algorithm 1: Pseudo code of GOA
Initialize Begin the swarm $X_{\mathrm{i}}(i = 1,2, \ldots, \mathrm{n})$, Initiate $cmax$, $cmin$ and maximal amount of iterations; Evaluate the fitness of every search agents; T = optimal search agent; while ($l \leq Max$ amount of iterations) Upgrade c; for every search agents

```
            Regulate the distance among grasshoppers in [1,4];
            Upgrade the location of the present search agent;
            Bring the present search agent back when it drives outside the boundaries;
        end for
        Upgrade T when it has an optimal solution;
        l = l + 1;
    end while
    return T;
End
```

Fig. 3 demonstrates the flowchart of GOA. In IGOA, to confront the drawback of fundamental GOA, GM and Levy flight are presented to GOA for keeping an appropriate balance among the exploitation & exploration.

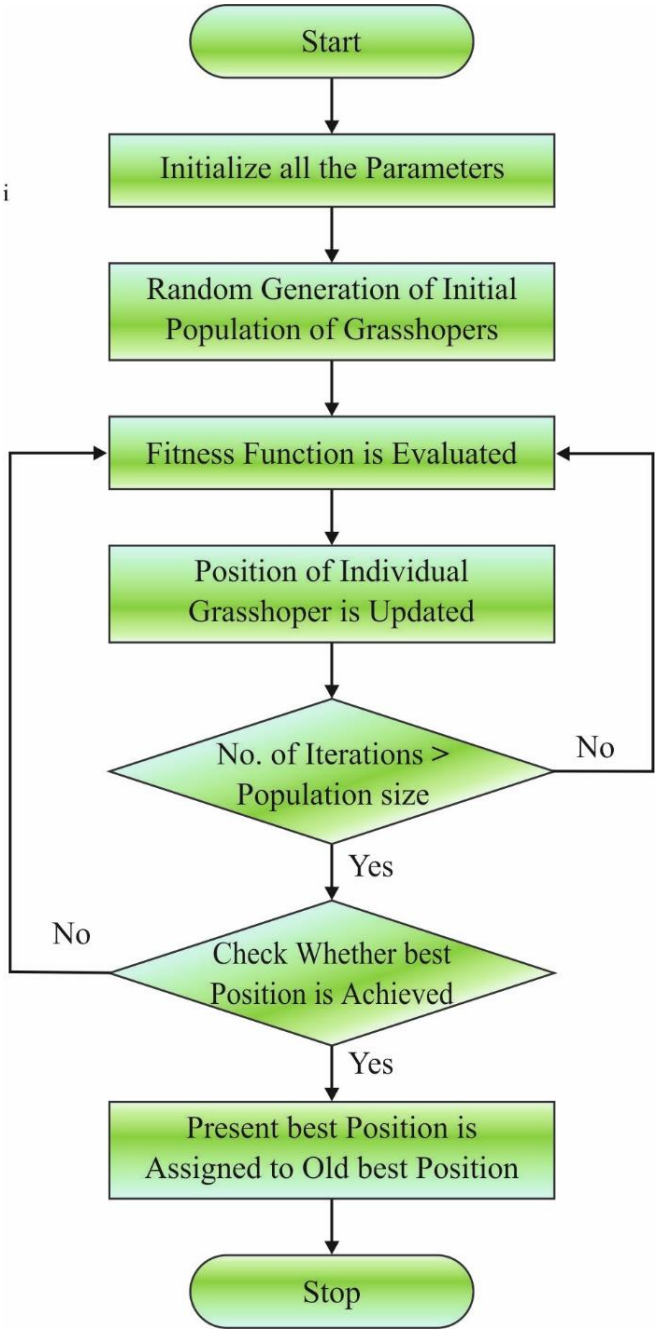

Fig. 3. Flowchart of GOA

The GM function was derived from Gaussian normal distribution and thier applications to evolution search [23]. This concept was represented by classical evolutionary programming (CEP). It is highly possible for creating a novel offspring nearby the original parent due to its narrow tail. Because of this, the search formula would take small steps permitting all the corners of the search space to be examined well. Henceforth it is predictable for providing comparatively fast convergence. The Gaussian density operation can be denoted as:

$$f_{gaussian(0,\sigma^2)}(\alpha) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{\alpha^2}{2\sigma^2}} \quad (7)$$

Whereas σ^2 denotes difference for every member of the population. This operation is additionally decreased for generating a single *n*-dimension arbitrary parameter by locating the mean value to 0 and SD to one. The arbitrary parameter created is employed for the common formula of metaheuristic method can be denoted by

$$X_i^d = X_i \oplus G(\alpha) \quad (8)$$

where $G(\alpha)$ denotes Gaussian step vector made by Gaussian density function using α as Gaussian arbitrary amount among zero and one.

LF was initially presented by the French mathematician in 1937 called Paul Levy. A varied kind of natural and artificial phenomena are defined based on Levy statistics. The LF is a well-regarded class of stochastic non Gaussian walks that step length value must be distributed regarding Levy stable distribution. It is obtained as:

$$Levy(\beta) \sim u = t^{-1-\beta}, 0 < \beta \leq 2 \quad (9)$$

β denotes significant Levy index for adjusting the stability. The Levy arbitrary amount is estimated using:

$$Levy(\beta) \sim \frac{\varphi \times \mu}{|\mathrm{v}|^{1/\beta}} \quad (10)$$

Whereas μ & v denotes regular distribution, Γ represents normal Gamma function, $\beta = 1.5$, & φ is given by:

$$\varphi = \left[\frac{\Gamma(1+\beta) \times \sin\left(\pi \times \frac{\beta}{2}\right)}{\Gamma\left(\left(\frac{1+\beta}{2}\right) \times \beta \times 2^{\frac{\beta-1}{2}}\right)} \right]^{\frac{1}{\beta}}. \quad (11)$$

For obtaining a tradeoff among the exploitation and exploration abilities of metaheuristic method, LF method is utilized for updating search agent location that can be given by:

$$X_i^{levy} = X_i + r \oplus levy(\beta) \quad (12)$$

where X_i^{levy} denotes novel location of ith search agent X_i afterward upgrading and r denotes random vector in zero and one $\oplus$ indicates dot product (entry wise multiplication).

As mentioned, the range of search agents is critical for metaheuristic method, since diversity provides the population a robust search ability to global optimal. In IGOA, GM method has been applied for increasing the range of GOA population. The altered numerical module is introduced by:

$$X_i^d = c\left(\sum_{\substack{j=i \\ j\neq i}}^{N} c\frac{ub_d - lb_d}{2} s\left(|x_j^d - x_i^d|\right)\frac{x_j - x_i}{d_{ij}}\right) \oplus G(\alpha) + \widehat{T_d}. \tag{13}$$

Afterward the location of ith grasshopper X_{i} is upgraded, Levy flight method would be adapted for generating a novel candidate solution that can be given by:

$$\mathrm{X}_i^{levy} = \mathrm{X}_i^* + rand(d) \oplus levy(\beta) \tag{14}$$

$$\mathrm{X}_i^{t+1} = \begin{cases} \mathrm{X}_i^{levy} \; fitness\left(\mathrm{X}_i^{levy}\right) > fitness(\mathrm{X}_i^*) \\ \mathrm{X}_i^* \; otherwise \end{cases} \tag{15}$$

whereas X_i^* denotes novel location of ith grasshopper afterward upgrading and $rand(d)$ denotes d-dimension arbitrary vector is zero and one. Since Levy flight is an arbitrary procedure where the jump size follows the Levy likelihood distribution functions, the novel candidate solution is made using Levy flight method is a higher likelihood of jumping beyond local optimal and attains optimum solutions. For ensuring the population quality, search agents using high fitness would be retained in the population.

4. Performance Validation

This section validates the performance of the proposed IGOA-PHE technique with other techniques interms of different measures.

Table 1 and Fig. 4 investigates the encryption time analysis of the IGOA-PHE technique with other encryption algorithms. The experimental outcomes demonstrated that the AES and RSA techniques have accomplished poor outcomes with the higher encryption time of 329ms and 338ms. At the same time, the ECC and Blowfish-ODHO techniques have gained slightly

reduced encryption time of 276ms and 258ms respectively. But the IGOA-PHE technique has required a minimum encryption time of 243ms.

Table 1 Result analysis of Encryption Time

Algorithms	**Encryption Time (ms)**
AES	329
RSA	338
ECC	276
Blowfish-ODHO	258
IGOA-PHE	243

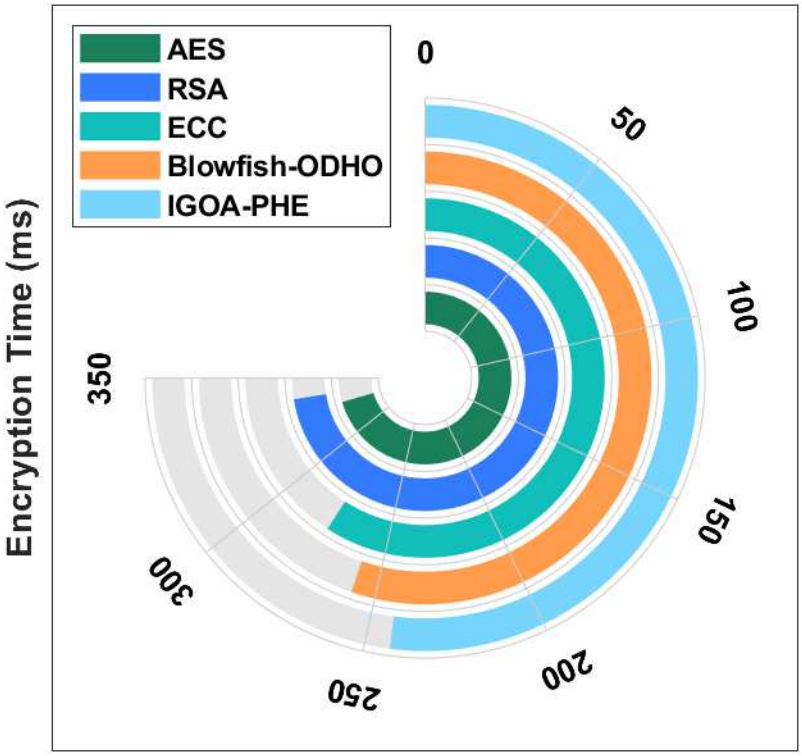

Fig. 4. Encryption time analysis of IGOA-PHE model

Key similarity analysis of the proposed IGOA-PHE technique with other encryption algorithms under different attacks is provided in Table 2 and Fig. 5. The resultant values demonstrated that the IGOA-PHE technique has showcased effective outcomes under all different types of attacks. Under the presence of DoS attack, the IGOA-PHE technique has accomplished a lower key similarity of 11.06% whereas the AES, RSA, ECC, and Blowfish-ODHO techniques have obtained a higher key similarity of 25.58%, 22.54%, 19.35%, and 12.21% respectively.

Table 2 Result analysis of key similarity analysis

Algorithms	Similarity (in %)			
	DOS attack	Sybil attack	Brute Force attack	MIM attack
AES	25.58	23.44	23.16	25.18
RSA	22.54	21.65	21.34	22.84
ECC	19.35	18.46	19.98	19.65
Blowfish-ODHO	12.21	13.32	13.43	14.06
IGOA-PHE	11.06	11.98	12.21	12.86

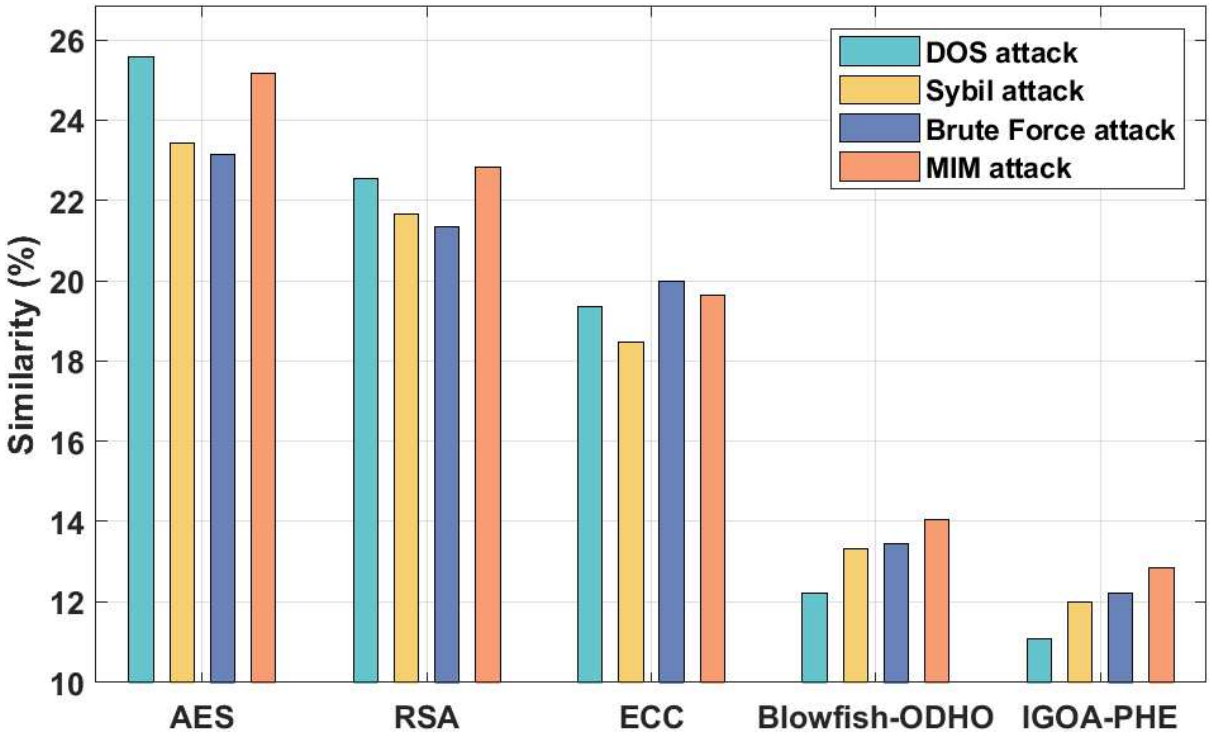

Fig. 5. Similarity analysis of IGOA-PHE model

In addition, under the presence of Sybil attack, the IGOA-PHE approach has accomplished a lesser key similarity of 11.98% whereas the AES, RSA, ECC, and Blowfish-ODHO methods have gained a maximum key similarity of 23.44%, 21.65%, 18.46%, and 13.32% correspondingly. Eventually, under the presence of Brute force attack, the IGOA-PHE manner has accomplished a minimum key similarity of 12.21% whereas the AES, RSA, ECC, and Blowfish-ODHO algorithms have obtained a higher key similarity of 23.16%, 22.34%, 19.98%, and 13.43% correspondingly. Meanwhile, under the presence of MIM attack, the IGOA-PHE technique has accomplished a minimal key similarity of 12.86% whereas the AES,

RSA, ECC, and Blowfish-ODHO methodologies have attained a superior key similarity of 25.18%, 22.84%, 19.65%, and 14.06% correspondingly.

Table 3 and Fig. 6 portrays the throughput analysis of the proposed IGOA-PHE technique under varying vehicle speed. The experimental results showcased that the IGOA-PHE technique has gained effective outcome over the other techniques with the maximum throughput values. For instance, under the vehicle speed of 50km/h, the IGOA-PHE technique has achieved a higher throughput of 91646kbps whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO techniques have attained a reduced throughput of 90542kbps, 84914kbps, 86053kbps, and 91325kbps respectively. Besides, under the vehicle speed of 70km/h, the IGOA-PHE approach has attained a superior throughput of 90862kbps whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO manners have gained a lower throughput of 90791kbps, 85982kbps, 86089kbps, and 90328kbps correspondingly. Moreover, under the vehicle speed of 100km/h, the IGOA-PHE method has achieved a superior throughput of 90079kbps whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO approaches have obtained a minimum throughput of 89402kbps, 83881kbps, 86801kbps, and 89509kbps correspondingly.

Table 3 Result analysis of IGOA-PHE model interms of Throughput

Throughput (kbps)					
Vehicle Speed (km/h)	**SSVC**	**BPAP**	**UMBP**	**Blowfish-ODHO**	**IGOA-PHE**
50	90542	84914	86053	91325	91646
60	89829	88155	84807	90791	91076
70	90791	85982	86089	90328	90862
80	89936	85733	86125	89616	90364
90	89473	88119	84807	89936	90506
100	89402	83881	86801	89509	90079

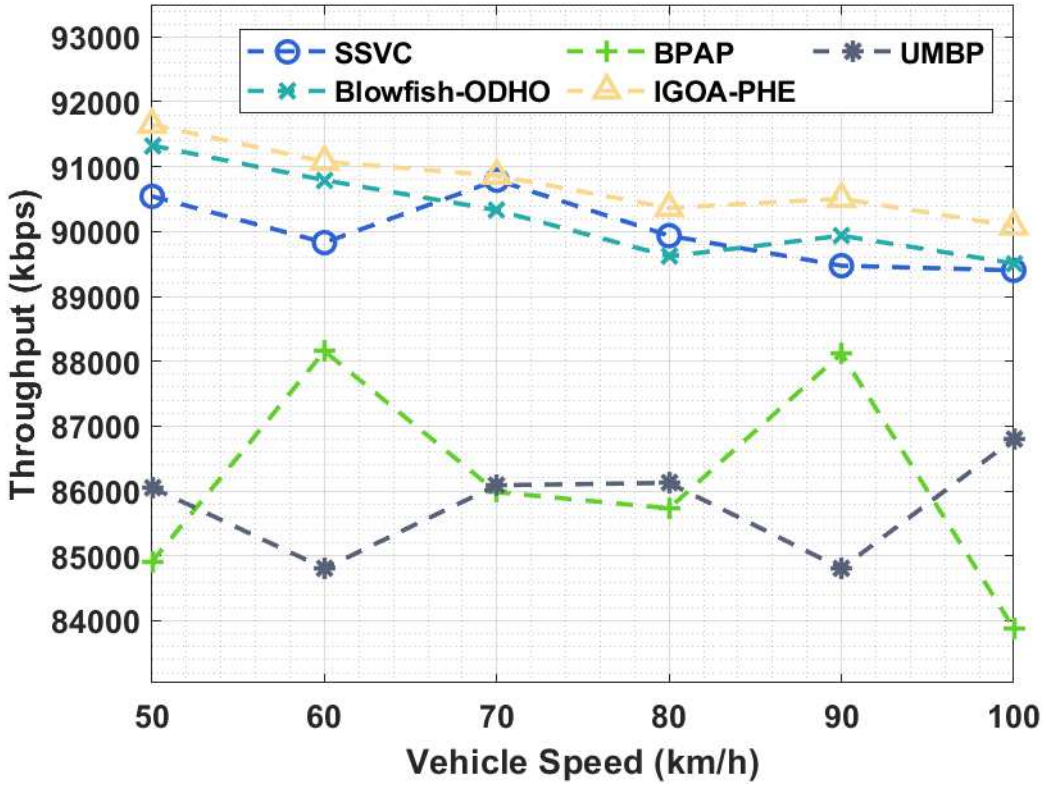

Fig. 6. Throughput analysis of IGOA-PHE model

Table 4 and Fig. 7 demonstrates the RCO analysis of the IGOA-PHE technique over the other methods under different vehicle speed. The experimental results highlighted that the IGOA-PHE technique has accomplished superior results with the lower RCO under distinct vehicle speed. For instance, with the vehicle speed of 50km/hr, the IGOA-PHE technique has showcased a lower RCO of 11.102% whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO techniques have obtained a higher RCO of 16.031%, 35.215%, 23.491%, and 12.700% respectively. Additionally, with the vehicle speed of 70km/hr, the IGOA-PHE method has outperformed a minimal RCO of 16.164% whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO manners have achieved a maximal RCO of 23.092%, 42.942%, 31.618%, and 18.829% correspondingly. Concurrently, with the vehicle speed of 100km/hr, the IGOA-PHE technique has demonstrated a lesser RCO of 25.223% whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO methodologies have attained a superior RCO of 34.283%, 49.870%, 40.011%, and 28.954% correspondingly.

Table 4 Result analysis of IGOA-PHE model with different vehicle speed

Routing Control Overhead (%)					
Vehicle Speed (km/h)	**SSVC**	**BPAP**	**UMBP**	**Blowfish-ODHO**	**IGOA-PHE**
50	16.031	35.215	23.491	12.700	11.102
60	19.628	39.878	26.556	14.565	13.100
70	23.092	42.942	31.618	18.829	16.164
80	26.556	45.074	34.682	21.759	19.228
90	30.019	47.072	36.681	25.090	22.292
100	34.283	49.870	40.011	28.954	25.223

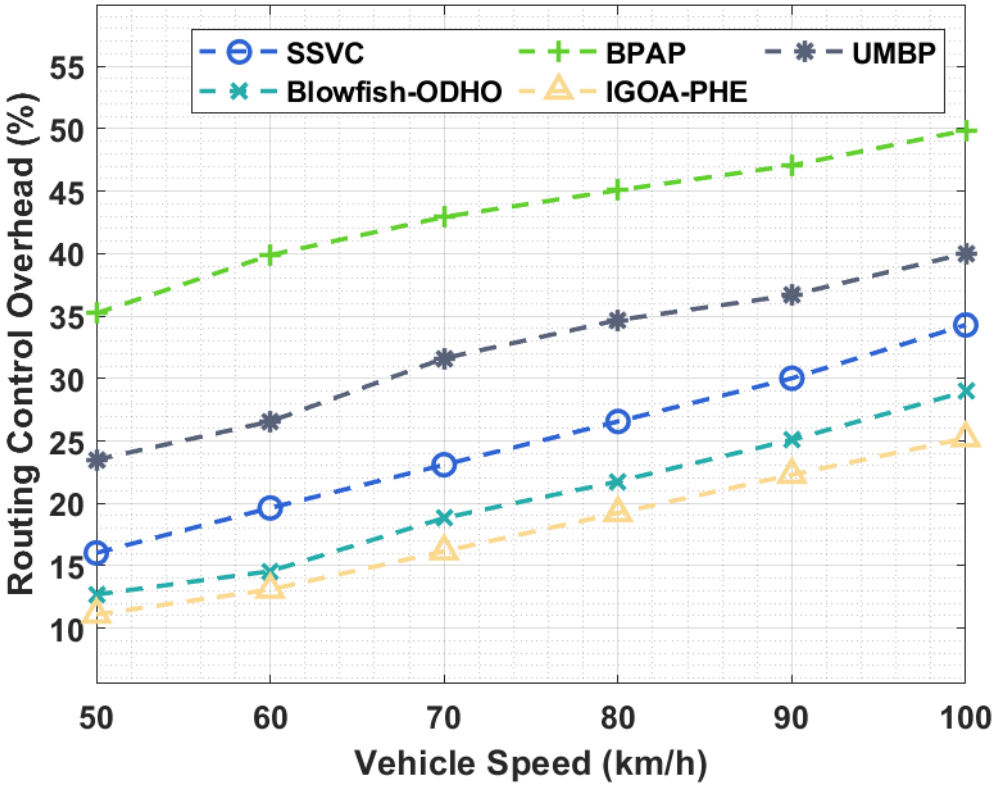

Fig. 7. Routing Control overhead analysis of IGOA-PHE model

Table 5 and Fig. 8 showcase the transmission delay analysis of the IGOA-PHE approach over the other techniques under various vehicle speeds. The experimental outcomes exhibited that the IGOA-PHE method has accomplished maximal results with the lesser transmission delay under various vehicle speeds. For sample, with the vehicle speed of 50km/hr, the IGOA-PHE algorithm has depicted a lower transmission delay of 121.297ms whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO methodologies have attained a superior transmission delay of

197.842ms, 601.681ms, 279.665ms, and 150.331ms correspondingly. Also, with the vehicle speed of 70km/hr, the IGOA-PHE manner has demonstrated a lower transmission delay of 145.052ms whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO techniques have obtained a maximum transmission delay of 261.189ms, 694.063ms, 340.373ms, and 171.447ms respectively. Simultaneously, with the vehicle speed of 100km/hr, the IGOA-PHE methodology has showcased a lower transmission delay of 176.726ms whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO techniques have obtained a superior transmission delay of 348.292ms, 892.023ms, 416.918ms, and 216.318ms correspondingly.

Table 5 Result analysis of IGOA-PHE model interms of transmission delay

Transmission Delay (ms)					
Vehicle Speed (km/h)	**SSVC**	**BPAP**	**UMBP**	**Blowfish-ODHO**	**IGOA-PHE**
50	197.842	601.681	279.665	150.331	121.297
60	221.597	646.552	292.863	150.331	131.855
70	261.189	694.063	340.373	171.447	145.052
80	300.781	791.723	372.047	176.726	145.052
90	313.978	841.873	395.802	205.760	163.528
100	348.292	892.023	416.918	216.318	176.726

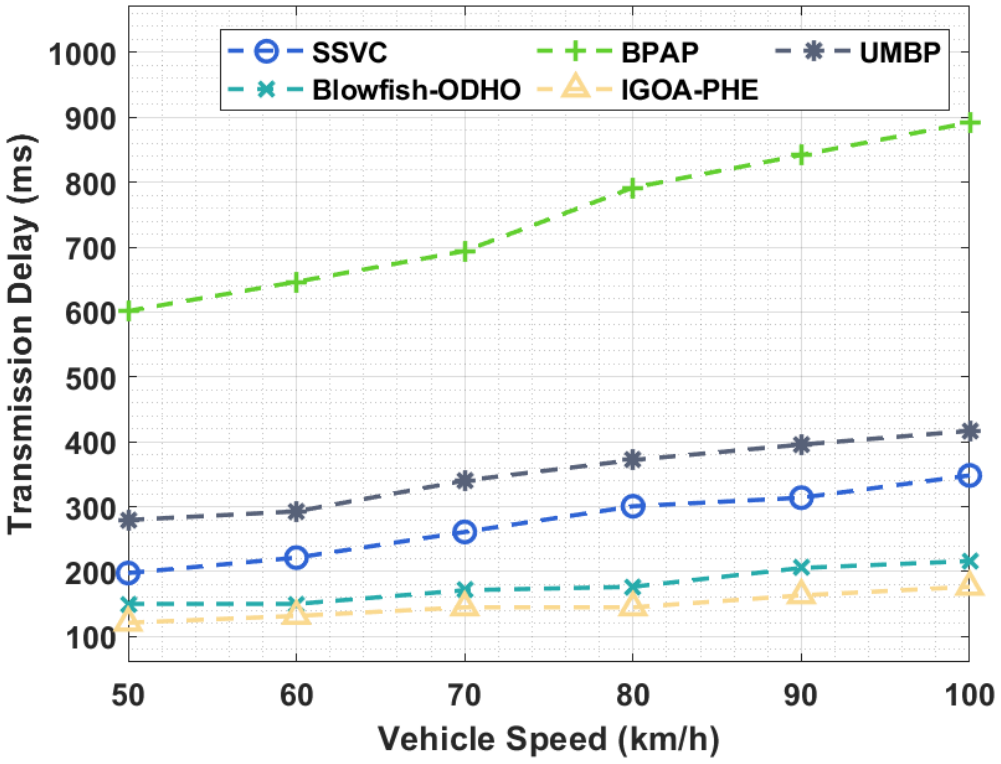

Fig. 8. Transmission delay analysis of IGOA-PHE model

Table 6 and Fig. 9 exhibits the KCT analysis of the IGOA-PHE approach over the other algorithms under distinct key sizes. The experimental results highlighted that the IGOA-PHE technique has accomplished superior results with the lower KCT under distinct key size. For instance, with the key size of 64bits, the IGOA-PHE technique has showcased a lower KCT of 1111.06ms whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO techniques have attained a higher KCT of 1975.19ms, 2787.27ms, 2995.50ms, and 1267.23ms correspondingly. Moreover, with the key size of 256bits, the IGOA-PHE scheme has showcased a minimum KCT of 1506.69ms whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO techniques have gained a higher KCT of 2662.34ms, 3495.24ms, 3870.04ms, and 1694.09ms correspondingly. At the same time, with the key size of 512bits, the IGOA-PHE manner has outperformed a lower KCT of 1714.91ms whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO methodologies have obtained a maximum KCT of 2974.68ms, 3849.22ms, 4182.38ms, and 1975.19ms respectively.

Table 6 Result analysis of IGOA-PHE model interms of KCT and KRT under different key sizes

Key Computation Time (KCT) (ms)					
Key size (bits)	**SSVC**	**BPAP**	**UMBP**	**Blowfish-ODHO**	**IGOA-PHE**
64	1975.19	2787.27	2995.50	1267.23	1111.06
128	2266.71	3172.49	3474.42	1465.04	1267.23
256	2662.34	3495.24	3870.04	1694.09	1506.69
512	2974.68	3849.22	4182.38	1975.19	1714.91
Key Recovery Time (KRT) (ms)					
Key size (bits)	**SSVC**	**BPAP**	**UMBP**	**Blowfish-ODHO**	**IGOA-PHE**
64	0.821	1.099	1.222	0.659	0.628
128	0.976	1.293	1.391	0.730	0.688
256	1.068	1.381	1.543	0.849	0.776
512	1.244	1.553	1.701	0.934	0.828

Fig. 10 defines the KRT analysis of the IGOA-PHE approach over the other techniques under distinct key size. The experimental outcomes outperformed that the IGOA-PHE technique has accomplished maximum results with the lower KRT under distinct key size.

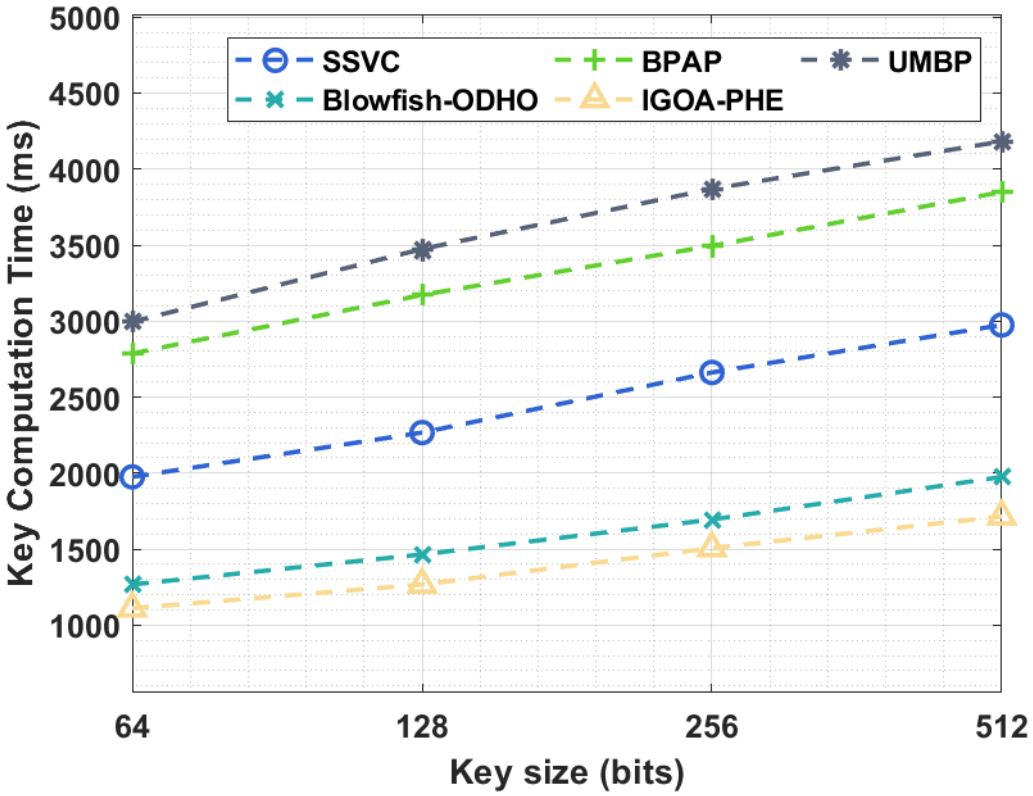

Fig. 9. Key computation time analysis of IGOA-PHE model

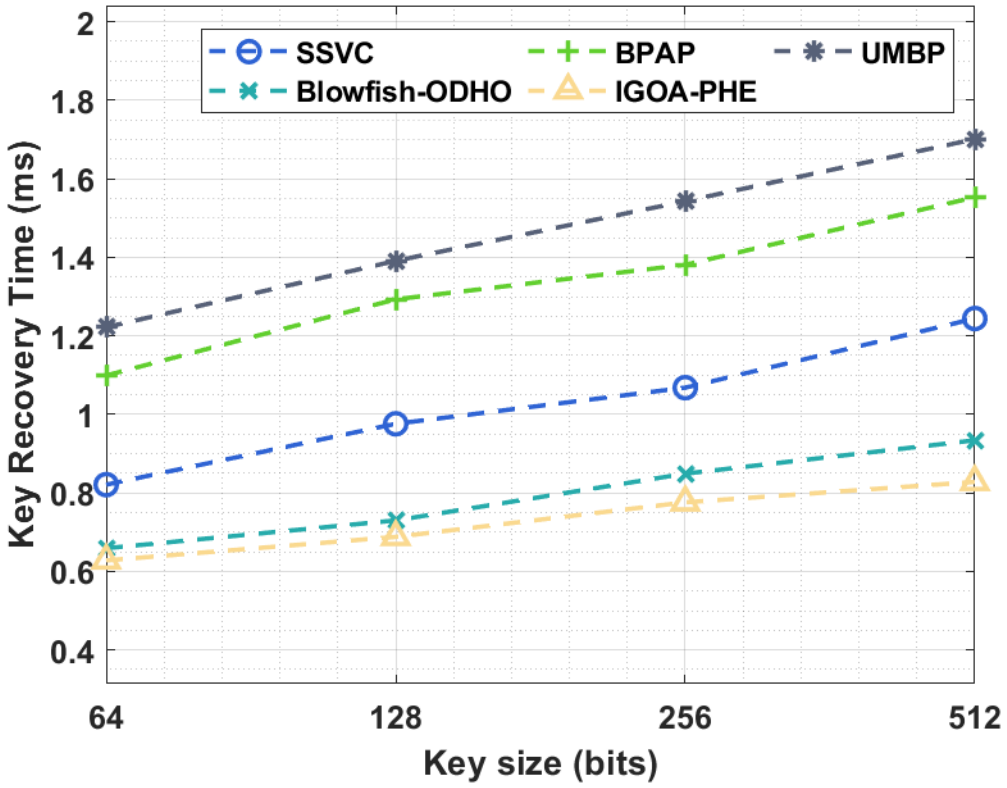

Fig. 10. Key recovery time analysis of IGOA-PHE model

For instance, with the key size of 640bits, the IGOA-PHE technique has showcased a lower KRT of 0.628ms whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO techniques have gained a superior KRT of 0.821ms, 1.099ms, 1.222ms, and 0.659ms respectively. Additionally, with the key size of 256bits, the IGOA-PHE method has exhibited a lower KRT of 0.776ms whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO techniques have obtained a higher KRT of 1.068ms, 1.381ms, 1.543ms, and 0.849ms correspondingly. Concurrently, with the key size of 512bits, the IGOA-PHE algorithm has demonstrated a lower KRT of 0.828ms whereas the SSVC, BPAP, UMBP, and Blowfish-ODHO approaches have gained a superior KRT of 1.244ms, 1.553ms, 1.701ms, and 0.934ms correspondingly.

5. Conclusion

This paper has developed a new IGOA-PHE technique to achieve privacy and security in VANET. The proposed model initially performs an encryption process using the EGPKC technique. Besides, the IGOA is employed to optimally choose the keys for EGPKC technique with an intention of improving security performance. The design of IGOA by the integration of Gaussian mutation and Levy flights helps to considerably boost the outcomes of the conventional IGOA. In order to assess the security results of the proposed IGOA-PHE technique, a wide range of simulations were performed and the results are investigated under several measures. The experimental results highlighted the betterment of the IGOA-PHE technique over the recent state of art techniques in terms of different aspects. In future, data aggregation with steganography techniques can be designed to enhance the network performance and accomplish overall security.

Acknowledgments: NIL

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

Availability of data and material : Available based on Request

Code availability : Available based on Request

References

[1] Khan, A.S., Balan, K., Javed, Y., Tarmizi, S. and Abdullah, J., 2019. Secure trust-based blockchain architecture to prevent attacks in VANET. *Sensors*, *19*(22), p.4954.

[2] Ghori, M.R.; Zamli, K.Z.; Quosthoni, N.; Hisyam, M.; Montaser, M. Vehicular ad-hoc network (VANET): Review. In Proceedings of the 2018 IEEE International Conference on Innovative Research and Development (ICIRD), Bangkok, Thailand, 11–12 May 2018.

[3] Gillani, S.; Shahzad, F.; Qayyum, A.; Mehmood, R. A survey on security in vehicular ad hoc networks. In Communication Technologies for Vehicles. Nets4Cars/Nets4Trains 2013. Lecture Notes in Computer Science; Berbineau, M., Jonsson, M., Bonnin, J., Cherkaoui, S., Aguado, M., Rico-Garcia, C., Ghannoum, H., Mehmood, R., Vinel, A., Eds.; Springer: Heidelberg/Berlin, Germany, 2013; pp. 59–74.

[4] Abbasi, I.A.; Khan, A.S. A review of vehicle to vehicle communication protocols for VANETs in the urban environment. Future Internet 2018, 10, 14.

[5] Malik, N.; Nanda, P.; Arora, A.; He, X.; Puthal, D. Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. In Proceedings of the 2018 17 th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering, New York, NY, USA, 1–3 August 2018.

[6] Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. Telecommun. Syst. 2012, 50, 217–241.

[7] Alaya, B. and Sellami, L., 2021. Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks. *Journal of Information Security and Applications*, *58*, p.102779.

[8] Bhoi, S.K.; Khillar, P.M.; Singh, M.; Sahoo, M.M.; Swain, R.R. A routing protocol for urban vehicular ad hoc networks to support non-safety applications. Digital Commun. Networks 2018, 4, 189–199.

[9] Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. Telecommun. Syst. 2012, 50, 217–241.

[10] Begum, R.; Raziuddin, S.; Prasad, V.K. A survey on VANETs applications and its challenges. In Proceedings of the International Conference on Advanced Computer Science & Software Engineering, Hyderabad, India, 11 March 2016.

[11] Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. VANET security surveys. Comput. Commun. 2014, 44, 1–13.

[12] Al-Shareeda, M.A., Anbar, M., Manickam, S. and Yassin, A.A., 2020. Vppcs: Vanet-based privacy-preserving communication scheme. IEEE Access, 8, pp.150914-150928.

[13] Cui, J., Wei, L., Zhong, H., Zhang, J., Xu, Y. and Liu, L., 2020. Edge computing in VANETs-an efficient and privacy-preserving cooperative downloading scheme. IEEE Journal on Selected Areas in Communications, 38(6), pp.1191-1204.

[14] Alfadhli, S.A., Lu, S., Chen, K. and Sebai, M., 2020. Mfspv: A multi-factor secured and lightweight privacy-preserving authentication scheme for vanets. IEEE Access, 8, pp.142858-142874.

[15] Ali, I. and Li, F., 2020. An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs. Vehicular Communications, 22, p.100228.

[16] Wang, Y., Zhong, H., Xu, Y., Cui, J. and Wu, G., 2020. Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for vanets. IEEE Systems Journal, 14(4), pp.5373-5383.

[17] Wang, S., Mao, K., Zhan, F. and Liu, D., 2020. Hybrid conditional privacy-preserving authentication scheme for VANETs. Peer-to-Peer Networking and Applications, 13, pp.1600-1615.

[18] Moni, S.S. and Manivannan, D., 2021. A scalable and distributed architecture for secure and privacy-preserving authentication and message dissemination in VANETs. Internet of Things, 13, p.100350.

[19] Benarous, L., Kadri, B., Bitam, S. and Mellouk, A., 2020. Privacy-preserving authentication scheme for on-road on-demand refilling of pseudonym in VANET. International Journal of Communication Systems, 33(10), p.e4087.

[20] Al-shareeda, M.A., Anbar, M., Manickam, S. and Hasbullah, I.H., 2020. An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network. Symmetry, 12(10), p.1687.

[21] S. Saremi, S. Mirjalili, and A. Lewis, "Grasshopper optimisation algorithm: theory and application," Advances in Engineering Software, vol. 105, pp. 30–47, 2017.

[22] Feng, H., Ni, H., Zhao, R. and Zhu, X., 2020. An enhanced grasshopper optimization algorithm to the Bin packing problem. *Journal of Control Science and Engineering*, *2020*.

[23] Luo, J., Chen, H., Xu, Y., Huang, H. and Zhao, X., 2018. An improved grasshopper optimization algorithm with application to financial stress prediction. *Applied Mathematical Modelling*, *64*, pp.654-668.