International Journal of Safety and Security Engineering
Vol. 15, No. 3, March, 2025, pp. 543-553
Journal homepage: http://iieta.org/journals/ijsse

Enhanced Gated Sway Network and Hybrid Henon Encryption for Secured VANET Communication

Thuvva Anjali[1*], Rajeev Goyal[1], G. N. Balaji[2]

[1] Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University Madhya Pradesh, Gwalior 474005, India
[2] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India

Corresponding Author Email: anjalithuvva.phd@gmail.com

https://doi.org/10.18280/ijsse.150313

Received: 31 January 2025
Revised: 18 February 2025
Accepted: 15 March 2025
Available online: 31 March 2025

Keywords:
VANETs, gated sway networks, advanced encryption schemes, centrality feature extraction, NIST, sybil attack detection, wormhole attack detection

ABSTRACT

Vehicular Ad-hoc networks (VANETs) which is regarded to be a major component in the intelligent transportation systems, have the defined target of assuring safe delivery of information between the vehicles. These networks consist of several essential elements, such as dynamic changing nodes, scattered networks, sensors, road-side components (RSC) and self-organizing topologies. But these networks are more vulnerable to the contentious attacks, security breaches and data privacy problems persist as a crucial threat in spite of the recent advancement of VANET. To overcome this challenge, an effective and high secured framework is mandatorily demanded. Consequently, this research introduces a novel routing framework that integrates the attack detection and hybrid encryption units. The cluster head (CH) is determined utilising novel gated sway networks, which combine centrality-based feature extraction with a gated neural network to ensure trusted CH selection. This enhances resilience and improves interfacing throughout the data transmission process in the VANET framework. The hybrid encryption schemes contain sandwich Henon maps (SHM) coupled with the Advanced Encryption schemes (AES). This combination strives to strengthen the network's security and privacy The proposed protocols are analysed using SUMO-OMNET++ simulation environment. Nearly 2,50,000 data traces comprise of normal and attack data were simulated and attacks such as sybil and wormhole attacks are injected using python 3.19 programming. Simulation results from the performance assessment demonstrate that the proposed framework has produced the 96.5% detection accuracy, 96.0% precision, 95.7% recall, 96.4% specificity, 97.5% F1-Score and it is apparent that the proposed framework has exhibited the better performance over other existing algorithms. Additionally, National Institute of Standard Technique (NIST) suite was performed to verify the randomness of the encrypted bits utilising the recommended method. The test outcomes demonstrated that the suggested encryption approach has produced the high randomness features capable of protecting the sybil and gray hole attacks.

1. INTRODUCTION

Recently, VANETS plays an inevitable role in building the intelligent transportation systems in offering end users with comfortable services encompassing traffic security, entertainment, navigation process, transport effectiveness, amusement and road traveling [1]. Due to the advantages of VANET, these networks are integrated in to public transportation entities and a range of automobile companies to facilitate the VANET establishment [2]. These networks depend on short-range communication to connect the vehicles [3].

In contrast to conventional wired frameworks, VANETs are vulnerable to threats and vulnerabilities. It may be affected by specific threats which focus on compromising safety and disseminating misleading data, along with traditional threats [4]. Among the foremost critical threats, currently impacting VANETs is the sybil threat [5]. When harmful vehicle nodes generate numerous counterfeit IDs, they can initiate sybil threats which directly influence service delivery for aspects including road security, traffic flow, multimedia services, and more. A strategic intruder aiming for personal gain and a malicious attacker intending to cause harm can both carry out a sybil attack.

A sybil attack occurs when a single adversarial entity pretends to be several distinct identities, deceiving the network into believing that numerous distinct nodes exist. This manipulation can distort traffic density readings, disrupt routing decisions, and mislead applications dependent on node consensus, ultimately jeopardizing traffic safety and efficiency. In contrast, a wormhole attack involves at least two colluding nodes that create a private link—known as a tunnel—through which packets are transmitted between distant locations, bypassing the normal routing path. This false

perception of a shorter route can mislead nearby vehicles, diverting traffic and allowing attackers to monitor, drop, or alter data. Both attacks significantly impair the reliability, trustworthiness, and safety of VANET communications by undermining authentication, routing integrity, and real-time data accuracy.

Numerous strategies have been suggested to shield vehicles from becoming targets of the aforementioned attacks. Key cryptographic methods such as digital signatures, rule-based detection, and encryption have been extensively employed as an initial defense to block various forms of external threats. However, these precautionary techniques are insufficient to protect VANET systems against internal threats. Given the collaborative nature of VANET, harmful nodes or attackers continue to perform malicious actions such as denial of service, vehicle hijacking, data leakage, tampering with information, spreading false data, and other similar activities.

Several authentication techniques [6-9], intrusion detection mechanism [10-12] and cryptographic mechanism [13-16] were proposed to maintain the privacy and to overcome the security breaches against the growing attacks. Nevertheless, most of the strategies outlined above involve significant computational overhead, forming it complex to overcome the security breaches caused by the growing sybil and wormhole attacks. These complexity and drawbacks prevent these methods from being designing an intelligent detection system for VANET to protect the users against the sybil and wormhole attacks.

Motivated by this drawback, this research article proposes the novel intelligent network named Enhanced Gated Sway Neural Network (EGSNN) which hybrids the intrusion detection system and high-end cryptographic system for detection and counterfeiting the sybil attacks in VANET environment. The proposed framework works on the principle of centrality-based feature extraction in which the feedforward gated units are used to detect the attacks [17]. In addition to the detection, strong encryption with the principle of Henon chaotic principles is designed to counterfeit the sybil and wormhole attacks. The major contribution of this research is outlined below:

1. Introduces the enhanced gated sway recurrent units which for predicting the sybil and wormhole attacks in VANET environment.
2. Proposes the High-End Cryptography technique based Chaotic Henon maps for counterfeiting the attacks.
3. Extensive experimentation has been conducted and its performance was evaluated against other cutting-edge learning models.

The remaining sections of the study are arranged as pursues: Section-2 introduces the reviews of different works regarding the security measures of the network. Section 3 outlines the system model utilised in the VANET scenario. The working mechanism of the recommended framework is detailed in Section 4. The experimentations, result evaluation, NIST tests and comparative studies are provided in Section 5. At last, the study wraps up with future enhancements in Section 6.

2. RELATED WORKS

El-Shafai et al. [18] developed an AI-based collective classifiers for identifying interference assaults in VANETs. The suggested framework combines machine learning and neural network classifiers to examine signal properties within VANET transmission pathways. Their ensemble classifier combines Random Forest, Extra Tree, and fine-tuned Convolutional Neural Network, achieving an impressive detection accuracy of 99.8125%, outperforming individual classifiers. This approach significantly enhances VANET security frameworks to counteract jamming assaults, strengthening the overall protection and dependability of VANET communication in smart city infrastructures. However, the model needs further validation in real-world dynamic VANET scenarios.

Bayan et al. [19] constructed a Deep Learning-driven intrusion recognition framework for detecting position falsification threats in VANETs. Their system employs Multi-Layer Perceptron (MLP) algorithm that considers RSSI aggregation of first-hop neighbors and Time Difference of Arrival (TDoA) as new detection features. Trained offline using the VeReMi dataset, the model can be deployed at a vehicle's Onboard Unit (OBU), reducing computational complexity and execution time. Their DL-IDS model demonstrates high accuracy and F1-score values, exceeding existing models by 2-7% with advantages in computational efficiency. However, the system may struggle with detecting complex hybrid attacks.

Suman et al. [20] proposed an Improved LeeNET (I-LeeNet) architecture to identify and mitigate various attacks including Botnet, sybil, DoS, wormhole, PortScan, Blackhole, and BruteForce. The architecture intelligently blends Convolutional Neural Networks (CNN) and Adaptive Neuro-Fuzzy Inference Systems (ANFIS) for real-time attack detection. Their approach includes KIDS module for known attack detection and UIDS module for learning previously unidentified attacks. Tested on three datasets (i-VANET, ToN-IoT, and CIC-IDS 2017), the proposed method achieved average accuracies of 97.21%, 97.75%, and 96.66% respectively, demonstrating promising real-time application potential. But the computational demands may challenge implementation in resource-limited environments.

Jabbar et al. [21] suggested the centrality relied clustering mechanism for the recognition of sybil and wormhole threats in VANET framework. The main idea is to maintain the network's reliability by choosing the appropriate cluster head (CH) based on the centrality measures to cluster the vehicles for an effective data transmission. The findings demonstrated the excellent performance of the recommended model regarding network lifetime and computational cost. However, the suggested framework requires brighter light of analysis in deploying the intelligent system for the detection of multiple attacks.

Rafsanjani et al. [22] proposed unmanned aerial vehicles (UAV) in the VANET environment to detect the malicious vehicles. A vehicle routing unit (VRU) has been introduced as a method to direct the data, thereby mitigating the malicious vehicles. The proposed framework has improved the packet delivery ratio by 16% and detection ratio by 7% evaluated against the other methods. However, these methods fail to throw the deeper light of counterfeiting the attacks especially sybil and wormhole attacks.

Polat et al. [23] proposed a stacked sparse autoencoder with Softmax classifier neural network architecture for identifying DDoS assaults aimed at SDN-powered VANET. Their approach dimensionally reduced features using SSAE to extract the important features, which are then utilised as input for the Softmax categorizer. Evaluation outcomes demonstrated that their recommended approach attained

96.9% precision, surpassing other models in identifying DDoS intrusions in SDN-driven VANET. However, the model's effectiveness against new attack patterns needs further testing.

Wang et al. [24] suggested a lightweight and effective authentication system for safe VANET transmission (LESPP) that preserves privacy. The proposed technique only requires the construction of a fast MAC re-generation and a lightweight symmetric encryption and message authorization code (MAC) for message signing. To safeguard security and conditional tracking, such strategy employs a self-created phony identity. The suggested approach significantly reduces calculation costs.

Alfadhli et al. [25] demonstrated the application of genetic hashing function to resolve the issues of unsafe driving sequences. Furthermore, the vehicle authorization is performed exclusively one time by the VANET framework manager thereby increasing the authentication process. To mitigate the attacks, the framework offers the confidentiality to maintain safety of the vehicles. The framework offers the more superior performance in maintaining the privacy of the vehicles against the multiple attacks. But the framework needs improvisation in detecting the attacks which will be occurring in unknown occasions.

Fatemidokht et al. [26] introduced a cluster-based routing protocol termed QoS-based Monitoring of Malicious Activity (QMM-VANET) to improve network QoS. The protocol comprises of three components: CH identification, optimal neighbor identification, and gateway renewal method. The experiment is carried out using NS2 in the highway situation. Packet delivery ratio, latency, and network reliability are the key metrics focused on in the result performance analysis. However, characteristics such as detection ratio and high-end privacy are overlooked.

Guo et al. [27] presented the game-theoretic-relied incentive framework for collaborative recognition of multiple –threats in the VANET framework. These algorithms combine the different machine learning models. But fails to improve the safety measures and confidentiality breaches in the VANET framework.

3. SYSTEM MODEL

The primary elements comprise in VANET are on-board unit (OBU), road-side unit (RSU), trusted authority (TA) and application units (AU). These modules help in implementing the vehicular network.

3.1 OBU

Each and every conveyance in the vehicular network will be equipped with OBU to support the ITS. Once OBU is fixed on the conveyances it helps in exchanging the data with the other conveyances OBUs or RSUs. All the information about conveyances is collected by Electrical Control Unit (ECU) and send to the AU. This AU process the collected data and generates the message based on collected data and shares that message to the other conveyances in the network. The OBU will be connected to the internet through RSU or hotspot or DSRC. Figure 1 depicts the secure and intelligent VANET framework.

3.2 RSU

RSU is a base station or a gateway for the conveyances in the network and the services on the road furnished by the VANET. RSU is a static and the ranges are fixed for the conveyance to memorandum with that particular RSU. Depending on the utilization of communication protocols, the distribution and frequency is made for RSUs. The communication from legitimate nodes to malicious nodes can be revoked by the TA that are assisted by the RSUs.

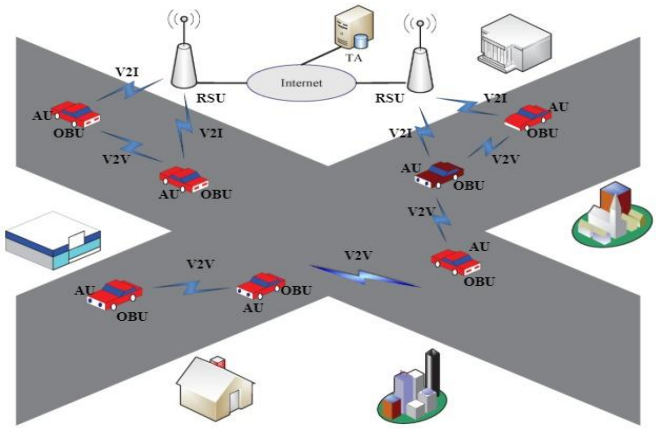

Figure 1. VANET communication framework

4. SYSTEM OVERVIEW

Figure 2 illustrates the recommended system consist of four components including Dataset Collection, Data-Preprocessing unit (DPU), Centrality (Sway) Extraction (CFU) and Modified Gated Recurrent learning network (MGRLN). In the event of classification, proposed model detects the two important parameters such as type of attack (TA) and malicious node provide in the VANET framework. The comprehensive explanation of the recommended framework is provided in the previous section.

4.1 Dataset collection

For an efficient data collection, powerful integration of the SUMO [28], VEINS [29] and OMNET [30] are used in this research. To induce the attacks in the networks, python-based attack injection module has been introduced. Nearly 4,00,000 data are collected, with 70% allocated for training and 30% for testing. The complete description of data generation process is depicted in Algorithm-1.

Algorithm-1 /Data Generation Process
Step 1: Start process
Step 2: Initialization of road traffic scenarios from source to destination
Step 3: Introduce the vehicles on the road scenarios
Step 4: Induce the attacks in the created road scenario
Step 5: Store the data in the SQL databases
Step 6: End process

4.2 Data pre-processing unit

The data gathered in the preceding phase may contain the misleading or null values, hence data prep-processing technique is needed before implementing to the proposed learning model. The pre-processing stage involves the data labelling and data normalization. Labeling the dataset is a crucial phase in data preprocessing. Based on the events

gathered from the prior phase, all traffic was classified as normal (0-label) and attack (1-sybil, 2-wormhole, 0-Normal) according to the information like source address, destination address, time, and duration. After categorizing the data, a min-max normalization method was applied to scale the features to a uniform range, typically between 0 and 1. This guarantees that every attribute plays an equal role in the training model and prevents bias towards attributes with greater ranges. The min-max normalization formula is expressed as:

$$Normalization = \frac{x-Min}{Max-Min} \quad (1)$$

where, *Min* denotes Minimum data, *Max* indicates maximum data and *x* is the collected raw data.

After normalizing the data, these data feed to the recommended DL model for the further identification of various threats.

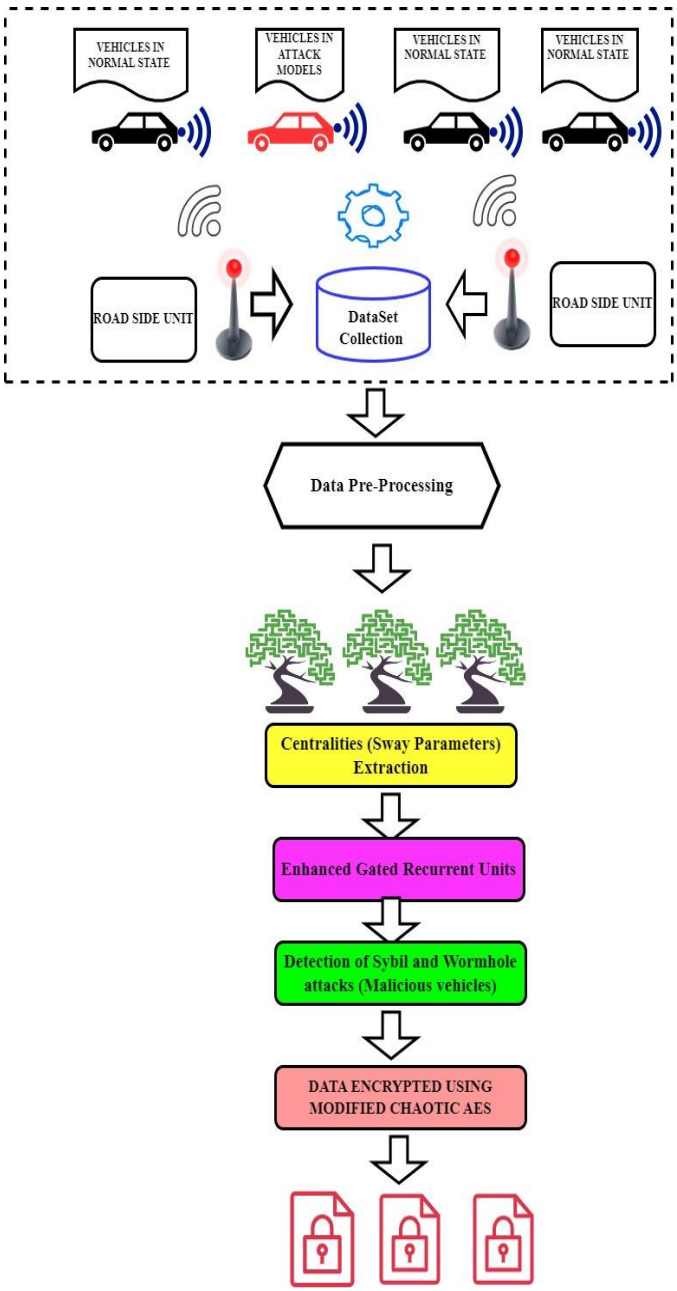

Figure 2. Proposed framework for the deep sway networks and hybrid encryption process

4.3 Centrality feature extractor

The major purpose of this research is to design an effective feature database capable of classifying normal and influential nodes. Numerous centrality measure detection techniques have been introduced in existing research to quantify node importance. However, this paper highlights the application of an expanded set of centrality metrics to attain the precise categorization of significant nodes.

To capture both the structural and functional traits of the nodes, the subsequent centralities are evaluated, as detailed below.

4.3.1 Degree centralities

It reflects the count of connections associated with the nodes. It consists of two variations: indegree and outdegree centrality. These measures can be computed utilising the subsequent formulas.

i) Indegree centrality

$$D_{in}(P_i) = \left|P_{ji} \in P\right|, j \neq i \quad (2)$$

P_{ji} represents the connection extending from P_i node to the assessed node P.

ii) Outdegree centrality

$$D_{ot}(P_i) = \left|P_{ij} \in P\right|, i \neq j \quad (3)$$

P_{ij} represents the connection strength (i.e., edge) from the assessed unit P_i to all another units P_j in the system.

4.3.2 Betweenness centralities

It signifies the proportion of all shortest routes traversing the nodes. The numerical representation for this measure is presented by:

$$D_B(P_i) = \sum_{P_m \neq P_i \neq P_n} \frac{\mu_{P_m,P_n}(P_i)}{\mu_{P_m,P_n}} \quad (4)$$

where, $\mu_{P_m,P_n}(P_i)$ represents the count of minimal routes among nodes P_m and P_n that traverse through P_i and μ_{P_m,P_n} denotes the count of all shortest paths among P_m and P_n.

4.3.3 Closeness centralities

It represents the interval of nodes within the systems and its mathematical formulations provided below:

$$D_c(P_i) = \frac{N}{\sum_{Py} d(P_y,P_i)} \quad (5)$$

where, N represents the count of vertices in the network and d (P_y, P_i) denotes the interval among Py and Pi nodes.

4.3.4 Eigen vector centralities

It is utilized for computing the centrality of other nodes in the network. The equation to calculate this is presented below:

$$E_v(P_i) = {}^{1}/_{\alpha} \sum_k \gamma_{P_k,P_i} * E_v(P_k) \quad (6)$$

where, A= $\alpha(k,i)$ represents the adjacent matrix of a graph and γ is a constant.

4.3.5 PageRank centralities

This calculates the node ranking according to their centrality within the systems. Its mathematical formulation is determined as:

$$R_p(P_i) = \rho \sum_k \frac{A_{P_k,P_i}}{d_k} * R_p(P_k) + \beta \quad (7)$$

where, ρ and β represent constants, and d_k signifies the out-degree of P_k, where this degree is positive, or d_k is 1 if the out-degree of P_k is zero. Furthermore, A = (ai,j) denotes the adjacent graph matrix, where A = α(k,i) is the adjacency matrix.

4.3.6 Position centrality

It is regarded as the major significant metric, representing the placement of the nodes in relation to the key nodes, that are computed using the Pagerank algorithm.

$$H_c(P_i) = \beta \sum_k \gamma_{P_i,P_k} * R_p(P_i) \quad (8)$$

where, A = (ai,j) denotes the adjacent graph matrix, and $R_p(P_i)$ represents the node PageRank, with β being a constant.

4.3.7 Clustering co-efficient

It signifies the proportion of triangles which are available within the total possible triangles in the neighborhood of the nodes. The numerical formula to calculate the clustering coefficient is expressed as:

$$C_c = 2M_{P,i}/K_i(K_i-1) \quad (9)$$

where, $M_{P,i}$ is the count of neighbor sets related to the hub pi. Within the expression, it is integrated to the count of potential neighbor sets of hub pi, where kpi = (kpi-1)/2, with kpi being the degree of hub pi. Figure 3 illustrates the representation of centrality measures used to analyze node importance within the VANET communication network.

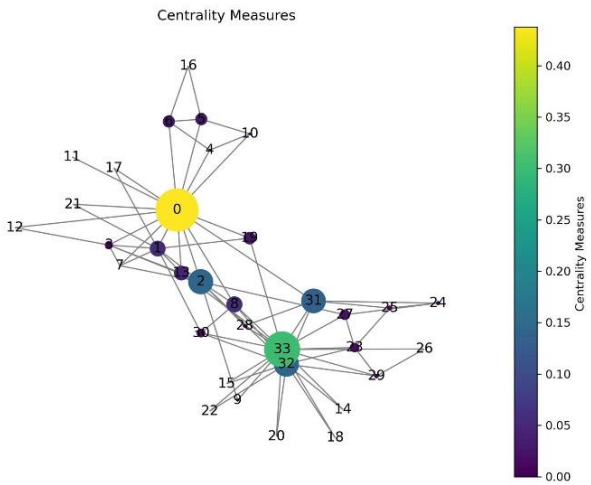

Figure 3. Representation of centrality measures in a VANET topology

Table 1 provides the summary of feature vectors employed for classification.

Table 1. Overview of features utilised for the suggested classification

Sl. No.	Centrality Features	Importance
01	In degree Centrality	Denotes the count of links integrated to the nodes.
02	Out degree Centrality	
03	Betweenness Centrality	Represents the proportion of shortest paths traversing through the nodes
04	Closeness Centrality	Depicts the spatial interval of nodes in the network
05	Eigen Vector Centrality	Utilized to calculate the centrality values of another nodes
06	PageRank Centrality	Evaluates the rank of nodes by considering their centrality
07	Position Centrality	Represents the nodes' position in relation to significant nodes
08	Clustering Co-efficient	Reflects the ratio of triangles present in the node's neighbourhood
09	K-shell Centrality	Represents the K value representing the disintegration of the network
10	K-Score Centrality	Calculates the count of pruned nodes (K) in the network
11	Time Stamp Centrality	Measures the time interval among the transmission and reception of messages
12	Transmitted Neighborhoodvariability (TNV)	Takes into account a group of neighbors for message transmission

4.4 MGRU network based classification

It is regarded as the most captivating form of Long Short-Term Memory (LSTM). This concept was introduced by Chung et al. [31], that seeks to integrate the forget gate and input array into a unified vector. This architecture accommodates extended sequences and prolonged memory. The intricacy is significantly minimized in contrast to the LSTM network.

The subsequent equations were defined by Chung to describe the features of GRU.

$$h_t = (1 - x_t) \odot h_{t-1} + x_t \odot h_t \quad (10)$$

$$\widetilde{h_t} = g(W_h x_t + U_h(r_t \odot h_{t-1}) + b_h \quad (11)$$

Two gates of GRU are presented as

$$z_t = \sigma(W_h x_t + U_z h_{t-1} + b_z) \quad (12)$$

$$r_t = \sigma(W_h x_t + U_r h_{t-1} + b_r) \quad (13)$$

The complete GRU defining formula is expressed by:

$$P = GRU(\sum_{t=1}^{n}[x_t, h_t, z_t, r_t(W(t), B(t), \eta(tannh))] \quad (14)$$

where, x_t is the input attribute at the present state, r_t is the resultant state, and h_t is the output of the element at the current

time step. z_t and r_t are the update and reset gates, while $W(t)$ and $B(t)$ represent the parameters and bias coefficients at the current point in time. To minimize the intricacy, each gate in the GRU is calculated using only the prior latent state and offset, thus reducing the overall count of variables by 2 times nm, compared with the established GRU model. Based on this modification, Eqn. (12) and (13) is modified as

$$z_t = \sigma(U_z h_{t-1} + b_z) \quad (15)$$

$$r_t = \sigma(U_r h_{t-1} + b_r) \quad (16)$$

Again, the overall GRU characteristics is modified and expressed mathematically in Eq. (17)

$$P = GRU(\sum_{t=1}^{n}[x_{t,} h_{t,} z_{t,} r_t(B(t), \eta(tannh))] \quad (17)$$

4.5 Modified AES encryption and decryption

The proposed uses the same operations of the original AES with some modifications. DNA encoding is adopted instead of the traditional permutation and shifting technique. This alteration aims in minimizing the duration for encryption and decryption procedure while maintaining commands with strong defense properties. Dual-level Henon chaotic maps are employed in the creation of robust encryption. To begin with, the VANET data is divided into two separate units depends on the byte positioning. Firstly, Henon maps are utilized to generate the S1 box. Using the outcomes from the first phase, the initial conditions of the Henon maps are set and utilised to create the hybrid S2 box. These two S-boxes are then encrypted with DNA processing to produce the combined S3 box. At last, the information is enciphered utilising the recently generated S3 box. All such process aims to make AES lightweight by reducing its encryption/decryption time simultaneously, still strength to avoid VANET attacks. The detailed description of henon chaotic maps and DNA encoding process is provided below

4.5.1 Key generation process

To eliminate the intricacy involved in using matrices within the encryption method, the first positions of the sensor input bytes are considered. Initially, Henon maps are generated at random as described in Algorithm-2. These created logistic maps are utilized to construct the intermediate S1 box. The intermediate S1 box is developed by combining the Henon maps (H) and the input data (K). Instead of traditional permutations and diffusions, DNA addition encoding is employed to produce a highly secure intermediate S1-Box sequence. The process for generating S1 is illustrated in Algorithm-2.

$$\text{H}= Heon\ maps(K) \text{ For K= Input data Bytes} \quad (18)$$

$$S1 = mod(byte\{\ (H)DNA\ K(input)) \quad (19)$$

Steps	Algorithm-2//Formulation of Intermediate S1-Box
1	Input: Input Series of henon maps/VANET data K
2	Output: S1-box with dimensions (16*16)
3	Begin
4	Develop random sequences as the starting criteria for Henon maps
5	Construct Henon maps utilising Eq. (18)
6	Construct the intermediate S1-box utilising the Eq. (19)
7	Stop

In the subsequent phase, Henon maps are once again generated, utilizing the outcome series from S1-box. The intermediate S2-box is formed utilising VANET inputs (O) and Henon maps (H). During this process, all permutations are substituted with DNA-based addition encrypting for developing a lightweight and easily deployable system, which still retains its robust defense capabilities resisting any threats.

$$\text{H}= Heon\ maps(K) \text{ For K= Input data Bytes} \quad (20)$$

$$S2 = mod(byte\{\ (H)DNA\ K(input)) \quad (21)$$

4.5.2 Encryption process

Ultimately, the intermediate variables (S1 and S2) are merged to generate the new hybrid S-boxes. Upon being processed repeatedly, the input data, along with the hybrid S-box keys, undergo the DNA XOR operation, as outlined in Algorithm 3. Consequently, it produces robustly encrypted bytes that vary separately with every iteration. The entire encryption process involving the S-box is depicted in Algorithm-3.

$$S = S1\ DNA - XoR - S2 \quad (22)$$

Steps	Algorithm-3// Entire Encryption Procedure
1	Input: Input sensor data saved in the central processing unit (CPU)
2	Output : Encrypted information
3	Begin
4	Divide the data into K and O relied on the byte positions
5	Create series at random for 3D logistic maps
6	Construct the 3D logistic maps
7	Construct the Intermediate S1-box
8	Develop the 3D logistic maps utilising preceding parameters and outcome series of the S1-box
9	Construct the Intermediate S2-box
10	S-box (keys)= S1 combines S2
11	Enciphered Information = S-box (DNA) Input sensor data
12	Stop

5. RESULTS AND DISCUSSIONS

5.1 Implementation and evaluation mechanism

All the experiments were implemented using SUMO OMENT++ and Python on a Windows 10 Pro Operating systems. The entire set of learning frameworks was executed utilizing the NVIDIA Tesla K40, powered by the TensorFlow v-4 infrastructure, alongside the Keras 5 advanced-level framework and CPU with 32GB RAM, 2TB hard disk, AMD Radeon CPU @3.0 GHZ. To assess the performance of the recommended approach and several existing learning classifiers on datasets, the following test scenarios were considered.

1. Classifying the vehicular network connectivity as either normal type or attack type with all features.
2. Categorizing the vehicular attacks into its different types will all features.
3. Classifying the vehicular network connectivity as either normal or abnormal with different intensity of attacks.

To analyse the efficiency of the suggested framework, indicators like precision, sensitivity, specificity, recall, and F1-score are calculated. Table 2 presents the numerical

formulations for determining the measures applied to assess the efficiency of the suggested approach. To validate the excellence of the suggested approach, Modified CNN [32] and its variant LiNET [33] are taken for the consideration.

Table 2. Performance measures utilized for evaluating the proposed framework

S.No.	Evaluation Measures	Formulation
01	Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
02	Sensitivity or recall	$\frac{\text{TP}}{\text{TP+FN}}$ x100
03	Specificity	$\frac{TN}{TN+FP}$
04	Precision	$\frac{TN}{TP+FP}$
05	F1-Score	$2.\frac{Precison*Recall}{Precision+Recall}$

TP indicates true positive, TN represents true negative, FP refers to false positive instances, and FN represents false negative instances.

Table 3. Performance of the modified CNN models in recognizing the normal instances from the simulated datasets

Speed of the Vehicles (Km/hr)	Evaluation Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F1-score
20	75	73.4	72.5	73	72
40	74.5	73.0	70.5	72	71.2
60	73	72.0	69.5	70	70.4
80	72	70.8	69.5	69	70

Table 4. Performance of the modified CNN models in identifying the sybil attacks from the real time datasets

Speed of the Vehicles (Km/hr)	Evaluation Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F1-score
20	74	72.3	70.5	72	72
40	72.1	71.3	69.3	71	71.2
60	70.4	70.3	68.4	69	70.4
80	69.2	68.4	67.8	68	70.3

Table 5. Performance of the modified CNN models in recognizing the wormhole attacks from the real time datasets

Speed of the Vehicles (Km/hr)	Evaluation Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F1-score
20	75	73.4	72.5	73	72
40	74.5	73.0	70.5	72	71.2
60	73	72.0	69.5	70	70.4
80	72	70.8	69.5	69	70

Table 6. Performance of the LiNET models in identifying the normal instance from the real time datasets

Speed of the Vehicles (Km/hr)	Evaluation Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F1-score
20	82	79.3	78.4	78	78.4
40	81	78.4	76.5	77.3	77.3
60	80.5	77.3	75.5	76.4	75.5
80	78.4	76.4	74.5	75.3	75.0

Table 7. Performance of the LiNET models in identifying the sybil attacks from the real time datasets

Speed of the Vehicles (Km/hr)	Evaluation Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F1-score
20	80	78.4	76.5	73	77.5
40	79.5	74.0	73.5	72	73.7
60	77.7	72.0	68.5	70	70.2
80	76.4	71.8	67.2	69	69.3

Table 8. Efficiency of the LiNET models in identifying the wormhole attacks from the real time datasets

Speed of the Vehicles (Km/hr)	Evaluation Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F1-score
20	82	79.3	78.4	78	78.4
40	81	78.4	76.5	77.3	77.3
60	80.5	77.3	75.5	76.4	75.5
80	78.4	76.4	74.5	75.3	75.0

Table 9. Performance of proposed models in detecting the normal instance from the real time datasets

Speed of the Vehicles (Km/hr)	Evaluation Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F1-score
20	96.3	96.0	95.7	96.1	96.2
40	96	95.3	95.0	96.0	95.9
60	96	95.3	95.0	96.0	95.9
80	95.9	95.2	95	95.9	95.9

Table 10. Performance of the suggested approach in identifying the sybil attacks from the real time datasets

Speed of the Vehicles (Km/hr)	Evaluation Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F1-score
20	96.3	96.0	95.7	96.1	96.2
40	96	95.3	95.0	96.0	95.9
60	96	95.3	95.0	96.0	95.9
80	95.9	95.2	95	95.9	95.9

Table 11. Performance of the suggested approach in identifying the wormhole attacks from the real time datasets

Speed of the Vehicles (Km/hr)	Evaluation Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F1-score
20	96.3	96.0	95.7	96.1	96.2
40	96	95.3	95.0	96.0	95.9
60	96	95.3	95.0	96.0	95.9
80	95.9	95.2	95	95.9	95.9

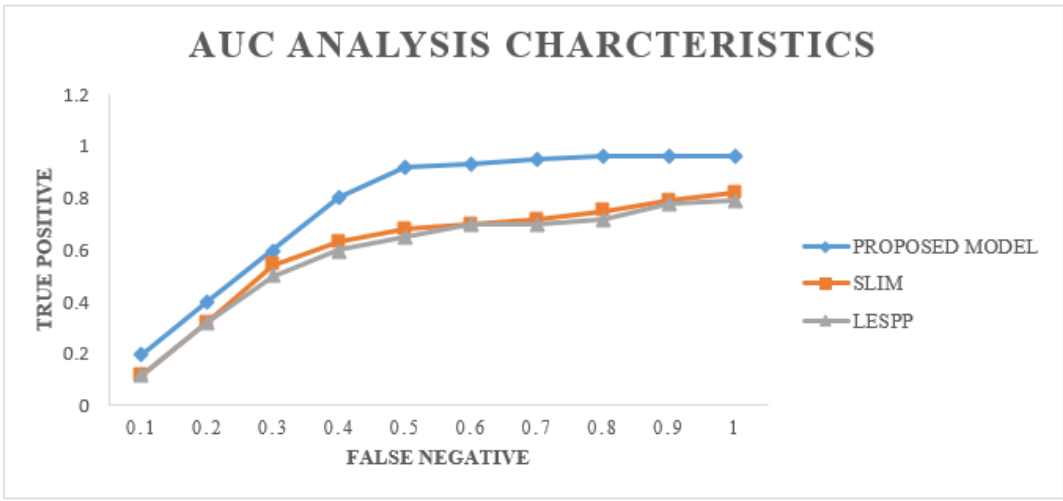

Figure 4. AUC characteristics of the different model in predicting the normal data from the generated datasets

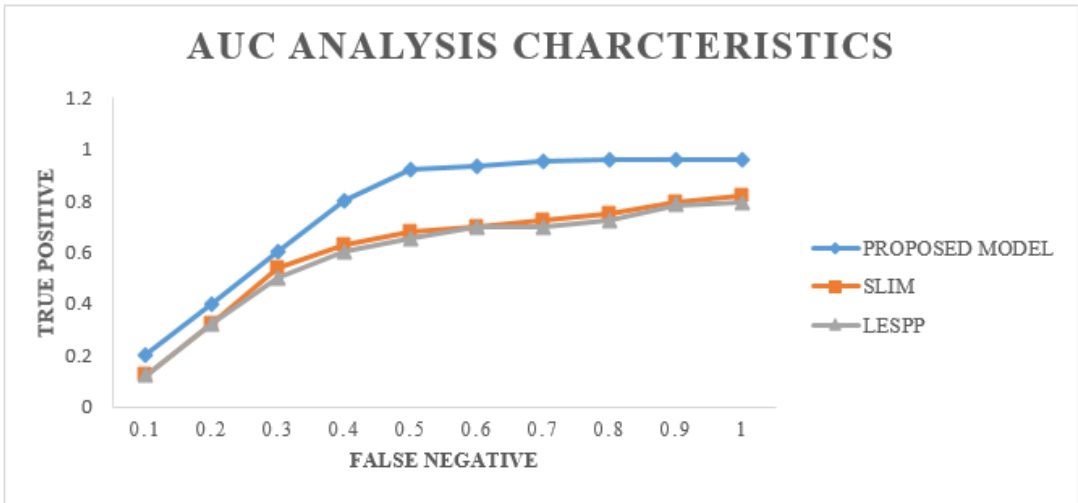

Figure 5. AUC characteristics of the different model in predicting the sybil and wormhole attacks from the generated datasets

5.2 Performance analysis

The collected datasets were utilised to analyze the efficiency of the existing techniques and recommended model to identify the attack in the vehicular scenario.

5.2.1 Discussions

Tables 3-11 illustrate the performance of the distinct techniques in identifying the sybil and wormhole threats with the changes in vehicle speed. Table 3-5 highlights the detection efficiency of the modified CNN. It is apparent that the efficiency degrades as the vehicles speed elevates in the road scenario. The efficiency decreases by 35% of CNN as the speed increases. The similar fashion of the performance is observed in LiNET which is observed from Table 6 to table 8. But in contrary, effectiveness of the recommended model remains the stable as there is an increase in speed of the vehicles [34-36]. Hence the proposed model finds its more suitability in detecting the sybil and wormhole attacks in a dynamic vehicular speed, as highlighted in Table 9-11. Figures 4-5 illustrate AUC performance of the proposed framework and other models. It is evident that the loss is very less for the detection of malicious users in the dynamic environment.

5.3 Security analysis

In this experimentation, randomness of encrypted bits is evaluated and examined. NIST tests are performed to verify the randomness of the encrypted bits, which can be utilized for transmitting private models to central servers. The 12 essential tests from NIST were carried out, and the results are presented in Table 12.

From Table 12, it is apparent that the encrypted bits demonstrate an increased randomness, making it significantly more challenging for an attacker to alter the medical data while transmitting.

Table 12. NIST benchmark evaluation results of the suggested framework

S.No	NIST Evaluation Standards	Test Results
1	Frequency Test	Approved
2	Lempel-ZIV Compression Test	Approved
3	Block Frequency Test	Approved
4	Overlapping Template of all One's Test	Approved
5	Random Excursion Test	Approved
6	Matrix Rank Test	Approved
7	DFT Test	Approved
8	Linear Complexity Test	Approved
9	Universal Statistical Test	Approved
10	Long Run Test	Approved
11	Frequency MonoTest	Approved
12	RunTest	Approved

5.4 Encryption time analysis

Table 13. Encryption time analysis for the different encryption model

Encryption Model	Encryption Time (secs)
[37]	50.45
[38]	34.45
[39]	45.89
[40]	34.89
[41]	33.90
Proposed Encryption Schemes	**18.89**

To calculate the communication cost of the recommended model, encryption time is evaluated for the recommended model and contrasted with the existing models including Homographic Encryption model and other hybrid encryption models [37-42].

Table 13 presents the encryption time analysis between the different schemes. From Table 13, it is evident that encryption time is 40% to 60% lesser than the exiting schemes used in VANET environments.

6. CONCLUSION AND FUTURE SCOPE

In this research, a hybrid intelligent detection and encryption schemes are proposed to increase the effectiveness of the VANET. The novelty of the proposed model is to introduce the centralities measures and enhanced gated recurrent units for the detection of sybil and wormhole attacks in the VANET topologies. Furthermore, Dual Henon chaotic encryption is integrated with the AES to formulate the strong counterfeiting mechanism to protect the VANET data against the attacks. These encryption algorithms are common for implementation in both OBUs as well as RSUs to safeguard personal data and vehicular data against threats. The comprehensive experimentation is conducted utilising the SUMO-OMNET++ datasets and effectiveness of the different models are calculated and analysed. The average performance of the model is found to be 96.5 % in detecting the sybil and wormhole attacks. The security tests were conducted using NIST test suites and encryption time was calculated. From the experimentation it was found that the proposed model consumes only 60% of encryption time than the other techniques. As a future enhancement, the method should be equipped with advanced optimization techniques such as lightweight evolutionary algorithms or energy-aware metaheuristics to reduce computational overhead and enable seamless deployment on resource-constrained embedded OBUs. Additionally, scalability toward large-scale datasets and real-time vehicular environments should be explored.

REFERENCES

[1] Fakhfakh, F., Tounsi, M., Mosbah, M. (2019). An evaluative review of the formal verification for vanet protocols. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, pp. 1209-1214. https://doi.org/10.1109/IWCMC.2019.8766783

[2] Mostafa, S.A., Mustapha, A., Ramli, A.A., Jubair, M.A., Hassan, M.H., Abbas, A.H. (2021). Comparative analysis to the performance of three Mobile ad-hoc network routing protocols in time-critical events of search and rescue missions. In Advances in Simulation and Digital Human Modeling: Proceedings of the AHFE 2020 Virtual Conferences on Human Factors and Simulation, and Digital Human Modeling and Applied Optimization, July 16-20, 2020, USA, pp. 117-123. https://doi.org/10.1007/978-3-030-51064-0_16

[3] Abbas, A.H., Ahmed, A.J., Rashid, S.A. (2022). A cross-layer approach MAC/NET with updated-GA (MNUG-CLA)-based routing protocol for VANET network. World Electric Vehicle Journal, 13(5): 87. https://doi.org/10.3390/wevj13050087

[4] Jubair, M.A., Mostafa, S.A., Muniyandi, R.C., Mahdin, H., Mustapha, A., Hassan, M.H., Mahmoud, M.A., Al-Jawhar, Y.A., Al-Khaleefa, A.S., Mahmood, A.J. (2019). Bat optimized link state routing protocol for energy-aware mobile ad-hoc networks. Symmetry, 11(11): 1409. https://doi.org/10.3390/sym11111409

[5] Touil, A., Ghadi, F. (2018). Efficient dissemination based on passive approach and dynamic clustering for VANET. Procedia Computer Science, 127: 369-378. https://doi.org/10.1016/j.procs.2018.01.134

[6] Khan, A.A., Abolhasan, M., Ni, W. (2018). An evolutionary game theoretic approach for stable and optimized clustering in VANETs. IEEE Transactions on Vehicular Technology, 67(5): 4501-4513. https://doi.org/10.1109/TVT.2018.2790391

[7] Mehmood, A., Khanan, A., Mohamed, A.H.H., Mahfooz, S., Song, H., Abdullah, S. (2017). ANTSC: An intelligent Naïve Bayesian probabilistic estimation practice for traffic flow to form stable clustering in VANET. IEEE Access, 6: 4452-4461. https://doi.org/10.1109/ACCESS.2017.2732727

[8] Banikhalaf, M., Khder, M.A. (2020). A simple and robust clustering scheme for large-scale and dynamic VANETs. IEEE Access, 8: 103565-103575. https://doi.org/10.1109/ACCESS.2020.2999368

[9] Alaya, B., Sellami, L. (2021). Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks. Journal of Information Security and Applications, 58: 102779. https://doi.org/10.1016/j.jisa.2021.102779

[10] Habelalmateen, M.I., Abbas, A.H., Audah, L., Alduais, N.A.M. (2020). Dynamic multiagent method to avoid duplicated information at intersections in VANETs. TELKOMNIKA (Telecommunication Computing Electronics and Control), 18(2): 613-621. http://doi.org/10.12928/telkomnika.v18i2.13947

[11] Kalpana, P., Almusawi, M., Chanti, Y., Kumar, V.S., Rao, M.V. (2024). A deep reinforcement learning-based task offloading framework for edge-cloud computing. In 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, pp. 1-5. https://doi.org/10.1109/ICICACS60521.2024.10498232

[12] Marwah, G.P.K., Jain, A. (2022). A hybrid optimization with ensemble learning to ensure VANET network stability based on performance analysis. Scientific Reports, 12(1): 10287. https://doi.org/10.1038/s41598-022-14255-1

[13] D'souza, F.J., Panchal, D. (2017). Advanced encryption standard (AES) security enhancement using hybrid approach. In 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, pp. 647-652. https://doi.org/10.1109/CCAA.2017.8229881

[14] Chen, S., Hu, W., Li, Z. (2019). High performance data encryption with AES implementation on FPGA. In 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, pp. 149-153. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00036

[15] Kalpana, P., Anandan, R., Hussien, A.G., Migdady, H., Abualigah, L. (2024). Plant disease recognition using residual convolutional enlightened swin transformer networks. Scientific Reports, 14(1): 8660. https://doi.org/10.1038/s41598-024-56393-8

[16] Akhtar, M., Moridpour, S. (2021). A review of traffic congestion prediction using artificial intelligence. Journal of Advanced Transportation, 2021(1): 8878011. https://doi.org/10.1155/2021/8878011

[17] Kalpana, P., Kodati, S., Smitha, L., Sreekanth, N., Smerat, A., Ahmad, M.A. (2025). Explainable AI-driven gait analysis using wearable internet of things (Wiot) and human activity recognition. Journal of Intelligent Systems & Internet of Things, 15(2): 55-75. https://doi.org/10.54216/JISIoT.150205

[18] El-Shafai, W., Azar, A.T., Ahmed, S. (2025). AI-driven ensemble classifier for jamming attack detection in VANETs to enhance security in smart cities. IEEE Access, 13: 50687-50713. https://doi.org/10.1109/ACCESS.2025.3552544

[19] Bayan, S., Mohammad, U., Al Mohammad, A. (2024). Position falsification attack detection in inter-vehicle networks using deep learning. In 2024 IEEE International Conference on Electro Information Technology (eIT), Eau Claire, WI, USA, pp. 621-626. https://doi.org/10.1109/eIT60633.2024.10609919

[20] Suman, P., Padhy, S., Kumar, N., Suman, A., Singh, A., Singh, K. K., Castilla, Á.K., AL-Zahrani, T.S.S. (2024). An improved deep learning-based intrusion detection for reliable communication in VANET. IEEE Transactions on Consumer Electronics. https://doi.org/10.1109/TCE.2024.3475823

[21] Jabbar, M.K., Trabelsi, H. (2022). A betweenness centrality based clustering in VANETs. In 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, pp. 1-4. https://doi.org/10.1109/SIN56466.2022.9970553

[22] Fatemidokht, H., Rafsanjani, M.K., Gupta, B.B., Hsu, C.H. (2021). Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems, 22(7): 4757-4769. https://doi.org/10.1109/TITS.2020.3041746

[23] Polat, H., Turkoglu, M., Polat, O. (2020). Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET. IET Communications, 14(22): 4089-4100. https://doi.org/10.1049/iet-com.2020.0477

[24] Wang, M., Liu, D., Zhu, L., Xu, Y., Wang, F. (2016). LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. Computing, 98(7): 685-708. https://doi.org/10.1007/s00607-014-0393-x

[25] Alfadhli, S.A., Lu, S., Fatani, A., Al-Fedhly, H., Ince, M. (2020). SD2PA: A fully safe driving and privacy-preserving authentication scheme for VANETs. Human-centric Computing and Information Sciences, 10: 1-25. https://doi.org/10.1186/s13673-020-00241-x

[26] Fatemidokht, H., Rafsanjani, M.K. (2020). QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks. Journal of Systems and Software, 165: 110561. https://doi.org/10.1016/j.jss.2020.110561

[27] Guo, Y., Zhang, H., Zhang, L., Fang, L., Li, F. (2019). A

game theoretic approach to cooperative intrusion detection. Journal of Computational Science, 30: 118-126. https://doi.org/10.1016/j.jocs.2018.11.003

[28] Wehrle, K., Günes, M., Gross, J. (2010). Modeling and Tools for Network Simulation. Springer Science & Business Media.

[29] Lopez, P.A., Behrisch, M., Bieker-Walz, L., Erdmann, J., Flötteröd, Y.P., Hilbrich, R., Lücken, L., Rummel, J., Wagner, P., Wießner, E. (2018). Microscopic traffic simulation using sumo. In 2018 21st International Conference on Intelligent Transportation Systems (ITSC), Maui, HI, USA, pp. 2575-2582. https://doi.org/10.1109/ITSC.2018.8569938

[30] Kalpana, P., Narayana, P., Smitha, L., Madhavi, D., Keerthi, K., Smerat, A., Nazzal, M.A. (2025). Health-Fots-A latency aware fog based IoT environment and efficient monitoring of body's vital parameters in smart health care environment. Journal of Intelligent Systems & Internet of Things, 15(1): 144-156. https://doi.org/10.54216/JISIoT.150112

[31] Chung, J., Gulcehre, C., Cho, K., Bengio, Y. (2014). Empirical evaluation of gated recurrent neural networks on sequence modeling. arXiv preprint arXiv:1412.3555. https://doi.org/10.48550/arXiv.1412.3555

[32] Huang, G.B., Zhu, Q.Y., Siew, C.K. (2006). Extreme learning machine: Theory and applications. Neurocomputing, 70(1-3): 489-501. https://doi.org/10.1016/j.neucom.2005.12.126

[33] Wang, B., Huang, S., Qiu, J., Liu, Y., Wang, G. (2015). Parallel online sequential extreme learning machine based on MapReduce. Neurocomputing, 149: 224-232. https://doi.org/10.1016/j.neucom.2014.03.076

[34] Vitalkar, R.S., Thorat, S.S., Rojatkar, D.V. (2022). Intrusion detection for vehicular ad hoc network based on deep belief network. In Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT 2021, Springer, Singapore, pp. 853-865. https://doi.org/10.1007/978-981-16-3728-5_64

[35] Guarino, I., Bovenzi, G., Di Monda, D., Aceto, G., Ciuonzo, D., Pescapé, A. (2022). On the use of machine learning approaches for the early classification in network intrusion detection. In 2022 IEEE International Symposium on Measurements & Networking (M&N), Padua, Italy, pp. 1-6. https://doi.org/10.1109/MN55117.2022.9887775

[36] Paranjothi, A., Atiquzzaman, M. (2022). A statistical approach for enhancing security in VANETs with efficient rogue node detection using fog computing. Digital Communications and Networks, 8(5): 814-824. https://doi.org/10.1016/j.dcan.2021.09.010

[37] Talib, M.S., Hassan, A., Alamery, T., Abas, Z.A., Mohammed, A.A.J., Ibrahim, A.J., Abdullah, N.I. (2020). A center-based stable evolving clustering algorithm with grid partitioning and extended mobility features for VANETs. IEEE Access, 8: 169908-169921. https://doi.org/10.1109/ACCESS.2020.3020510

[38] Vijayakumar, P., Azees, M., Kannan, A., Deborah, L.J. (2015). Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 17(4): 1015-1028. https://doi.org/10.1109/TITS.2015.2492981

[39] Kazi, A.K., Khan, S.M., Haider, N.G. (2021). Reliable group of vehicles (RGoV) in VANET. IEEE Access, 9: 111407-111416. https://doi.org/10.1109/ACCESS.2021.3102216

[40] Kalpana, P., Anandan, R. (2023). A capsule attention network for plant disease classification. Traitement du Signal, 40(5): 2051-2062. https://doi.org/10.18280/ts.400523

[41] Anjali, T., Goyal, R., Balaji, G.N. (2024). Prevention of attacks in vehicular adhoc networks. In 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, pp. 1-8. https://doi.org/10.1109/SCEECS61402.2024.10482267

[42] Karne, R.K., Sreeja, D.T. (2022). A novel approach for dynamic stable clustering in VANET using deep learning (LSTM) Model. IJEER, 10(4): 1092-1098. https://doi.org/10.37391/IJEER.100454