*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

# RSU based Joint Congestion-Intrusion Detection System in Vanets Using Deep Learning Technique

***Sunanthini.J*[a*], Dr. K. Siva Sankar[b], Dr.C.Brintha Malar[c]**
[a]Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kanyakumari,India
[b]Department of Information Technology, Noorul Islam Centre for Higher Education, Kanyakumari, India.
[c]Department of Physics, TDMNS College, Tirunelveli, India
Corresponding Author Email: sunakenny@gmail.com

**Abstract:** Vehicular Ad hoc Network (VANET) is a technology that makes it possible to provide many practical services in intelligent transportation systems, but it is also susceptible to several intrusion threats. Through the identification of unusual network behavior, intrusion detection systems (ID Ss) can reduce security vulnerabilities. However, rather than detecting anomalous network behaviors throughout the whole VANET, current IDS systems are only able to do so for local sub-networks. Hence there is a need for a Joint Congestion and Intrusion Detection System (JCIDS). We designed an JCICS model that can collect network data cooperatively from vehicles and Roadside Units (RSUs).This paper, proposes a new deep learning model to improve the performance of JCIDS by using k-means and a posterior detection based on coresets to improve the detection accuracy and eliminate the redundant messages. The efficacy of the current Recurrent Neural Network (RNN) and Honey badger Algorithm (HBA)on the fundamental AODV protocol is combined with the advantages of the JCIDS is suggested in this protocol. First, formation of clusters using vehicle's mobility parameters like, velocity and distance to enhance route stability. Moreover, a vehicle will be chosen as Cluster Head with highest route stability. Second, the efficient intrusion detection is achieved with the consumption using RNN method. In the RNN, the optimal weighting factor is selected with the help of HBA. The RNN is performing efficient prediction with the assistance of HBA. The finest path for data dissemination is selected by choosing link lifetime, hop count and residual energy along the path.As a result, multimedia data streaming is improved network life time, in terms of reduced packet loss ratio and energy consumption as compared to existing DNN and SVM scheme for different node density and speed.

Keywords: Vehicular Ad hoc Network (VANET), AODV protocol, Roadside Units (RSUs), Joint Congestion and Intrusion Control System (JCICS), Recurrent Neural Network (RNN), K-means and Honey badger Algorithm (HBA)

## 1. INTRODUCTION

One of the primary study topics for intelligent transportation systems is enhancing transportation safety. (ITS). Data distribution through Vehicular Ad-Hoc Network (VANET), comprising vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) connections, is a crucial facilitator for secure and dependable traffic movement. VANET is a potential technology that facilitates communication between conventional cars driven by a human and driverless autonomous vehicle, which are anticipated to dominate future traffic. Applications for traffic control and safety on the VANET may be divided into two categories [1-3]. Applications for traffic management include those that help drivers plan their routes. The road condition apps and accident information systems serve as examples of safety-related applications. The density of receivers and actions is essential to this vehicle-based communication mechanism. The roadside unit (RSU) that is used to send information from one car to another is managed by the VANET based on the acquired vehicle communication. The sent signals aid in successfully establishing the intelligent transport system and controlling the VANET [4, 5]. The discussions indicate that Fig. 1 depicts the V2V communication method.

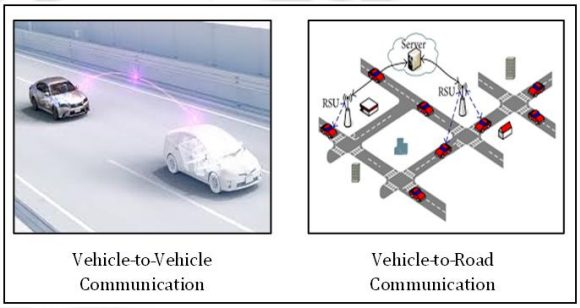


Fig.1: VANET communication in vehicles

Roads may become safer because to VANETs, particularly in situations that are now regarded as risky and inevitable. Imagine being able to drive securely in situations that would otherwise be very hazardous, such as fog, collisions, and black ice. Before the full potential of VANETs can be realized, however, certain very critical security challenges must be resolved [6]. Because of how quickly and dynamically information moves over vehicular networks, it is crucial that the information exchanged be reliable and useful. The credibility of the information must be determined immediately since contacts will be brief and actions on the information must be taken promptly [7, 8].

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

The main automakers have announced that from 2015, their cars have been fitted with wireless access vehicular environment (WAVE), indicating the impending rollout of VANETs. The IEEE 802.11p standard, which offers the fundamental radio standard for short-range communication (DSRC) in VANETs, is the foundation upon which WAVE protocols are founded. Vehicle to infrastructure (V2I) and vehicle to vehicle (V2V) communication between the cars in VANETs may both be accomplished via the usage of DSRC. (V2I). Road travel will become considerably safer and more efficient because to these technology advancements in automobiles, which will profoundly alter how people see it [9].

VANET technology is one of the smart technologies that play a major role in critical infrastructure systems that are necessary for the national health, security, and economy [10] because of the high data dissemination via V2X communications. As a consequence of the frequent alternation between sparse and busy traffic circumstances in VANETs, dynamic, unpredictable, and highly mobile vehicle nodes are produced, which impairs the performance of applications. Channel congestion problems have a negative impact on the majority of safety applications, particularly in scenarios with heavy traffic when several car nodes transmit safety warnings to other vehicles. To enable efficient system operation, such as detecting anomalies and failures, forecasting electricity usage, and assessing power quality, for instance, the smart grids infrastructure necessitates transmitting a massive amount of real-time data to computing centers through communication networks [11, 12]. In this case, VANET might be used as a temporal computing core to efficiently acquire, handle, and analyse the growing amount of data. As a consequence, as VANET provides real-time processing needs, it may increase the reliability of the smart grid system. Network security concerns continue to have a substantial impact on VANET and its integration with crucial systems that must quickly store, transfer, preserve, and retrieve data through networks [13]. However, for VANET to grow and prevent assaults that might have negative effects, data-driven intrusion detection systems (IDSs) must be developed [14, 15].

In this research, a deep learning-based congestion management technique that use RSUs to manage congestion is provided. In this architecture, each RSU has free access to a machine learning algorithm that filters and clusters the data. The appropriate priorities are then established for each cluster based on the base deferral and criticality for transmitting messages across different classes. The messages are then sent to numerous cars in order to avert accidents or traffic jams. The performance of VANETs is improved by appropriately managing network congestion.

*Our Contributions*

*The main contributions in this paper are:*

- A novel deep learning detector for RSU is proposed for bogus information attack, impersonation attack and RSU replication attack.
- Deep learning-based algorithms and models may assist reliable resource management and communication analysis, as well as the rising communication and computation needs of new networking applications.
- Security-based Recurrent Neural Network (RNN) with Honey badger Algorithm (HBA) technique was utilized to identify RSU replication attacks. The RNN-HBA technique demonstrated the most outstanding feature selection and parameter optimization capabilities compared with other well-known metaheuristic algorithms.
- In the RNN, the weighting parameter is selected with the help of the Honey badger Algorithm (HBA). The optimization techniques further improve the congestion and intrusion control in VANET.
- By reducing message transmissions, or preventing broadcast storms, the suggested technique manages network message congestion. Furthermore, we demonstrate that even when up to 40% of nodes are malicious and contribute false parameter values, cars may maintain network functionality utilizing the suggested model and joint congestion Intrusion detection.
- The effectiveness of the suggested technique was assessed using performance metrics including energy consumption, throughput, latency, and packet delivery ratio. Software called MATLAB was used to complete the implementation.

The rest of this paper is organized as follows: related work is discussed in Section 2. The system and the attack model are presented in Section 3. In Section 4, overview of the proposed JCIDS is presented. Section 5 evaluates the security performance of the proposed JCIDS in detail. The results are discussed in Section 6 and the conclusions and future work are given in Section VII.

## 2. LITERATURE REVIEW

The security of VANETs is a crucial problem that has been the subject of study for a long time. The users of the vehicular networks will be making potentially life-saving choices based on the information received, which makes them special. Therefore, a system for identifying bogus information is essential. on order to guarantee message integrity and non-repudiation on VANETs, researchers have suggested utilizing cryptography and digital signatures to protect and sign messages.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

A weight-based ensemble machine learning algorithm (WBELA) has been developed by Zhang et al. [16] to recognize aberrant messages of the vehicular Controller Area Network (CAN) bus network. Then, we create a model based on multi-objective optimization for CAN bus network intrusion detection. A many-objective optimization algorithm based on balance convergence and diversity (MaOEA-BCD) is created to accommodate this paradigm. The efficacy of the proposed technique for various ID data frames is assessed using open-source CAN bus message data sets and tamper attack scenarios.

For automotive Ad Hoc networks, Zhou et al. [17] have proposed a distributed collaborative intrusion detection system based on invariant. Stochastic Petri Net is utilized in this instance to define the system's security state after describing the system's state and dynamic transfer. The simulation findings show that the DCDIV has a greater detection rate, a lower false alarm rate, a quicker attack detection rate, and assures system security throughout the detection process when compared to current approaches.

A hybrid VANET architecture has been developed by Theerthagiri et al. [18] for efficient vehicle communication. The multihop routing method is used in the proposed hybrid architecture to enable automobiles to increase their driving performance and road safety. The proposed hybrid vehicular multihop routing algorithm with intelligent transportation system (Hybrid VMR-ITS) efficiently enables instantaneous communications between vehicles and roadside units (RSUs) and vehicles-traffic servers.

Using the safe AODV routing algorithm, Kumar et al. [19] built a black hole attack detection method for vehicle ad-hoc networks. The source and destination nodes are verified using a cryptographic function-based encryption and decryption as an extra layer of security. Using various network factors, including lose packets, end-to-end latency, packet delivery ratio (PDR), and routing request overhead, the suggested technique is shown using an NS-2.33 simulator.

In order to raise detection efficiency and improve detection accuracy, Bangui et al. [20] studied a machine learning model to enhance the performance of IDSs. They used Random Forest and a posterior detection based on coresets. The results of the experiments demonstrate that, when compared to machine learning models used in traditional applications, the suggested model may greatly improve detection accuracy.

Throughput, signal strength index, and fitness function were used by Sefati et al. [21] to study identifying Sybil attacks in vehicle ad-hoc networks. The nearby nodes carry out the first identification. Each node checks its ID with the IDs of messages from other nodes when it gets a message from surrounding nodes. Neighboring nodes transmit a sample of the data to the RSU if the messages are identical but came from different nodes. RSU creates a database of metrics, including a delay, packet loss, and throughput, if it has any questions about an ID.

Tosunoglu et al.[22] have presented a detection of abnormalities in VANETs is based on the combination of K-Means and C5.0, two potent machine learning algorithms. A complex technique called K-Means is used to efficiently combine data based on similarities between the data. A decision tree may be built using the C5.0 decision tree method to categorize data. The characteristics that have the greatest or least influence on the outcome have been identified, depending on the data's information. The research did not do any particular feature normalization, and the impact of the feature on the outcome was also noted.

## 3. PROPOSED METHODOLOGY FOR ROBUST JOINT CONGESTION AND INTRUSION DETECTIONTHROUGH DEEP LEARNING ALGORITHM

The Mobile Ad-hoc Network (MANET) subtype known as VANET is unique and has caught the interest of many academics worldwide. VANET applications are connected to life and include sensitive data. With the development of each new technology, there are opportunities for its exploitation, and VANET is no different. VANET is subject to several security assaults because of elements like the lack of a centralized regulating authority and significant mobility, among others. In order to address these security concerns, a unique Honey Badger Algorithm (HBA) JCIDS for VANET based on Recurrent Neural Networks (RNN) has been suggested in this research. The combined congestion and intrusion management in VANET are intended to be improved by the suggested hybrid optimal detection system. To take use of these two characteristics and stop RNN-HBA in VANETs, several changes are made to the AODV routing protocol's standard operations. The AODV protocol, as is known, operates on demand. The route information is always updating since the nodes are mobile. Due to this, each node between the source and destination nodes chooses whether to relay or discard the RREQ packets during the route discovery process. Attacks are carried out in the scenario utilizing RREQ packets. Figure 2 displays the block diagram for the proposed technique.

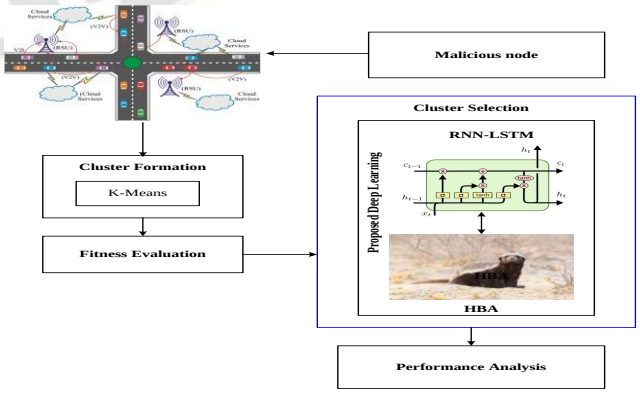


Fig 2: Block diagram for the proposed research methodology

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

*3.1. VANET Model*

As shown in Figure 3, a typical highway traffic flow is taken into account. The suggested IDSs, however, are not limited to a particular kind of road; they may function well in a variety of situations, including one-way traffic, two-way traffic, urban areas, highway areas, etc. The suggested VANET concept uses broadcast-based vehicle-to-vehicle (V2V) and vehicle-to-RSU (V2I) communications to transmit beacon signals. Generally speaking, the contents of such communications may vary. In this study, we take into account that each vehicle routinely transmits signals in the format (ID, speed, location, direction) [23]. To ensure authenticity and identity, we assume that unique pseudonyms are given to each vehicle by a centralized authority. Thus, the RSUs are constantly aware of each vehicle's ID. Although collected messages may be utilized for a variety of things, they are often employed to alert other moving objects on the road. For instance, an RSU uses the beacon signals it receives from the cars in its range to determine the average speed and the density of the road. It then transmits these calculated messages to the other RSUs to alert the vehicles that are not in range. RSUs are crucial to the security of the VANET. As a result, we suggest an IDS that runs statistically at each RSU. Although the beacon messages are already encrypted for secure communications, it is still important to ensure the integrity—that is, the accuracy of the message content—as well as the availability of VANET communications.

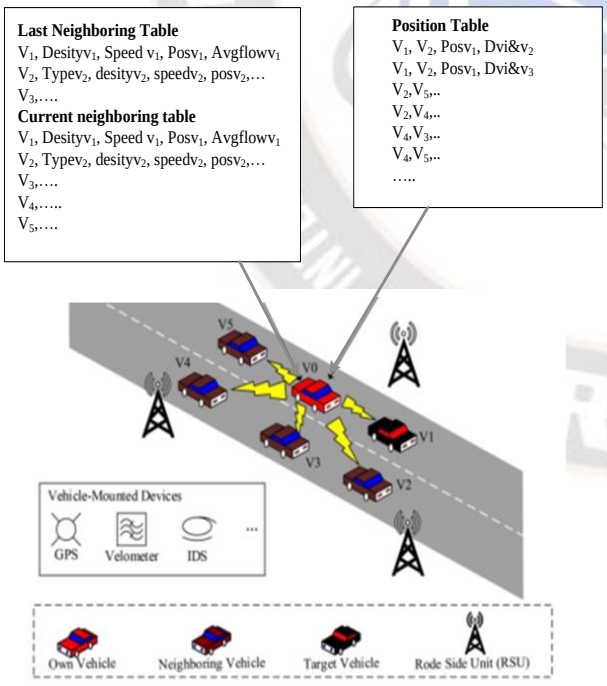


Fig 3: Traffic model for the nominal case where all vehicles broadcast messages and RSU collects these messages

The connection between and traffic flow ($O_{TFlow}$) of the own vehicle to be $O_{Speed}$ described as follows using equations (1) and (2) from the Green-Shields model:

$$O_{Speed} = Max_{speed} - \frac{O_{Density}}{Max_{Density}} * Max_{speed} \quad (1)$$

$$O_{TFlow} = O_{Speed} * O_{Density} \quad (2)$$

where $Max_{Density}$ denotes the free flow speed at zero density, $Max_{Speed}$ is also the point at which traffic is snarled at zero speed. The following to be deduced from equations (1) and (2) as $AvgO_{TFlow}$ indicated in equation (3):

$$AvgO_{TFlow} = \frac{1}{n}\left(\sum_{i=1}^{n-1} AvgNeg^{t}{}_{TFlow} + O_{TFlow}\right) \quad (3)$$

where $n-1$ is the number of nearby cars at the time point and $AvgO^{t}{}_{TFlow}$ is the average traffic flow of nearby vehicles at the previous time point. Equation (4), which is based on the free space model, may be used by the own vehicle to determine how far it is from either a nearby or a target vehicle:

$$D_{i,j} = \sqrt{\frac{PS_j * LW_j^2}{(4\pi)^2 RS_j}}, i = O(own), j \in \{n(neg), t(tag)\} \quad (4)$$

Where, $RS_j$ $LW_j$ and $PS_j$ are the received signal intensity, wave length, and transmitting power of the nearby (or target) vehicle.

## *Message Format*

The own vehicles constantly transmit a beacon message $(Msg_{BC})$ at the same interval $(t_{BC})$ while speaking to nearby vehicles, or an emergency message $(Msg_{EMG})$ in the event of an accident [24]. Equations (5) and (6) illustrate the message format as follows:

$$(O_{ID}, O_{Density}, O_{Speed}, O_P, AvgO_{TFlow}) \quad (5)$$

$$(O_{ID}, O_{Type}, O_{Density}, O_{Speed}, O_P, AvgO_{TFlow}) \quad (6)$$

Where $O_{Type}$ is the sort of emergency and $O_{ID}$ is the identification of the own vehicle. As the own car is also the neighbor for its surrounding vehicles, it should be noted that the messages from the own vehicle to the nearby vehicles will be changed to $(O_{ID}, O_{Type}, O_{Density}, O_{Speed}, O_P, AvgO_{TFlow})$ in transmission.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Equation (7) states that the own vehicle will broadcast a request message $(Msg_{RQT})$ when it wants to know the location of its target vehicle.

$$Msg_{RQT}(O_{ID}.Tag_{ID}) \quad (7)$$

Where $Tag_{ID}$ is the name of the intended target vehicle. Following receipt, $Msg_{RQT}$ the target vehicle's surrounding vehicles broadcast their locations as well as the distances between them and the target vehicle. The own vehicle may be able to receive the response messages $Msg_{RSP}$ for a certain waiting time ($t_{WAIT}$, which is less than $t_{BC}$), and whose format is as follows:

$$Msg_{RSP}(Neg_{ID}.Tag_{ID}, Neg_{P}, NegTag_{D}) \quad (8)$$

The distance between the target car and its nearby neighbors $NegTag_{D}$ is located.

## *Information Tables*

Each vehicle contains three tables, namely the position table, the last nearby table, and the current neighboring table, to store the messages inside a communication window, as illustrated in Fig. 3. The position table is used to preserve, and the two adjacent tables are utilized to store $Msg_{BC}$ and $Msg_{EMG}$ receive from its adjacent cars. These things' lifespans in the three tables are fixed. The elements in the final neighboring table and the position table are erased when the lifetime is over. The entries in the current adjacent table are then transferred to the final neighboring table, where $(O_{ID^t}, O_{Type^t}, O_{Density^t}, O_{Speed^t}, O_{P^t}, AvgO_{TFlow^t})$ are recorded as illustrated in Fig. 3.

## *Congestion Detection Phase*

The network collision will be identified using a measurement-based technique. This phase detects the presence of a collision by sensing the channel, reading the channel busy time value, and comparing it to the predetermined criteria. In our approach, we assume that the messages in the queue have already been delivered. Phase considers that data congestion took place if the Busy Time value exceeds the cutoff [25].

## *Data Control Phase*

Data collection, data filtering, and data clustering are the three steps that make up the data control phase's three-step process for managing data flow. Data gathering involves gathering communications sent and received by vehicles. The duplicate signals that RSU received from numerous cars are removed in the filtering phase to reduce the need for extra processing. The message content, message ID, and sender address are all parts of every message that is received. If the RSU gets the identical message after it has been transmitted by a different vehicle, it will identify it as duplicate. The K-means algorithm is used to group data in the clustering component on the basis of multiple dimensions. This method is effective for arranging and grouping large information sets because it has a short operating time, automatically detects patterns, predicts future records, and efficiently manages expansive information.

## *Congestion Control Phase*

Setting the proper cluster priorities at this period reduces network congestion. After the clusters are formed, they are dispersed, evaluated, and the fitting parameters are adjusted for each bunch to ensure that the prioritized high-speed vehicle cluster receives the most urgent messages with the highest transmission range and rate. As a result, the emergency messages are sent with less delay and the appropriate messages are transmitted to the appropriate vehicles with a reduced packet loss ratio. By alerting the appropriate group of cars, this manages network congestion and averts any dangerous circumstances like accidents in the future.

### *3.2 Cluster Formation using K-means algorithm*

The source node sets the backoff time in accordance with the vehicle ID and weight value it gets before checking to see whether it has received any messages from other nodes. When a node gets a message from one of the cluster heads, it joins CH. The node assumes the role of a new cluster head when it receives no information from any cluster heads. Link Life Time is specified for the node to choose the cluster head when it gets more than two messages from various CHs. There are two options available if the node gets messages from numerous CHs. If messages are received quickly, a cluster head with a higher LLT [26] value will be chosen as the cluster head and established as the direct gateway for two neighboring clusters. If it is already a member of a cluster head and it learns about a change in location from another cluster head, it could switch its status from member to gateway. Assume that if it is already a member of one cluster and gets a message from a head that is not a member of that cluster, it switches to the state of an indirect gateway. If the node's LLT value is below the required minimum LLT, it will not be a member of any cluster. In order to identify congestion, the congestion detection unit evaluated the degree of channel utilization. The data control unit gathered the messages, filtered them to remove any duplicates, and then used a K-means clustering algorithm to divide the messages into four groups. The following are the definitions of the terms:

$$Sim_{M} = \frac{\sum_{n=1}^{N} M_{S*A*D}}{N} \quad (9)$$

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Here, the target node's neighbors are shown $N$ , $M_{S*A*D}$ along closely their speeds, accelerations, and directions resemble those of the target node. The mobility similarity describes how similar the target node's motion state is to all of its surrounding nodes. The mobility state of the node is more similar to the motion states of the nearby cars the higher the value of the mobile similarity. Additionally, the choice of cluster heads is influenced by the vehicle's position as well as the average distance between it and its neighbors. As a result, average adjacency as well as location must also be considered. The placement element reveals the position of the car on the street, i.e., if it is close to the middle of the street. The cluster's utilization rate rises as the cluster head gets nearer to the road's center, which allows it to accommodate more cluster member nodes [27]. What constitutes a location factor is:

$$L = 1 - \frac{|w_i - w_o| * |v_i - v_o|}{|w_o| * |v_o|} \quad (10)$$

Here, $(v_i, w_i)$ denotes the coordinates of the vehicle node and $(v_0, w_o)$ denotes the coordinates of the road center. The cluster structure will be more compact and communication will be more effective if the cluster head is closer to the surrounding neighbors. It defines the average adjacency.

$$D = 1 - \frac{\sum D_{ij}}{N} \quad (11)$$

$D_{ij}$ normalized distance between the target node i and the neighbor node j is represented by N, N is the total number of neighbors of the target node.

$$D_{ij} = \frac{\sqrt{(v_i - v_j)^2 + (w_i - w_j)^2}}{T_R} \quad (12)$$

Here, $T_R$ is the communication radius, $(v_j, w_j)$ is the neighbor nodes' coordinates, and $(v_i, w_i)$ is the destination node's coordinates.

The cluster head selection factor is $\Psi$ defined as follows:

$$\Psi = \lambda_1 * S_M + \lambda_2 * L + \lambda_3 * D \quad (13)$$

It is beneficial to utilize public transportation as much as possible as cluster leaders for local communications. Therefore, we make the assumption that buses are uniformly scattered on the route and that the cluster head will be chosen from $\Psi$ among buses in the research cluster head selection procedure. The bus with the highest cluster head selection factor is $\Psi$ chosen as the cluster head after calculating the values for each bus.

## 4. JOINT CONGESTION AND INTRUSION CONTROL USING RNN-LSTM IN VANETS

The deployment of an intrusion detection system in a VANET context adds additional overhead and delays to both nodes and the network. A combined RNN-optimized congestion-based intrusion detection is therefore presented. Here, extracted feature F is used as the input to the RNN-LSTM to forecast whether an intrusion into the VANET would occur or not. The loss error between the data acquired after the dimension reduction and the original data is reduced by using these two matrices. After obtaining a low-dimensional representation of high-dimensional data characteristics, recurrent neural network classifiers may utilize this information as input. A sort of RNN that may preserve sequential information is the LSTM. For sequential data, RNNs perform better than ANNs, although they also have vanishing gradient issues. Since any two significant events in the time series might occur with significant gaps, this hinders the network's capacity to recall information over extended periods of time. With its relative insensitivity to this gap length, LSTMs are designed to address the issue of disappearing gradients. Due to the cells' capacity to retain values over almost any time period, LSTM networks are best suited for classification issues involving time series data [28]. Fig. 4 depicts the LSTM network's design.

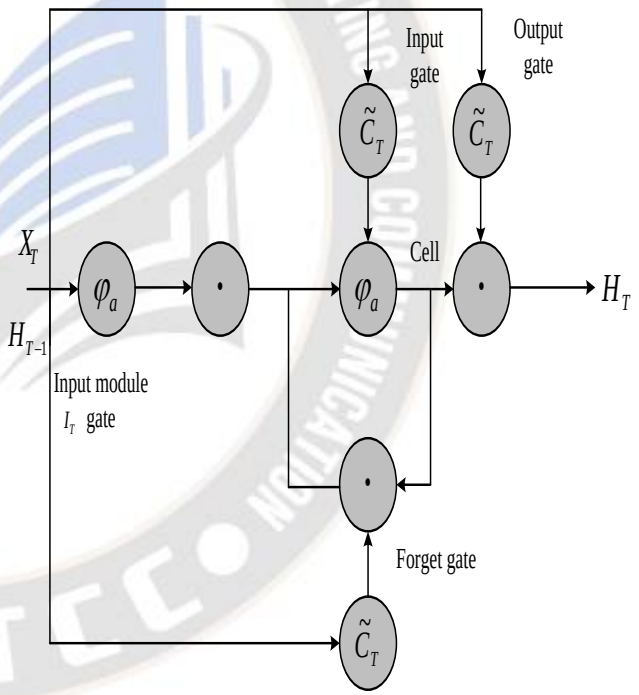


Fig 4: Architecture of the proposed RNN-LSTM

The hyperparameters can be efficiently managed to enhance the proposed system accuracy. Various combinations of this hyperparameter parameter within the specific period can be connected for implementation to compute accuracy of the projected technique. However, the constraints of the hyperparameters (hidden units, epochs) can be defined due to the response remains almost the similar higher than maximum parameter. It causes only wastage of resources and time. The efficient combination with low RMSE can be selected for efficient performance.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

*Formulation of LSTM*

Utilizing contextual data to link output and input sequences, the LSTM network is equipped with the ability to handle time series data. One way this is accomplished is through its three-gate workflow design: an output gate, input gate, and forget gate. An overview of these functions looks like this:

*Memory cell*

A tanh layer generates a selection of fresh candidate parameters to be incorporated into the state.

$$\widetilde{C}_T = \tanh\left(W_C * \left[H_{T-1}, X_R\right] + B_C\right) \quad (14)$$

$$H_T = O_T * \tanh\left(C_T\right) \quad (15)$$

The old memory cell's condition may be improved to a new memory cell,

$$C_T = F_T * C_{T-1} + I_T * \widetilde{C}_T \quad (16)$$

*Output gate*

This paper will explain how an output gate may be used to manage memory cell output.

$$O_T = \varphi_a\left(W_{out} * \left[H_{T-1}, X_T\right] + B_{OUT}\right) \quad (17)$$

*Input gate*

The input gate may control how data enters the cell.

$$I_T = \varphi_a\left(W_{IN} * \left[H_{T-1}, X_T\right] + B_{IN}\right) \quad (18)$$

*Forget gate*

This forgetting gate takes into account the memory block's most recent input and output. As a general rule, the logistic sigmoid activation function of the forget gate may be used, which calculates how much data can be retained for the higher cell.

$$F_T = \varphi_a\left(W_{IN} * \left[H_{T-1}, X_T\right] + B_F\right) \quad (19)$$

The various layer structures of the RNN-LSTM algorithm are explained in this section. The automated movie recommendation system is made more effective by using the suggested RNN-LSTM controller. The HBA method generates the training sets, and a detailed description is provided in the section below.

*4.1. Optimal weight parameter selection using Honey badger Algorithm (HBA)*

The Honey badger Algorithm (HBA) algorithm is used to perform out the learning function in the RNN-LSTM approach. Additionally suggested and contrasted with the numerical projections are the optimal column design forecasts based on European and North American codes. Black and white hair critters called bees are renowned for their courage. In Africa, Southwest Asia, and the Indian subcontinent, it may be found in semi-desert areas and tropical woods. The HBA simulates badger eating habits. The hawk uses its nose, digs, or tracks the birds it consumes to locate food. The first condition is referred to as the dig technique, and the second as the honey method. It's recognized his victims by scent ever since he was a youngster. They are trying to find a good spot to dig. In the second instance, the bird immediately utilizes it as a guide to locate the nest while looking for honey [29].

*Procedure of proposed HBA optimization*

*Step 1: Initialization phase*

Configure the badger population (of size N), the VANETs parameters, number of nodes (vehicles), distance between vehicular, message transmission, LSTM learning function and its starting location using Equation (20).

$$\beta_x = BL_x + \lambda_1 * \left(BU_x - BL_x\right) \quad (20)$$

Where $\lambda_1$ is a random number between 0 and 1, $BL_x$ and $BU_x$ denotes the bottom and upper boundaries of the search range, and $I_x$ indicates the xthhoney rate for a candidate solution deceits in the population $N$.

*Step 2:Establishing intensity* $(I)$*:*

Intensity affects the prey's absorption phase and the distance between $I_x$ and $x^{th}$ the honey badger. the scent of the prey; Prey may react swiftly to powerful scents $I_x$, according to equation (21).

$$I_x = \lambda_2 * \frac{S}{4\pi D_x^2} \quad (21)$$

Where,

$$S = \left(\beta_x - \beta_{x+1}\right)^2$$

$$D_x = \beta_{prey} - \beta_x$$

$S$ is a measure of the badger's basis or attention. This $D_x$ is an illustration of the separation between the $x^{th}$ badger and the prey.

*Step 3: Fitness Function Evaluation*

The fitness function is calculated once the original population has been finished. The suggested approach initializes the VANETs settings at random. The ideal VANETs parameter is determined based on the fitness function. With statistical analysis and error value of congestion is reduced, the fitness function is assessed. To ensure efficient intrusion detection operation, statistical analysis should be increased. As a result, the minimizing of

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

error value is how the fitness function is defined. The best parameter value is chosen to fulfil the fitness function. The following is a mathematical formulation of the fitness function:

$$FF = Min\{VANET_{congestion} \quad (22)$$

*Step 4: Update the density parameter*

To guarantee a gradual connection from exploration to exploitation, the density factor $\rho$ regulates time-varying randomization. A $\delta$ lowering component that decreases over repetitions is added to Equation (23) to minimize unpredictability over time:

$$\rho = \beta * \exp\left(\frac{-i}{Max_i}\right) \quad (23)$$

Where $\beta$ is a constant $\geq 1$ (default value of 2) and is the number of iterations that may be made.

*Step 5:* Agent location updates.The "digging phase" and the "honey phase" are the two phases of the HBA position updating technique ( $\beta_{prey}$ ).

*Phase of digging:* Euclidean distance betweenhoney badger does activity that resembles a cardioid shape.Equation (24) can replicate the cardioid motion.

$$\beta_{new} = \beta_{prey} + \Omega \times \mu \times I \times \beta_{prey} + \Omega \times \lambda_3 \times \delta \times D_x \times \left|\cos(2\pi\lambda_4) * \left[1 - \cos(2\pi\lambda_5)\right]\right| \quad (24)$$

Where,

$$\Omega = \begin{cases} 1 \ if \ \lambda_6 \leq 0.5 \\ -1 \quad else \end{cases}$$

$\beta_{prey}$ is the prey's position, which has been determined to be the best position thus far — the world's finest position. The $x^{th}$ honey badger has a feeding capacity of $\mu \geq 1$ (default = 6).With reference to equation (24), either the distance between the badger $D_x$ and its prey, $\lambda_3$, $\lambda_4$, and $\lambda_5$ represents random numbers varying from 0 to 1. $\Omega$ denotes signals to change the search direction.

*Honey phase:* A honey badger following a honey guide bird to a beehive might be modeled using an equation (25).

$$\beta_{new} = \beta_{prey} + \Omega \times \lambda_7 \times \beta \times D_x \quad (25)$$

Where, $\beta_{prey}$ is the location of the target, $\Omega$ and $\delta$ are obtained using Equation (23), respectively. $\beta_{new}$ it marks the original location of the honey badger. Giving to Equation (25), the badger searches nearby $\beta_{prey}$, it has already found food based on distance data as $D_x$ .At this moment $(\delta)$, the search is being impacted by evolving search trends. A honey badger may also notice an unexpected event $\Omega$.

*Step 6:* There are many automobiles present in the VANET environment, which increases traffic and increases the risk of an accident. Therefore, the RNN-LSTM method enhances the intelligence of the JCIDS-VANET to control the traffic utilizing the concept of HBA. Swarming tendency in an RNN-LSTM based VANET refers to the propensity of honey badger prey to group together and approach the center of their neighbors' nodes. (vehicles). The RNN approach has been experimenting with HBA optimization in this case.

*Step 7:* Update the current optimal HBA position $\beta_{prey}$

*Step 8: Termination process*

A honey badger arrives to the beehive after the first iteration and follows a honey guide bird there. If the criteria are not satisfied, steps 2 through 6 are repeated until the convergence conditions are satisfied. In figure 5 shows that the flowchart of proposed RNN-LSTM with HBA model has been illustrated.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:*** *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

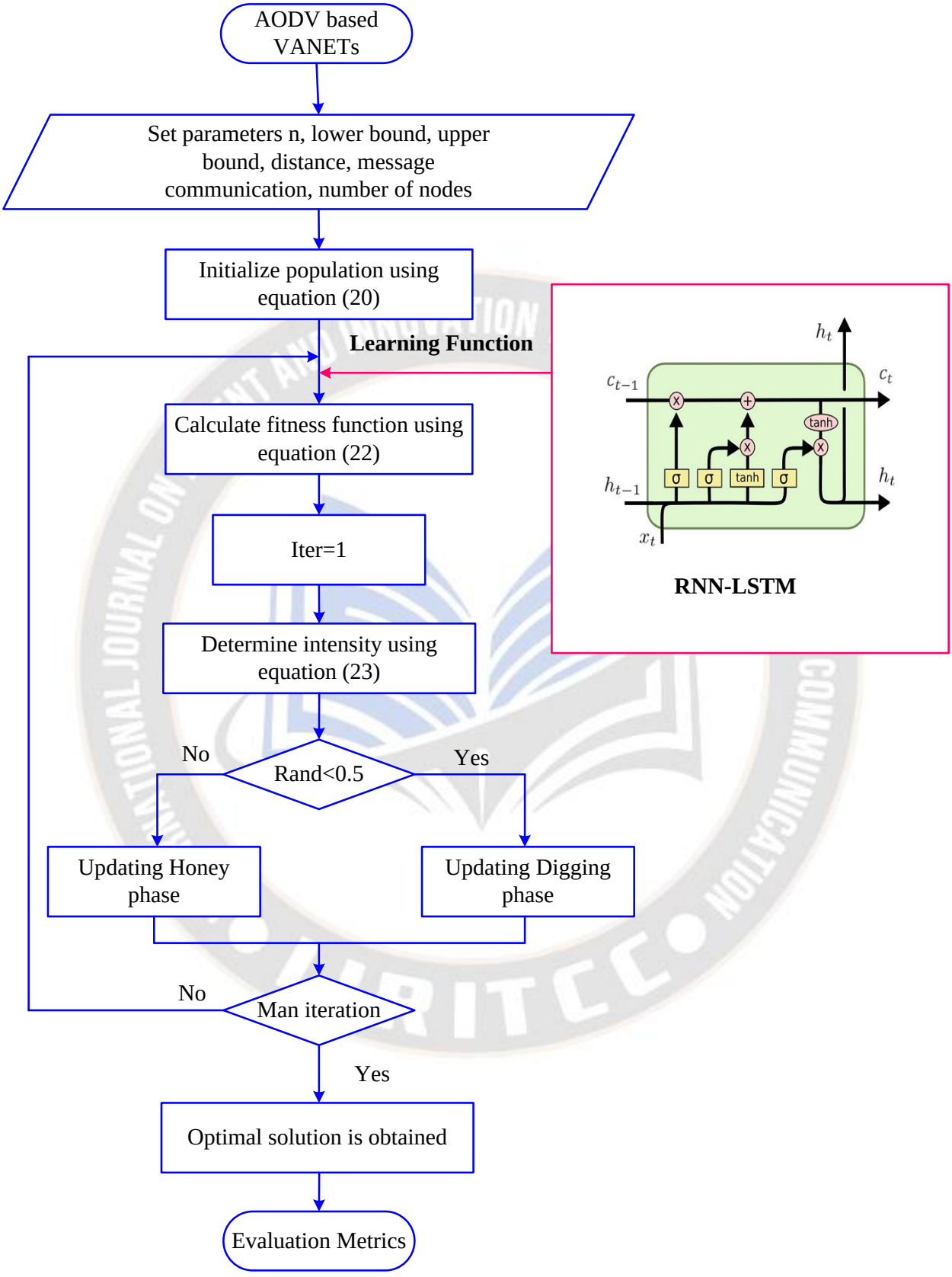


Fig.5: Flowchart of proposed RNN-LSTM with HBA Model

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

In this case, the Cluster Head choice based on Fitness value is quite important. In order to make sure that every node gets allocated the greatest fitness value, the procedure is then repeated to the neighboring node. The HBA-based RNN-LSTM algorithm is enhanced by regulating VANETs' combined congestion incursion management mechanism. The RNN with HBA-VANET outcomes achieved in this model are assessed using all ensemble learning strategies. By recognizing and categorizing the assaults, each will create a distinct set of findings, which will aid in deciding the optimum outcomes. The suggested model's flowchart demonstrates how the deep learning technique combined with RNN, HBA, and VANET helped the model perform better.

## 5. PERFORMANCE EVALUATION

The simulation environment and settings are initially represented in this section. Network Simulator (NS, version 2.35) was also used to simulate vehicular networks running Linux Ubuntu 12.04 in order to test the performance of the VANET routing components. An object-oriented and discrete event simulator called NS2 can mimic multicast protocols, the AODV protocol, and routing across wired and wireless networks [30]. A 4 x 4 km2 urban environment with 40 two-way road segments and 25 crossroads has been developed for our simulation. Additionally, it is anticipated that VANET fly continuously at an altitude of no more than 200 m.

TABLE 1 Simulation parameters used in the urban scenario

| Parameters | Value |
|---|---|
| Total road length | 1000m * 1000m |
| Number of lanes | 4(2 in each direction) |
| Number of vehicles | 50, 100,150, 200, 250, 300, 350, 400, 450, 500 |
| Vehicles speed | 0-40 km/h |
| Transmission rate | 3-27 Mbps |
| Bandwidth | 10MHz |
| Message size | Beacon:400 Bytes, Emergency: 300 Bytes |
| MAC type | IEEE 802.11p |
| Propagation control | Nakagami (m-3) |
| Routing protocol | DSDV |
| Simulation | 1000 s |
| Simulation runs | 20 |

### *5.1. Performance Metrics*

The parameters such as delay, delivery ratio, accuracy and throughput were used to evaluate the performance of the proposed protocols and compare them with other protocols. Each of these parameters is explained in this section, and all three proposed AODV protocols, Deep Neural Network (DNN) and Support Vector Machine (SVM) are compared.

*Packet delivery ratio (PDR)*

$$PDR = \frac{Number\ of\ \ packets\ received\ by\ the\ destination}{Number\ of\ \ packets\ sent\ by\ the\ source} \tag{26}$$

*Delay*

$$D = \frac{\sum_{x=0}^{q}\left(\left(time\ \ of\ receiving\ the\ xth\ \ packet\right)-\left(time\ of\ \ sending\ the\ xth\ \ packet\right)\right)}{total\ \ number\ of\ \ packets\ received\ by\ the\ destination} \tag{27}$$

*Throuput*

$$T = \frac{\sum_{x=0}^{q}\left(packets\ \ received\right)}{t} \tag{28}$$

The accuracy performance comparison is shown in Figure 6. The proposed approach is contrasted with traditional approaches like DNN and SVM. The accuracy of the recommended method is 0.95. The DNN and SVM both have accuracy values of 0.91 and 0.918, respectively. The recommended method's accuracy was tested, and it was found to be successful for the closed-loop congestion management technique.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:*** *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

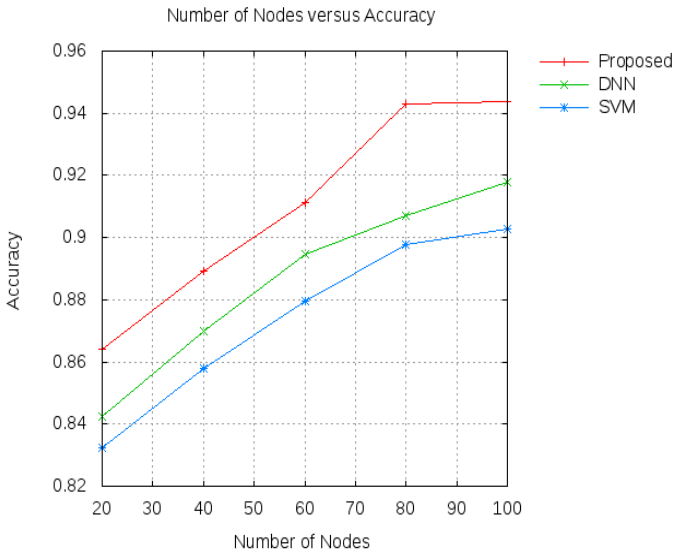


Fig.6: Simulation output of accuracy

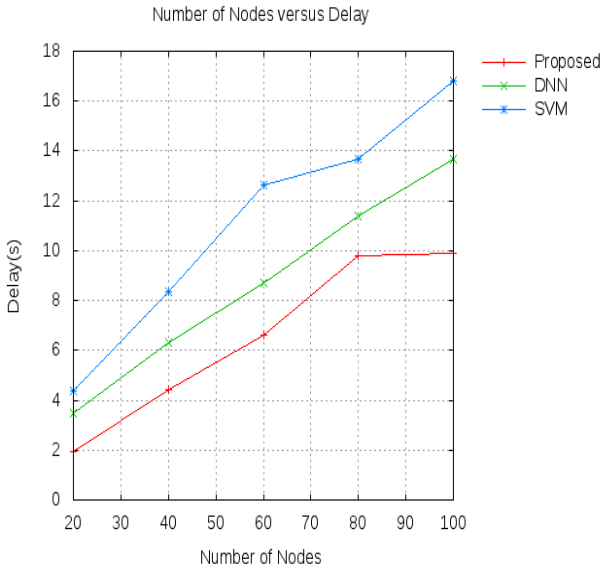


Fig.7: Simulation output of Delay

The time period between when a vehicle produces a service request and when other vehicles get this information is known as the average reception delay. Fig.7 displays the simulation findings. The delay becomes worse as there are more vehicles. On the other hand, the real-time performance of the method suggested in this study is improved and the latency is slightly reduced.

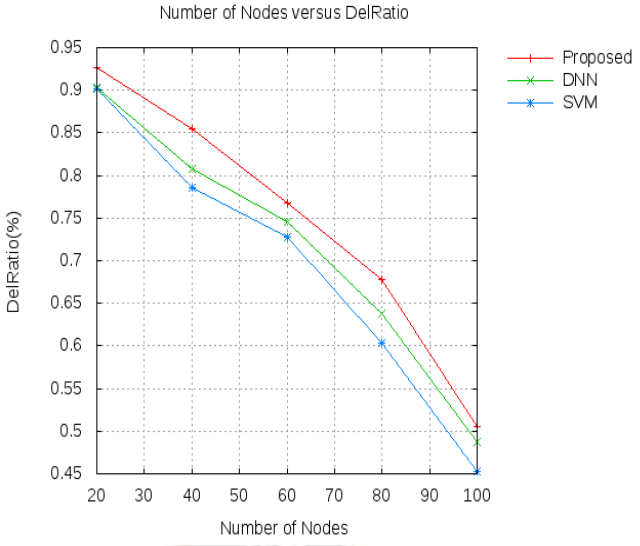


Fig.8: Performance analysis of Delivery ratio

The performance of an information dissemination method is assessed using this metric, which is of utmost significance. Here, we compare the suggested algorithm's performance using the DNN (deep neural network) and SVM (support vector machine) methods. The average packet delivery rate of the information distribution mechanism based on clustering varies rather slowly with the rise in the number of nodes, as illustrated in figure 8, in contrast to the other two algorithms. Delivering messages successfully has increased significantly.

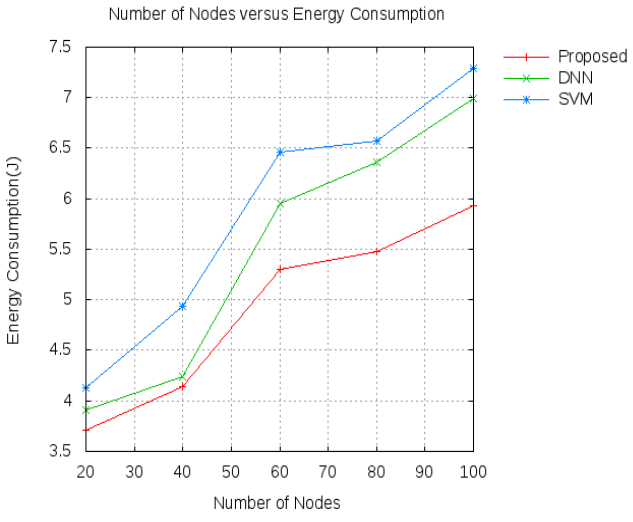


Fig.9: Comparison analysis of Energy Consumption

The energy consumption of the sink node for the suggested technique is compared to that of the DNN and SVM in Fig. 9. Here, the suggested RNN-HBA uses the best possible combination of each on-board unit's minimum distance, remaining energy, and channel condition. This decreases overall energy usage while increasing the success

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

rate of data gathering at the sink node. The sensor hubs are positioned along the optimum path to complete the information collection, and the suggested RNN-HBA uses recursive verification for the best information collecting. This method may lessen the amount of labour involved in acquiring information, which lowers overall energy costs.

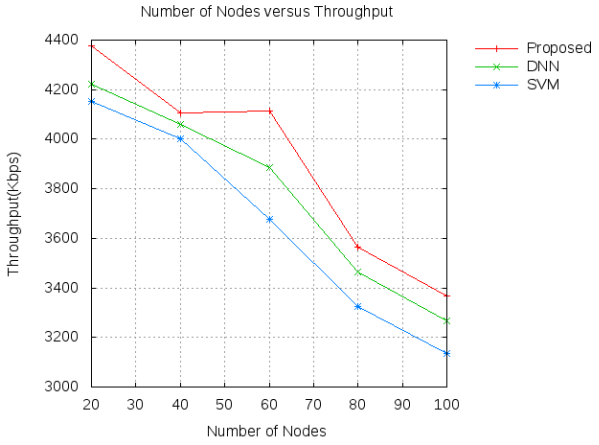


Fig.10: Comparison analysis of Throughput

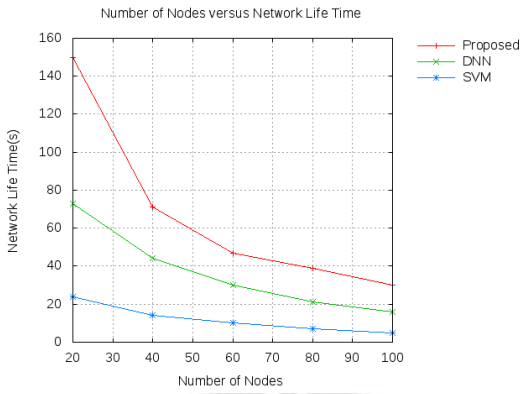


Fig.11: Comparison analysis of Network life time

Figure 10 compares the proposed and existing approaches' total efficacy (throughput). Each node's throughput rate is recorded. At node 100, the suggested method's throughput was 3397 Kbps, the DNN technique's throughput was 3320 Kbps, and the SVM throughput was 2800 Kbps. Throughput increases as the number of nodes increases. Figure 11 displays the network's lifespan for the proposed and current approaches. Each node's network lifespan was recorded. The network lifespan of the suggested techniques at node 100 is 37 seconds, 19 seconds for DNN methods, and 5 seconds for SVM methods. Network lifespan also increased as the number of nodes increased.

## 6. Conclusion

The main issues with VANET applications are safety and security. Numerous roadside services, such traffic updates and accident alerts, may effectively assist safety standards. However, because to their highly dynamic, decentralized nature, and protocol design issues, VANETs are susceptible to a number of security risks and assaults. This research study focused on the security component of VANETs. An inventive and successful method known as RNN-HBA was put up to safeguard and enhance the general performance of VANETs. It could identify and stop Joint congestion-intrusion detection security in the new AODV routing protocol. The method was based on creating a fake RREQ packet and computing a dynamic threshold value. For stability in vehicle networks, quick and dependable communication was made possible in order to use the expected information after validation. Performance measures included energy consumption, throughput, accuracy, and packet delivery ratios to evaluate the effectiveness of the proposed strategy. A new protocol called RNN based LSTM with HBA-VANET was created to improve the efficiency of the routing process in VANETs. The performance and effectiveness of the suggested RNN-HBA were assessed in the NS-2 simulator, and its results were contrasted with those of other approaches like DNN and SVM.

Joint congestion-intrusion detection security, which is thought to be part of the severe congestion on VANETs, is a topic for future study. In a similar vein, further efforts will be made in the future to investigate cutting-edge developments in the industry and solve numerous security challenges related to vehicle networks.

## References

[1] Qureshi, Kashif Naseer, et al. "Nature-inspired algorithm-based secure data dissemination framework for smart city networks." Neural Computing and Applications 33 (2021): 10637-10656.
[2] Sontakke, Prakash Vijay, and Nilkanth B. Chopade. "Optimized Deep Neural Model-Based Intrusion Detection and Mitigation System for Vehicular Ad-Hoc Network." Cybernetics and Systems (2022): 1-29.
[3] Alsarhan, Ayoub, et al. "Machine learning-driven optimization for intrusion detection in smart vehicular networks." Wireless Personal Communications 117 (2021): 3129-3152.
[4] Nandy, Tarak, et al. "T-BCIDS: Trust-based collaborative intrusion detection system for VANET." 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA). IEEE, 2020.
[5] Ullah, Ata, et al. "Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing." IEEE Access 7 (2018): 1570-1585.
[6] Garg, Sahil, et al. "Edge computing-based security framework for big data analytics in VANETs." IEEE Network 33.2 (2019): 72-81.
[7] Zang, Mingyuan, and Ying Yan. "Machine learning-based intrusion detection system for big data analytics in VANET." 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring). IEEE, 2021.
[8] Ayoob, Ayoob, et al. "Intrusion Detection System Classifier for VANET Based on Pre-processing Feature Extraction." Future Network Systems and Security: 5th International Conference, FNSS 2019, Melbourne, VIC, Australia, November 27–29, 2019, Proceedings 5. Springer International Publishing, 2019.

[9] Zhai, Weidong, and Zhou Su. "Intrusion Detection Scheme for Autonomous Driving Vehicles." Security and Privacy in Digital Economy: First International Conference, SPDE 2020, Quzhou, China, October 30–November 1, 2020, Proceedings 1. Springer Singapore, 2020.
[10] Adhikary, Kaushik, et al. "Hybrid algorithm to detect DDoS attacks in VANETs." Wireless Personal Communications 114 (2020): 3613-3634.
[11] Poongodi, M., et al. "Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics." IEEE Access 7 (2019): 158481-158491.
[12] Cherkaoui, Badreddine, et al. "Road traffic congestion detection in VANET networks." Procedia Computer Science 151 (2019): 1158-1163.
[13] Zhou, Man, et al. "Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant." Computer Networks 172 (2020): 107174.
[14] Sharma, Sparsh, and Ajay Kaul. "Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET." Vehicular Communications 12 (2018): 23-38.
[15] Shu, Jiangang, et al. "Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach." IEEE Transactions on Intelligent Transportation Systems 22.7 (2020): 4519-4530.
[16] Zhang, Zhixia, Yang Cao, Zhihua Cui, Wensheng Zhang, and Jinjun Chen. . "A many-objective optimization based intelligent intrusion detection algorithm for enhancing security of vehicular networks in 6G." IEEE Transactions on Vehicular Technology 70.6 (2021): 5234-5243.
[17] Zhou, Man, Lansheng Han, Hongwei Lu, and Cai Fu. "Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant." Computer Networks 172 (2020): 107174.
[18] Theerthagiri, Prasannavenkatesan, and Chandrasekaran Gopala Krishnan. "Vehicular multihop intelligent transportation framework for effective communication in vehicular ad-hoc networks." Concurrency and Computation: Practice and Experience 34.10 (2022): e6833.
[19] Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S.S., Kumar, V.A., Panigrahi, B.K. and Veluvolu, K.C.,. "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm." Microprocessors and Microsystems 80 (2021): 103352.
[20] Bangui, Hind, Mouzhi Ge, and Barbora Buhnova. "A hybrid machine learning model for intrusion detection in VANET." Computing 104.3 (2022): 503-531.
[21] Sefati, Seyed Salar, and Sara Ghiasi Tabrizi. "Detecting sybil attack in vehicular ad-hoc networks (vanets) by using fitness function, signal strength index and throughput." Wireless Personal Communications (2022): 1-21.
[22] Tosunoglu, B. A., and C. Kocak. "Feature Selection For Clustering And Classification Based Attack Detection Systems In Vehicular Ad-Hoc Networks." Microprocessors and Microsystems (2023): 104808.
[23] Abdan, Masoud, and Seyed Amin Hosseini Seno. "Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET)." Wireless Communications and Mobile Computing 2022 (2022): 1-12.
[24] Liang, Junwei, et al. "A filter model for intrusion detection system in Vehicle Ad Hoc Networks: A hidden Markov methodology." Knowledge-Based Systems 163 (2019): 611-623.
[25] Nandy, Tarak, et al. "T-BCIDS: Trust-based collaborative intrusion detection system for VANET." 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA). IEEE, 2020.
[26] Ramalingam, M., and R. Thangarajan. "Mutated k-means algorithm for dynamic clustering to perform effective and intelligent broadcasting in medical surveillance using selective reliable broadcast protocol in VANET." Computer Communications 150 (2020): 563-568.
[27] Saleem, Muhammad Asim, et al. "Deep learning-based dynamic stable cluster head selection in VANET." Journal of Advanced Transportation 2021 (2021): 1-21.
[28] Yu, Yantao, et al. "LSTM-Based Intrusion Detection System for VANETs: A Time Series Classification Approach to False Message Detection." IEEE Transactions on Intelligent Transportation Systems 23.12 (2022): 23906-23918.
[29] Hashim, Fatma A., et al. "Honey Badger Algorithm: New metaheuristic algorithm for solving optimization problems." Mathematics and Computers in Simulation 192 (2022): 84-110.
[30] Arvind Narayan, S., R. Rajashekar Reddy, and J. S. Femilda Josephin. "Secured congestion control in VANET using greedy perimeter stateless routing (GPSR)." Artificial Intelligence and Evolutionary Computations in Engineering Systems. Springer Singapore, 2020.