International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I7P203

Volume 70 Issue 7, 24-31, July 2022
© 2022 Seventh Sense Research Group®

Original Article

Privacy Preserving Lightweight Cryptography Scheme for Clustered Vehicular Adhoc Networks

Shaji K.A.Theodore[1], K. Rajiv Gandhi[2], V. Palanisamy[3]

[1]*Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India*
[2]*Department of Computer Science, Alagappa University Model Constituent College, Paramakkudi,Tamilnadu, India*
[3]*Department of Computer Applications, AlagappaUniversity ,Karaikudi- 630003 , Tamilnadu, India*

[1]drtheodore7733@hotmail.com

Received: 18 May 2022 Revised: 14 June 2022 Accepted: 28 June 2022 Published: 18 July 2022

Abstract *- Vehicular ad hoc network (VANET) is typically used in intelligent transportation systems (ITS), which permits the interchange of traffic information amongst close atmosphere and vehicles to establish an efficient driving experience. Security and privacy are becoming a difficult problem that prevails from the safety requirements of the VANET. Some of the specific leakage of vehicle details like route data may lead to severe effects, and thus, privacy-preserving protocols were required to improve security in VANET. This article introduces a novel Sunflower Optimization with Privacy Preserving Lightweight Cryptography (SFO-PPLWC) scheme for Clustered VANET. The major goal of the SFO-PPLWC technique is to cluster the vehicles and enable secure data transmission using the LWC approach. The proposed SFO-PPLWC model comprises a three-stage process: weighted cluster scheme, encryption, and optimal key generation. Primarily, the presented SFO-PPLWC model comprises a weighted clustering scheme (WCS) model to group the vehicles. Besides, the Tiny Encryption Algorithm (TEA) is employed to transmit the data securely. Moreover, the SFO algorithm is exploited to choose the keys related to the TEA model optimally. The experimental outcome analysis of the SFO-PPLWC model is tested and compared with existing models. The simulation results highlighted the enhancements of the SFO-PPLWC model over recent models.*

Keywords – *VANET, Clustering, Privacy preserving, Lightweight cryptography, Security, Metaheuristics.*

1. Introduction

The Vehicular Ad Hoc Network (VANET) is a division of the wireless network model[1].VANETs were considered as effective as it supplies travel effectiveness and security via real-time data backing through introducing links vehicle to infrastructure (V2I) and vehicle to vehicle (V2V), which could improve the driving incidents via smart control and provide superior relaxation and travel incidents to traveller [2]. A VANET primarily contains roadside units (RSUs), trusted authority (TA), and vehicles armed with onboard units (OBUs) for V2I and V2V transmissions responsibility [3]. The TA is a high computational power trusted by third parties and has a huge storage capacity; it accounts for managing and producing the system variables and presenting confidential tackles [4]. An RSU is a transmission link party with superior calculating capabilities and storage potentiality over OBU and is placed as a roadside structure for particular coordination and management tasks. Even though the enthusiasm encircling the advantages of VANETs seems to be rising, the active feature of VANETs, together with the multitude of systems and application-based necessities, results in high complexity for designing effective methodologies for assuring vehicles secrecy [5, 6]. Secrecy is the privacy of vehicles (drivers) and the place of vehicles [7].

Meanwhile, every message a vehicle forward must be validated earlier, and processing is done. Since such issues are resolved for optimum fulfillment of the end users, extensive arrangements of VANETs could not perform [8,9]. The basic rule of message authentication is eased through the sender's signing of messages, after which it verifies the integrity and authenticity of messages on the receiver side. Some validation or authentication necessities like efficient and scalable certificate revocation, minimum computational overhead, and strong and scalable validation must be met and resolved to assure secure transmission in VANETs [10].

In [11], the authors presented an RFID-related authentication substructure for dispersed IoT applications appropriate for the forthcoming smart city atmospheres. Then, a lightweight RFID-related validation scheme can be presented for grant fair accomplishment time compared with the existing schemes. Our scheme offers anonymity, the untraced ability of RFID-tag, secure localization, and forward confidentiality. In [12], the authors suggest a Secure Data and Privacy Preservation Sharing Scheme in Fog-oriented VANET by examining crucial data and using data secrecy by utilizing Hierarchical Attribute-based Encryption (HABE) as an effective key exchange. Prateek et al. [13]

suggest a restricted privacy preserving validation scheme based on quantum key dispersal protocol for V2I transmission. It is not necessary that a confidential validation key that forwarded conservatively and is resilient to quantum assaults. The research in [14] provides a resolution for controlling the attacks beyond the VANET security. To enhance the security measures of data communication via network context, the enthused Random Firefly (RFF) development is utilized for finding the dependable vehicles in formulated VNET topology. Wei et al. [15] suggest restricted privacy preserving AKA and lightweight scheme, in which the primary stages are devised with symmetric cryptography methodologies. The project could diminish the communication and computational overhead of the AKA function. This article introduces a novel Sunflower Optimization with Privacy Preserving Lightweight Cryptography (SFO-PPLWC) scheme for Clustered VANET. The experimental outcome analysis of the SFO-PPLWC model is tested and related to the presented methods.

2. The Proposed Model

In this article, an intelligence SFO-PPLWC technique has been developed to cluster the vehicles and enable secure data transmission using the LWC approach in VANET. The proposed SFO-PPLWC model comprises a three-stage process: weighted cluster scheme, TEA based encryption, and SFO based optimal key generation. Fig. 1 depicts the overall process of the SFO-PPLWC algorithm.

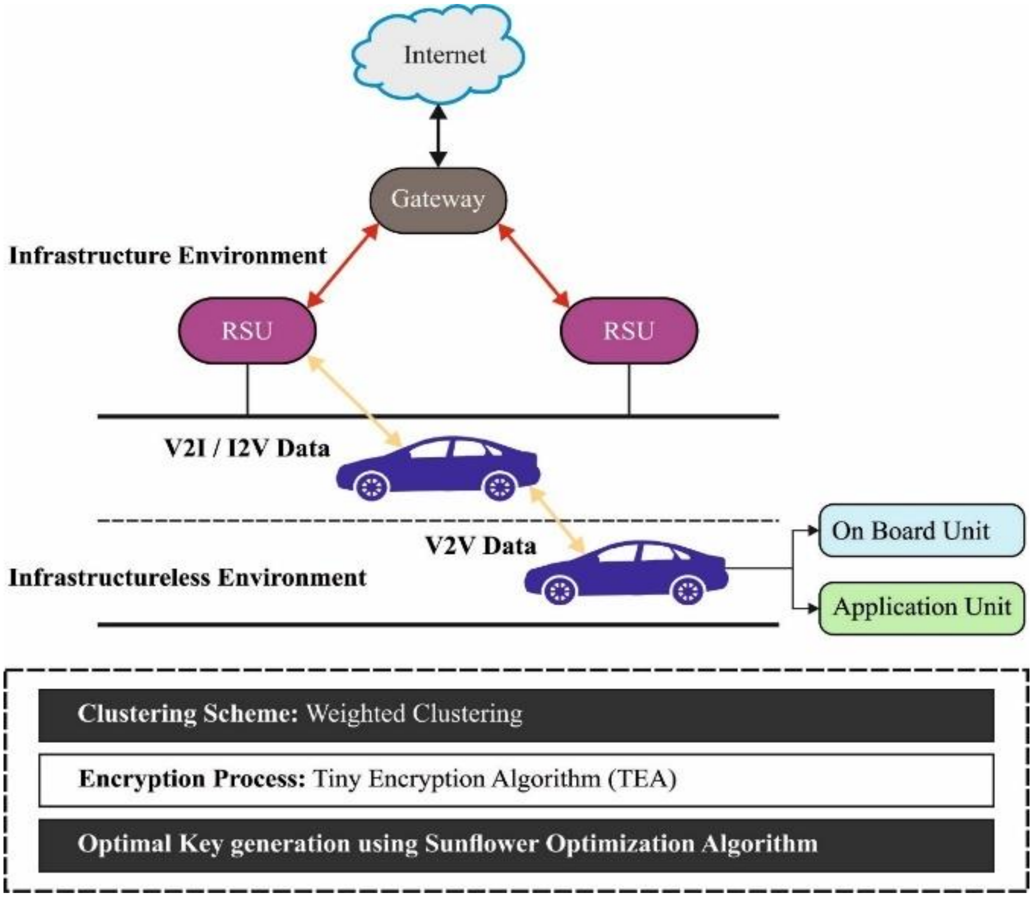
Internet
Gateway
Infrastructure Environment
RSU
RSU
V2I / I2V Data
V2V Data
On Board Unit
Application Unit
Infrastructureless Environment
Clustering Scheme: Weighted Clustering
Encryption Process: Tiny Encryption Algorithm (TEA)
Optimal Key generation using Sunflower Optimization Algorithm

Fig. 1 Overall process of SFO-PPLWC algorithm

2.1 Clustering Process

The presented model cluster the vehicle using vehicle centrality (NC), remaining energy, and distance to BS (DBS). Residual Energy (RE): It is a fundamental parameter used for selecting a vehicle as CH since the CH could use a considerable quantity of energy in comparison with CM. For that reason, a high energy level is required for a vehicle to become CH.

Vehicle Centrality (NC): Determines the 1-hop neighboring vehicle amount in the broadcast range of the vehicle is called vehicle degree. The minimal value of NC leads to a high possibility of becoming CH, as follows:

$$\mathrm{NC} = \frac{\sqrt{\sum_{i=1}^{ND} \mathrm{dist}_i^2 / \mathrm{ND}}}{\mathrm{Ntk\_Dimension}}. \tag{1}$$

Distance to BS: Energy use for data broadcast gets improved with increased distance between the receiving and transmitting vehicles. The distance between the BS and CHs should be minimum to accomplish energy efficacy.

$$Distance\ to\ BS = \frac{d_i}{\alpha \cdot \text{Ntk\_Dimension}}, \qquad (2)$$

$$\alpha = \frac{d_{\max}}{\text{Ntk\_Dimension}}.$$

In Eq. (2), α represents the network dimension-specific constant, d_i denotes the distance between the BS and the vehicle i, $d_{\max}$ characterize the highest distance between the BS and the vehicles in the network. For all the vehicles in WSN, the probabilities of becoming CH P_i is defined by the following equation:

$$P_i = w_1 * Er_i + w_2 * D_i + w_3 * ND_i \qquad (3)$$

Let w_1, w_2 and w_3 be the coefficients of the system, thus

$$w_1 + w_2 + w_3 = 1 \qquad (4)$$

2.2. Process involved in TEA

TEA is an asymmetric Feistel form cipher generated by David Wheeler and Roger Needham of Cambridge University that comes in a particular class having iterated block cipher [16]. The ciphertext has been created in the plain text by frequently executing a similar alteration or round function. During this procedure of ciphers, there are 2 phases of encrypt procedure. An initial phase is an application of round functions F on the primary part utilizing a sub-key, and the resultant of this phase is XORed with the residual part. The pattern, as mentioned earlier, was monitored in all the rounds but the last round, whereas the swapping could not be executed. The double shift function from TEA frequently mixes the key and each bit comprising the data. The 128bit key K_y was separated into four 32bit blocks $(K_y = (K_y[0], K_y[1], K_y[2], K_y[3])$ by utilizing the key shift technique. Afterward, it is integrated and finally results in the development of ciphertext block $(C = Left[64], Right[64])$.

2.3. Optimal Key Generation Process

To optimally generate keys related to the TEA model, the SFO algorithm has been employed. SFO [18] is a population-based metaheuristic model motivated by the attack alternating technique from the group of hunting sailfish that hunting a school of sardine. This technique offers an upper hand to hunters by offering the possibility of saving their power. It comprises sailfish and sardine populations. The problem parameter represents the location of sailfish in searching space, and the sailfish is considered a candidate solution. The system tries to randomize the search agent motion (that is, sailfish and sardine) as feasible.

For sardine, the 'injured' indicates an optimal fitness value and position in i^t iteration is indicated by $P^i_{SrdInjured}$. The sailfish using optimal fitness values are called 'elite' sailfish, and their position in i^t iteration is denoted by $P^i_{SlfBest}$. In every iteration, the position of sailfish and sardine are advanced. During $i + 1^t$ iteration, an original position P^{i+1}_{Slf} of sailfish can be advanced by 'injured' sardine and 'elite' sailfish as follows.

$$P^{i+1}_{Slf} = P^i_{SlfBest} - \mu_i \times \left(rnd \times \frac{P^i_{SlfBest} + P^i_{SrdInjured}}{2} - P^i_{Slf} \right) (5)$$

In Eq. (5), rnd characterizes arbitrary values amongst [0, 1], P^i_{Slf} symbolizes preceding position Slf^{th} sailfish and μ_i characterizes coefficient specifically generated as follows.

$$\mu_i = 2 \times rnd \times PrD - PrD \qquad (6)$$

In Eq. (6), PrD represents prey density and symbolizes the quantity of prey in every iteration. In all the iterations, the values of PrD, evaluated by the following equation, are decreased using prey amount in group hunting.

$$PrD = 1 - \frac{Num_{Slf}}{Num_{Slf} + Num_{Srd}} \qquad (7)$$

In Eq. (7), Num_{Slf} and Num_{Srd} Correspondingly symbolizes sardine and sailfish numbers.

$$Num_{Slf} = Num_{Srd} \times\ Prcnt \qquad (8)$$

In Eq. (8), $Prcnt$ indicates the proportion of the sardine population that generates the earlier sailfish population. The initial amount of sardines are frequently considered higher than the sailfish amount. The location of the sardine can be advanced in every iteration as follows.

$$P^{i+1}_{Srd} = rnd(0,1) \times \left(P^i_{SLfBest} - P^i_{Srd} + ATK\right) (9)$$

$$ATK = A \times \left(1 - (2 \times itr \times \kappa)\right) \qquad (10)$$

From the above equations, P^i_{Srd} and P^{i+1}_{Srd} correspondingly indicates the preceding and advanced position of sardine and ATK designates sailfish attack strength at all the iterations itr. At this point, the sardine count upgrades the location, and displacement quantity depends upon ATK. Decrease the ATK supports the convergence of the searching agent. Using ATK parameter, the sardine count upgrades the position (γ), and the parameter count (δ) is evaluated as follows:

$$\gamma = Num_{Srd} \times ATK \qquad (11)$$

$$\delta = v \times ATK \tag{12}$$

From the equations, parameter amount can be denoted as v, and sardine count can be denoted by Num_{Srd}. After the sardine becomes appropriate compared to other sailfishes, the sailfish upgrade its position afterward the sardine and is eradicated in the population. Because the attack strength of sailfish minimizes after each iteration, it provides a chance for a sardine to escape from an optimal sailfish, which supports the exploitation stage. The ATK parameter tries to discover a balance between exploration and exploitation stages. Fig. 2 showcases the flowchart of the SFO technique.

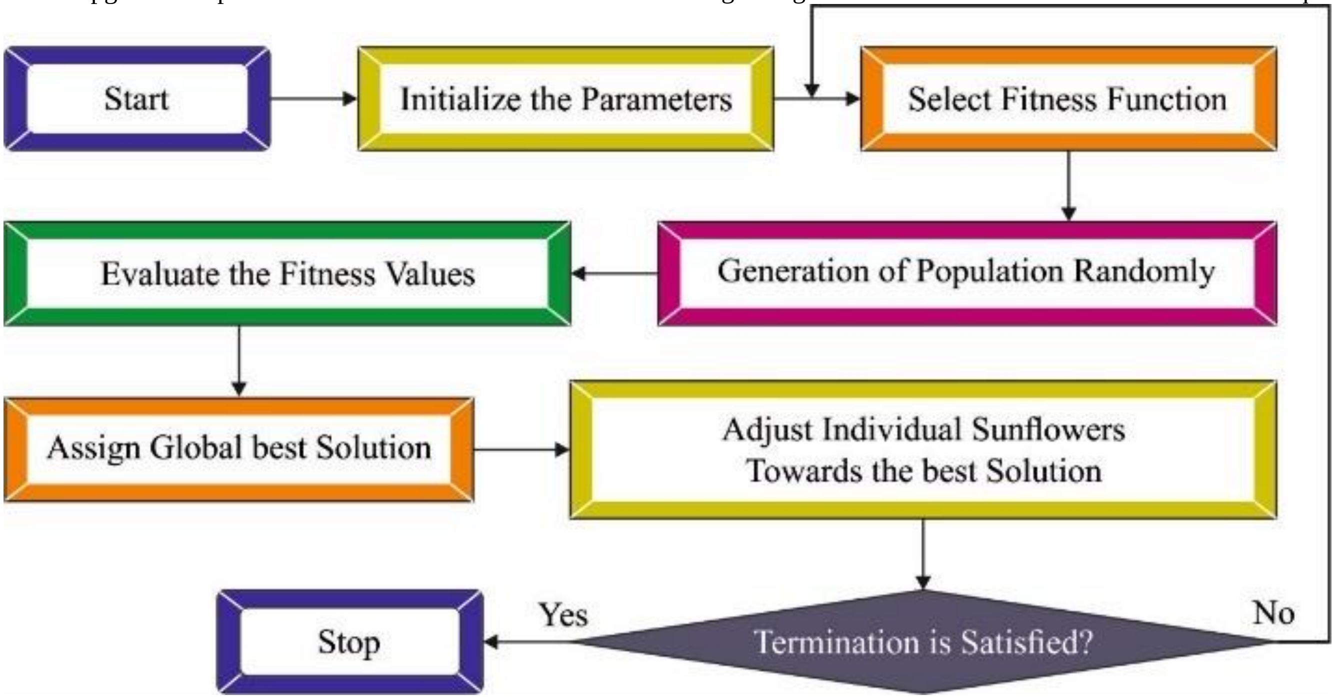
Start
Initialize the Parameters
Select Fitness Function
Generation of Population Randomly
Evaluate the Fitness Values
Assign Global best Solution
Adjust Individual Sunflowers Towards the best Solution
Termination is Satisfied?
Yes
No
Stop

Fig. 2 Flowchart of SFO technique

3. Results and Discussion

In this section, the experimental validation of the SFO-PPLWC model is tested under varying speeds of vehicles. Table 1 provides a detailed comparative study of the SFO-PPLWC model with recent models under several vehicles' in terms of packet delivery ratio (PDR), throughput (THPT), and routing control overhead (RCO) [19]. Fig. 3 offers a comparative PDR examination of the SFO-PPLWC model with existing models under distinct vehicle speed (VS). The figure indicated that the SFO-PPLWC approach has increased PDR values over other methods. For instance, with VS of 50km/h, the SFO-PPLWC model has shown an enhanced PDR value of 98.58%, whereas the UMBP, SSVC, and ITESLA-CF models have demonstrated reduced PDR values of 90.56%, 93.53%, and 97.56% respectively. Along with that, with VS of 100km/h, the SFO-PPLWC technique has shown a higher PDR value of 92.47%, whereas the UMBP, SSVC, and ITESLA-CF models have demonstrated lower PDR values of 78.69%, 82.93%, and 91.20% correspondingly.

Table 1. Comparative analysis of SFO-PPLWC algorithm under distinct vehicle speeds

Packet Delivery Ratio (%)				
VS (km/h)	**UMBP**	**SSVC**	**ITESLA-CF**	**SFO-PPLWC**
50	90.56	93.53	97.56	98.58
60	89.29	92.68	96.71	98.16
70	82.08	84.84	92.26	94.35
80	82.51	86.75	92.05	93.84
90	79.75	83.78	90.77	92.79
100	78.69	82.93	91.20	92.47
Throughput (kbps)				
VS (km/h)	**UMBP**	**SSVC**	**ITESLA-CF**	**SFO-PPLWC**
50	86344.75	90563.60	90956.06	91462.00
60	84807.65	89647.88	90563.60	92630.00
70	86148.52	90759.83	90825.24	92165.00
80	86475.57	89876.81	90400.08	91987.00
90	84807.65	89582.48	90007.63	92267.00
100	86671.79	89615.18	90105.74	92589.00

Routing Control Overhead (%)				
VS (km/h)	**UMBP**	**SSVC**	**ITESLA -CF**	**SFO-PPLWC**
50	23.34	16.45	13.64	10.68
60	27.42	19.40	16.17	13.51
70	32.20	22.78	18.28	14.68
80	35.16	27.00	21.51	19.87
90	37.55	29.11	24.33	22.91
100	40.78	33.05	27.28	24.51

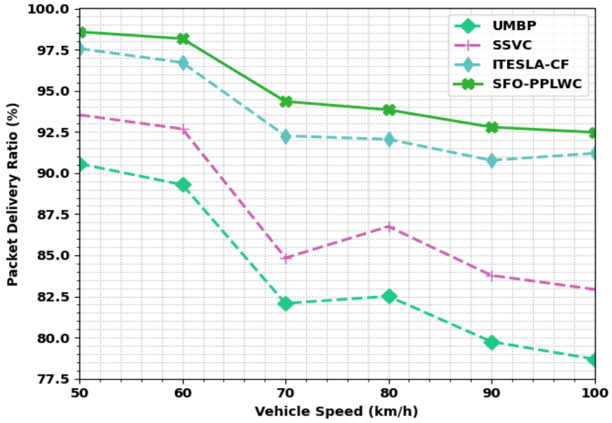

Fig. 3 PDR analysis of SFO-PPLWC algorithm under distinct vehicle speeds

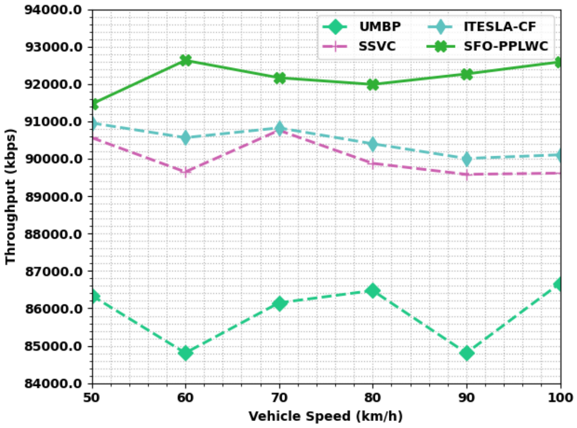

Fig. 4 Throughput analysis of SFO-PPLWC algorithm under distinct vehicle speeds

Fig. 4 offers a comparative THPT inspection of the SFO-PPLWC approach with existing models under varying VS. The figure indicated that the SFO-PPLWC method had increased THPT values over other methods. For instance, with VS of 50km/h, the SFO-PPLWC algorithm has exposed an enhanced THPT value of 91462.00kbps, whereas the UMBP, SSVC, and ITESLA-CF models have demonstrated reduced THPT values of 86344.75kbps, 90563.60kbps, and 90956.06kbps correspondingly. Also, with VS of 100km/h, the SFO-PPLWC algorithm has displayed an enhanced THPT value of 92589.00kbps, whereas the UMBP, SSVC, and ITESLA-CF models have revealed reduced THPT values of 86671.79kbps, 89615.18kbps, and 90105.74kbps correspondingly.

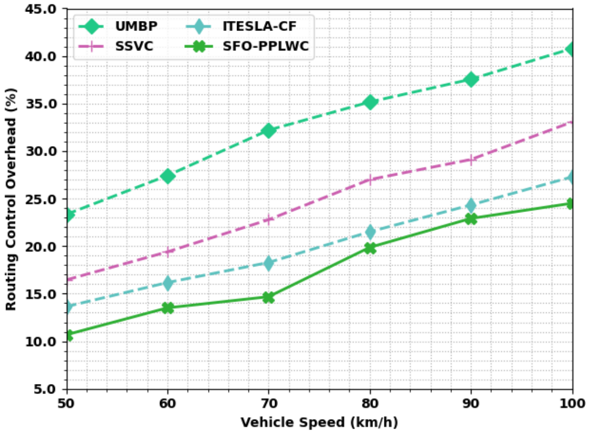

Fig. 5 RCO analysis of SFO-PPLWC algorithm under distinct vehicle speeds

An RCO inspection of the SFO-PPLWC model with recent models under different levels of VS has depicted in Fig. 5. The results indicated that the SFO-PPLWC algorithm had accomplished better performance over other models. For instance, on VS of 50km/h, the SFO-PPLWC model has demonstrated the least RCO of 10.68%, whereas the UMBP, SSVC, and ITESLA-CF models have exhibited increased RCO values of 23.34%, 16.45%, and 13.64% respectively. Also, on VS of 100km/h, the SFO-PPLWC system has outperformed the least RCO of 24.51%, whereas the UMBP, SSVC, and ITESLA-CF approaches have outperformed higher RCO values of 40.78%, 33.05%, and 27.28% correspondingly.

Table 2 provides a detailed comparative study of the SFO-PPLWC algorithm with recent models concerning transmission delay (TD), key computation time (KCT), and key recovery time (KRT). A TD inspection of the SFO-PPLWC model with recent approaches under different levels of VS is represented in Fig. 6. The results indicated that the SFO-PPLWC algorithm had accomplished better performance than other models. For instance, on VS of 50km/h, the SFO-PPLWC approach has demonstrated the least TD of 140.32ms. In contrast, the UMBP, SSVC, and ITESLA-CF techniques have exhibited maximal TD values of 283.53ms, 205.80ms, and 161.38ms correspondingly. Moreover, on VS of 100km/h, the SFO-PPLWC algorithm has demonstrated the least TD of 271.45ms. In contrast, the UMBP, SSVC, and ITESLA-CF techniques have correspondingly exhibited higher TD values of 430.66ms, 364.03ms, and 302.96ms.

Table 2. Comparative analysis of SFO-PPLWC technique with existing algorithms under distinct measures

Transmission Delay (ms)				
VS (km/h)	UMBP	SSVC	ITESLA-CF	SFO-PPLWC
50	283.53	205.80	161.38	140.32
60	308.51	241.89	186.36	150.21
70	347.38	266.87	216.90	200.23
80	372.36	300.18	244.66	216.26
90	405.67	336.27	269.65	234.87
100	430.66	364.03	302.96	271.45
Key Computation Time (ms)				
Key size (bits)	EGKM	SSVC	ITESLA-CF	SFO-PPLWC
64	2733.21	2090.98	1889.14	1524.26
128	3173.60	2402.92	2109.33	1863.41
256	3448.84	2696.51	2256.13	2061.61
512	3907.58	3081.85	2623.12	2198.26
Key Recovery Time(ms)				
Key size (bits)	EGKM	SSVC	ITESLA-CF	SFO-PPLWC
64	1.10	0.84	0.77	0.74
128	1.28	0.97	0.90	0.88
256	1.39	1.07	0.97	0.94
512	1.57	1.23	1.08	1.01

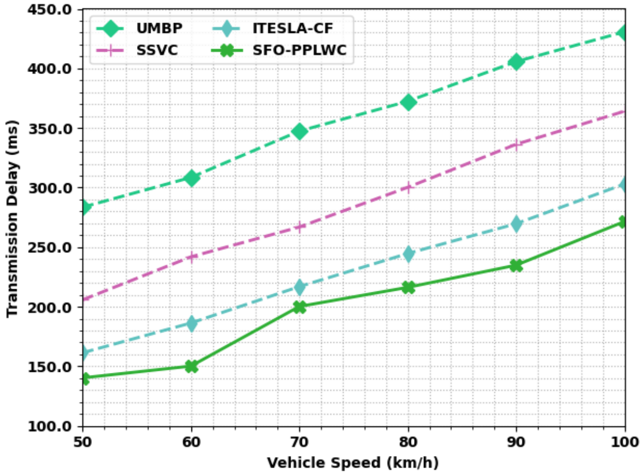

Fig. 6 TD analysis of SFO-PPLWC algorithm under distinct vehicle speeds

A KCT analysis of the SFO-PPLWC model with recent methods under different key sizes is established in Fig. 7. The obtained outcomes revealed that the SFO-PPLWC system had accomplished better performance than other approaches. For instance, on key size of 64bits, the SFO-PPLWC model has demonstrated the least KCT of 1524.26ms, whereas the UMBP, SSVC, and ITESLA-CF models have exhibited increased KCT values of 2733.21ms, 2090.98ms, and 1889.14ms correspondingly. Also, on a key size of 512bits, the SFO-PPLWC methodology has demonstrated a minimal KCT of 2198.26ms. In contrast, the UMBP, SSVC, and ITESLA-CF techniques have exhibited increased KCT values of 3907.58ms, 3081.85ms, and 2623.12ms correspondingly.

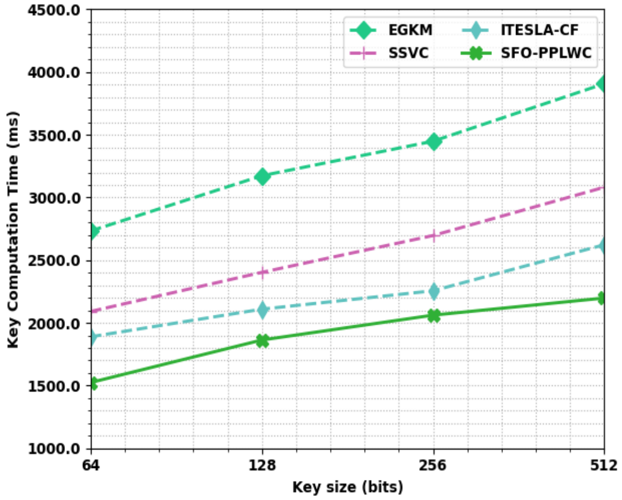

Fig. 7 KCT analysis of SFO-PPLWC algorithm under distinct key sizes

A KRT examination of the SFO-PPLWC model with recent methods under different key sizes is revealed in Fig. 8. The obtained outcomes exposed that the SFO-PPLWC approach has accomplished better performance over other models. For instance, on key size of 64bits, the SFO-PPLWC system has demonstrated the least KRT of 0.74ms, whereas the UMBP, SSVC, and ITESLA-CF approaches have displayed increased KRT values of 1.10ms, 0.84ms, and 0.77ms respectively. Also, on key size of 512bits, the SFO-PPLWC approach has outperformed reduced KRT of 1.01ms, whereas the UMBP, SSVC, and ITESLA-CF algorithms have exhibited higher KRT values of 1.57ms, 1.23ms, and 1.08ms correspondingly.

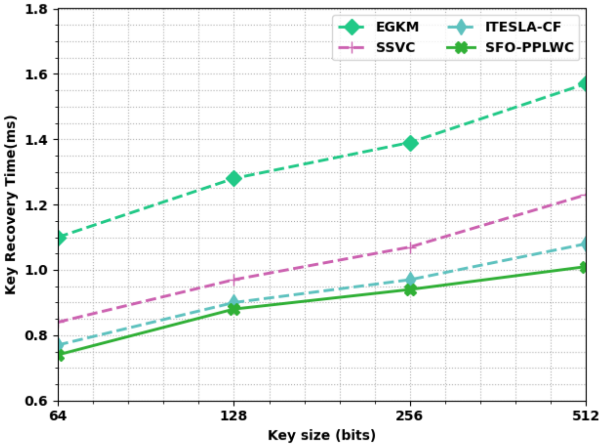

Fig. 8 KRT analysis of SFO-PPLWC algorithm under distinct key sizes

These results and discussion highlighted the betterment of the SFO-PPLWC model over recent approaches.

Conclusion

In this article, an intelligence SFO-PPLWC technique has been developed to cluster the vehicles and enable secure data transmission using the LWC approach in VANET. The proposed SFO-PPLWC model comprises a three-stage process: weighted cluster scheme, encryption, and optimal key generation. The SFO-PPLWC model primarily comprises the WCS model to group the vehicles. Besides, the TEA is employed to transmit the data securely. Moreover, the SFO algorithm is exploited to choose the keys related to the TEA model optimally. The experimental outcome analysis of the SFO-PPLWC model is tested and compared with existing models. The simulation results highlighted the enhancements of the SFO-PPLWC model over recent models. In the future, the SFO-PPLWC approach's performance will be improved using hybrid DL models.

References

[1] D. Manivannan, S. S. Moni and S. Zeadally, “Secure Authentication and Privacy-Preserving Techniques in Vehicular Ad-Hoc Networks (VANETs),” *Vehicular Communications*, vol. 25, pp. 100247, 2020.

[2] K. Rabieh, M. M. Mahmoud, and M. Younis, “Privacy-Preserving Route Reporting Scheme for Traffic Management in VANETs,” In *2015 IEEE International Conference on Communications (ICC)*, pp. 7286-7291, 2015.

[3] C. T. Li, M. S. Hwang, and Y. P. Chu, “A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular Ad Hoc Networks,” *Computer Communications*, vol. 31, no. 12, pp. 2803-2814, 2008.

[4] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, “Computationally Efficient Privacy Preserving Authentication and Key Distribution Techniques for Vehicular Ad Hoc Networks,” *cluster computing*, vol. 20, no. 3U , pp. 2439-2450, 2017.

[5] U. Rajput, F. Abbas, and H. Oh, “A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET,” *IEEE Access*, vol. 4, pp. 7770-7784, 2016.

[6] P. Mundhe, S. Verma, and S. Venkatesan, “A Comprehensive Survey on Authentication and Privacy-Preserving Schemes in VANETs,” *Computer Science Review*, vol. 41, pp. 100411, 2021.

[7] S. Gavaskar, E. Ramaraj, R. Surendiran, “A compressed anti IP spoofing mechanism using cryptography,” *IJCSNS International Journal of Computer Science and Network Security*, vol. 12, no. 11, pp.137-140, 2012.

[8] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, “Edge computing in VANETs-An Efficient and Privacy-Preserving Cooperative Downloading Scheme,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1191-1204, 2020.

[9] S. O. Ogundoyin and I. A. Kamil, “An Efficient Authentication Scheme with Strong Privacy Preservation for Fog-Assisted Vehicular Ad Hoc Networks Based on Blockchain and Neuro-Fuzzy,” *Vehicular Communications*, vol. 31, pp. 100384, 2021.

[10] T. Nandy, M.Y.I. Idris, R.M. Noor, A.W.A. Wahab, S. Bhattacharyya, R. Kolandaisamy, and M. Yahuza, “A Secure, Privacy-Preserving, and Lightweight Authentication Scheme for VANETs,” *IEEE Sensors Journal*, vol. 21, no. 18, pp. 20998-21011, 2021.

[11] A. Abdallah, and X. Shen, “Lightweight Security and Privacy Preserving Scheme for Smart Grid Customer-Side Networks,” *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1064-1074, 2015.

[12] P. Gope, R. Amin, S. H. Islam, N. Kumar, and V. K. Bhalla, “Lightweight and Privacy-Preserving RFID Authentication Scheme for Distributed Iot Infrastructure with Secure Localization Services for Smart City Environment,” *Future Generation Computer Systems*, vol. 83, pp. 629-637, 2018.

[13] C. P. Navdeti, I. Banerjee, and C. Giri, “Privacy Preservation and Secure Data Sharing Scheme in Fog Based Vehicular Ad-Hoc Network,” *Journal of Information Security and Applications*, vol. 63, pp. 103014, 2021.

[14] K. Prateek, F. Altaf, R. Amin, and S. Maity, “A Privacy Preserving Authentication Protocol Using Quantum Computing for V2I Authentication in Vehicular Ad Hoc Networks,” *Security and Communication Networks*, 2022.

[15] P. Manickam, K. Shankar, E. Perumal, M. Ilayaraja, and K. Sathesh Kumar, “Secure Data Transmission Through Reliable Vehicles in VANET Using Optimal Lightweight Cryptography,” in *Cybersecurity and secure information systems*, Springer, Cham, pp. 193-204, 2019.

[16] L. Wei, J. Cui, H. Zhong, I. Bolodurina, and L. Liu, “A Lightweight and Conditional Privacy-Preserving Authenticated Key Agreement Scheme with Multi-TA Model for Fog-based VANETs,” *IEEE Transactions on Dependable and Secure Computing,* 2021.

[17] K. M. Rajashekarappa, K. A. SunjivSoyjaudah, Sumithra Devi, ”Study on Cryptanalysis of the Tiny Encryption Algorithm,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 2, no. 3, pp. 88-91, 2013.

[18] N .Krishnaraj, and S.Sangeetha, “A Study of Data Privacy in Internet of Things Using Privacy Preserving Techniques with Its Management,” *International Journal of Engineering Trends and Technology*, vol. 70, no. 2, pp. 43-52, 2022.

[19] G. F. Gomes, S. S. da Cunha, and A. C. Ancelotti, “A Sunflower Optimization (SFO) Algorithm Applied to Damage Identification on Laminated Composite Plates,” *Engineering with Computers*, vol. 35, no. 2, pp. 619-626, 2019.

[20] S. K. Theodore, K. R. Gandhi, and V. Palanisamy, “A Novel Lightweight Authentication and Privacy-Preserving Protocol for Vehicular Ad Hoc Networks,” *Complex & Intelligent Systems*, pp. 1-11, 2021.