International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V70I3P238

Volume 70 Issue 3, 334-341, March 2022

Original Article

Fuzzy Logic Based Clustering with Optimal Lightweight Cryptography for Privacy-Preserving Data Transmission in Vehicular Adhoc Networks

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

[1]*Research Scholar, Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India.*
[2]*Assistant Professor, Department of Computer Science, Alagappa University Model Constituent College, Paramakkudi, Tamilnadu, India.*
[3]*Professor & Head, Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India.*

[1]prithvi678@gmail.com, [2]dr.krajiv.84@gmail.com, [3]vpazhanisamy@yahoo.co.in

Abstract *- Recently, vehicular ad hoc networks (VANETs) have received significant intention in the domain of wireless and communication technologies. It plays a vital role in intelligent transportation systems (ITS), providing safety and preventive measures to drivers and passengers. Despite the merits provided by VANET, it has some major challenging issues such as high mobility, clustering, routing, and security of the network. Owing to the decentralized and adaptive topologies of VANET, security among the users, data, and vehicles becomes important as the recognition of malicious nodes becomes mandatory. Therefore, this research work involves the design of privacy-preserving encryption with reliable data transmission for cluster-based VANETs. The proposed model involves a novel Fuzzy Logic-Based Clustering with Optimal Lightweight Cryptography with Chaotic Shell Game Optimization (FLC-OLCCSGO) algorithm for Privacy-Preserving Data Transmission through Reliable Vehicles in VANET. The major intention of the FLC-OLCCSGO approach is to accomplish security and privacy in VANET. The presented FLC-OLCCSGO technique undergoes a three-stage process such as clustering, encryption, and optimum key generation. To enhance the secrecy of the LWC technique, the optimum key generation process is performed using the CGSO algorithm. The simulation analysis of the FLC-OLCCSGO technique has been assessed under several sets of experimentations, and the outcomes are investigated in terms of distinct metrics. The experimental results showed that the provided strategy had the best results over the most current methods.*

Keywords - *VANET, Light Weight, Privacy-Preserving, Data Transmission.*

I. INTRODUCTION

The research community has given VANET a great deal of attention as a key component of the Intelligent Transportation System (ITS), and significant efforts have been made in this area. There are two types of transmission in VANET [1]. It is possible to transmit between vehicles and between vehicles and infrastructure using the VANET network [2]. In VANET, the infrastructures and vehicles, for example, Roadside Unit (RSU) and application server, interchange data for safe driving, entertainment, navigation, etc. In general, communication in VANET is classified into two groups based on the adapted radio interface. The first approach depends on Dedicated Short Range Communication (DSRC). Next, it depends on the current cellular technique [3, 4]. The mobile cellular network provides larger and wider coverage when their delay is lengthier than DSRC to real-time data exchange from local areas [4]. Thus, DSRC and mobile cellular networks could not entirely satisfy the need of ITS.

Consequently, VANET supports transmission through LTE and DSRC. Separating vehicles into clusters is a reasonable and common technique for VANET management [5]. A single eNodeB handles several clusters. Within a cluster, a minimum of one vehicle executes as a Cluster Head (CH) to gather data of each Cluster Member (CM) through DSRC and exchange the information with eNodeB through TLE [6]. Compared with other MANETs, the node in VANET has high speed and mobility.

CH changing and Cluster reforming should be more common when compared to other MANET. To increase communication quality and reduce the management overhead, the clustering approach for VANET must be capable of forming a stable cluster. Security in VANET should satisfy the requirement, as debated in [7]. Firstly, the driver needs to have a unique identifier; for mutually authenticating, they will not accept any system that induces the disclosure of the identity. Maintaining the anonymity of drivers is a paramount and critical issue. Next, security solutions in VANET need to offer non-repudiation, whereby a sender of data cannot deny having transmitted the data [8].

Furthermore, application in VANET consists of disseminating and exchanging data about possible ongoing events on the road. Consequently, data legitimacy and consistent enforcement of messages are major problems. In addition, an evolutionary, strong, and scalable security architecture is needed as a considerable amount of vehicles are registered in distinct countries and travel across borders [9]. Intrinsically, PKI appears to be an effective solution to allow secured inter-vehicle communication [10].

[11], LEACH protocol-based clustering and Light Weight cryptography (LWC) method were considered. Primarily, grouping the vehicle to cluster and sort out the network by cluster is a standout among the comprehensive and more appropriate manners. This progress offers a solution for controlling the assault on VANET security. The simulated Random Firefly (RFF) enhancement was used to identify the dependable vehicle from the created VNET architecture to increase the security dimensional of data broadcast. If it can be recognized, the LWC with Hash function is utilized for securing the data from sender to receiver.

The improved lifespan of classes, higher data transmission rates, less inter-class overburden, and improved global circumstances were some of [12]'s innovations. A scalable technique was utilized for optimizing the parameter of the GCMAV. In [13], a trust-based authentication approach to clustered VANET was presented. An objective function of the presented technique is to create a trustworthy and stable cluster that leads to the stability of the total network. Therefore, it can evaluate the trust degree of all the vehicles by integrating the trust among vehicles and Road Side Units (RSUs), and CHs are chosen dependent upon their evaluated trust degree. For the detection of suspicious data and the malicious CH node using the fog server, Gu et al. [14] established a strategy for recognizing malicious nodes in clusters based on downstream false data from fog computing VANETs. This presented technique is more constructing a trajectory clustering approach amongst vehicle nodes, whereas the CH node and the equivalent edge observing node are accurately chosen. Tangade et al. [15] presented a TMHC for securing VANET to a higher extent. The presented TMHC combines HC-based authentication with an effective and comprehensive trust management system to build trust and secure communication between vehicles. [16] demonstrated VANET's Cluster-Based Secure Communication and Certificate Revocation Scheme. The node (vehicle) is primarily collected as to different clusters, and CH are chosen depending upon the trusty node.

This paper presents a novel Fuzzy Logic-Based Clustering with Optimal Lightweight Cryptography with Chaotic Shell Game Optimization (FLC-OLCCSGO) algorithm for Privacy-Preserving Data Transmission through Reliable Vehicles in VANET. The major intention of the FLC-OLCCSGO approach is to accomplish security and privacy in VANET. The presented FLC-OLCCSGO technique undergoes a three-stage process such as clustering, encryption, and optimum key generation. To enhance the secrecy of the LWC technique, the optimum key generation process is performed using the CGSO algorithm. FLC-simulation OLCCSGO's analysis has been tested in various ways, and the results have been analyzed in terms of several metrics.

II. THE PROPOSED MODEL

The FLC-OLCCSGO approach aims to accomplish security as well as privacy in VANET. The presented FLC-OLCCSGO technique undergoes a three-stage process such as FLC based clustering, LWC based encryption, and CSGO based optimum key generation. Fig. 1 illustrates the overall framework of the proposed model.

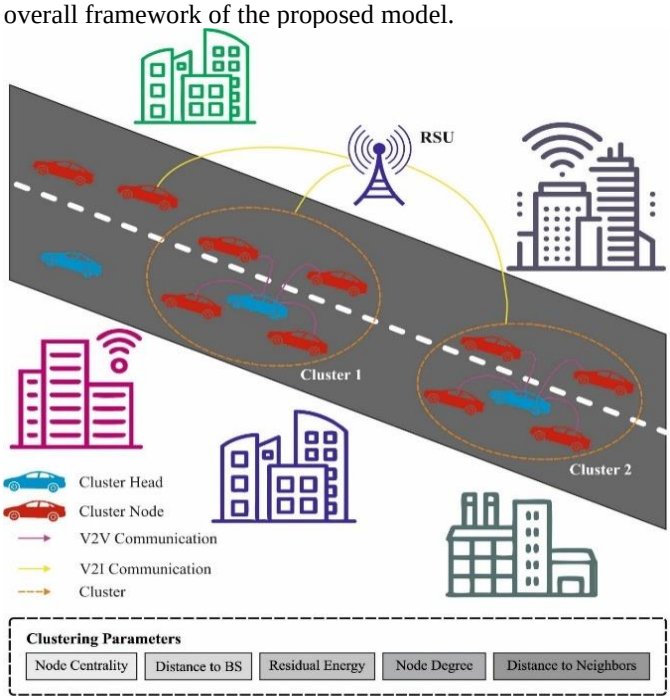

Fig. 1 VANET structure

A. Design Process of FLC Technique

Fuzzy logic comprises:

- Fuzzification of input variable: Transform the crisp input and map them to the proper linguistic variable (LV)
- Membership Function (MF); Trapezoidal and Triangular MF (TMF)
- Fuzzy decision block/Rule base: A rule base is a group of if-then rules related to the input and fuzzy output parameters utilizing LVs.
- Defuzzification: It converts the fuzzy outcome possibility to crisp values.

The TMF characterizes boundary variables, and triangular membership characterizes middle variables. It can be formulated in the following equation [17]:

$$\mu_{A1}(x) = \begin{cases} 0 & x \le a1 \\ \dfrac{x - a1}{b1 - a1} & a1 \le x \le b1 \\ \dfrac{c1 - x}{c1 - b1} & b1 \le x \le c1 \\ 0 & c1 \le x \end{cases} \quad (1)$$

$$\mu_{A1}(x) = \begin{cases} 0 & x \le a1 \\ \dfrac{x - a2}{b2 - a2} & a2 \le x \le b2 \\ 1 & b2 \le x \le c2 \\ \dfrac{d2 - x}{d2 - c2} & c2c2 \le x \le d2 \\ 0 & d2 \le x \end{cases} \quad (2)$$

The fuzzy if-then rules for selecting CH and cluster size. Rule (i) IF x_1 is A_1^i AND $x_2 is A_2^i$ AND $x_3 is A_3^i$ AND $x_4 is A_4^i$ AND $x5 is A_5^i$ THEN $y_1 is B_1^i$ AND $y_2 is B_2^i$ (5) whereas i denotes the i^{th} the rule in fuzzy rule, A_1, A_2, A_5 denotes the equivalent fuzzy set of $x1, x2x5$. The rule base comprises 243 rules and is created according to the simplest Madame Inference scheme and yields optimal outcomes. The centroid of Area (COA) is applied for defuzzification as follows

$$COA = \frac{\int \mu_A(x).xdx}{\int \mu_A(x).dx} \tag{3}$$

Afterwards, the computation of the Probability of becoming CH, all the vehicles transmit a CH-CANDIDATE-MSG to their adjacent vehicle. The vehicle receives the message, and the vehicle with a high possibility would choose them as CH and transmits its status CH-WON to the neighbour. Few vehicles might obtain several CH WON from their neighbours.

B. Process involved in optimal LWC Technique

LWC is a cryptographic procedure or protocol custom-made for use from the compelled condition. It adds to the security of the VANET network considering small impression efficiency. In this provided technique, the security for VANET employed Light Weight Hash Function (LWHF) for protecting the information [18].

- Collision resistance: It is complex to determine 2 dissimilar messages; consider accepting two messages, as,= f1 and f2; with the ultimate aim H(f1)=H(f2); this needs at any rate 2n/2 work
- Preimage-resistance: The known hash value H(f) is complex for determining f; this includes 2n work.
- Second Preimage-resistance: specified f1, it can be difficult to discover various input f2 so that H(f1) = H(f2), which includes minimum 2n work.

In the hash function, several developments have been exploited here. Sponge construction is exploited:

$$bi = br + cp \geq m \tag{4}$$

- Firstly, the bits of state are fixed to zero. Here, the input messages are separated and padded as blocks of br-bit.
- The construction encompasses squeezing and absorbing phases.
- In the absorbed phase, the r-bit input message block is XOR-ed using the br-bit of state beforehand, embedding the function P.
- The initial br-bit of the state has returned as a resultant block, trailed by considering function P.
- The user commands the number of output blocks. LWC algorithm reduces cycle rate, key size, devour less power, limits calculation time, are quicker naive, and assurance each conceivable security

To determine optimum keys for LWC, the CSGO algorithm has been developed. The shell game was simulated to invent a new optimized approach called SGO. Thus, the subsequent assumption was considered [19]:

- During this game, an individual has pondered a game operator.
- The 3 shells and 1 ball are accessible to the operator.
- All the players have only 2 chances to guess the correct shell.

At this point, a group of N people has assumed that the game player. In Eq. (5), the place '*d*' of player '*I*' is demonstrated as χ_{i}^{d}.

$$X_i = \left(x_i^1, \ldots, x_i^d, \ldots, x_i^n\right) \tag{5}$$

Now, X_i Signifies the arbitrary value to the problem parameter. Based on X_iThe value of FF was computed for all the players. Then, estimating the FF value for all players, the game operator choose 3 shells that most shells are connected to the place of the optimal player, and 2 other shells were chosen arbitrarily utilizing Eq. (6).

$$game's\ operator: \begin{cases} shell_1 = ball = X_{best} \\ shell_2 = X_{k_1} \\ shell_3 = X_{k_2} \end{cases} \tag{6}$$

Whereas, X_{best} defines the place of lesser (in minimalized problem) or higher (in maximized problem) fitness, X_{k_1} and X_{k_2} Demonstrated the place of 2 members of the population. k_1 and k_2 refers to the arbitrary amounts amongst 1 to N, which are chosen arbitrarily. The accuracy value is defined utilizing in Eq. (7).

$$AI_i = \frac{fit_i - fit(X_{worst})}{\sum_{j=1}^{N}\left[fit_j - fit(X_{worst})\right]} \tag{7}$$

Whereas AI_i refers to the intelligence and accuracy of players i and X_{worst} Implies the place of lesser (from the maximized problem) or higher (in minimalized problem) fitness. The guess vector referred by G_v It was simulated utilizing Eq. (8) to all the players.

$$G_v(x) = \begin{cases} state1: [1\ 0\ 0], & at\ first \\ state2: \begin{cases} [0.5\ 0.5\ 0] \\ 0.5\ 0\ 0.5 \end{cases}, & at\ second \\ state3: [0\ 0.5\ 0.5], & else \end{cases} \tag{8}$$

The probability of selective most states to shell selection was simulated utilizing Eq. (9).

$$state = \begin{cases} state\ 1: if AI_i > r_{g1} \\ state2: if AI_i > r_{g2} \\ state3: else \end{cases} \tag{9}$$

Whereas r_{g1}signifies the possibility of accurate guess at primary selective and r_{g2} stands for the possibility of an

accurate guess next time. Finally, X_{i} vector has been regarded as a place where all members of populations are upgraded depending on Eqs. (10)-(13).

$$dx_{i,ball}^{d} = r_1 \times \left(ball - x_i^d\right) \times state\ (1,1) \quad (10)$$

$$dx_{i,shell_2}^{d} = r_2 \times \left(shell_2^d - x_i^d\right) \times sign\left(fit_i - fit_{shell_2}\right) \times state(1,2) \quad (11)$$

$$dx_{i,shell_3}^{d} = r_3 \times \left(shell_3^d - x_i^d\right) \times sign\left(fit_i - fit_{shell_3}\right) \times state(1,3) \quad (12)$$

$$x_i^d = x_i^d + dx_{i,ball}^{d} + dx_{i,shell_2}^{d} + dx_{i,shell_3}^{d} \quad (13)$$

Whereas r_{I} refers to the arbitrarily value from the range of 0 and 1, $dx_{i,ball}^{d}$, $dx_{i,shell_2}^{d}$, &$dx_{i,shell_3}^{d}$ represents the displacement of dimensional 'd' of player 'i' dependent upon $shell_1$, $shell_2$, and $shell_3$. Fig. 2 depicts the flowchart of the SGO technique.

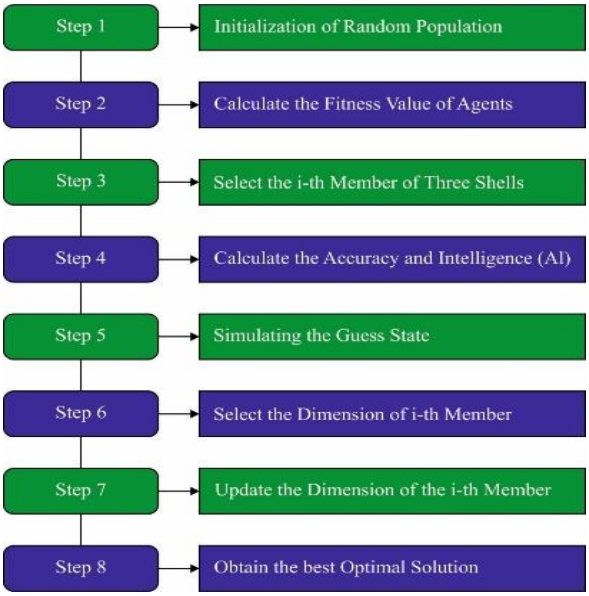

Fig. 2 Flowchart of SGO

Chaos map exploits chaotic variables with changeable nature rather than arbitrary variables. This sequence is found in non-dynamic and linear systems and non-convergent, are bounded, and non-periodic systems [20]. This offers a simple search and a high convergence rate compared to random searches. The current research employs the sinusoidal chaotic map function for improving the convergence speed and premature convergence of the SGO approach for considering a trade-off between exploitation and exploration to give better outcomes in the solution space; thus, it doesn't get stuck into the local optimum[21-22]. To change the SGO approach with a chaos map, the chaos value is replaced with a random number as follows

$$r_{i+1} = P.r_i^2 \sin(\pi.r_i) \quad (14)$$

Whereas P represent the control variable, r_i and r_{i+1} denotes the chaotic random number generated in the earlier and the existing iterations, correspondingly. Now$r_0 = 0.7$ and $P = 2.3$.

III. PERFORMANCE VALIDATION

This section inspects the experimental result analysis of the FLC-OLCCSGO model under varying aspects. Table 1 provides a brief examination of the performance of the FLC-OLCCSGO model in terms of packet delivery ratio (PDR), network lifetime (NLT), and energy consumption (ECM). The results indicated that the FLC-OLCCSGO model had improved NLT, PDR, and ECM outcomes under all vehicles, as shown in Table 1 and Fig. 3. For instance, with 50 vehicles, the FLC-OLCCSGO model has offered a PDR of 98.55%, NLT of 130hrs, and ECM of 101.32J. Also, with 150 vehicles, the FLC-OLCCSGO approach has offered a PDR of 91.64%, NLT of 141hrs, and ECM of 119.50J. Simultaneously, with 200 vehicles, the FLC-OLCCSGO method has an obtainable PDR of 88.13%, NLT of 147hrs, and ECM of 125.56J.

Table 1. Result analysis of FLC-OLCCSGO technique undercount of vehicles

No. of vehicles	Packet Delivery Ratio	Network Life Time (hrs)	Energy Consumption (J)
50	98.55	130.00	101.32
100	97.46	134.00	105.02
150	91.64	141.00	119.50
200	88.13	147.00	125.56

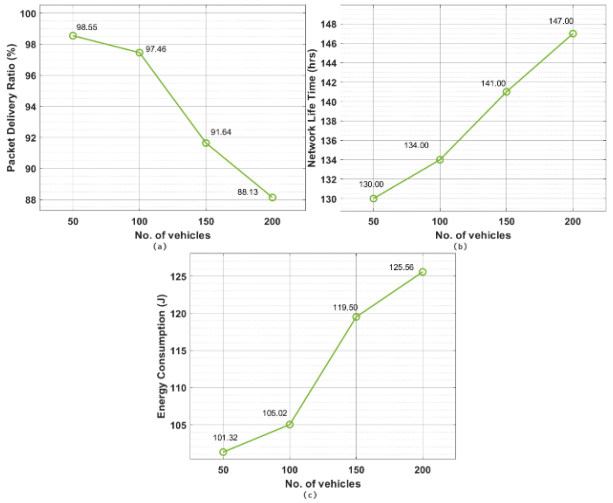

Fig. 3. Result analysis of FLC-OLCCSGO technique undercount of vehicles

Table 2 and Fig. 4 portray the encryption time (ET) and decryption time (DT) inspection of the FLC-OLCCSGO model under distinct vehicles. The experimental values indicated that the FLC-OLCCSGO model has resulted in effective ET and DT. For the sample, with 50 vehicles, the FLC-OLCCSGO model has offered ET and DT of 9.56s and 12.33s, respectively. Besides, with 150 vehicles, the FLC-

OLCCSGO method has offered ET and DT of 19.83s and 23.78s, correspondingly. In addition, with 200 vehicles, the FLC-OLCCSGO algorithm has offered ET and DT of 24.79s and 28.52s correspondingly.

Table 2. Encryption and Decryption time analysis of the FLC-OLCCSGO model

No. of vehicles	Encryption time (sec)	Decryption time (s)
50	9.56	12.33
100	14.24	21.52
150	19.83	23.78
200	24.79	28.52

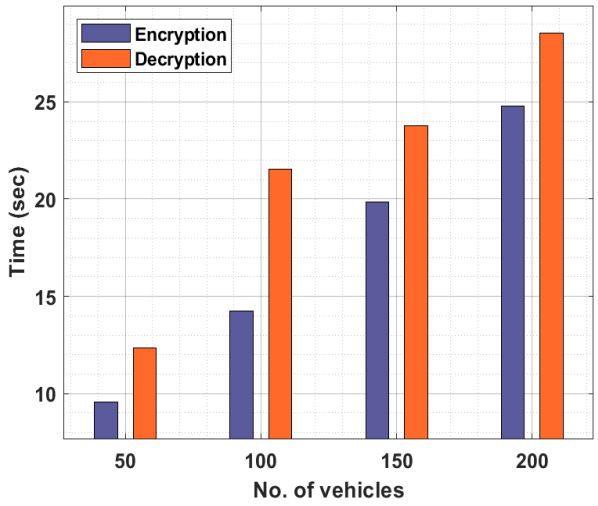

Fig. 4 ET and DT time analysis of FLC-OLCCSGO algorithm

Table 3. Clustering and security level analysis of the FLC-OLCCSGO method

No. of vehicles	Clustering level	Security Level
50	90.88	98.00
100	93.12	90.00
150	98.30	89.00
200	97.36	85.00

Table 3 and Fig. 5 depict the clustering level (CL) and security level (SL) inspection of the FLC-OLCCSGO approach under distinct vehicles. The experimental values indicated that the FLC-OLCCSGO methodology has resulted in effective CL and SL. For example, the FLC-OLCCSGO method provided CL and SL of 90.88 per cent and 98 per cent, respectively, using 50 cars. Likewise, with 150 vehicles, the FLC-OLCCSGO algorithm has offered CL and SL of 98.30% and 89% correspondingly. Besides, with 200 vehicles, the FLC-OLCCSGO technique has offered CL and SL of 97.36% and 85% correspondingly.

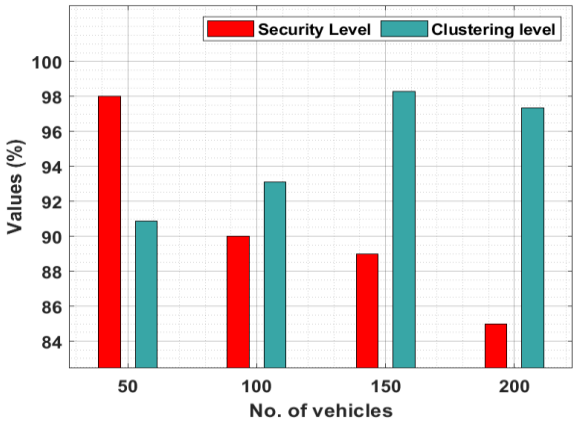

Fig. 5 SL and CL analysis of FLC-OLCCSGO technique

Table 4 and Fig. 6 provide comparative reliability (REL) inspection of the FLC-OLCCSGO model with existing techniques. The results reported that the FLC-OLCCSGO model had reached improved outcomes with increased REL under all vehicles. For instance, with 50 vehicles, the FLC-OLCCSGO model has provided increased reliability of 84.6 whereas the LEACH-RFF, LEACH-FF, and AODV-FF models have decreased reliability of 80.36, 70.9, and 67.66, respectively. Simultaneously, with 150 vehicles, the FLC-OLCCSGO technique has improved reliability by 95.06, whereas the LEACH-RFF, LEACH-FF, and AODV-FF models have decreased reliability by 88.83, 79.62, and 76.38, correspondingly. Concurrently, with 200 vehicles, the FLC-OLCCSGO method has provided an increased reliability of 98.05 whereas the LEACH-RFF, LEACH-FF, and AODV-FF models have decreased reliability of 93.32, 86.84, and 83.85, respectively.

Table 4. Reliability analysis of FLC-OLCCSGO technique with recent approaches

No. of Vehicle Nodes	FLC-OLCCSGO	LEACH-RFF	LEACH-FF	AODV-FF
50	84.6	80.36	70.9	67.66
100	91.57	87.09	77.62	79.37
150	95.06	88.83	79.62	76.38
200	98.05	93.32	86.84	83.85

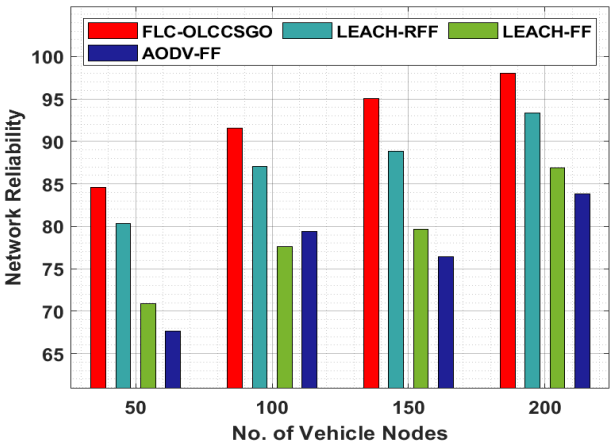

Fig. 6 Reliability analysis of FLC-OLCCSGO technique with recent approaches

Table 5. Network Lifetime analysis of FLC-OLCCSGO technique with recent approaches

No. of Vehicles	FLC-OLCCSGO	LWC-Hash	AES	DES
50	130	117	99	95
100	134	123	102	106
150	141	135	126	124
200	147	143	126	125

Table 5 and Fig. 7 examine a comparative NLT inspection of the FLC-OLCCSGO model with existing techniques. According to the results, all vehicles in the FLC-OLCCSGO system achieved improved outcomes with an increase in NLT. Using 50 cars, the FLC-OLCCSGO strategy gave a 130-hour increase in NLT, whereas the LWC-Hash, AES, and DES models provided a drop-in NLT of 117 hours, 99 hrs, and 95 hrs, respectively. There was an increase in NLT of 141 hours with FLC-OLCCSGO, whereas the NLT was reduced by 135 hours with the LWC-Hash model, 135 hours with the AES model, and 124 hours with the DES model with 150 cars. Eventually, with 200 vehicles, the FLC-OLCCSGO model has provided an increased NLT of 147hrs, whereas the LWC-Hash, AES, and DES methodologies have lower NLT of 143hrs, 126hrs, and 125hrs correspondingly.

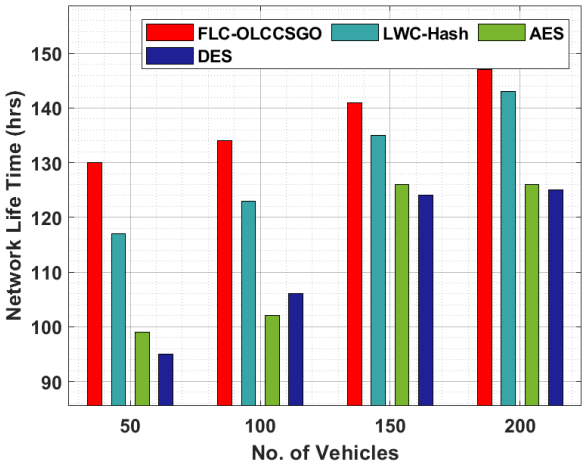

Fig. 7 NLT analysis of FLC-OLCCSGO technique with recent approaches

Table 6. Packet Delivery Ratio analysis of FLC-OLCCSGO technique with recent approaches

No. of Vehicles	FLC-OLCCSGO	LWC-Hash	AES	DES
50	98.55	97.95	88.61	87.52
100	97.46	95.4	87.64	82.43
150	91.64	85.46	74.92	68.13
200	88.13	83.16	73.71	69.71

Table 6 and Fig. 8 offer a comparative PDR inspection of the FLC-OLCCSGO model with existing techniques. The results reported that the FLC-OLCCSGO model had reached improved outcomes with increased PDR under all vehicles. Using 50 cars, the FLC-OLCCSGO approach produced a better PDR of 98.55 per cent, whereas the LWC-Hash, AES, and DES systems offered lesser PDR of 97.95 per cent, 88.51%, and 87.52 per cent, accordingly. Afterwards, with 150 vehicles, the FLC-OLCCSGO technique has provided an improved PDR of 91.64%, whereas the LWC-Hash, AES, and DES algorithms have decreased PDR 85.46%, 74.92%, and 68.13%, respectively. Finally, with 200 vehicles, the FLC-OLCCSGO model has provided an increased PDR of 88.13%, whereas the LWC-Hash, AES, and DES approaches have resulted in minimum PDR of 83.16%, 73.71%, and 69.71%, respectively.

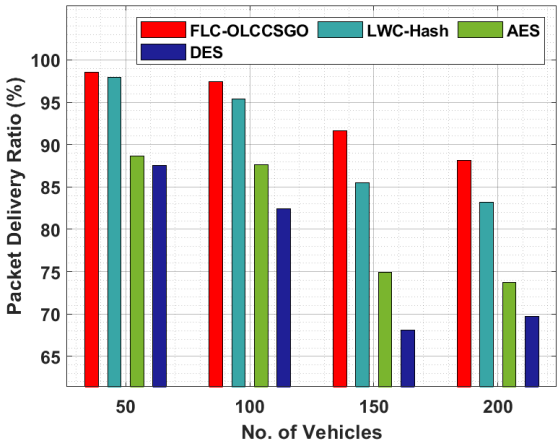

Fig. 8 PDR analysis of FLC-OLCCSGO technique with recent approaches

Table 7 and Fig. 9 provide a comprehensive ECM examination of the FLC-OLCCSGO model using modern methodologies. The findings showed that the FLC-OLCCSGO model could minimize ECM more effectively than the other models. With 50 cars, the FLC-OLCCSGO model reduced the ECM by 101.32J, whereas the LWC-Hash, AES, and DES models increased it by 105.69J, 117.31J, and 133.81J correspondingly. Simultaneously, with 150 vehicles, the FLC-OLCCSGO system has decreased ECM of 119.50J, whereas the LWC-Hash, AES, and DES approaches have obtained superior ECM of 131.79J, 139.03J, and 138.18J, correspondingly. Using 200 cars, the FLC-OLCCSGO technique reduced ECM by 125.56, whereas the LWC-Hash, AES, and DES methods produced maximum ECM of 133.64J, 139.03J, and 140.20J, respectively.

Table 7. Energy Consumption analysis of FLC-OLCCSGO technique with recent approaches

No. of Vehicles	FLC-OLCCSGO	LWC-Hash	AES	DES
50	101.32	105.69	117.31	133.81
100	105.02	109.73	118.99	128.59
150	119.50	131.79	139.03	138.18
200	125.56	133.64	139.03	140.20

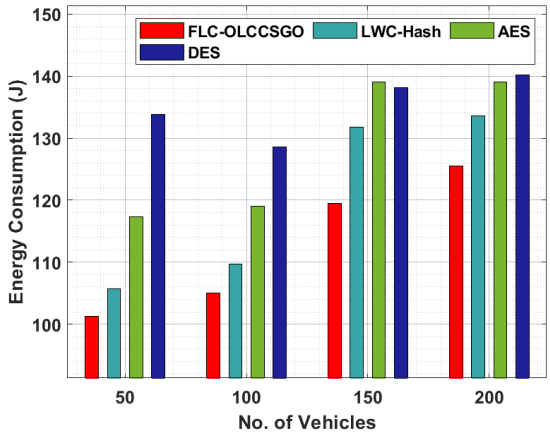

Fig. 9 ECM analysis of FLC-OLCCSGO technique with recent approaches

Table 8. Security Level analysis of FLC-OLCCSGO technique with recent approaches

No. of Vehicles	FLC-OLCCSGO	LWC -Hash	AES	DES
50	97.75	95.88	89.91	88.05
100	89.91	87.67	76.85	66.03
150	89.17	87.30	65.66	64.54
200	85.06	83.57	64.54	60.06

Table 8 and Fig. 10 offer a comparative security level (SL) inspection of the FLC-OLCCSGO technique with existing techniques. The results revealed that the FLC-OLCCSGO model had reached improved outcomes with increased SL under all vehicles. With 50 cars, the FLC-OLCCSGO method increased the SL to 97.75 per cent, whereas the LWC-Hash, AES, and DES models decreased it to 95.88 per cent, 89.91, and 89.05 per cent. Concurrently, with 150 vehicles, the FLC-OLCCSGO method has provided an increased SL of 89.17%, whereas the LWC-Hash, AES, and DES models have lower SL of 87.30%, 65.66%, and 64.54% correspondingly. At last, with 200 vehicles, the FLC-OLCCSGO model has provided an enhanced SL of 85.06%, whereas the LWC-Hash, AES, and DES techniques have resulted in lesser SL of 83.57%, 64.54%, and 64.06% correspondingly.

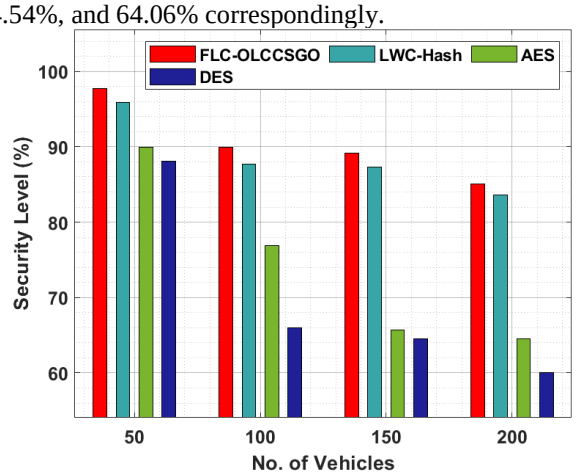

Fig. 10 SL analysis of FLC-OLCCSGO technique with recent approaches

IV. CONCLUSION

An innovative FLC-OLCCSGO method for cluster-based VANETs has been described in this research for privacy-preserving encryption with reliable data transmission. The FLC-OLCCSGO model intends to accomplish security as well as privacy in VANET. There are three stages to the FLC-OLCCSGO technique: clustering, encoding, and optimal key generation. In order to boost the secrecy of the LWC technique, the optimum key generation process is performed by the use of the CGSO algorithm. The simulation analysis of the FLC-OLCCSGO technique has been assessed under several sets of experimentations and the outcomes are investigated interms of distinct metrics. The results of the experiments showed that the new strategy had the best results when compared to other current approaches.

REFERENCES

[1] B. Ayyappan and P. M. Kumar, Vehicular Ad Hoc Networks (Vanet): Architectures, Methodologies and Design Issues, In 2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM), (2016) 177-180.

[2] W. Liang, Z. Li, H. Zhang, S. Wang and R. Bie, Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends, International Journal of Distributed Sensor Networks, 11(8) (2015) 745303.

[3] F.J.Martinez, C. K.Toh, J.C.Cano, C.T.Calafate and P.Manzoni, A Survey and Comparative Study of Simulators for Vehicular Ad Hoc Networks (VANETs), Wireless Communications and Mobile Computing, 11(7) (2011) 813-828.

[4] W.Chen, R.K.Guha, T.J.Kwon, J.Lee and Y.Y.Hsu, A Survey and Challenges in Routing and Data Dissemination in Vehicular Ad Hoc Networks, Wireless Communications and Mobile Computing, 11(7) (2011) 787-795.

[5] M.S.Sheikh, J.Liang and W.Wang, A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs), Sensors, 19(16) (2019) 3589.

[6] S.Zeadally, R.Hunt, Y.S.Chen, A.Irwin and A.Hassan, Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges, Telecommunication Systems, 50(4) (2012) 217-241.

[7] E.C.Eze, S.Zhang and E.Liu, Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, Potentials and Way Forward, In 2014 20th international conference on automation and computing, (2014) 176-181.

[8] F. Yang and Y.Tang, Cooperative Clustering-Based Medium Access Control for Broadcasting in Vehicular Ad-Hoc Networks, IET Communications, 8(17) (2014) 3136-3144.

[9] B.Yu and C. Xu, Vehicular Ad-Hoc Networks: An Information-Centric Perspective, ZTE communications, 8(3) (2010) 42-49.

[10] C. Jeremiah and A.J. Nneka, Issues and Possibilities in Vehicular Ad-Hoc Networks (VANETs). In 2015 International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE), (2015) 254-259.

[11] S. Manickam, K. Shankar, E. Perumal, M. Ilayaraja and K. SatheshKumar, Secure Data Transmission through Reliable Vehicles in VANET using Optimal Lightweight Cryptography, In Cybersecurity and Secure Information Systems. Springer, Cham, (2019) 193-204..

[12] B. Alaya and L. Sellami, Clustering Method And Symmetric/Asymmetric Cryptography Scheme Adapted to Securing Urban VANET networks, Journal of Information Security and Applications, 58 (2021) 102779.

[13] F. Mirsadeghi, M.K.Rafsanjani and B.B.Gupta, A Trust Infrastructure Based Authentication Method for Clustered Vehicular Ad Hoc Networks, Peer-to-Peer Networking and Applications, 14(4) (2021) 2537-2553.

[14] K. Gu, X. Dong, X. Li and W. Jia, Cluster-Based Malicious Node Detection for False Downstream Data in Fog Computing-Based VANETs, IEEE Transactions on Network Science and Engineering, (2022) 1-18.

[15] S. Tangade, S. S. Manvi and P. Lorenz, Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs, IEEE Transactions on Vehicular Technology, 69(5) (2020) 5232-5243.
[16] Brijilal Ruban, C. and Paramasivan, B., Cluster-Based Secure Communication and Certificate Revocation Scheme for VANET. The Computer Journal, 62(2) (2019) 263-275.
[17] J.S.Lee and W.L.Cheng, Fuzzy-Logic-Based Clustering Approach for Wireless Sensor Networks Using Energy Predication, IEEE Sensors Journal, 12(9) (2012) 2891-2897.
[18] M.Priyatham, Light Weight Cryptography for Secure Data Transmission, International Journal of Engineering Trends and Applications, 7(5) (2020) 30-35.
[19] M. Dehghani, Z.Montazeri, O.P.Malik, H.Givi and J.M.Guerrero, Shell Game Optimization: A Novel Game-Based Algorithm, Int. J. Intell. Eng. Syst, 13 (2020) 246-255.
[20] J. Bielawski, T. Chotibut, F. Falniowski, G. Kosiorowski, M. Misiurewicz and G. Piliouras, Follow-The-Regularized-Leader Routes to Chaos in Routing Games, In International Conference on Machine Learning, (2021) 925-935. PMLR.
[21] 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, 70(2) (2022) 43-52.
[22] M. V. S. S. Nagendranth, M. Rajesh Khanna, N. Krishnaraj, Mohamed Yacin Sikkandar, Mohamed Abdelkader Aboamer& R. Surendran, Type II fuzzy-based clustering with improved ant colony optimization-based routing (T2FCATR) protocol for secured data transmission in manet, The Journal of Supercomputing, First Online, (2022).