*Intelligent Automation & Soft Computing*
DOI:10.32604/iasc.2022.021467
***Article***

# Intrusion Detection System for Energy Efficient Cluster Based Vehicular Adhoc Networks

**R. Lavanya[1,*] and S. Kannan[2]**

[1]Department of Information Technology, E.G.S. Pillay Engineering College, Nagapattinam, 611002, India
[2]Department of Computer Science and Engineering, E.G.S. Pillay Engineering College, Nagapattinam, 611002, India
*Corresponding Author: R. Lavanya. Email: lavanya.ngpt1@gmail.com
Received: 04 July 2021; Accepted: 18 August 2021

**Abstract:** A vehicular ad hoc network (VANET), a subfield of mobile adhoc network (MANET) is defined by its high mobility by demonstrating the dissimilar mobility patterns. So, VANET clustering techniques are needed with the consideration of the mobility parameters amongst the nearby nodes for constructing the stable clustering techniques. At the same time, security is also a major design issue in VANET, this can be resolved by the intrusion detection systems (IDS). In contrast to the conventional IDS, VANET based IDS are required to be designed in such a way that the functioning of the system does not affect the real-time efficiency of the performance of VANET applications. With this motivation, this paper presents an efficient Fuzzy Logic based Clustering with optimal fuzzy support vector machine (FSVM), called FLC-OFSVM based on the Intrusion Detection System for VANET. The proposed FLC-OFSVM model involves two stages of operations namely clustering and intrusion detections. Primarily, FLC technique is employed for selecting an appropriate set of cluster heads (CHs) and for constructing the clusters. Besides, a lightweight anomaly IDS model named FSVM optimized with krill herd (KH) optimization algorithm is developed for detecting the existence of malevolent attacks in VANET. The KH algorithm based on the herding behavior of krills is used for optimally tuning the parameters of the FSVM model. In order to investigate the performance of the FLC-OFSVM model, an extensive set of simulations have been carried out and the results thus showcased that the OFSVM model has gained maximum outcome with an accuracy of 99.98%.

**Keywords:** Clustering; intrusion detection; vehicular communication; VANET; machine learning; krill herd optimization; fuzzy logic

## 1 Introduction

Vehicle ad hoc networks (VANET) were developed as a part of the mobile ad hoc network (MANET) [1] application. It is observed as a significant methodology for the intelligent transportation systems (ITS). Recently, many scientists are giving more importance and working in the field of wireless mobile data transmission. In VANET, vehicles are utilized as network nodes. It comprises of three main data

transmission types that are feasible in VANET: a) Vehicle to Vehicle (V2V), b) Vehicle to Infrastructure (V2I), and c) Hybrid. However, this current data transmission type suffers from several drawbacks such as the requirement of huge amount of Road Side Units (RSU) at standard location in V2I data transmission that aren't financially possible, security and privacy problems in V2V based data transmissions [2], hence the clustering data transmission type is chosen as it offers several benefits on above three data transmission types [3]. This method portrays a congested traffic scenario that increases the load on the cluster head (CH), this causes delay in the data transmission process and thus affects the network performances. For handing this issue, a novel clustering framework stimulated from the dolphin swarm behavior has been introduced in this study, here, many nodes can perform as a CH in a cluster and therefore could allocate their load in heavy traffic situations, this enhances the efficiency level of the entire network. Fig. 1 depicts the architecture of cluster VANET.

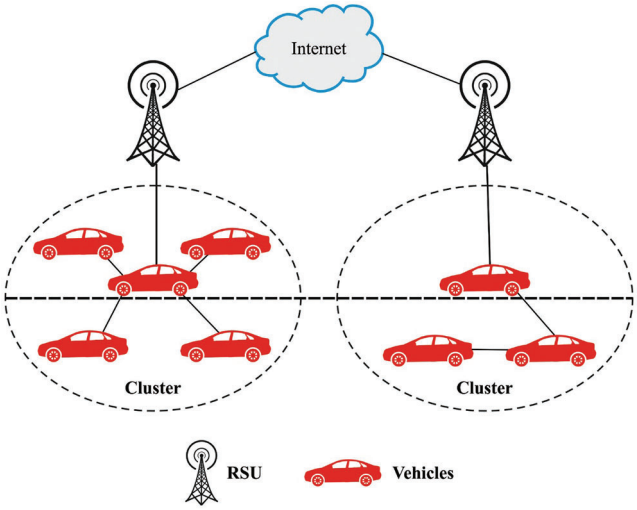


**Figure 1:** Architecture of Clustered VANET

VANET provides several applications and services to the clients involved in the security of the navigational aid, drivers, and infotainments. It comprises of two types of data allocated in VANET: safety (curve warning, vehicle speed warning) and non-safety data (value added comfort application) [4]. The standard safety data provides high priority in VANET related to the non-safety data, the safety data informs the driver of predictable danger and permits for earlier responses. In spite of the advantages provided by VANET, it has several problems based on the transmitted messages, security, and privacy of the clients. Since vehicles exit and enter highways, they would rely on specific safety information's such as the traffic road conditions and congestions, decision making on that route for reaching their destination. It is vital that this data be sent at an appropriate time; or else, it can lead to delay in attaining the destination securely [5]. In certain conditions, few malicious nodes would refuse to transmit or would even purposefully change the required safety messages before transferring the same to the requested client, this can cause long delays or mortalities. Moreover, the features of VANET (such as volatility, higher mobility) appear to be different from those of the wireless data transmission networks that have made VANET vulnerable to several external and internal attacks [6]. Because of the dynamic topology and the decentralized structure of VANET, the safety of the vehicles, clients, and data have become the most significant factors as the detection of faulty nodes/malicious/user becomes complex [7].

Alternatively, those that are different from the conventional Intrusion Detection Systems (IDS) such as the VANET based IDS should be placed with care in this manner as the process shouldn't delay the real-time

efficiency of the VANET application. The survey comprises of several resolutions for the VANET based issues [8]. Mostly, it comprises of challenges such as higher false positives, lower detection rates, additional overheads on the network, higher detection time, and so as the ones related to them. On the other hand, it cannot detect the modified and the newer attacks. Abnormality based IDS possesses several benefits over the rule-based IDS in such a way that it can detect the novel attacks where the signature isn't existing in the database. However, this class of IDS requires settings of an optimum threshold and a large trained set for making it proficient for differentiating the normal and the malicious nodes.

This paper presents an efficient Fuzzy Logic based Clustering technique with optimal fuzzy support vector machine (FSVM), called FLC-OFSVM based Intrusion Detection System for VANET. The proposed FLC-OFSVM model makes use of the FLC technique with different input parameters for selecting the cluster heads (CHs) and for organizing the clusters. In addition, a lightweight anomaly IDS model named FSVM optimized with krill herd (KH) optimization algorithm has been developed for detecting the existence of malevolent attacks in VANET. For optimally tuning the parameters involved in the FSVM model the KH algorithm has been employed in such a way that the intrusion detection rate can be effectively enhanced. For examining the outcomes of the FLC-OFSVM model, a comprehensive set of experimental analysis have been performed and the results have been inspected in-terms of various defined aspects.

## 2 Literature Review

Several security systems have been presented by numerous scientists for addressing both the privacy and the security-based problems in VANETs. This segment emphasizes on few of the present methodologies that focus on the related issues in VANET with identical methods. An anonymous and lightweight authentication system smart card (ASC) is presented in Ying et al. [9] for addressing the privacy preserving issues such as the legitimacy of the user and the message transferred over the network. Low-cost cryptographic operations are used in the user and message verification procedures. This protocol doesn't authenticate the user identity nor verifies the transmitted messages, however it assures the privacy of the concerned user. Wazid et al. [10] introduced a decentralized lightweight authentication and key agreement protocol (LAKAP) for VANET, this makes use of the bitwise exclusive OR (XOR) operation and the one-way hash function.

Rajput et al. [11] presented a hybrid method for the privacy preserving authentication scheme (HEPPA) that integrates the features of the pseudonym and the group signature-based methods with conditional anonymity. This technique utilizes the lightweight and the simple pseudonyms that provides conditional privacy. Tangade and Manvi [12] presented an efficient, scalable, and privacy preserving authentication (ESPA) protocol by a hybrid cryptography method for inter-vehicle data transmissions.

Cui et al. [13] projected a secure privacy preserving authentication scheme for VANET with cuckoo filter (SPACF) for enhancing the privacy and security of the clients, and for reducing the data transmission overheads. Moreover, the investigators projected a novel authentication system without bilinear pairings that could lead to heavy computational costs. The cuckoo filter is a data structure that offers an optimum search time and searches for accuracy by utilizing the hash functions. The present methods deliberated have been chosen as the standard protocol for this work since this approach focuses on the improvement of security and privacy preservations of a user in the network. It has been observed that the present methodologies mainly focus on the authentication and privacy preserving systems. But, the other security necessities of VANET such as non-repudiation, availability, and integrity have not been dealt with at most interest. This provides a gap for the additional development in VANET security with the deliberation of executing a novel security-based technique which is available in the present times. Hence, the resolution presented in this work tries to enhance the VANET security by employing a modern technology which

can tackle the security needs and enhance the road security aspect with the help of vehicle resources and data transmission schemes.

## 3 The Proposed Model

The overall system architecture of the proposed FLC-OFSVM model has been demonstrated below. Initially, the vehicles in the VANET are placed randomly in the target area. Then, the network initialization process takes place where the single hop neighboring vehicles interact with one another. Next, the FLC technique is performed for optimally selecting the CHs and for constructing the clusters proficiently. Followed by which, the FSVM model is employed for the identification of intrusions in the network. Finally, the KH algorithm is used for optimally choosing the parameters involved in the FSVM model.

### *3.1 Design of FLC Technique*

At this stage, the FLC technique with three input parameters is utilized for selecting the CHs as shown in Fig. 2. In this presented scheme, every node transmits its mobility data, average velocity to its neighbor via HELLO packet with the succeeding formats: Average Velocity, Node ID, Direction, and Location.

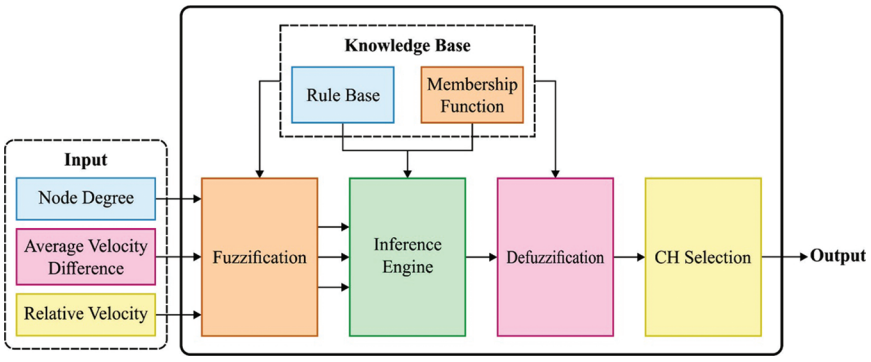


**Figure 2:** Process involved in FLC technique

Node Degree

The amount of velocity variances between the adjacent vehicles is the main problem in the construction of relatively stable clustering topologies. The neighbourhood relation is thus formed by the location data embedding from the periodic messages transmitted by the vehicles. Vehicles transmit their present state to every node with their broadcast range $R$:

$$N_i = \{v_j;\ \mathrm{dis}_{i,j} \leq R\}, \tag{1}$$

Whereas $\mathrm{dis}_{i,j}$ denotes the average distance among the vehicles $i$ and $j$. According to this determination, they acquire the other terms such as the node degree of a node ($\psi_i$), that is determined by the overall amount of $R$-neighbors. Then, clusters are made with vehicles travelling in similar directions, every $R$-neighboring vehicle travel in the opposite direction isn't deliberated [14]. Thus, every $R$-neighboring nodes utilized in this analysis are restricted to this vehicle that travels in a similar direction, located in other lanes and estimated by:

$$\psi_i = |N_i|. \tag{2}$$

The node degree of node $i$ is assumed by the cardinality of set $N_i$.

Average velocity differences

In all time intervals, every vehicle will comprise of data regarding their individual vehicles, their transmission ranges and therefore would be able to estimate its average velocity variance $\phi_i$ from every vehicle by:

$$\phi_i = \frac{1}{\psi_i - 1} \sum_{j=1}^{\psi_i - 1} |v_j - v_i|, \tag{3}$$

Whereas $j$ denotes the possible neighboring vehicle, and $v_i$, $v_j$ indicates the velocities of the vehicles $i$ and $j$, correspondingly in m/s. The node can attain its velocity by the commercial navigation services such as the Garmin Traffic.

Relative velocity

For building a relatively stable cluster, they would tend to assume the vehicles related to the optimum neighborhood degree ($\psi_i$). A relatively low velocity simply implies that the neighbor of a particular node has consumed a long time in its broadcast range. Thus, they could accomplish that the stated node comprises of additional stable situations. The relative velocity of a node $i$ is estimated by:

$$\omega_i = \frac{\phi_i}{v_i}. \tag{4}$$

The lesser the value of $\omega_i$, the nearer the velocity of a node for an average velocity of their neighbour that improves the neighbourhood steadiness. In this presented system, every node calculates its neighbors based on link connectivity, average velocity difference, and relative velocity. If a node wants to transmit a packet, then it would make use of FL for calculating the fit factor value for every neighbor in terms of link connectivity duration, average absolute distance, and average velocity.

*3.1.1 Fuzzification Process*

Fuzzification is the procedure of transforming the mathematical values to the fuzzified values by a MF. The transmitter node utilizes the average absolute distance and the MF for calculating the degree to which the distance factors belong to Large, Small, and Medium ranges. The transmitter node utilizes the average velocity and the MF for calculating that degree the average velocity comes under Fast, Slow and Medium ranges. The transmitter node utilizes the link connectivity duration and the MF for calculating the link connectivity. When the fuzzy values of link connectivity, duration average absolute distance, and average velocity are estimated, the fuzzy inference engine would map the fuzzy values to the IF or THEN rules and would be restricted in the knowledge base for calculating the fit factor for every node. The fuzzy inference scheme is thus implemented based on the introduced twenty seven rules. Therefore, their equivalent calculation results should be integrated.

*3.1.2 Defuzzification Process*

Defuzzification is the procedure of generating a numerical result on the basis of the output MF and the equivalent membership degree. Now, they would utilize the center of gravity (CoG) technique for defuzzifying the fuzzy results. Particularly, they would cut the output MF with a straight horizontal line based on the equivalent degree and would eliminate the top part. Later, they would estimate the Centroid of this shape.

### *3.2 Design of IDS Technique*

Once the vehicles in the VANET are clustered, the next stage would be to identify the presence of intruders in the network using the OFSVM model. In addition, the KH algorithm is employed for optimally tuning the parameters of the FSVM model in such a way that the intrusion detection rate can be enhanced.

*3.2.1 FSVM Model*

In a conventional SVM, every data point is deliberated with an equivalent significance and allocated with a similar penal variable in its objective function. To resolve this problem, the system of FSVM was presented in [15]. Fuzzy membership to every instance point is presented; thus, the distinct instance points could create various contributions to the creation of decision surfaces. Assume that the trained instance are represented as follows,

$$S = \{(x_1,\ y_i,\ \ s_i),\ \ i = 1,\ \ \ldots,\ \ N\}, \tag{5}$$

Whereas $x_1 \in R^n$ denotes the $n$-dimension instance point, $y_i \in \{-1,\ +1\}$ denotes the class label, and $s_i (i = 1, \ldots, N)$ indicates the fuzzy membership that fulfils $\sigma \le s_i \le 1$ with adequately smaller constant $\sigma > 0$. Re quadratic optimization problem for classification is deliberated as:

$$\min_{w,\ s,\ \xi} \ \frac{1}{2} w^T w + C \sum_{i-1}^{l} s_i \xi_i \tag{6}$$

$$s.t.\ y_i(w^T x_l + b) \ge 1 - \xi_i,\ \xi_i \ge 0,\ i = 1,\ \ldots,\ l,$$

Whereas $w$ denotes the normal vector of the splitting hyperplane, $b$ indicates the bias term, and $C$ represents the variable that should be defined before for controlling the trade-off among the classification margin and the cost of misclassification error [16]. Then $s_i$ would denote the attitude of the equivalent point $x_1$ to a single class and the slack parameters $\xi_i$ would denote the measure of error, later the expression $s_i\xi_i$ is deliberated as a measure of error with distinct weights. It can be stated that the larger $s_i$ is, the more prominently the equivalent point would be processed; the lesser the $s_i$ is, the lesser prominently the equivalent point would be processed; therefore, the distinct input points could create various contributions for learning the decision surfaces. Hence, the FSVM could detect the stronger hyperplane by increasing the margin allowing a few misclassifications of the lesser significant points.

To resolve the FSM optimum problem, (6) is converted to the succeeding two problems by presenting the Lagrangian multipliers $\alpha_i$:

$$\max \sum_{i=1}^{N} \alpha_i - \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i \alpha_j y_i y_j x_i x_j \tag{7}$$

$$s.t. \sum_{i=1}^{N} y_i \alpha_i = 0,\ 0 \le \alpha_i \le s_i C,\ i = 1,\ \ldots,\ N.$$

Related to the regular SVM, the aforementioned representation has a slight variance, that is the upper bound of the values of $\alpha_i$. By resolving these two problems in (3) for optimum $\alpha_i$, $w$ and $b$ are recovered in a similar manner as in the regular SVM.

*3.2.2 Overview of KH Algorithm*

The KH algorithm is a type of swarm intelligence technique that is inspired from the herding characteristics of the krills. In the procedure of predation, the predator would alter the distribution of the krill population, this would urge them to move quickly and would later decrease their distribution density and the distance among the predator and the food would now become farther than in the first stage of the KH. In this method, the distribution of the krill population is defined in the succeeding 3 conditions: the impact of the other krill individuals, arbitrary diffusion, and the behaviour of acquiring the food. The KH method is defined as:

$$dX_i dt = N_i + F_i + D_i \tag{8}$$

Whereas $N_i$ denotes the impact of the other krill individuals, $F_i$ represents the behaviour of acquiring food, and $D_i$ indicates the behaviour of arbitrary diffusion; $i = 1, 2, \ldots, N$, and $N$ represents the population size.

For the impact of the other krill individuals, the movement $N_{i,new}$ of the krill $i$ induced by another krill can be determined using the following relationship:

$$N_{i,new} = N_{\max}\alpha_i + \omega_n N_{i,\,old} \tag{9}$$

where, $N_{\max}$ denotes the maximal induced velocity, $N_{i,old}$ indicates the earlier induced motion, $\omega_n$ denotes the inertia weight and the value range zero and one and $\alpha_i$ represents the individual $i$ that is caused by the induction direction of the adjacent neighbors [17].

The succeeding behaviour $F_i$ is to get food, by:

$$F_i = V_f\ \beta_i + \omega_f F_{i,old} \tag{10}$$

where, $V_f$ represents the maximal foraging speed, and its value is a constant, that is 0.02 ($ms^{-1}$); $\omega_f$ indicates the inertia weight of the foraging motion, and its range is zero and one; $F_{i,old}$ denotes the earlier foraging motion; and $\beta_i$ represents the foraging direction. Fig. 3 demonstrates the flowchart of the KH technique. The individual $D_i$ in the final behavior is represented by the following equation:

$$D_j = D_{\max}\left(1 - \frac{I}{I_{\max}}\right)\delta \tag{11}$$

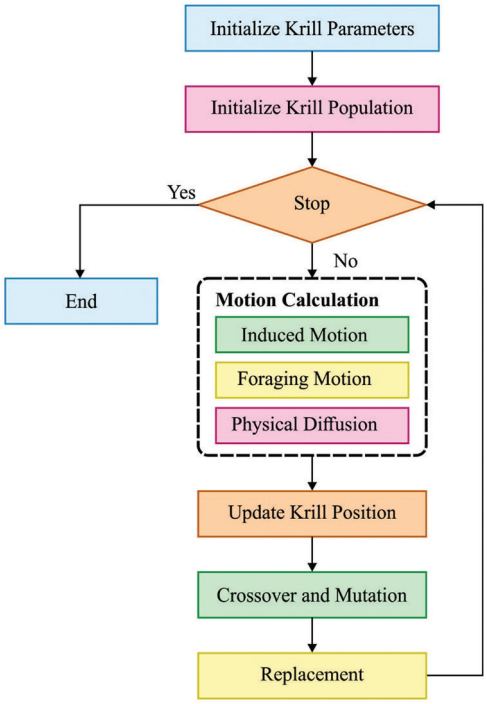


**Figure 3:** Flowchart of KH

where $D_{\max}$ denotes the maximal arbitrary diffusion speed; $\delta$ indicates the direction of the arbitrary diffusion; and $I$ and $I_{\max}$ denotes the present amount and the maximal number of iterations, correspondingly. From the

aforementioned procedure, they could attain the krill upgrade procedure of the KH method by using the following relationships:

$$X_i(t+\Delta t) = X_i(t) + \Delta t \frac{dX_i}{dt} \tag{12}$$

$$\Delta t = Ct \sum_{j=1}^{NV} (UB_j - LB_j) \tag{13}$$

where $\Delta t$ denotes time the interval relevant to the concerned application; $NV$ represents the dimension of the decision parameter; step factor $Ct$ indicates the constant among (0,2); and $UB_j$ and $LB_j$ denotes the upper and the lower bounds of the equivalent parameter $j$ $(j = 1,\ 2, \ldots, NV)$ , correspondingly.

The process of the KH algorithm (Algorithm 1) is given as follows.

**Algorithm 1:** Pseudo code of KH algorithm

Begin

Step 1: Initiation. Initiate the generation counter $G$, the population $P$, $V_f$, $D_{\max}$, and $N_{\max}$.

Step 2: Fitness evaluation. Evaluate the fitness function of every krill based on theirearly position.

Step 3: While $G <$ Max Generation do

Arrange the population based on its fitness.

for $i = 1{:}N$ (all krill) do

Execute the succeeding movement evaluation.

Movement induced by other individuals

Foraging movement

Physical diffusion

Execute the genetic operator.

Upgrade the krill location from the search space.

Evaluate the fitness to every krill based on its novel place

end for i

$$G = G + 1.$$

Step 4: end while.

End.

*3.2.3 Parameter Tuning of FSVM Model Using KH Algorithm*

In the OFSVM model, the parameters (weight and bias) in the FSVM model are optimally adjusted by the KH algorithm. The FSVM model is trained with the parameters of the KH algorithm. Besides, 10 fold cross validation process is employed for determining the fitness function where the training data is split arbitrarily into 10 parts. Then, 9 sets of data are employed for training the process and the final one is utilized for testing the process. This process gets iterated ten times; therefore, every set is utilized once for testing the model. The fitness function can be represented as $1\text{-}CA_{validation}$ of the 10-fold cross-validation (CV) technique in the training data, as given in equations. (14) and (15). Besides, the solution with higher $CA_{validation}$ holds the lower fitness value.

$$Fitness = 1 - CA_{validation} \tag{14}$$

$$CA_{validation} = 1 - \frac{1}{10}\sum_{i=1}^{10}\left|\frac{y_c}{y_c + y_f}\right| \times 100 \tag{15}$$

where $y_c$ and $y_f$ refers to the count of true and false classifications correspondingly.

## 4 Performance Validation

A brief comparative study of the FLC with the other techniques in-terms of NLT, EC, and throughput is represented in Tab. 1. The proposed model is simulated using the NS3 tool and the results are investigated under the distinct number of vehicles. Fig. 4 examines the NLT analysis of the FLC technique with the other methodologies under varying number of vehicles. The proposed FLC technique has gained the maximum NLT under all distinct numbers of vehicles. For instance, with 20 vehicles, the proposed FLC technique has accomplished a higher NLT of 4600 rounds whereas the HEPPA, ASC, and LAKAP techniques have attained a lower NLT of 4400, 4000, and 3800 rounds respectively. In addition, with 60 vehicles, the presented FLC approach has accomplished a superior NLT of 4100 rounds whereas the HEPPA, ASC, and LAKAP techniques have attained a lower NLT of 3700, 3600, and 3500 rounds correspondingly. Also, with 100 vehicles, the proposed FLC technique has accomplished a higher NLT of 3600 rounds whereas the HEPPA, ASC, and LAKAP methodologies have obtained a minimum NLT of 3300, 3200, and 3100 rounds correspondingly.

**Table 1:** Result analysis of the proposed FLC with the other techniques

| Network Lifetime (Rounds) | | | | |
|---|---|---|---|---|
| Number of Vehicles | Proposed FLC | HEPPA | ASC | LAKAP |
| 20 | 4600 | 4400 | 4000 | 3800 |
| 40 | 4400 | 4100 | 3700 | 3600 |
| 60 | 4100 | 3700 | 3600 | 3500 |
| 80 | 3700 | 3500 | 3300 | 3200 |
| 100 | 3600 | 3300 | 3200 | 3100 |
| Energy Consumption (mJ) | | | | |
| Number of Vehicles | Proposed FLC | HEPPA | ASC | LAKAP |
| 20 | 32 | 40 | 46 | 56 |
| 40 | 58 | 64 | 69 | 79 |
| 60 | 79 | 91 | 94 | 114 |
| 80 | 94 | 109 | 118 | 127 |
| 100 | 103 | 136 | 153 | 172 |
| Throughput (Kbps) | | | | |
| Number of Vehicles | Proposed FLC | HEPPA | ASC | LAKAP |
| 20 | 67.01 | 65.75 | 57.00 | 53.28 |
| 40 | 72.42 | 70.35 | 64.45 | 60.65 |
| 60 | 77.27 | 74.23 | 69.24 | 64.72 |
| 80 | 81.61 | 78.75 | 72.21 | 69.19 |
| 100 | 83.91 | 80.85 | 78.36 | 73.48 |

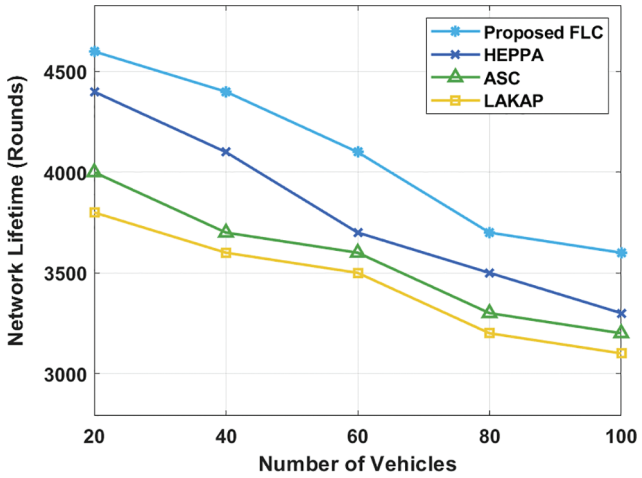


**Figure 4:** Network lifetime analysis of FLC model

An EC analysis of the proposed FLC technique with the recent methods is represented in Fig. 5. The figure portrays superiority of the FLC technique with minimal EC over the other techniques, whereas, the LAKAP technique has displayed insufficient performance with the maximum EC. For instance, with 20 vehicles, the proposed FLC technique has resulted in the least EC of 32mJ whereas the HEPPA, ASC, and LAKAP techniques have demonstrated a maximum EC of 40mJ, 46mJ, and 56mJ, respectively. Additionally, with 60 vehicles, the proposed FLC method has resulted in the lesser EC of 79mJ, whereas, the HEPPA, ASC, and LAKAP approaches have showcased a maximal EC of 91mJ, 94mJ, and 114mJ, correspondingly. Besides, with 100 vehicles, the presented FLC algorithm has resulted in the least EC of 103mJ whereas the HEPPA, ASC, and LAKAP techniques have revealed a higher EC of 136mJ, 153mJ, and 172mJ, correspondingly.

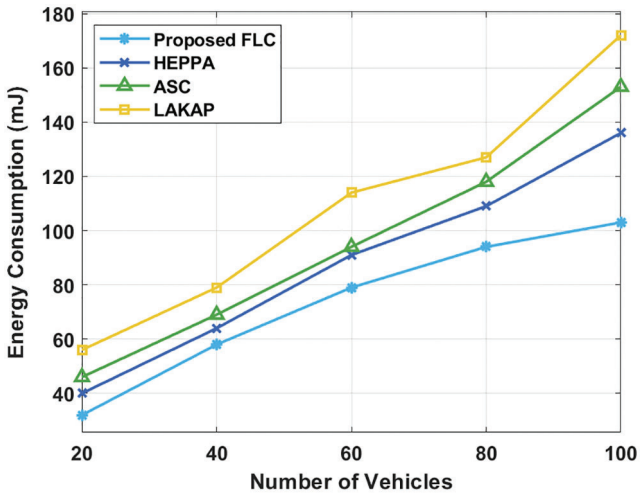


**Figure 5:** Energy consumption analysis of FLC model

Fig. 6 examines the throughput analysis of the FLC technique with the other methods under varying number of vehicles. The proposed FLC technique has gained maximum throughput under all distinct number of vehicles. For instance, with 20 vehicles, the proposed FLC technique has accomplished a higher throughput of 67.01Mbps whereas the HEPPA, ASC, and LAKAP techniques have attained a

lower throughput of 65.75Mbps, 57Mbps, and 53.28Mbps respectively. Moreover, with 60 vehicles, the presented FLC manner has accomplished a maximum throughput of 77.27Mbps whereas the HEPPA, ASC, and LAKAP techniques have achieved a lesser throughput of 74.23Mbps, 69.24Mbps, and 64.72Mbps correspondingly. Furthermore, with 100 vehicles, the projected FLC technique has accomplished a maximal throughput of 83.91Mbps whereas the HEPPA, ASC, and LAKAP approaches have attained a lower throughput of 80.85Mbps, 78.36Mbps, and 73.48Mbps rounds correspondingly.

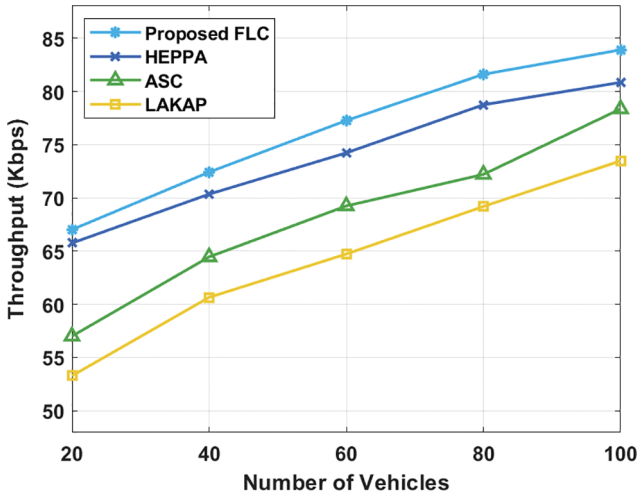


**Figure 6:** Throughput analysis of FLC model

A brief comparison study of the FLC with the other techniques in-terms of PDR and ETE delay has been represented in Tab. 2 [18]. Fig. 7 inspects the PDR analysis of the FLC algorithm with the other techniques under varying number of vehicles. The presented FLC technique has gained maximal PDR under all distinct number of vehicles. For instance, with 20 vehicles, the proposed FLC technique has accomplished a higher PDR of 0.98% whereas the HEPPA, ASC, and LAKAP techniques have attained a lesser PDR of 0.95%, 0.93%, and 0.82% correspondingly. In the meantime, with 60 vehicles, the proposed FLC method has accomplished a superior PDR of 0.78% whereas the HEPPA, ASC, and LAKAP approaches have achieved minimal PDR of 0.74%, 0.71%, and 0.62% respectively. At the same time, with 100 vehicles, the proposed FLC method has accomplished a higher PDR of 0.69% whereas the HEPPA, ASC, and LAKAP methodologies have attained a lower PDR of 0.63%, 0.55%, and 0.48% correspondingly.

An ETE delay analysis of the proposed FLC technique with the recent techniques has been represented in Fig. 8. The figure has demonstrated that the FLC approach has offered superior results with the minimal ETE delay over the other methods, whereas, the LAKAP algorithm has portrayed insufficient performance with the higher ETE delay. For instance, with 20 vehicles, the proposed FLC technique has resulted in a least ETE delay of 7.57 ms whereas the HEPPA, ASC, and LAKAP manners have demonstrated a maximal ETE delay of 7.97 ms, 8.07 ms, and 10.57 ms, correspondingly. Meanwhile, with 60 vehicles, the proposed FLC technique has resulted in the least EC of 8.39 ms whereas the HEPPA, ASC, and LAKAP techniques have outperformed a higher EC of 9.04 ms, 9.57 ms, and 11.61 ms, correspondingly. Eventually, with 100 vehicles, the projected FLC technique has resulted in the least EC of 9.38 ms whereas the HEPPA, ASC, and LAKAP methods have showcased a maximal EC of 10.14 ms, 10.4 ms, and 13.11 ms, correspondingly.

**Table 2:** PDR and ETE delay analysis of the proposed FLC with the other techniques

| Packet Delivery Ratio (%) | | | | |
|---|---|---|---|---|
| Number of Vehicles | Proposed FLC | HEPPA | ASC | LAKAP |
| 20 | 0.98 | 0.95 | 0.93 | 0.82 |
| 40 | 0.87 | 0.84 | 0.80 | 0.71 |
| 60 | 0.78 | 0.74 | 0.71 | 0.62 |
| 80 | 0.72 | 0.67 | 0.60 | 0.55 |
| 100 | 0.69 | 0.63 | 0.55 | 0.48 |
| End-to-End Delay (ms) | | | | |
| Number of Vehicles | Proposed FLC | HEPPA | ASC | LAKAP |
| 20 | 7.57 | 7.97 | 8.07 | 10.57 |
| 40 | 8.13 | 8.47 | 8.69 | 11.11 |
| 60 | 8.39 | 9.04 | 9.57 | 11.61 |
| 80 | 8.92 | 9.80 | 10.17 | 12.04 |
| 100 | 9.38 | 10.14 | 10.40 | 13.11 |

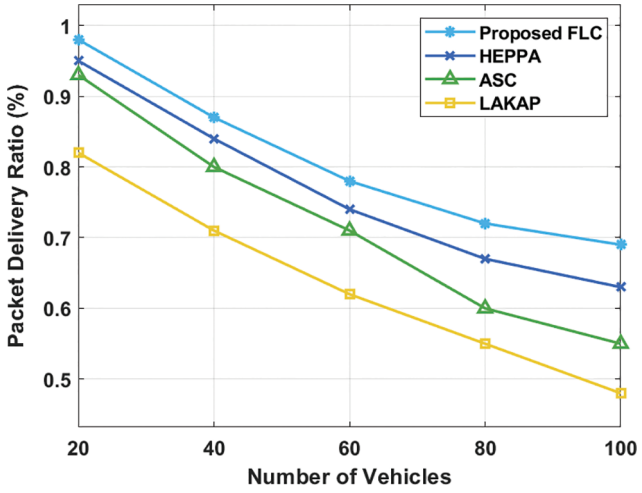


**Figure 7:** PDR analysis of FLC model

For validating the IDS performance of the OFSVM method, it is tested using the NSL-KDD 2015 dataset that includes a set of 125973 instances with 51 class labels and 2 classes. Tab. 3 and Fig. 9 demonstrates the detailed detection accuracy analysis of the OFSVM with the other methods [19]. The table values showcased that the CS-PSO algorithm has gained lowest performance with the accuracy of 75.51% whereas a certainly enhanced performance is obtained by the DNN-SVM and Cuckoo optimization methods with the accuracy of 92.03% and 96.88% correspondingly. Besides, the behavior-based IDS, PSO-SVM, MLIDS, and DBN models have exhibited moderately closer accuracy of 98.89%, 99.1%, 99.93%, and 99.96% respectively. However, the proposed OFSVM model has gained maximum outcome with an accuracy of 99.98%. From the above-mentioned tables and figures, it is evident that the presented method is an effective tool for achieving a secure and reliable data transmission in a cluster based VANET.

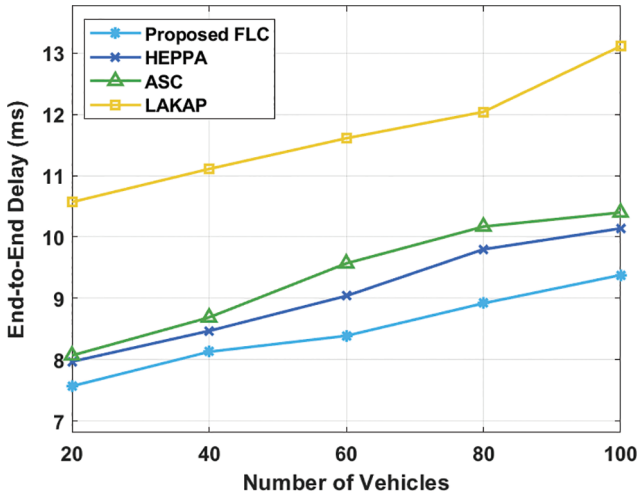


**Figure 8:** ETE delay analysis of FLC model

**Table 3:** Result analysis of the Proposed OFSVM method with the existing methods for the applied dataset

| Methods | Accuracy |
|---|---|
| Proposed OFSVM | 99.98 |
| Deep Belief Network (2020) | 99.96 |
| MLIDS (2019) | 99.93 |
| CS-PSO (2019) | 75.51 |
| PSO-SVM (2019) | 99.10 |
| Behaviour Based IDS (2019) | 98.89 |
| Cuckoo Optimization (2018) | 96.88 |
| DNN+SVM (2018) | 92.03 |

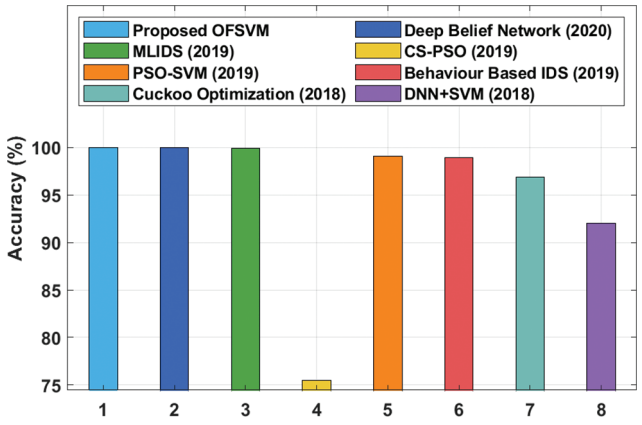


**Figure 9:** Accuracy analysis of OFSVM model with existing techniques

## 5 Conclusion

This paper has presented an effective FLC-OFSVM model for achieving security and effective communication in VANET. The proposed FLC-OFSVM model begins with the deployment of vehicles in a random way and is thus initialized together. Then, the FLC technique is executed for identifying the proper set of the CHs in VANET and the neighboring vehicles thus join the CH for developing the cluster. Moreover, the OFSVM model is applied for identifying the existence of the intruders from VANET. In order to optimally tune the parameters involved in the FSVM model, the KH algorithm is employed in such a way that the intrusion detection rate can be enhanced. For examining the outcomes of the FLC-OFSVM model, a comprehensive set of experimental analysis have been performed and the results are thus inspected in-terms of several aspects. The resultant experimental values highlighted the promising performance of the FLC-OFSVM model over the state of art methods. As a part of the future work, the security of the VANET can be improved by designing secure multihop routing protocols for enhancing the privacy preservations of the data transmission procedures with reliable vehicles in VANET.

**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.

## References

[1] M. R. Ghori, K. Z. Zamli, N. Quosthoni, M. Hisyam and M. Montaser, "Vehicular ad-hoc network (VANET): Review," *in Proc. IEEE Int. Conf. on Innovative Research and Development (ICIRD)*, Bangkok, Thailand, pp. 1–6, 2018.

[2] E.Vishnupriya, T. Jayasankar and P. Maheswara Venkatesh, "SDAOR: Secure data transmission of optimum routing protocol in wireless sensor networks for surveillance applications," *ARPN Journal of Engineering and Applied Sciences,* vol. 10*,* no.16*,* pp. 6917–6931, 2015.

[3] H. Lu, J. Li and M. Guizani, "Secure and efficient data transmission for cluster-based wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems,* vol. 25*,* no. 3*,* pp. 750–761, 2013.

[4] S. K. Bhoi, P. M. Khilar, M. Singh, R. R. Sahoo and R. R. Swain, "A routing protocol for urban vehicular ad hoc networks to support non-safety applications," *Digital Communications and Networks,* vol. 4*,* no. 3*,* pp. 189–199, 2018.

[5] C. Lai, K. Zhang, N. Cheng, H. Li and X. Shen, "SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Transactions on Intelligent Transportation Systems,* vol. 18*,* no. 6*,* pp. 1559–1574, 2016.

[6] R. G. Engoulou, M. Bellaiche, S. Pierre and A. Quintero, "VANET security surveys," *Computer Communications,* vol. 44*,* pp. 1–13, 2014.

[7] N. J. Patel and R. H. Jhaveri, "Trust based approaches for secure routing in VANET: A survey," *Procedia Computer Science,* vol. 45*,* pp. 592–601, 2015.

[8] O. Depren, M. Topallar, E. Anarim and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," *Expert Systems with Applications,* vol. 29*,* no. 4*,* pp. 713–722, 2005.

[9] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Transactions on Vehicular Technology,* vol. 66*,* no. 12*,* pp. 10626–10636, 2017.

[10] M. Wazid, A. K. Das, N. Kumar, V. Odelu, A. G. Reddy *et al.*, "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks," *IEEE Access,* vol. 5*,* pp. 14966–14980, 2017.

[11] U. Rajput, F. Abbas, H. Eun and H. Oh, "A hybrid approach for efficient privacy-preserving authentication in VANET," *IEEE Access,* vol. 5*,* pp. 12014–12030, 2017.

[12] S. Tangade and S. S. Manvi, "Scalable and privacy-preserving authentication protocol for secure vehicular communications," in *Proc. IEEE Int. Conf. on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1-6, 2016.

[13] J. Cui, J. Zhang, H. Zhong and Y. Xu, "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Transactions on Vehicular Technology,* vol. 66*,* no. 11*,* pp. 10283–10295, 2017.

[14] S. K. Apolin, B. Veniston and N. Krishnaraj, "Efficient routing in vanets using tabu search algorithm," *Journal of Critical Reviews,* vol. 7*,* no. 13*,* pp. 989–994, 2020.

[15] C. F. Lin and S. D. Wang, "Fuzzy support vector machines," *IEEE Transactions on Neural Networks,* vol. 13*,* no. 2*,* pp. 464–471, 2002.

[16] X. Gu, T. Ni and H. Wang, "New fuzzy support vector machine for the class imbalance problem in medical datasets classification," *The Scientific World Journal,* vol. 2014*,* Article ID 536434, pp. 1-12, 2014.

[17] C. L. Wei and G. G. Wang, "Hybrid annealing krill herd and quantum-behaved particle swarm optimization," *Mathematics,* vol. 8*,* no. 9*,* pp.1403, 2020.

[18] A. S. Khan, K. Balan, Y. Javed, S. Tarmizi and J. Abdullah, "Secure trust-based blockchain architecture to prevent attacks in VANET," *Sensors,* vol. 19*,* no. 22*,* pp. 4954, 2019.

[19] M. Maheswari and R. A. Karthika, "A novel qos based secure unequal clustering protocol with intrusion detection system in wireless sensor networks," *Wireless Personal Communications,* vol. 118*,* pp. 1535–1557, 2021.