International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(18s) 2026 pp. 243-264
https://doi.org/10.70917/ijcisim-2026-4864
Article

DEEP NEURAL BASED LIGHTWEIGHT ROUTING AND PROBABILITY PLOT CORRELATION FOR SECURE VANET COMMUNICATION

M. Selvi[1], R. Rajesh[2]

[1]PG and Research Department of Computer Science, Kaamadhenu Arts and Science College, Sathyamangalam, Tamilnadu, India.
[2]Department of Computer Science with Cyber Security, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamilnadu, India.

Abstract: Vehicular Ad-Hoc Networks (VANETs) are pivotal for controlling traffic flow and intensifying safety in Intelligent Transportation Systems (ITS) through effective transmission of data between nodes. In spite of that, VANETs pose notable issues, like, vulnerability to malicious activities and intricate routing issues that can compromise network security and performance. However there still remains room for improvement in the development of VANETs, considering, security weaknesses and latency in data transfer process. Most of the routing methods right now are not effective and secure, specifically when utilized in high-mobility environments. The requirement to design an intelligent and secure routing protocol that establishes low latency, high packet delivery ratio and resilience against malicious attacks is what motivates this work. A novel secure route based data transfer in VANET called, Deep Neural Lightweight Multi-objective and Ryan-Joiner Correlation (DNLM-RJC) is proposed. The DNLM-RJC method for secure route based data transfer in VANET is split into four layers, namely, one input layer, two hidden layers and finally one output layer. The network traffic patterns obtained are processed in the input layer. In the first hidden layer, the authentication mechanism of vehicle nodes is implemented by using Lightweight Multi-objective Secure Route-based Authentication model. This model enhances network security by preventing data manipulation from malicious nodes. After the node authentication is done, the second objective, secure data transfer is executed via second hidden layer. In order to perform effective and secure data transfer in VANET, Ryan-Joiner Correlation Coefficient is applied. The experiments are conducted on the Comprehensive Vehicular Communication Network Attack Dataset. We demonstrated the significance of the proposed DNLM-RJC method in comparison with studies employing secure route based data delivery in an extensive manner. Experimental results show that the proposed method can improve the authentication delay with improved attack detection rate and also reduces end to end delay significantly on different size samples.
Keywords: Vehicular Ad hoc Network, Intelligent Transportation Systems Deep Neural, Lightweight Multi-objective, Ryan-Joiner Correlation Coefficient

1. Introduction

The growing traffic pattern complexity in contemporary urban environments calls for intelligent and scalable solutions for predicting traffic within the Vehicular Ad Hoc Networks (VANETs). Also the dynamic aspects of VANETs insist reliable and secure communication over wireless network. Nevertheless, there are notable inconsistencies in VANETs associated to security and privacy.

A lightweight Deep Neural Network (DNN) with Convolutional Neural Network (CNN) framework (DNN-CNN) was proposed in [1] to ensure secure and scalable traffic management. Moreover to ensure effective prediction of traffic Geographic Routing Protocols (GRP) were also incorporated in resource-constrained V2X frameworks. The

method incorporated the potentiality of spatial feature extraction using CNNs and temporal strength of DNNs with the intent of obtaining vehicular patterns in dynamic fashion. This in turn improved accuracy with minimal latency.

An Enhanced Location Aided Ant colony Routing (ELAACR) was proposed in [2] for VANETs with the objective of achieving seamless secure data transmission. The ELAACR method initially implemented Location-Aided Key Management (LAKM) and Ant Colony Routing (ACR) via two-fold mechanism. On one hand the LAKM was designed on the basis of group signature to formulate a secure network. On the other hand, the ACR was utilized in identifying secure and shortest path to ensure seamless data transmission. With this the method saw an overall improvement throughput and packet delivery ratio and also reducing overhead with end to end delay significantly.

Deep Learning algorithms with improved feature selection techniques were employed in [3] to not only enhance the reliability but also to ensure safety of vehicles while performing communication. This ensured VANET security with real time attack detection. However the communication cost involved in detection was not focused. To address on this aspect Fisher Information Matrix along with Differential Privacy was applied in [4] for maintaining accuracy stability. In addition to that intrusion was detected accurately. Nevertheless routing complexities and excessive control overhead was not focused. To address on this research gap, improved deep reinforcement learning was proposed in [5] that in turn decreased latency.

Routing within a VANET is a complex procedure involving successful data packets transmission between source and destination vehicle while making certain secure and dependable communication framework is the need of hour. A multi-layered defense framework was proposed in [6] to impart a dynamic and secured framework. However they compromise the secure content dissemination within VANET. To focus on this issue, an artificial neural network model was designed in [7] that in turn facilitated the assessment of end to end delay with improved throughput. Moreover it can provide route planning, however, data privacy and security are demanding issues that need to be handled properly. In [8] a flexible policy encryption based method was designed that in turn shared and stored data with less overhead.

The advancement of vehicular networks from VANETs to Internet of Vehicles (IoVs) has posed a demanding role in the ITS. In spite of their advantages, VANETs pose vulnerable to several security threats, like, Sybil, wormhole and blackhole attacks. To avoid blackhole attacks a deep neural network framework was applied in [9]. Moreover by applying random waypoint reduced routing delay with minimal control overhead. A comprehensive survey of providing security and privacy employing reinforcement learning in VANET was investigated in [10]. Conventional identity authentication and key agreement frameworks less frequently [11] took into consideration the influence of effectiveness that in turn caused increased communication costs and reduced efficiency. To address on this part a lightweight authentication mechanism was proposed in [12], therefore ensuring minimal computation cost.

Authentication algorithm was included in [13] using machine learning to ensure secure communication between vehicles in VANET. Yet another lightweight authentication mechanism was designed in [14] with cuckoo filter to accomplish privacy and resist against attacks, therefore ensuring minimal memory requirement. Moreover the critical issue of security was addressed in [15] by utilizing machine learning driven model.

The overarching objective of this research is to ensure secure routing and combating against three different types of VANET routing attacks while improving attack detection rate and reducing authentication latency considerably. The key objective is to make efficient and secure routing in VANET and imparting difference between three different attacks. In order to achieve this, we perform a systematic analysis of deep learning based Deep Neural Lightweight Multi-objective and Ryan-Joiner Correlation (DNLM-RJC) in VANET. Moreover, we analyze the requirements and consequences of utilizing deep learning based technique quality of service in terms of authentication delay, authentication latency, packet delivery rate, end to end delay and attack detection rate in the design of the proposed DNLM-RJC method for VANETs.

1.1 Contributions of the work

As presented in the above section, numerous works are presented in literature concerning secure routing and data delivery in VANET. This research proposes following novel contributions.

- To ensure secure routing and data delivery in VANET accurately and precisely, a deep learning based method called, Deep Neural Lightweight Multi-objective and Ryan-Joiner Correlation (DNLM-RJC) is developed based on one input layer, two hidden layers and one output layer.
- First, in the input layer network traffic patterns are obtained from the Comprehensive Vehicular Communication Network Attack Dataset. Next, in the first hidden layer, Lightweight Multi-objective Secure Route-based Authentication model is model in the proposed DNLM-RJC method key set generation and multi-objective function is designed with which the Node Authentication Score (NAS) are evaluated. Based on this NAS secure routing is modeled.
- In the second hidden layer, Ryan-Joiner Correlation Coefficient Secure Route-based Data Transfer model is applied to improve attack detection rate and packet delivery ratio. Here, the correlation coefficient accurately detects network anomalies and identifies malicious traffic patterns, therefore ensuring secure data delivery.
- Finally, an extensive experimental assessment is performed with five distinct performance metrics to analyze and validate the proposed DNLM-RJC method over traditional methods.

1.2 Organization of the work

The rest of this work is structured as follows. Section 2 discusses different secure routing methods in VANET with an overview of related work and narrates their indispensable features. Section 3 describes the proposed deep learning based method, DNLM-RJCand presents strategies for algorithms. Section 4 provides detailed case study and derive inferences. In Section 5 experimental setup, followed by simulation results and comparisons with the traditional methods with the aid of table and graphical representation is provided. Finally, the conclusions of this research are provided in section 6.

2. Related works

With the evolution of autonomous vehicles, security concerns associating VANETs have increased. VANETs still pose issues associated to privacy with full-scale deployment owing to lack of user trust. Some of the critical aspects shaping VANETs include their dynamic topology and high mobility characteristics. A survey of authentication mechanisms in VANET was investigated in [16]. The communication overheads are less for these computations and there are numerous security requirements that should be maintained. An efficient message authentication mechanism with a privacy preservation protocol was proposed in [17]. This protocol minimized the overall communication overheads. A neural network based intelligent routing mechanism was designed in [18] for communicating between vehicular nodes in VANET in a secure manner. A formal security analysis was performed in [19] for resource constrained environments.

A secure VANET architecture was proposed in [20] supporting layered operation and also mitigate against attacks via ITS. A method to ensure accuracy employing bi-directional sparse attention network was used in [21] for malicious attack detection with VANET with improved security. However secured route selection was not ensured. To address on this aspect, in [22] resilient routing algorithm was designed. By using this algorithm secure route selection was ensured with improved accuracy. However due to frequent network disconnection causes high end to end delay. To address on this aspect a honey badger optimization algorithm was designed in [23] therefore making informed decisions on routing.

A review of vulnerability classification and algorithms for ensuring secure routing in VANET was detailed in [24]. A holistic review of security attacks and its counter measures were investigated in [25]. A method to minimize computation and communication cost employing certificateless aggregate signature scheme in VANET was presented in [26].

However with the inclusion of false positive attacks the vulnerability detection rate was said to be compromised. To focus on this issue, bagging ensemble learning was proposed in [27]. By applying this ensemble method in turn ensured scalable and robust solution for VANET security. Yet another safety message delivery scheme in VANET was presented in [28] with minimal computational overhead. A throughput and packet delivery ratio improved VANET communication method was proposed in [29] using enhanced cluster based routing.

Except for the above works, most other researches only concentrate on either reducing the overall training time or reducing the error rate. The objectives of most existing DDoS attack detection types in wireless network are to reduce the training time without concentrating about the rate of accuracy. Different from the researches aforementioned, our deep learning based method called, Deep Neural Lightweight Multi-objective and Ryan-Joiner Correlation (DNLM-RJC) aims at minimizing the authentication delay along with the overall attack detection rate extensively. The elaborate description of the NTK-SN method is provided in the following sections.

3. Materials and Methodology

3.1 Data Collection and Description

The Comprehensive Vehicular Communication Network Attack Dataset extracted from https://data.mendeley.com/datasets/x7tdmsf27x/1 [30] captures three different critical vehicular-specific attacks, like, Spoofing, Sybil and Wormhole in Vehicular Communication Networks (VCNs). It includes both legitimate and malicious samples generated employing realistic positional dynamics, mobility patterns and temporal interactions. The dataset possess over 100000 samples including thirty one different features. The details about the Comprehensive Vehicular Communication Network Attack Dataset are listed in table 1.

Table 1 Dataset details

S. No	Attack	Legitimate	Malicious
1	Spoofing	45975	589
2	Wormhole	52237	5219
3	Sybil	14829	1753
Total		113041	7561

The features included in the above dataset are mobility dynamics, comprising of speed, rate of distance change, positional features, consisting of location, inter-vehicle distances, temporal features, comprising of time intervals and communication metrics, like, packets count, hop counts, transmission rates and reception rates in addition to three different types of attack specific labels, like, spoofing, Sybil and wormhole. With the above dataset details secure routing with data transmission is performed in VANET.

3.2 Deep Neural Lightweight Multi-objective and Ryan-Joiner Correlation based optimal routing with authentication for secure data transmission

Owing to the reason that data transmission occurs via an unprotected and vulnerable medium, it is pivotal to safeguard data from threats and unauthorized access. Mutual authentication is demanding for ascertaining the vehicular communication security and application's integrity. For VANET's several solutions have been generated to make certain key exchange and mutual authentication. In order to safeguard the vehicular-specific attacks from distinct security risks and to minimize the communication and computational demands, a reliable and effective authentication mechanism should be setup. In this section a novel Deep Neural Lightweight Multi-objective and Ryan-Joiner Correlation (DNLM-RJC) based optimal routing with authentication for secure data transmission in VANET is presented. To accomplish authenticated node access within the source-destination pair, initially node authentication is performed in our work for secure data transmission in VANET. Figure 1 show the block diagram of DNLM-RJC based optimal routing with authentication for secure data transmission.

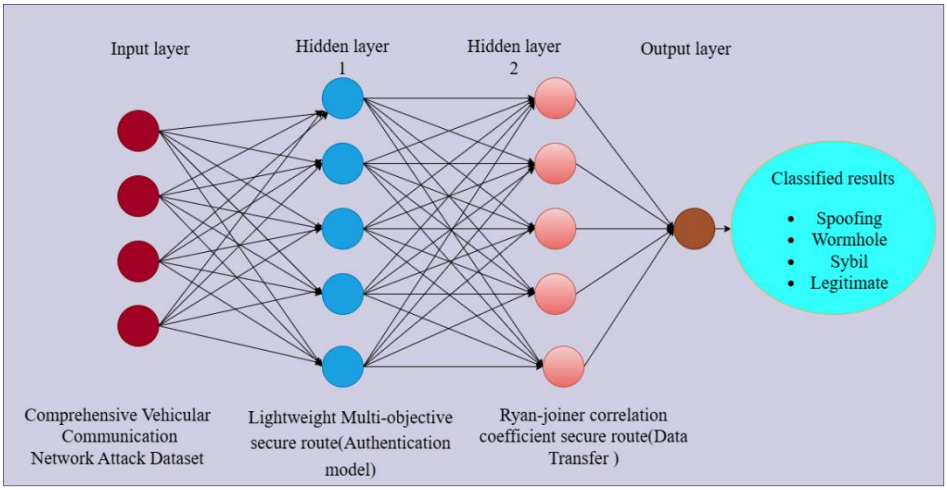

Figure 1 Block diagram of DNLM-RJC

As illustrated in the above figure, the overall process of secure routing and authenticated data delivery in VANET using Deep Learning (DL) is split into four layers. They are one input layer, two hidden layers and finally one output layer. In the input layer all the details of Comprehensive Vehicular Communication Network Attack Dataset are obtained. Followed by which in the first hidden layer a secure route based authentication model using Lightweight Multi-objective Secure Route-based Authentication model is designed. With the secure route generated for the network traffic samples next in the second hidden layer, Ryan-Joiner Correlation Coefficient Secure Route-based Data Transfer is performed. Accordingly the classified results are provided as output in the output layer. The elaborate description of the proposed method is provided in the following sub-sections.

3.2.1 Input Layer

To start with an input layer constituting secure routing and authenticated data delivery in VANET is designed. Here, initially in the input layer all the feature inputs corresponding to mobility dynamics, temporal features, positional features along with communication metrics and three different attack-specific labels are obtained. These feature inputs constitutes the input to be model for secure routing and authenticated data delivery. The vehicular nodes that need to involve in communication has to register with the VANETs so that node information is maintained. Each vehicular node is identified with the registered ID to avoid malicious nodes access in the VANET. The vehicular node information processing is done as given below.

$$NInfo[S_N] = \sum_{S=1}^{N} \quad getSID(S) + getF(S) \tag{1}$$

From the above equation (1) '$getSID$' considers the vehicular node ID and '$getF$' extracts the vehicular node features in VANET.

3.2.2 Lightweight Multi-objective Secure Route-based Authentication model

Since the communication between vehicular nodes in VANET take place in open channel, there exists several threats caused by the malicious nodes. In addition most of the existing authentication mechanisms suffer from communication and computational overhead. With the intent of providing effective lightweight authentication with secure routing, a novel Lightweight Multi-objective Secure Route-based Authentication model has been proposed to ensure efficient end to end security in VANET via the first hidden layer. Figure 2 shows the structure of Lightweight Multi-objective Secure Route-based Authentication model.

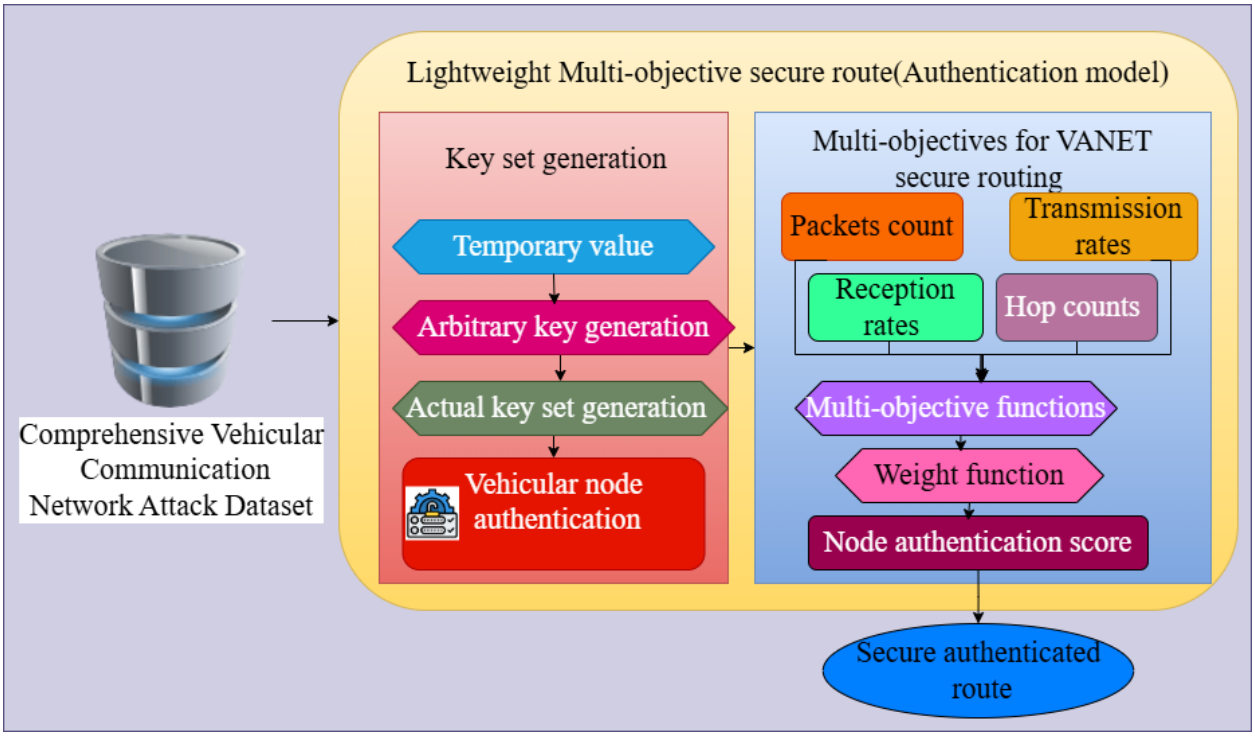

Figure 2 Structure of Lightweight Multi-objective Secure Route-based Authentication

As illustrated in the above figure, with the information obtained from the input layer, a secure route-based authentication using Lightweight Multi-objective Secure Route-based Authentication is designed. The information from the input layer is initially subjected to two different processes via the first hidden layer. They are generation of key set and designing of multi-objectives for VANET routing. As the name implies in the key set generation model, key set is generated for all the registered vehicular nodes and are accordingly distributed for further processing. Next, multi-objective function by considering packets count, transmission rates, reception rates and hop counts are employed and accordingly Node Authentication Score (NAS) is generated. Higher the NAS higher is the probability of vehicular node being legitimate and vice versa. Accordingly secure and authenticated route is generated between the source and target vehicular nodes.

3.2.2.1 Key set generated results

Next, the proposed method generates key sets that are utilized in performing node authentication to ensure secure routing in the VANET. The key set is used for node authentication. The key set generation is performed as given below.

$$Temp_1 = \sum_{S=1}^{N} \quad getVal(S) \tag{2}$$

$$AK_1 = \frac{\sum_{S=1}^{N} \quad (Temp_1)}{N} \ll 2 \tag{3}$$

$$Key[N] = \sum_{S=1}^{N} \quad \frac{(AK_1)}{Temp_1} \& (Temp_1 <\oplus AK_1) \tag{4}$$

From the above equations (2), (3) and (4) initially a temporary value '$Temp_1$' is generated with which an arbitrary key 'AK_1' is generated. The key set generated in the VANET is then distributed to all the registered vehicular

nodes in the network. Followed by which the actual key set '$Key[N]$' is generated for performing secure route authentication.

3.2.2.2 Multi-objectives for VANET secure routing

The multi-objectives like packets count 'PC', transmission rates 'TR', reception rates 'RR' and hop counts 'HC' are considered during the vehicular node authentication process. The multi-objective function is defined mathematically as given below.

$$Obj = (W_1 * F_1) + (W_2 * F_2) + (W_3 * F_3) + (W_4 * F_4) \quad (5)$$

From the above equation (5), 'F_1', 'F_2', 'F_3' and 'F_4' points to the fitness function corresponding to packets count 'PC', transmission rates 'TR', reception rates 'RR' and hop counts 'HC' respectively. Moreover, 'W_1', 'W_2', 'W_3' and 'W_4' denotes the corresponding weights. This is mathematically defined as given below.

$$W = \{0, if\ low < F\ \frac{high-F}{low-F}, if\ F\ \leq high \leq low\ \frac{mid-high}{mid-low}, if\ low\ \leq high \leq mid\ 0, if\ high \geq low \quad (6)$$

From the above equation (6) '$low = 0$' points to the lower threshold value, '$mid = 1$' points to the mid threshold value and '$high = 1$' pointing the high threshold value respectively. Moreover the values of maximum and minimum of 'F_1', 'F_2', 'F_3' and 'F_4' points to the fitness function corresponding to packets count 'PC', transmission rates 'TR', reception rates 'RR' and hop counts 'HC' respectively.

With the above actual key set generated results and multi-objective functions defined is considered to perform node authentication to ensure secure routing. The vehicular nodes that are authenticated are then considered for initiating communication. The vehicular node authentication is performed as given below.

$$Auth[N] = \sum_{S=1}^{N} \quad get\big(Key(S)\big) = \{Auth \rightarrow 1, if\ \big(Key(S)\big) == get\big(Key(S)\big)\ and\ NAS\ \ Auth \rightarrow 0, Otherwise \quad (7)$$

In addition to physical attributes, the proposed method utilizes Node Authentication Score obtained from as given below.

$$NAS = \sum_{S=1}^{N} \quad \omega_S[PC(\downarrow), TR(\downarrow), RR(\uparrow), HC(\downarrow)] \quad (8)$$

From the above equation (8) 'ω_S' denotes the weight factor along with the fitness function corresponding to packets count 'PC', transmission rates 'TR', reception rates 'RR' and hop counts 'HC' respectively.

3.2.3 Ryan-Joiner Correlation Coefficient Secure Route-based Data Transfer

Data security is highly pivotal as far as safety-related vehicular applications are concerned. Critical issues of limited bandwidth, frequently changing topology and high speed arise due to the distributed characteristic of VANET. A secure transmission model called Ryan-Joiner Correlation Coefficient Secure Route-based Data Transfer is proposed in this work to focus on these aspects. This is performed in the second hidden layer. Figure 3 shows the structure of Ryan-Joiner Correlation Coefficient Secure Route-based Data Transfer.

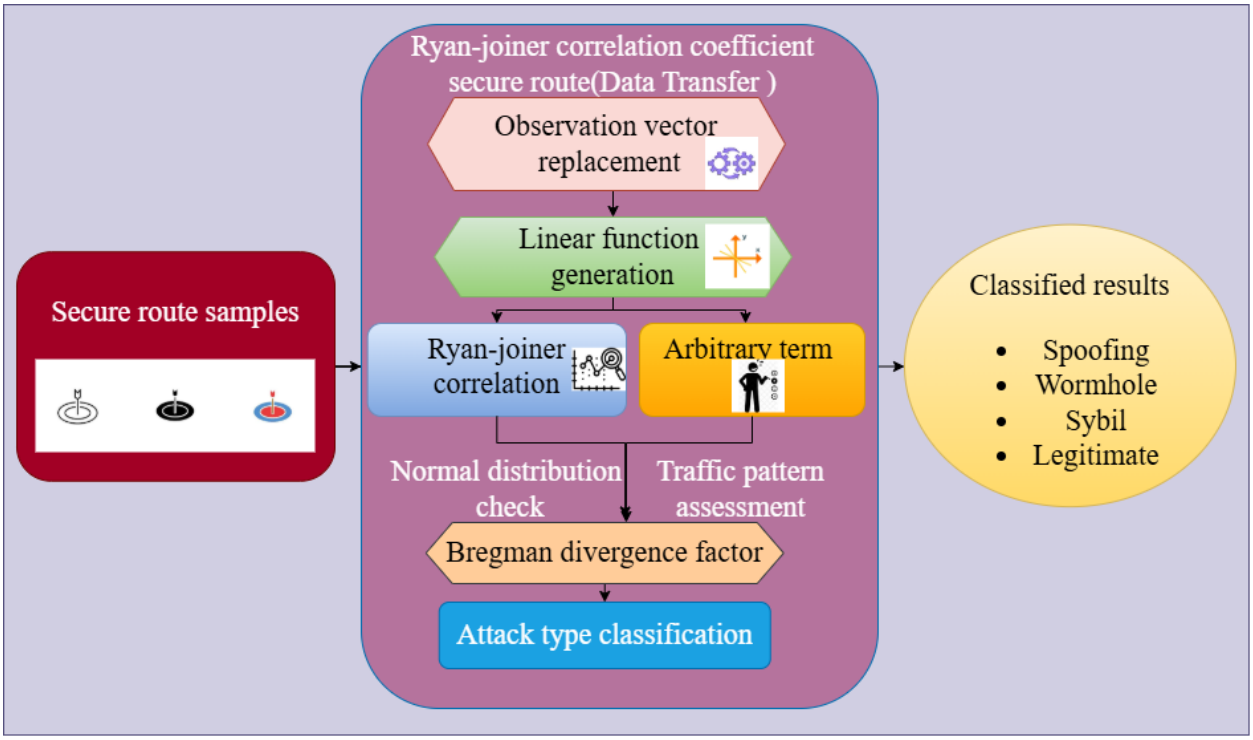

Figure 3 Structure of Ryan-Joiner Correlation Coefficient Secure Route-based Data Transfer

As illustrated in the above figure, with the secure route samples obtained as input from the first hidden layer is then subjected to data transfer for comprehensive VANET. The secure route samples are initially replaced by a vector. Followed by which linear function is generated and then Ryan–Joiner correlation coefficient is applied based on the observed feature samples to assess whether the network traffic exhibits a normal distribution. It ensures traffic patterns for abnormalities to ensure secure data transmission against routing attacks. Finally Bregman Divergence factor is evaluated to measure the difference between two probability distributions (i.e. attack or types of attack).

Given a set of samples possessing secure routing '$S_1, S_2, \dots, S_N$' denoted by 'S' where each observation or sample is designed via a row vector of 'M' features. The dataset 'DS' is hence denoted by a matrix 'S_{N*M}'. Then each observation vector '$S_i(i = 1,2, \dots, N)$' in our work is replaced by a vector mathematically defined as given below.

$$Res_i = \sum_i \quad (S_i - \mu_i), where \ \sum_i \quad = cov|S_i| \& \mu_i = E|S_i| \tag{9}$$

From the above equation (9) 'μ_i' and '$\sum_i \quad (.)$' are the sample mean and variance covariance matrix respectively. Moreover in VANETs not all the feature samples are binary values. Then the linear function among feature sample values is mathematically defined as given below.

$$Res = aS + b \tag{10}$$

From the above equation (10) the linear function results among feature sample 'S' values 'Res' are arrived at based on the Ryan–Joiner correlation coefficient 'a' and an arbitrary term 'b' respectively. The correlation coefficient 'a' is mathematically defined as given below.

$$a = \frac{\sum \; S_i Sc_i}{\sqrt{(S_i - S')^2 \sum \; Sc_i^2}} \quad (11)$$

From the above equation (11) the Ryan–Joiner correlation coefficient 'a' result is arrived at based on the observed feature samples with '$i = 1,2, \ldots, N$' and 'Sc_i' denoting the normal scores of the observed data respectively. Followed by which arbitrary term 'b' is mathematically defined as given below.

$$b = \frac{NRes \sum \; S^2 - \sum \; S \sum \; SRes}{N \sum \; S^2 - \left(\sum \; S\right)^2} \quad (12)$$

From the above equation (12) 'S' denotes the feature sample with 'Res' representing the data class. The Bregman Divergence 'Dis_i' at time 't' for incoming vehicular network traffic vector '$S_i(t)$' is the mathematically defined as given below.

$$Dis_i\,(t) = \sqrt{\left(S_i(t)\right) - \mu_i(t) \sum_t^{-1} \; (S_i(t) - \mu_i)} \quad (13)$$

With the above distance '$Dis_i\,(t)$' factor results for the corresponding incoming vehicular network traffic, finally the attack type classification results are generated as given below.

$$\begin{aligned} Class_i(t) = \{ & srcVmaxDeviation \\ & > 0.10 \; Or \; avgDstnc \; NOT \; in \; (53.75.55.83) \; Or \; srcVmaxDeviation \\ & \leq 0.10 \; Or \; destVmaxDeviation > 0.10 \; Or \; flowDuration \\ & > -1010.64 \; Or \; srcVmaxDeviation \leq 0.10 \; Or \; destVmaxDeviation \\ & > 0.10 \; or \; flowDuration \leq -1010.64 Or \; destEnd(x) \leq 540.43, then \; attack \\ & = SPOOFING \; xStrtTime \leq 1419.62, then \; attack = WORMHOLE \; destID \\ & \leq 7.50 \; Or \; destEnd(y) \leq 1413.64 \; Or \; txStrtTime > 439.53 \; Or \; destID \\ & \leq 7.50 \; Or \; avgDestSpeed > 8.91 \; Or \; txStrtTime > 409.40 \; Or \; destID \\ & > 7.50 \; Or \; avgSrcSpeed \leq 5.26 \; Or \; srcStrt(y) \leq 1316.75 \; Or \; txStrtTime \\ & \leq 366.24 \; Or \; destID > 7.50 \; OR \; avgDestSpeed > 9.94 \; Or \; txStrtTime \\ & > 452.32 \; then \; attack = SYBIL \; Else \; NORMAL \, . \end{aligned} \quad (14)$$

The pseudo code representation of Deep Neural Lightweight Multi-objective and Ryan-Joiner Correlation based optimal routing with authentication for secure data transmission is given below.

Input: Dataset 'DS', Samples '$S = \{S_1, S_2, \ldots, S_N\}$', Features '$F = \{F_1, F_2, \ldots, F_M\}$'
Output: secure route and data delivery
Step 1: **Initialize** '$N = 100000$', '$M = 31$'
Step 2: **Begin**
Step 3: **For** each Dataset 'DS' with Samples 'S' and Features 'F'
//Input layer
Step 4: Obtain vehicular node information according to (1)
//Secure routing [first hidden layer]

//Key set generated results

Step 5: Obtain the key set according to (2), (3) and (4)

Step 6: **Return** key set generated results

//Multi-objectives for VANET routing

Step 7: Formulate multi-objective function according to (5) and (6)

Step 8: Generate node authentication score and vehicular node authentication results according to (7) and (8)

Step 9: **If** '$\left(Key(S)\right) == get\left(Key(S)\right)\ and\ NAS == True$'

Step 10: **Retur**n authenticated vehicular node

Step 11: Perform secure routing

Step 12: **Go to** step 18

Step 13: **End if**

Step 14: **If** '$\left(Key(S)\right) \neq get\left(Key(S)\right)\ and\ NAS == False$

Step 15: Do not perform routing

Step 16: **Go to** step 4

Step 17: **End if**

//Data delivery [second hidden layer]

Step 18: **For** each Dataset 'DS' with Samples 'S' and Features 'F'

Step 19: Generate observation vector according to (9)

Step 20: Generate linear function among feature sample values according to (10)

Step 21: Evaluate Ryan–Joiner correlation coefficient results according to (11)

Step 22: Evaluate arbitrary term according to (12)

Step 23: Measure Bregman Divergence at time 't' for incoming vehicular network traffic vector according to (13)

Step 24: Generate the classified results according to (14)

Step 25: **End for**

//Output layer

Step 26: **Return** classified results

Step 27: **End for**

Step 28: **End**

Algorithm Deep Neural Lightweight Multi-objective and Ryan-Joiner Correlation

As given in the above algorithm the entire process of optimal routing with authentication for secure data transmission is split into four layers. They are one input layer, two hidden layers and one output layer. In the input layer network traffic patterns are obtained. Next in the first hidden layer, to ensure secure routing, Lightweight Multi-objective Secure Route-based Authentication model is designed. The Lightweight Multi-objective Secure Route-based Authentication model employed in our work is designed with the objective of ensuring secure communication in VANETs by preventing malicious attacks. This in turn filters false data packets and ensures only verified vehicles to take part in data delivery. Followed by which in the second hidden layer, to ensure data delivery with higher rate of attack detection, Ryan-Joiner Correlation Coefficient Secure Route-based Data Transfer is performed. The correlation

coefficient accurately detects network anomalies and identifies malicious traffic patterns with improved packet delivery ratio and higher rate of attack detection.

4 Case Study and Inferences

In this section case analysis of secure route based data transfer in VANET called, Deep Neural Lightweight Multi-objective and Ryan-Joiner Correlation (DNLM-RJC) is analyzed and validated. To perform simulation 20 samples are obtained from the Comprehensive Vehicular Communication Network Attack Dataset. Figure 4 shows the input samples.

txStrtTime	srcID	srcStrt(x)	srcStrt(y)	destID	destStrt(x)	destStrt(y)	strtDstncTx
456.2500	118	781.5400	633.3600	0	47.8700	292.2400	809.0950
456.2530	75	319.9900	324.2600	118	781.5400	633.3600	555.4920
456.2530	75	319.9900	324.2600	0	47.8700	292.2400	273.9970
458.0350	112	374.6400	657.5400	176	722.0200	682.5600	348.2800
458.0560	118	768.0200	637.7900	223	778.1800	461.3600	176.7220
458.0560	115	705.5100	623.7200	223	778.1800	461.3600	177.8810
253.2540	256	1821.7200	1454.4600	147	1951.4700	1187.1900	297.1000
253.2540	256	1821.7200	1454.4600	0	1912.6600	1337.1000	148.4700
253.2540	284	1821.7200	1454.4600	147	1951.4700	1187.1900	297.1000
0.1758	52	-0.5200	341.2300	69	1136.2700	1141.4800	1390.2100
0.2590	86	4.6900	343.0500	36	22.8800	349.4200	19.2731
0.3651	22	1134.2500	1138.5000	71	21.0900	348.7900	1364.8300

txtimeLastRx	flowDuration	srcEnd(x)	srcEnd(y)	destEnd(x)	destEnd(y)	endDstncTxRx	avgDelay
593.7530	137.5030	408.7500	369	47.8700	292.2400	368.9530	0.0463
1085.7300	629.4740	319.9900	324.2600	415.4700	367.7000	104.8970	0.0136
1191.0200	734.7640	319.9900	324.2600	47.8700	292.2400	273.9970	0.0354
957.2730	499.2380	756.6600	275.2700	493.5400	105.6100	313.0760	0.2812
879.2960	421.2400	415.4700	367.7000	778.1800	461.3600	374.6070	1.2161
1192.7900	734.7330	3.6100	370.8900	47.1000	292.4600	89.6808	0.1569
0	-253.2540	1821.7200	1454.4600	1943.2000	1199.0800	282.8010	0.1604
457.4720	204.2180	1901.9800	1433.0400	1783.0700	1428.7500	118.9870	0.1294
255.3200	2.0658	1821.7200	1454.4600	1943.2000	1199.0800	282.8010	1.3686
4.8229	4.6471	14.7407	322.0287	1138.1364	1133.3994	1385.7635	0
2.0193	1.7603	11.4846	360.8259	22.9890	365.2474	12.3248	0.1201
4.5539	4.1888	1128.1462	1131.7813	5.8530	337.8029	1374.7522	0.0482

rxBytes	txPkts	rxPkts	throughput	deliveryRatio	hopCount	avgSrcSpee
49312	551	536	2869.0100	97.2777	100	7.6650
214	6	5	2.7197	83.3333	0	0
126	6	3	1.3719	50	0	0
282	7	7	4.5189	100	0	9.1500
136	4	3	2.5829	75	0	7.0100
436	16	10	4.7473	62.5000	0	8.6750
0	4	0	0	0	0	0
144	3	3	5.6410	100	0	3.9750
136	4	3	526.6800	75	0	0
0	1	0	0	0	0	25.8500
482	17	17	2190.4739	100	0	29.7100
704	23	22	1344.5341	95.6522	0	24.8600

avgDestSpeed	avgDstnc	rateDstncChng	srcVmax	destVmax	srcVmaxDeviat	destVmaxD
0	589.0240	-3.2010	0	0	0	0
7.2950	330.1950	-0.7158	0	7.7400	0	-1
0	273.9970	0	0	0	0	0
3.5500	330.6780	-0.0705	8.9400	0	13.0941	0
0	275.6650	0.4698	7.7400	0	2.3603	0
4.1750	133.7810	-0.1200	9.0300	0	2.6256	0
7.6850	289.9500	0.0565	0	0	0	0
6.0550	133.7290	-0.1444	0	0	0	0
7.6850	289.9500	-6.9219	0	0	0	0
25.8900	1390.2100	-0.9568	0	0	0	0
26.6900	19.2731	-3.9471	0	0	0	0
26.9500	1364.8300	2.3687	0	0	0	0

Figure 5 Input samples

As illustrated in the above figure twenty different samples involving thirty features from the dataset obtained in the input layer are subjected to secure routing process. With the above input samples obtained in the input layer are then fed to the first hidden layer where the actual secure routing process is initiated. Figure 6 shows the key set generated results.

▶ Key Set Generation

#	srcID	NInfo	Temp1	AK1	KeyN
1	118	59415.2460	59297.2460	8176	41040
2	75	7165.9968	7090.9968	976	4128
3	75	5434.1553	5359.1553	736	1536
4	112	7697.8837	7585.8837	1044	4244
5	118	7834.0251	7716.0251	1064	0
6	115	6961.5416	6846.5416	944	6144
7	256	14118.0529	13862.0529	1912	8528
8	256	14910.5660	14654.5660	2020	11288
9	284	15391.6025	15107.6025	2080	12320
10	52	9575.3777	9523.3777	1312	8192
11	86	4516.5434	4430.5434	608	4352
12	22	11696.1466	11674.1466	1608	11088

Figure 6 Key set generated results

From the above results the key set are generated for all the twenty samples present in the input layer. This key set generated results is then distributed to all the registered vehicular nodes in the VANET. Following which multi-objectives taking into consideration, the packets count, transmission rates, reception rates and hop counts are modeled for secure routing. Figure 7 shows the secure routing results generated based on multi-objective functions.

#	srcID	Stored Key	Recv Key	Key Match	NAS	NAS OK	Auth	Auth Delay(ms)	Result
1	118	41040	41040	✓ YES	0.2432	✓ YES	1	0.052400	✓ AUTHEN
2	75	4128	4128	✓ YES	0.9558	✓ YES	1	0.056000	✓ AUTHEN
3	75	1536	1536	✓ YES	0.8726	✓ YES	1	0.017900	✓ AUTHEN
4	112	4244	4256	✗ NO	0.9969	✓ YES	0	0.047900	✗ REJECTE
5	118	0	93	✗ NO	0.9359	✓ YES	0	0.145300	✗ REJECTE
6	115	6144	6159	✗ NO	0.8990	✓ YES	0	0.049500	✗ REJECTE
7	256	8528	8472	✗ NO	0.7486	✓ YES	0	0.045600	✗ REJECTE
8	256	11288	11301	✗ NO	0.9986	✓ YES	0	0.041400	✗ REJECTE
9	284	12320	12341	✗ NO	0.8902	✓ YES	0	0.036200	✗ REJECTE
10	52	8192	8275	✗ NO	0.7500	✓ YES	0	0.023700	✗ REJECTE
11	86	4352	4439	✗ NO	0.8019	✓ YES	0	0.022900	✗ REJECTE
12	22	11088	11035	✗ NO	0.8620	✓ YES	0	0.021800	✗ REJECTE

#	srcID	Stored Key	Recv Key	Key Match	NAS	NAS OK	Auth	Auth Delay(ms)	Result
1	118	41040	41040	✓ YES	0.2432	✓ YES	1	0.052400	✓ AUTHEN
2	75	4128	4128	✓ YES	0.9558	✓ YES	1	0.056000	✓ AUTHEN
3	75	1536	1536	✓ YES	0.8726	✓ YES	1	0.017900	✓ AUTHEN
4	112	4244	4256	✗ NO	0.9969	✓ YES	0	0.047900	✗ REJECTE
5	118	0	93	✗ NO	0.9359	✓ YES	0	0.145300	✗ REJECTE
6	115	6144	6159	✗ NO	0.8990	✓ YES	0	0.049500	✗ REJECTE
7	256	8528	8472	✗ NO	0.7486	✓ YES	0	0.045600	✗ REJECTE
8	256	11288	11301	✗ NO	0.9986	✓ YES	0	0.041400	✗ REJECTE
9	284	12320	12341	✗ NO	0.8902	✓ YES	0	0.036200	✗ REJECTE
10	52	8192	8275	✗ NO	0.7500	✓ YES	0	0.023700	✗ REJECTE
11	86	4352	4439	✗ NO	0.8019	✓ YES	0	0.022900	✗ REJECTE
12	22	11088	11035	✗ NO	0.8620	✓ YES	0	0.021800	✗ REJECTE

Figure 7 Multi-objective function based secure routing results

As provided in the above results with the satisfaction of the multi-objective function and the network traffic samples possessing high threshold are allotted with secure routing and vice versa. By following this pattern in turn reduces both authentication delay and latency involved during secure routing process. With the secure route generated results finally secure data transfer is ensured by applying Ryan-Joiner Correlation Coefficient via the second hidden layer. Figure 8 shows the data transfer results.

#	srcID	destID	srcVmaxDeviation	destVmaxDeviation	avgDstnc	Flow Duration	txStrtTime	destEnd_y	avgDestSpeed	avgSrcSpeed	Predicted Cla
1	118	0	0.0000	0.0000	589.0240	137.5030	456.2500	292.2400	0.0000	7.6650	NORMAL
2	75	118	0.0000	-1.0000	330.1950	629.4740	456.2530	367.7000	7.2950	0.0000	NORMAL
3	75	0	0.0000	0.0000	273.9970	734.7640	456.2530	292.2400	0.0000	0.0000	NORMAL
4	112	176	13.0941	0.0000	330.6780	499.2380	458.0350	105.6100	3.5500	9.1500	SPOOFING
5	118	223	2.3603	0.0000	275.6650	421.2400	458.0560	461.3600	0.0000	7.0100	SPOOFING
6	115	223	2.6256	0.0000	133.7810	734.7330	458.0560	292.4600	4.1750	8.6750	SPOOFING
7	256	147	0.0000	0.0000	289.9500	-253.2540	253.2540	1199.0800	7.6850	0.0000	SYBIL
8	256	0	0.0000	0.0000	133.7290	204.2180	253.2540	1428.7500	6.0550	3.9750	SYBIL
9	284	147	0.0000	0.0000	289.9500	2.0658	253.2540	1199.0800	7.6850	0.0000	SYBIL
10	52	69	0.0000	0.0000	1390.2100	4.6471	0.1758	1133.3994	25.8900	25.8500	WORMHOLE
11	86	36	0.0000	0.0000	19.2731	1.7603	0.2590	365.2474	26.6900	29.7100	WORMHOLE
12	22	71	0.0000	0.0000	1364.8300	4.1888	0.3651	337.8029	26.9500	24.8600	WORMHOLE

▶ **Secure Data Transfer Status**

#	srcID	destID	Predicted Class	Data Transfer Status	End-to-End Delay(m
1	118	0	NORMAL	→ DATA TRANSFERRED	0.075300
2	75	118	NORMAL	→ DATA TRANSFERRED	0.052900
3	75	0	NORMAL	→ DATA TRANSFERRED	0.047100
4	112	176	SPOOFING	✗ BLOCKED — SPOOFING	0.045200
5	118	223	SPOOFING	✗ BLOCKED — SPOOFING	0.044000
6	115	223	SPOOFING	✗ BLOCKED — SPOOFING	0.043600
7	256	147	SYBIL	✗ BLOCKED — SYBIL	0.053400
8	256	0	SYBIL	✗ BLOCKED — SYBIL	0.042900
9	284	147	SYBIL	✗ BLOCKED — SYBIL	0.042100
10	52	69	WORMHOLE	✗ BLOCKED — WORMHOLE	0.042300
11	86	36	WORMHOLE	✗ BLOCKED — WORMHOLE	0.042500
12	22	71	WORMHOLE	✗ BLOCKED — WORMHOLE	0.042600

Figure 8 Classification results

Finally as illustrated in above results based on correlation coefficient values, the traffic patterns are classified as normal or into three different attack types, spoofing, Sybil or wormhole. This in turn improves overall packet delivery ratio with enhanced attack detection rate.

5 Experimental setup and Discussion

In this section, performance measure of the proposed secure route based data transfer in VANET called, Deep Neural Lightweight Multi-objective and Ryan-Joiner Correlation (DNLM-RJC) is proposed. Detailed comparison is made with two existing methods Deep Neural Network – Convolutional Neural Network (DNN-CNN) [1] and Enhanced Location Aided Ant Colony Routing (ELAACR) [2] are analyzed and validated in Python high-level general-purpose programming language using Comprehensive Vehicular Communication Network Attack Dataset acquired from https://data.mendeley.com/datasets/x7tdmsf27x/1. The experiments were conducted on an Intel Core

i5- 6200U CPU @ 2.30GHz 4 cores with 4 Gigabytes of DDR4 RAM for the corresponding 45000 samples and 24 features. The software stack includes Python 3.11, along with PyTorch 2.0 for training and model development. To perform data manipulation and analysis Pandas 2.0.3 and NumPy 1.26.4 are used. Simulations are analyzed using five performance parameters, authentication delay, authentication latency, packet delivery ratio, end-to-end delay and attack detection rate. Fair comparison is made using similar samples from dataset for all the three methods, DNLM-RJC, DNN-CNN [1] and ELAACR [2] respectively for detecting different types of attacks.

5.1 Performance analysis of authentication delay

Authentication delay in VANETs denotes the time consumed for vehicles and infrastructure to verify identities or vehicular nodes before establishing secure routes and transmitting data.

$$AD = \sum_{i=1}^{N} \quad S_i * Time\ (SR + DT) \tag{15}$$

From the above equation (15) the authentication delay 'AD' performance metric is measured based on the time consumed in identifying optimal and secure routes 'SR' along with the time consumed in performing data transmission 'DT' with respect to the corresponding samples 'S_i'. It is measured in terms of seconds (sec). The obtained results of authentication delay for DNLM-RJC, DNN-CNN [1] and ELAACR [2] are presented in table 2.

Table 2 Statistical analysis on authentication delay

Samples	Authentication delay		
	DNLM-RJC	DNN-CNN [1]	ELAACR [2]
10000	250.03	280.03	320.04
20000	283.35	325.55	375.15
30000	315.45	374.15	395.35
40000	335.55	375.95	415.55
50000	365.15	415.25	435.55
60000	385	425.15	485.25
70000	415.25	445.55	505.15
80000	435	505.65	525.35
90000	455.25	515.15	550.15
100000	485	532.35	585.65

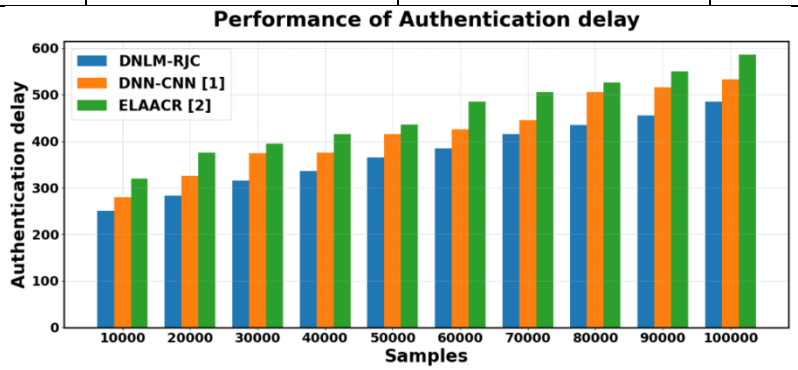

Figure 9 Analysis of authentication delay for proposed DNLM-RJC as well as existing DNN-CNN [1], ELAACR [2]

Figure 9 illustrates the graphical representation of authentication delay using the proposed DNLM-RJC and two existing methods, DNN-CNN [1] and ELAACR [2]. The horizontal axis in the above graph represents the samples ranging between 10000 and 100000 and vertical axis denotes the authentication delay. From the above figure an increase in sample size causes a subsequent increase in the authentication delay. However simulations performed for ten iterations showed minimal authentication delay using DNLM-RJC upon comparison to [1] and [2]. The reason was by replacing computationally heavy public-key mechanism with lightweight primitive minimizes message verification times. Moreover instead of performing cumbersome handshakes at every hop count, by using dynamic session tokens to fast track authentications in turn minimizes authentication delay using DNLM-RJC method by 13% compared to [1] and 24% compared to [2].

5.2 Performance analysis of authentication latency

Authentication latency in VANETs is the time consumed in verifying a vehicle's identity prior to the data delivery process. This is mathematically defined as given below.

$$AL = T_{req} - T_{res} \tag{16}$$

From the above equation (16) the authentication latency 'AL' performance metric is measured based on the time when the initial access request for certain packets hits the server 'T_{req}' and the time when the final access accept or reject 'T_{req}' is transmitted. The obtained results of authentication latency for DNLM-RJC, DNN-CNN [1] and ELAACR [2]are presented in table 3.

Table 3 Statistical analysis on authentication latency

Samples	Authentication latency (sec)		
	DNLM-RJC	DNN-CNN [1]	ELAACR [2]
10000	1.35	1.95	2.15
20000	1.65	2.05	2.25
30000	1.85	2.25	2.45
40000	2	2.45	2.65
50000	2.15	2.55	2.75
60000	2.35	2.85	3.05
70000	2.55	3.05	3.25
80000	2.85	3.35	3.55
90000	3.05	3.55	3.75
100000	3.15	3.85	4.05

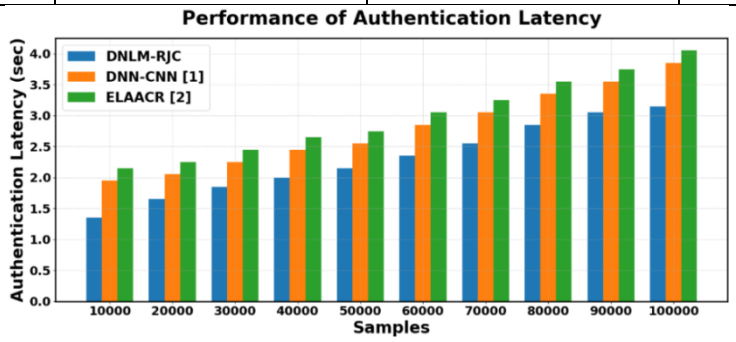

Figure 10 Analysis of authentication latency for proposed DNLM-RJC as well as existing DNN-CNN [1], ELAACR [2]

Figure 10 illustrates the graphical representation of authentication latency by applying the proposed DNLM-RJC and two existing methods, DNN-CNN [1] and ELAACR [2]. The blue chart in the above figure represents the authentication latency for proposed DNLM-RJC method whereas the orange and green char denotes the authentication latency for existing DNN-CNN [1] and ELAACR [2] methods. With the increase in the sample size, a corresponding increase is observed in the network traffic patterns. This in turn causes a proportionate increase in the authentication latency also using all the three methods. However comparison between the three methods saw a dip in proposed DNLM-RJC method in terms of authentication latency when compared to [1] and [2]. The reason was by incorporating optimized cryptographic methods with multi-objective routing, notably minimize computational and communication overheads on contrary to traditional methods. Also by heavily depending on effective mathematical operations on contrary to resource-heavy public key generation drastically cuts down signature verification delays. This in turn minimizes the authentication delay of proposed DNLM-RJC method by 23% compared to [1] and 32% compared to [2].

5.3 Performance analysis of packet delivery ratio

Packet Delivery Ratio (PDR) denotes the ratio of number of samples or packets successfully received to the number of samples or packets sent. The packet delivery ratio is mathematically defined as given below.

$$PDR = \frac{S_{recvd}}{S_{sent}} * 100 \quad (17)$$

From the above equation (17) the packet delivery ratio 'PDR' is denoted based on the samples received 'S_{recvd}' to the sample sent 'S_{sent}' for a simulation setup. It is measured in terms of percentage (%). The obtained results of packet delivery ratio are presented in table 4.

Table 4 Statistical analysis on packet delivery ratio

Samples	Packet delivery ratio		
	DNLM-RJC	DNN-CNN [1]	ELAACR [2]
10000	98.35	95.25	93.35
20000	96.25	83.45	78.55
30000	95	82.35	77.35
40000	93.15	80.05	75.25
50000	90	77.85	72.15
60000	88.45	75.55	70.35
70000	91.35	78.65	73.45
80000	94	81.35	76.15
90000	96.25	83.55	78.55
100000	98	85.25	80.25

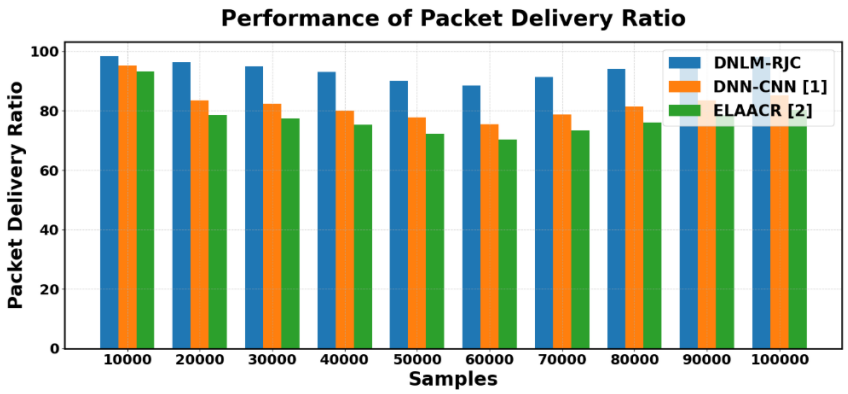

Figure 11 Analysis of packet delivery ratio for DNLM-RJC, DNN-CNN [1] and ELAACR [2]

Figure 11 given above shows the graphical plot made for packet delivery ratio using DNLM-RJC, DNN-CNN [1] and ELAACR [2]. The packet delivery ratio is a predominant quality of service performance metric using in measuring network reliability. As far as VANET is concerned, the packet delivery ratio straightforwardly controls the data delivery security, acting as a pivotal performance factor that reveals routing overhead and vulnerability to security attacks. While performing the task of attack detection, security alone cannot ensure that all data packets will reach their destination. To sustain high packet delivery ratio, the detection method is incorporating with a secure and optimal routing mechanism. This integration avoids malicious or compromised network traffic patterns, by routing data packets over the optimal and the most secure paths available, thereby minimizing packet loss and increasing packet delivery ratio of DNLM-RJC by 13% compared to [1] and 18% compared to [2].

5.4 Performance analysis of end-to-end delay

In VANETs, end-to-end (E2E) delay represents the total time a packet or network traffic sample takes to traverse the network from the source vehicle to the destination. The end-to-end delay is mathematically defined as given below.

$$E2ED = \sum_{i=1}^{N} \quad S_i * \left[D_{Trans} + D_{Prop} + D_{Proc} + D_{Queue}\right] \tag{18}$$

From the above equation (18) the end-to-end delay result '$E2ED$' is arrived at based on the transmission delay 'D_{Trans}', propagation delay 'D_{Prop}', processing delay 'D_{Proc}' and queue delay 'D_{Queue}' with respect to the samples 'S_i'. The obtained results of end-to-end delay are presented in table 5.

Table 5 Statistical analysis on end-to-end delay

Samples	End to end delay		
	DNLM-RJC	DNN-CNN [1]	ELAACR [2]
10000	750	940	1030
20000	775	985	1025
30000	805	1015	1055
40000	925	1035	1085
50000	840	1055	1095
60000	855	1085	1110
70000	885	1105	1128
80000	905	1135	1145

90000	925	1155	1185
100000	945	1185	1205

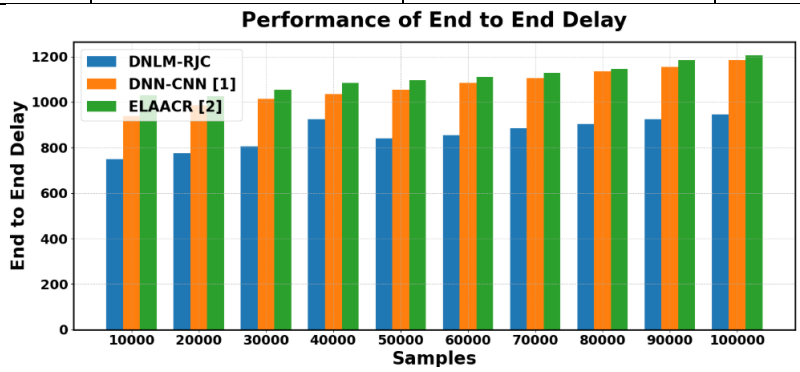

Figure 12 Analysis of end to end delay for DNLM-RJC, DNN-CNN [1] and ELAACR [2]

Figure 12 illustrates the graphical representation of end to end delay using the three methods, DNLM-RJC, DNN-CNN [1] and ELAACR [2]. From the above figure samples ranging between 10000 and 100000 were provided in the x-axis and the recordings of end to end delay were made in the y-axis. The end to end delay performance metric was found to be directly proportional to the sample size. To be more specific, increasing the samples saw a proportionate increase in the end to end delay. But comparative analysis show minimal end to end delay using DNLM-RJC method than [1] and [2]. The reason was the lightweight concept makes certain that the fitness function employed necessitate fewer CPU cycles to execute. This wards-off vehicular node processing obstructions prior data transmission happens. Also by treating packets count, transmission rates, reception rates and hop counts, the routing mechanism surpasses high-hop paths. It segregates malicious traffic patterns to prevent dropped data packets, hence reducing latency and discarding the requirement for time-consuming data retransmissions. This in turn aided in minimizing the end to end delay of proposed DNLM-RJC method by 24% compared to [1] and 29% compared to [2] respectively.

5.5 Performance analysis of attack detection rate

The attack detection rate measures how efficiently the proposed method identifies attack labels. It is the ratio of successfully identified attack labels to the total number of attack labels present. The attack detection rate is mathematically denoted as given below.

$$ADR = \frac{TP}{TP+FN} \tag{19}$$

From the above equation (19) the attack detection rate 'ADR' is evaluated based on the true positive rate 'TP' and false negative rate 'FN' respectively. The obtained results of attack detection rate are presented in table 6.

Table 6 Statistical analysis on attack detection rate

Samples	Attack detection rate		
	DNLM-RJC	DNN-CNN [1]	ELAACR [2]
10000	0.97	0.97	0.96
20000	0.94	0.82	0.77
30000	0.92	0.8	0.75
40000	0.9	0.78	0.73
50000	0.88	0.76	0.71

60000	0.85	0.73	0.68
70000	0.87	0.75	0.7
80000	0.89	0.77	0.72
90000	0.92	0.8	0.75
100000	0.94	0.82	0.77

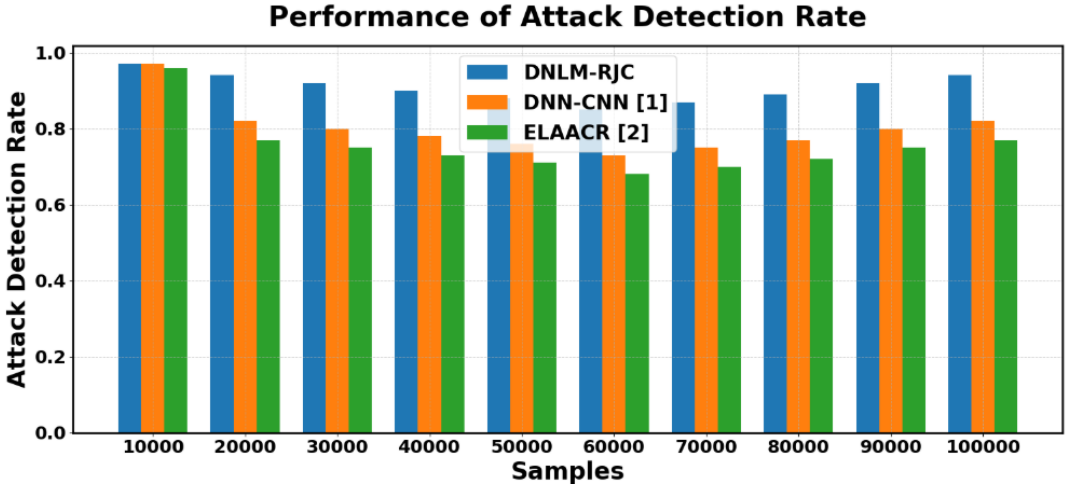

Figure 13 Analysis of attack detection rate for DNLM-RJC, DNN-CNN [1] and ELAACR [2]

Figure 13 illustrates the graphical representation of attack detection rates using DNLM-RJC, DNN-CNN [1] and ELAACR [2]. From the above figure though the attack detection rate using all the three methods were found to be decreasing for the first six set of iterations whereas for the rest of four iterations they were observed to be increasing. So increase in or decrease in sample size does not affect attack detection rate, therefore improving the overall performance of optimal and secure routing. The reason was by applying the Ryan-Joiner Correlation Coefficient statistical test data traffic is evaluated by verifying its conformity to multivariate normality assumption. By evaluating this coefficient across various time instances, the attack specific labels establish a baseline of normal behavior. This in turn accurately identifies attack specific labels (such as spoofing, wormhole, sybil attacks or legitimate samples) when the coefficient drops below standard critical values. With this the overall attack detection rate is improved significantly using DNLM-RJC method by 12% compared to [1] and 17% compared to [2].

6. Conclusion

Vehicular ad hoc network with high speed mobility and rapidly changing topology makes it demanding to ensure secure communication because malicious drivers in the network disrupt the system performance. A plethora of secure routing algorithms have been deployed to prevent the system from various attacks. In this work, a secure route based data transfer method called, Deep Neural Lightweight Multi-objective and Ryan-Joiner Correlation (DNLM-RJC) for VANET is proposed. To begin, with the network traffic patterns were obtained as input in the input layer. Followed by which in the first hidden layer, Lightweight Multi-objective Secure Route-based Authentication model was designed to ensure minimal authentication latency and delay. Next, in the second hidden layer, Ryan-Joiner Correlation Coefficient Secure Route-based Data Transfer was applied therefore not only increasing the attack detection rate but also the packet delivery ratio involved. Results showed that the DNLM-RJC method outperformed the counterpart. Moreover, the introduced DNLM-RJC method minimizes the end to end delay, authentication latency with improved packet delivery ratio and attack detection rate compared to the counterpart.

REFERENCES

1. Sonika Bhardwaj, Ramesh Saha, “A secure and scalable traffic management framework using hybrid DNN-CNN and geographic routing in V2X networks”, Peer-to-Peer Networking and Applications, Springer Nature Link, Vol. 19, Feb 2026 [Deep Neural Network – Convolutional Neural Network (DNN-CNN)]
2. [2] Raghu Ramamoorthy, “An Enhanced LocationAided Ant Colony Routing for Secure Communication in Vehicular Ad Hoc Networks”, Human-Centric Intelligent Systems, Springer Nature Link, Vol. 4, Jan 2024[Enhanced Location Aided Ant Colony Routing (ELAACR)]
3. Fida Muhammad Khan, Taj Rahman, Asim Zeb, Zeeshan Ali Haider, Inam Ullah Khan, Hazrat Bilal, Muhammad Abbas Khan, Inam Ullah, “Vehicular Network Security Through Optimized Deep Learning Model with Feature Selection Techniques”, ICCK Transactions on Sensing, Communication, and Control, Vol. 1, Dec 2024
4. Rui Chen, Xiaoyu Chen, Jing Zhao, “Sparsified federated learning with differential privacy for intrusion detection in VANETs based on Fisher Information Matrix”, PLOS ONE, Apr 2024
5. Pratima Upadhyay, Venkatadri Marriboina, Samta Jain Goyal, Sunil Kumar, El-Sayed M. El-Kenawy, Abdelhameed Ibrahim, Amel Ali Alhussan, Doaa Sami Khafaga, “An improved deep reinforcement learning routing technique for collision-free VANET”, Scientific Reports, Oct 2023
6. Naramalli Jayakrishna, N. Narayanan Prasanth, “A hybrid deep learning model for detection and mitigation of DDoS attacks in VANETs”, Scientific Reports, Oct 2025
7. Mahmoodul Hassan, Amin A. Al-Awady, Abid Al, Sifatullah, Muhammad Akram, Muhammad MunwarIqbal, Jahangir Khan, Yahya Ali Abdelrahman Ali, “ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV”, Sensors, MDPI, Nov 2024
8. Xiaoxuan Chen, Yineng Chen, Xiayu Wang, Xinghui Zhu, Kui Fang, “DSVN:AFlexible and Secure Data-Sharing Model for VANET Based on Blockchain”, Applied Sciences, MDPI, Dec 2023
9. Amalia Amalia, Yushintia Pramitarini, Beongku An, Ridho Hendra, Yoga Perdana, Kyusung Shim, “A Deep-Learning-Based Secure Routing Protocol to Avoid Blackhole Attacks in VANETs”, Sensors, MDPI, Nov 2023
10. Elham Mohammadzadeh Mianji, Gabriel-Miro Muntean, Irina Tal, “Enhancing Vehicular Network Security, Privacy, and Trust Through Reinforcement Learning: A Comprehensive Survey”, IEEE Transactions on Intelligent Transportation System, Vol. 26, Dec 2025
11. Rui Shi, Jianguo Xie, Xiaolin Li, Mengxin Li, Liwei Xu, Huamin Feng, “Lightweight identity authentication and key agreement scheme for VANETs based on SSL PUF”, Scientific Reports, Dec 2025
12. Deepak choudhary, Roop Pahuja, “Awareness routing algorithm in vehicular ad-hoc networks (VANETs)”, Journal of Big Data, Springer Nature Link, Vol. 10, Jul 2023
13. Jarallah Alqahtani, Mahmoodul Hassan, Abid Ali, Muhammad Akram, “A Machine Learning Approach for Secure Communication Using Blockchain for IoT-Based VANETs”, The Institution of Engineering and Technology, Wiley, Nov 2025
14. Shaji K. A. Theodore, K. Rajiv Gandhi, V. Palanisamy, “A novel lightweight authentication and privacy-preserving protocol for vehicular ad hoc networks”, Complex &Intelligent Systems, Springer Nature Link, Vol. 9, Oct 2021
15. Himanshu Setia, Amit Chhabra, Sunil K. Singh, Sudhakar Kumar, Sarita Sharma, Varsha Arya, Brij B. Gupta, Jinsong Wu, “Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments”, Cyber Security and Applications, Elsevier, Vol. 2, Nov 2024
16. Sheraz Mazhar, Abdur Rakib, Lei Pan, Frank Jiang, Adnan Anwar, Robin Doss, Jeremy Bryans, “State-of-the-art authentication and verification schemes in VANETs: Asurvey”, Vehicular Communications, Elsevier, Vol. 49, Oct 2024
17. Taha M. Mohamed, Islam Z. Ahmed, Rowayda A. Sadek, “Efficient VANET safety message delivery and authenticity with privacy preservation”, Peer Journal of Computer Science, May 2021
18. Wisal Jereis Alrabadi, “Neural Network-Based Intelligent Routing for Secure VANET Communication”, International International Conference Conference on Appliedon Applied Innovations in IT, Jul 2025
19. Sagheer Ahmed Jan, Noor Ul Amin, Junaid Shuja, Mazhar Ali, Assad Abbas, Mohammed Maray, “SELWAK: A Secure and Efficient Lightweight and Anonymous Authentication and Key Establishment Scheme for IoT Based Vehicular Ad hoc Networks”, Sensors, MDPI, Sep 2022
20. Naramalli Jayakrishna, Narayanan Prasanth, “Detection of DDOS attacks in Vehicular Ad Hoc Networks using Ensemble Deep Learning Model and Optimization Technique”, Results in Engineering, Elsevier, Vol. 27, Sep 2025
21. R. Gopi, V. Thiruppathy Kesavan, Md. Jakir Hossen, Nor Hidayati Binti Abdul Aziz, “Bi directional sparse attention recurrent autoencoder based intrusion detection for VANET security with tuna swarm optimization”, Scientific Reports, Dec 2025
22. N Agaraju Pacharla, K. Srinivasa Reddy, “Vehicle Authentication-Based Resilient Routing Algorithm With Dynamic Task Allocation for VANETs”, IEEE Access, Vol. 12, Dec 2024
23. Madhuri Husan Badole, Anuradha D. Thakare, “An optimized framework for VANET routing: A multi-objective hybrid model for data synchronization with digital twin”, International Journal of Intelligent Networks, Elsevier, Vol. 4, Dec 2023
24. Vamshi Krishna K, Ganesh Reddy K, “VANET Vulnerabilities Classification and Countermeasures: A Review”, Majlesi Journal of Electrical Engineering, Vol. 16, Sep 2022
25. Tarak Nandy, Rafidah Md Noor Sananda Bhattacharyya, Raenu Kolandaisamy, Mohd Yamani Idna Idris, “A review of security attacks and intrusion detection in the vehicular networks”, Journal of King Saud University - Computer and Information Sciences, Elsevier, Vol. 36, Feb 2024

26. Huimin Li, Chucheng Shen, Hui Huang, Chenhuang Wu, “A certificateless aggregate signature scheme for VANETswith privacy protection properties”, Plos One, Feb 2025
27. Bekan Kitaw Mekonen, Lemi Bane, Negasa Berhanu Fite, “Detection of false position attacks in VANETs through bagging ensemble learning”, PLOS ONE, Aug 2025
28. Taha M. Mohamed, Islam Z. Ahmed, Rowayda A. Sadek, “Efficient VANET safety message delivery and authenticity with privacy preservation”, Peer Journal of Computer Science, May 2021
29. M Gayathri, C. Gomathy, “AI-TASFIS: An Approach to Secure Vehicle-to Vehicle Communication”, Taylor & Francis, Applied Artificial Intelligence, Vol. 36, Oct 2022
30. https://data.mendeley.com/datasets/x7tdmsf27x/1