International Journal of Basic and Applied Sciences, 14 (5) (2025) 114-130

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/m4s0q161
Research paper

An Efficient Cybersecurity Spoofing Attacks Detection Framework in Vehicular Networks Using Hybridized Dilated and Attention-Based Network

Vishal Ramdas Deshmukh [1] *, Dr. Indrabhan S. Borse [2]

[1] Ph. D Scholar, Department of Computer Science and Engineering, P.K. University, Shivpuri, Madhya Pradesh, India
[2] Associate Professor, Department of Computer Science and Engineering, P.K. University, Shivpuri, Madhya Pradesh, India
**Corresponding author E-mail: deshmukh.vishal07@gmail.com*

Received: July 14, 2025, Accepted: August 24, 2025, Published: September 4, 2025

Abstract

Due to the growing cybersecurity threats, the privacy and security of modern vehicles have become increasingly significant. Cyber offenses in vehicular networks are recognized using an Intrusion Detection System (IDS). The rapid growth of multimedia technologies has made cybersecurity an essential concern.. Automated and internet-connected cars are exposed to spoofing and jammer attacks. GPS location spoofing is an imminent danger to Connected and Autonomous Vehicles (CAV), threatening security and even exposing motorists and pedestrians to risk. Because of flawed protocol design and increased interconnectivity among modern autonomous vehicles, the Controller Area Network (CAN) bus is insecure. The identification of spoofing attacks on the CAN bus is critical. Hence, it is necessary to develop an efficient spoofing attack detection method to address the limitations of existing models. The major phases of the developed framework are (a) Data Collection, (b) Data Pre-processing, (c) Weighted Feature Selection, and (d) Attack Detection. At first, essential data utilized for the validation is collected in the standard dataset. Further, the gathered time series data is given as input to the data pre-processing phase. Later, the attained pre-processed data is utilized to collect the essential features. Further, in the weighted feature selection phase, the Restricted Boltz-mann Machine (RBM) technique is utilized to attain the significant features. Unlike the conventional CMPA, the proposed FE-CMPA introduces a fitness-entrenchment mechanism that improves the optimization of RBM feature weights and enhances relief score maximization. Subsequently, the acquired weighted RBM features are provided for the attack detection phase. Fur-Furthermore, the spoofing attacks are detected using the developed Hybrid Dilated and Attention-based Network (HD-ANet), which holds the Deep Temporal Convolution Network (DTCN) and Residual Long Short Term Memory (RLSTM) network for effective validation. Hence, the implemented spoofing attack detection model is more secure and achieves a comparatively higher detection rate than traditional approaches in various experimental evaluations.

Keywords: *Cybersecurity Spoofing Attack Detection; Vehicular Network; Fitness Entrenched Coronavirus Mask Protection Algorithm; Restricted Boltz-mann Machine; Hybrid Dilated and Attention-Based Network; Deep Temporal Convolution Network; Residual Long Short Term Memory network.*

1. Introduction

The automotive sector is shifting towards greater computerization and connectivity, which increases the occurrence of attacks and raises the risk of cybersecurity intrusions. [35]. At present, modern cars are equipped with various electronic components, such as actuators, sensors, Electronic Control Units (ECUs), and communication modules that connect through different in-vehicle networks. [22]. The CAN bus is one of the most widely used technologies in the automobile industry [27]. The safety of the CAN bus has been thoroughly examined, and it is widely used in the automotive field [10]. The message-based CAN bus protocol is employed to meet the unique demands of the in-vehicle environment, including rapid processing, great durability, and affordability [8]. Broadcasting communication is deployed by CAN bus technology to send information across ECUs that are attached to the in-vehicle network. IDS has become a widely used cybersecurity technique. It identifies uncontrolled intrusions and infrastructure-based threats [18]. In the automobile sector, the computational competence of the business vehicle is limited, which may be used to set up the IDS [24]. Exporting the IDS to cloud-based systems with strong computational capabilities is defined as the most important concern in recent days [30]. However, this approach needs a lot of association to transfer the information of traffic logs from the in-vehicle system [37].

In modern automobiles, the multi-master serial CAN protocol is frequently employed for exchanging the safety data between ECUs [33]. Smart transportation research has demonstrated the need for CAN bus security. In transportation research, the security of the CAN bus is considered the most important matter. Human safety is greatly endangered by vehicle attacks in comparison with other cybersecurity attacks [39]. Although great efforts have been made to ensure the performance, reliability, and safety of computerized vehicles,

Copyright © Vishal Ramdas Deshmukh, Dr. Indrabhan S. Borse. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

comparatively less effort has been devoted to safeguarding them from malicious attacks. [28]. The attackers insert spoofing messages for violating the CAN bus to harm a car or gain total control of the ECUs, However, most existing approaches either suffer from high computational demands (e.g., RNN-LSTM) or scalability limitations (e.g., CARAMEL), making them less practical for real-time vehicular environments and the CAN bus is an essential part of in-vehicle services and embedded with ssecurity vulnerabilities [13]. The Information and Communications Technology (ICT) industry is utilized to address cybersecurity problems in CAV. It is used for evaluating the risks and effects of possible future cyber-attacks. In contrast, previous automotive cybersecurity projects strengthened the privacy of interconnected vehicles. The security risk is initiated by the currently developed techniques like intelligent charging for Electric Vehicles (EV), and autopilot, where 5G is not handled in an effective way [29].

Additionally, the CAN network's load is augmented with the implementation of authentication and encryption; this load needs to be kept under 50% of its maximum capacity to transfer important information [5]. Thus, a successful assessment cannot alter the operating system of the ECU and should work with the current CAN network protocol [4]. Experts have proposed ideas regarding the physical layer as well as the data connection layer of conventional CAN protocols. Nonetheless, most of these techniques are unable to precisely evaluate the fraudulent message [2]. The use of Deep Neural Networks (DNN), including Recurrent Neural Network (RNN) and Convolutional Neural Network (CNN), has seen incredible success in the field of hardware security. In contrast to the widely used CNN, the basic RNN's repetitive design provides strength for training the time series data [43], [44]. When training an RNN, vanishing gradient problems are frequently encountered, particularly if the data includes a large step size. RNN can overcome these training challenges and achieve outstanding efficiency along with excellent detection accuracy because of the long-term storage units [44], [46]. Additionally, deep learning has been recently applied to IDS for in-vehicle networks, achieving more accurate outcomes than inadequate machine learning. However, deep learning necessitates an extensive amount of processing power, which is not found in a vehicle installed in a cloud system. During a spoofing attack in the network, saved data of sensitive information like personal details and financial details is stolen by the attacker. Data loss is an incident where hackers delete and corrupt data in software applications. Poor security and improper storage cause data loss issues, which can lead to unreadable, reputational, and network damage. Recognizing and identifying spoofing attacks is critical, as attackers can mask their identity and cause delays in data transmission. This research work designs an effective deep model for identifying the spoofing attack in vehicular networks.

The most beneficial contributions of the deep model-based cyber security spoofing attack recognition structure are listed below.

- To build a deep learning model for spoofing attack detection in vehicular networks to identify false data generated by attackers. This ensures better management of the transportation system with reduced traffic congestion and enables early attack minimization..
- To propose a feature extraction process using the RBM method for removing unnecessary or redundant data. By multiplying optimized weights with selected features, a weighted fused feature is obtained, which increases the relief score value and maximizes spoofing detection accuracy
- To design the FE-CMPA algorithm, inspired by CMPA, for optimal feature selection. The developed FE-CMPA can effectively handle complex and high-dimensional problems, significantly enhancing the precision and accuracy of cybersecurity attack detection and mitigation.
- To design an HD-ANet classifier for identifying spoofing attacks. The HD-ANet integrates DTCN and Residual LSTM with dilation and attention mechanisms to reduce parameter usage and improve detection accuracy. It also helps filter unnecessary data in vehicular networks, reducing congestion and enhancing detection performance.

The structure of the paper is as follows: Section II reviews conventional spoofing attack detection methods along with their advantages and limitations. Section III presents the system model of vehicular networks, the motivation behind the work, and the architecture of the proposed spoofing attack detection model. Section IV describes the preprocessing of the collected time series dataset and optimal weighted feature selection using the developed heuristic strategy. Section V explains the intelligent spoofing attack detection framework based on dilation and attention-based hybrid deep learning networks. Section VI discusses the experimental results, and Section VII concludes the paper with key findings.

2. Literature survey

2.1. Related works

Baldini (2022) proposed an innovative IDS method using Recurrence Quantification Analysis (RQA) and an adaptive window based on the CAN bus communication arrival time data [1]. This method has been evaluated via machine learning techniques utilizing two publicly available datasets. In general, a spoofing assault was hard to recognize. This approach was compared with entropy metrics for attack detection. The outcomes demonstrated that the RQA-based approach outperformed current frameworks in terms of accuracy in detection and consistency over an assortment of sliding windows in both datasets when compared with entropy measurements. The influence of the sliding window size and hyperparameters used in the RQA and machine learning algorithms was thoroughly evaluated [1].

Vitale et al. (2021) created the CARAMEL model for enhancing communication privacy and security for interconnected and self-driving vehicles [38]. This architecture consisted of the following components: (a) A communication infrastructure that allowed simultaneous 802.11p and LTE-U connectivity for multi-radio access; (b) the MEC structure containing detection and mitigation algorithms; (c) the automated on-board section that included anti-hacking characteristics within the vehicle; and (d) an external key infrastructure that checked the authenticity of data transmissions in the vehicle. The CARAMEL model's entity-to-entity connections have been demonstrated using a GPS spoofing attack model. Suggested attack detection procedures utilized the advantages of reliable in-vehicle and collaborative approaches that depend on observations provided by the CARAMEL architecture rather than encrypted GPS signals [38].

Dasgupta et al. (2022a) established a GNSS-based sensor fusion framework for spoofing attack identification in Autonomous Vehicles (AVs) [6]. [7]. This framework encompassed two approaches, including (i) contrasting predicted location shifts, also (ii) identifying and categorizing shifts in combination with vehicle motion state recognition. The initial approach involved merging and feeding data to the LSTM neural network using low-cost in-vehicle inertial sensors. The subsequent method used the angle of steering sensor data to identify left and right shifts using a combination of Dynamic Time Warping (DTW) algorithms and K-Nearest Neighbors (k-NN). To increase the framework's efficacy, the speed determined by the GNSS was compared to the speedometer output of both techniques. The sensor fusion-based detection system could identify every type of spoofing attack under the threshold. However, this approach requires large memory resources and can suffer from overfitting, limiting its scalability in real vehicular systems [6].

Yang et al. (2020) presented a sender identity verification approach based on biometric signal features using RNN-LSTM. Due to its high computational complexity, the suggested RNN-LSTM model has been simplified to support a detection performance in real-time [40]. The

potential of the suggested RNN-LSTM model for in-vehicle CAN bus security has been showcased through experimental findings in most of the recent research. Although effective, the high computational complexity of RNN-LSTM makes it unsuitable for real-time vehicular environments, motivating the hybrid approach in our work[4].

Dasgupta et al. (2022b) have utilized inexpensive in-vehicle sensor data for establishing a deep Reinforcement Learning (RL)-based turn-by-turn spoofing attack detection technique [41]. The effectiveness of the deep RL-based attack identification system was assessed. In general, the deep RL model has acquired high precision and recall. Turn-by-turn spoof identification of attacks was effectively carried out by the reinforcement learning model [7].

In 2020, Sanders and Wang (Sanders and Wang 2020) proposed vehicle-to-vehicle communications to identify and pinpoint GPS spoofing incidents on vehicles. Linking Doppler shift data with commercial GPS devices was the primary focus of this work. It could be established with mobile spoofers that might be installed in a vehicle. To confirm the efficacy of the suggested method, experimental and numerical simulations were carried out [32].

Shabbir et al. (2023) proposed an innovative strategy for safeguarding Connected and Autonomous Vehicles (CAVs) against GPS position spoofing attacks by utilizing machine learning models like Support Vector Machines (SVM) and deep models like CNN. The recommended approach was verified by the CARLA simulator and several learning algorithms. GPS coordinates, spoof supervises, and localization system values have been included in training and testing datasets. Higher precision was achieved in both the best and worst-case scenarios via the recommended machine learning approach. Deep learning produced better results in both the ideal and worst-case scenarios [34].

Li et al. (2020) have created an area-oriented confidentiality model to offer a first authentication by eliminating the need for multiple reference vectors. The standard deviation of the real user, or spoofer, would be properly noticed at any place within a particular area and statistically analyzed. The results have shown that the developed system delivered helpful information for network administrators, so they can implement the best preventative steps. Lastly, simulations were used to validate analytical results and demonstrate the characteristics of the system [21].

Theyazn et al. (2022) have developed a hybrid Convolution Neural Network Long Short-Term Memory (CNN-LSTM) method with the help of a real automatic vehicle network dataset for determining the attack messages in earlier stages. The developed method could produce better results by evaluating several measures like, F1 score, recall, precision, and accuracy. Thus, it has reached a higher 97.30% accuracy compared to other conventional approaches [36].

Jannu and Vanambathina (2023a) have investigated several deep-learning techniques for speech improvement. For further processing, diverse frameworks were utilized to maximize the system performance. Also, various methods such as Gammatone Frequency Cepstral Coefficients (GFCCs), Logarithmic Power Spectrum (LPS), and Mel-Frequency Cepstral Coefficients (MFCCs)have attained essential features [15].

Jannu and Vanambathina (2023b) have developed a time-domain hybrid system for utilizing U-Net with attention-based skip links to enhance the temporal context aggregation. The detailed information was generated by context aggregation and dense connections through diverse layers at different dilation rates. Extensive experimental outcomes have demonstrated that the developed approach has outperformed traditional methods [15].

Dora and Naga Lakshmi (2024) have developed an ensemble learning model for detecting and mitigating DDoS attacks using a hybrid optimization algorithm to enhance the detection performance. The pre-processed data was given to the process of feature extraction by autoencoder approaches for acquiring deep features. The attack detection was employed through the Improved Ensemble learning (IEL) framework. Finally, the experiments were used to establish the best detection efficacy of the developed attack mitigation and detection method [9].

Kumari and Babu (2024) have developed the hybrid Quantum Dilated Convolutional Neural Network fused Deep-Stacked Auto Encoder (QDCNN-F-DSAE) model with a Genetic Fuzzy System (GFS) method for network protection. The developed method can easily classify and analyze attacks with the help of GFS and firewall tuning, and alert the users. The developed model was examined in terms of accuracy, sensitivity, and specificity measures to provide better outcomes, such as 0.915, 0.908, and 0.920 [20].

2.2. Problem statement

Presently, enormous developments are being achieved in multimedia technology and systems. But these advanced technologies face different security issues due to jamming and spoofing. Here, the spoofing attacks generate more complications in the vehicular network and create more trouble for the user. Several advancements and issues given in the existing cybersecurity spoofing attack detection models are tabulated in Table 1. RQA [1] offers an effectively higher accuracy rate than the entropy metrics with various sliding window sizes. However, it reduces the pattern detection rate in the presence of noisy data. CARAMEL [38] attains a superior end-to-end verification rate while transmitting the data between the CAV entities. However, it suffers from network traffic overhead and scalability limitations. LSTM [6] achieves a higher performance rate in overshoot, stop, and wrong turn conditions, and it has a good computational latency threshold rate. However, it requires high memory to save the details, and it easily falls into overfitting issues. RNN-LSTM (Yang et al. 2020) easily identifies the malicious spoofing in the EUC nodes, and it handles the enormous data and attains accurate outcomes. Moreover, its implementation procedure is complicated, and the training procedure takes more time. Deep reinforcement learning [7] implementation cost is low, and it effectively resolves complex tasks. Yet, it attains poor outcomes in some cases due to overload issues. Static spoofer case [32] effectively minimizes the localization errors and has a higher robustness rate. But it utilized a limited number of antennas in the moving space. CNN and SVM [34] work efficiently in the higher-dimensional spaces, and also resolve the non-linearity issues. Still, it requires resolving the overlapping issues, and training time is higher due to more complications. The two-dimensional space model [21] effectively minimizes the false detection rate, and the security rate of the system is increased. Yet, it needs to reduce the silent probability rate between the destination and the spoofer. Thus, it is essential to tackle different complications attained in the conventional cybersecurity spoofing attack detection model by designing an effective spoofing attack identification mechanism with deep learning approaches [47, [48]. To address these challenges—such as computational overhead in RNN-LSTM, scalability in CARAMEL, and noisy data limitations in RQA—our work introduces a hybrid HD-ANet model combined with FE-CMPA for optimized feature selection, designed specifically for real-time vehicular networks.

Table 1: Advantages and Disadvantages of Existing Cybersecurity Spoofing Attack Detection Systems in Vehicular Networks

Author [citation]	Methodology	Advantages	Disadvantages
(Baldini 2022)	RQA	• It offers an effectively higher accuracy rate than the entropy metrics with various sliding window sizes.	• It minimizes the pattern detection rate due to noisy data.
(Vitale et al. 2021)	CARAMEL	• It attains a superior end-to-end verification rate while transmitting the information between the CAV entities.	• It requires resolving the overhead issue in the network traffic load distribution. • It needs to overcome the scalability issues.
(Dasgupta et al. 2022a)	LSTM	• It achieves a higher performance rate in overshoot, stop, and wrong turn conditions. • It has a good computational latency threshold rate.	• It requires a large memory to save the details. • It easily falls into overfitting issues.
(Yang et al. 2020)	RNN-LSTM	• It easily identifies the malicious spoofing in the EUC nodes. • It handles enormous data and attains accurate outcomes.	• Its implementation procedure is complicated. • The training procedure takes more time.
(Dasgupta et al. 2022b)	Deep reinforcement learning	• Its implementation cost is low. • It effectively resolves the complex tasks.	• It attains poor outcomes in some cases due to overloading issues.
(Sanders and Wang 2020)	Static spoofer case	• It effectively minimizes localization errors. • It has a higher robustness rate.	• It utilized a limited number of antennae in the moving space.
(Shabbir et al. 2023)	CNN and SVM	• It works proficiently in higher-dimensionality spaces. • It resolves the non-linearity issues.	• It requires resolving the overlapping issues. • Its training time is higher due to more complications.
(Li et al. 2020)	Two-dimensional space model	• It successfully reduces the false detection rate. • The security rate of the system is increased.	• It needs to reduce the silent probability rate between the destination and the spoofer.

3. A Novel Cybersecurity Spoofing Attack Detection Scheme with The Support of An Advanced Deep Learning Network

3.1. System model of vehicular networks

In the vehicular network, each vehicle is considered an important entity and functions as a node. The server, vehicles, and Roadside Units (RSU) are the three most significant requirements of the vehicular network. In the vehicular network, the vehicles are considered the most important components. The onboard unit is attached to the individual vehicle in the vehicular network. Here, the wireless communication is employed to transfer and receive the messages. Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications are the most common methods used in vehicular networks. On the roadside of the vehicular network, the RSU is placed to perform communication between the sensors and vehicles. The server in the network grasps the environmental data that is gathered by the vehicles. The sensed reports are transferred by the RSU and the remaining vehicles of the network. The system model of the vehicular network is presented in Fig. 1.

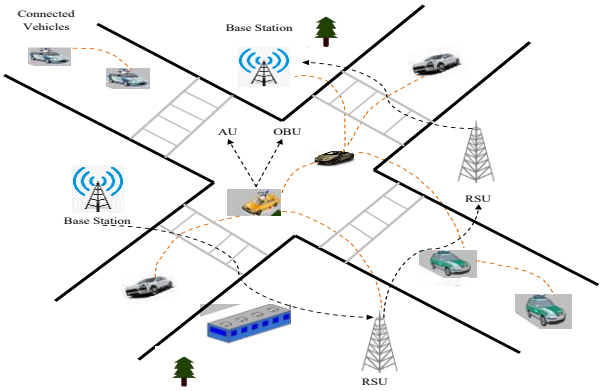


Fig. 1: System Model of the Vehicular Network.

3.2. The motivation behind the work

In recent days, the occurrence of cybersecurity attacks in modern vehicles has greatly increased. The likelihood of cyber-attacks in vehicular networks has increased due to the growing complexity of modern vehicles. In the vehicular network, the moving vehicles are considered as nodes that are used to form the autonomous network. The efficiency of data transportation is highly increased by the networks. The direction and location mapping information is provided with the aid of the vehicular networks. The vehicular network is affected by the spoofing attack and is quite difficult to identify. The safety of human life is greatly affected by the cybersecurity threats on the vehicular network. The spoofer injects the spoofing messages into the control unit of the vehicle so that the vehicle can be fully controlled by the spoofer. Due to the spoofing messages, the communication between the RSU and the sensor of the vehicle is damaged so which leads to a collision risk during transportation. The spoofing attack may affect the GPS of the vehicle, and it confuses the driver by providing a false signal. This false signal can guide the driver into false path. Due to this action, the congestion in the road network increases and it can result in a collision between the two vehicles. For this reason, the researcher developed numerous spoofing attack detection techniques for detecting the spoofing attack in the vehicular network. However, they did not identify the falsified data in the signal received at the sensor

of the network. In addition, the existing approach does not recognize the messages from the attacker and the genuine vehicle. So it is necessary to develop the spoofing attack detection model in vehicular communication using deep learning techniques. Moreover, practical deployment of spoofing detection systems must consider constraints such as limited computational resources in vehicle ECUs and compatibility with existing CAN bus protocols, which motivated the design of our lightweight HD-ANet framework.

3.3. Architectural explanation of developed spoofing attack detection model

A deep learning-assisted spoofing attack recognition approach is designed to identify spoofing messages received at vehicular network nodes in real time, thereby reducing traffic congestion and preventing accidents. Likewise, the suggested cyber spoofing assault discovery approach identifies the attack in the vehicular network with high throughput as well as low false negative and positive rates. The implemented approach increases the sensing and communication capability of the vehicles by identifying the spoofing attack with high accuracy. This work is commenced by accumulating the data from the standard dataset. Simultaneously, the gathered data is given through the preprocessing technique. Here, the data filling, data cleaning, replacement of NaN value, and outlier removal are employed in the collected data. So, the consistency and the exactness of the spoofing attack recognition are increased. Further, the RBM is utilized to extract the features in the preprocessed data. From the extracted feature, some specific features are optimally selected by the FE-CMPA. In addition to this process, the weight is also optimized by the FE-CMPA. This optimized weight and features are multiplied to form the weighted fused feature. The weighted feature fusion is executed to lower the prediction error in the developed model. Because of the optimization process, the relief score value is highly augmented. Consequently, the weighted feature is passed to the HD-ANet model to get the final detected outcome. The dilation mechanism incorporated into the model reduces the number of parameters required for spoofing attack detection. Further, the attention mechanism in the developed approach concentrates on extracting the important features for the attack detection process. Finally, the predicted result in the DTCN and residual LSTM is averaged to attain the final detected result. The HD-ANet effectively identifies spoofed data in vehicular networks and helps prevent traffic congestion, ensuring efficient transportation.. Finally, the result from the implemented method is analyzed with the conventional frameworks to verify the effectuality of the offered spoofing attack detection model. The detailed model of the deep network-based spoofing attack detection method in the vehicular network is indicated in Fig. 2.

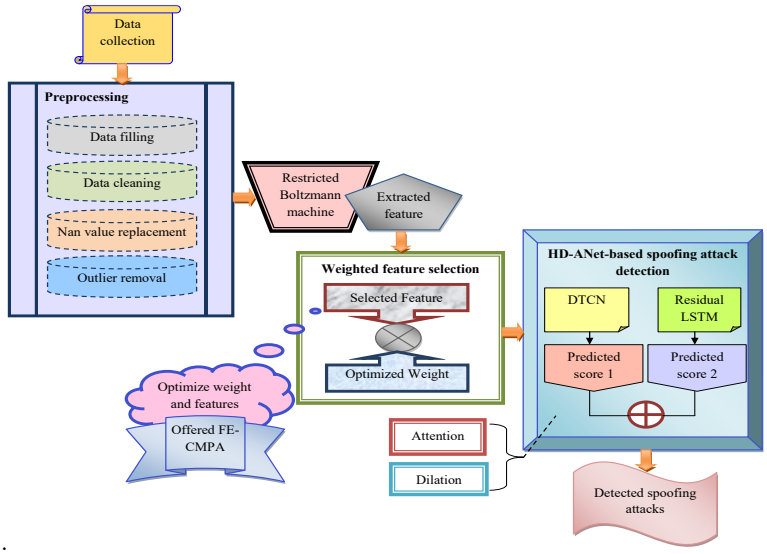


Fig. 2: Detailed Model of the Deep Network-Based Spoofing Attack Detection Method.

3.4. Time series dataset representation

The datasets used for spoofing attack detection are listed in Table 2.

Table 2: Dataset Employed for the Deep Learning-Based Spoofing Attack Detection Process

Number	Link	Description
1	"https://www.kaggle.com/datasets/yashwanthkumbam/apaddos-dataset"	The name of the first dataset used in the spoofing attack detection process is APA-DDoS Dataset and it was accessed on 2023-11-13. The identification of malicious connections is quite difficult to perform due to the increase in connected devices. For identifying the malicious activities, the IDS are used. The type of attack and the traffic patterns are analyzed by the IDS.
2	"https://www.cse.wustl.edu/~jain/iiot/index.html"	The second dataset used in this work is the WUSTL-IIOT-2018 dataset and it is accessed on 2023-11-13. The SCADA system is used to build this dataset. The real-world industrial system is emulated using SCADA. The development of the future attack is also identified by scanning this network. The vulnerabilities of the device in the network are also identified for securing the network.

The data collected for the spoofing attack detection in vehicular networks using the three datasets and it is indicated as S_l^o, here $l = 1,2 \ldots L$, and $L$is the total amount of data collected from the standard resources. The APA-DDoS dataset contains XX instances with features such as traffic patterns and attack types including DDoS and spoofing scenarios. The WUSTL-IIoT-2018 dataset includes YY records from a SCADA-based industrial IoT environment with both normal and malicious traffic. These datasets are relevant to vehicular networks as they reflect time-series traffic patterns and spoofing/jamming behaviors similar to those occurring in CAN bus environments.

4. Preprocessing Over Collected Time Series Dataset and Optimal Weighted Feature Selection Using Developed Heuristic Strategy

4.1. Data pre-processing

In the spoofing attack recognition process, preprocessing is a crucial step. Inconsistent information in the collected data is removed during preprocessing. This can lead to the occurrence of errors in the attack detection process. The main preprocessing steps used in spoofing attack detection are as follows.

Data filling: The collected data S_l^o is passed to the data filling process. The quality of the gathered data is improved by the data-filling process since it fills the missing characters in the collected data. The collected data S_l^o are not processed by the developed structure. The data can be filled by global constant values like 0 and NA to enhance the prediction process accuracy rate. The filled data from this step is represented as S_l^{DF}.

Data cleaning: The data filled S_l^{DF} is agreed to this process for the purpose of maximizing the data quality. Here, the error and the discrepancy in the data are recognized by the data-cleaning process. The invalid data in the filled data is also identified by the data cleaning process. In preprocessing, data cleaning is the most important step and it is patiently carried out to increase the superiority of the information. The cleaned information of this process is denoted as S_l^C.

NaN value replacement: The cleaned data S_l^C is given in this step for replacing the NaN values. Here, the (Not available) NA values in the cleaned data are substituted with zeros. In the data-filling process, some undefined values are used to fill the gaps in the composed data S_l^o and these undefined values are replaced with zero to improve the prediction accuracy. The Nan value replaced data is signified as S_l^{NAN}

Outlier removal: The outlier removal process takes NaN value replaced data is considered as an input S_l^{NAN}. Before executing the attack detection process, outliers must be removed from the data. Because it greatly affects the training process of the developed spoofing attack discovery model. In the given data, the attributes are considerably away from the other attributes (lonely manner), and this attribute is removed from the data. The outlier removed data is represented as S_l^{OUT}.

4.2. Proposed FE-CMPA

The FE-CMPA is a new optimization algorithm, modeled on the conventional CMPA (Yuan et al. 2023). Considering the traditional CMPA algorithm, it can provide optimal solutions for optimizing complex structures and problems. The CMPA is a bionic-based algorithm and it has the ability to solve nonlinear high dimensional difficulties. Especially, it is designed to solve engineering design issues. Yet, the high-design optimization problems are not resolved by the CMPA and it is stuck with high-dimensional optimization issues. The linear issues are not solved by the CMPA. To solve these problems, the FE-CMPA is recommended. Unlike the original CMPA, which often struggles with high-dimensional optimization and noisy data, FE-CMPA introduces a fitness-entrenchment mechanism in the random number update (Eq. 1). This modification helps the algorithm escape local optima, achieve better convergence, and maximize the relief score more effectively for feature selection.

Novelty of the implemented FE-CMPA algorithm: The FE-CMPA is suggested to get the maximized the relief score value in the deep model-based spoofing attack detection process. In the cyber security spoofing attack detection process, the relief score value is maximized by the developed FE-CMPA since it optimally selects the feature and weight values. The FE-CMPA is designed to optimize the weight values and features obtained from the RBM structure for creating the weighted fused feature. The weight optimization process helps to solve high dimensional issues in the spoofing attack framework. The FE-CMPA is executed by identifying the random number. This random number is calculated using the best, worst, and current fitness values and expressed in Eq. (1). Here, the random number s is calculated using the best, worst, current, and mean fitness values, as shown in Eq. (1). This ensures balanced exploration and exploitation during optimization

$$s = \frac{b}{((w+m)+c)} \tag{1}$$

Where, the best fitness is denoted as b, worst fitness is expressed as w, current fitness is pinpointed as c, mean fitness is termed as m, and the random number calculated in the developed FE-CMPA is indicated as s, in the traditional CMPA, this random number is updated in Eq. (2). As a result of the updated random number, ultra-high design optimization issues can be easily solved and also the value of relief score is maximized in the spoofing attack detection process.

Coronavirus Mask Protection Algorithm (CMPA) (Yuan et al. 2023): The CMPA is the bionic-based optimization algorithm used to solve high dimensional difficulties. The CMPA is designed on the basis of the self-protecting characteristics of the human.

Motivation: In December 2019, the COVID-19 epidemic has initiated. At the initial stage of the COVID, there is no treatment procedures are developed to defeat the disease. So many people die from this dangerous infection. To reduce the dispersion of the COVID-19 infection, people are advised to wear masks in the epidemic situation. Further, the vaccine research is carried out by the developing nation to lower the effects of the COVID-19 infection. The droplets produced by the sneezing and coughing action of the COVID-affected person that may lead to the dissemination of COVID-19 to healthier people who are not wearing masks in the epidemic situation.

The immune, suspected and the infected individual considerably affects the efficacy and the robustness of the CMPA. The people who improperly wearing the mask are easily affected by the COVID. COVID-19 is easily dispersed when the two people make close communication with each other. The infected person does not have any symptoms regarding the COVID at the initial stage. Moreover, social distancing is considered the most important factor for preventing the dispersion of COVID to others. The sickness phase, transmission phase, and invulnerable phase are the three important phases of the sickness and exemption process. The infected person is identified by the communal distancing factor and it is agreed in Eq. (2).

$$y_j(u+1) = \begin{cases} y_j(u) s > s_t \\ J\left(y_j(u)\right) 0 < s \le \frac{1}{3} s_t sickness \\ T\left(y_j(u) \frac{1}{3} s_t < s \le \frac{2}{3} s_t transmission \right. \\ S\left(y_j(u) \frac{2}{3} s_t < s \le s_t invlunerable \right. \end{cases} \tag{2}$$

Here, the communal space is represented as$s$, this is also considered as the random number in the region of[0,2], this random number is upgraded in Eq. (1), the safe social distance is termed ass_t, at the social communication$(u+1)$, and physical condition of j^{th} person is elucidated as$y_j(u+1)$.
Sickness phase: The healthier person is affected by the disease if the communal space between the infected person and the healthier person is too small that is$0 < s \leq \frac{1}{3}s_t$. The expression involved in the sickness phase is offered in Eq. (3).

$$y_j(u+1) = J\big(y_j(u)\big) \tag{3}$$

$$J\big(y_j(u)\big) = y_j(u) + \omega_j(u) * s(u) * ||y_j(u) - y_q(u)|| \tag{4}$$

Thus, at the communal interaction$u$, the spot of the infected person is represented as$y_q(u)$, and the protection factor of the j^{th}person is indicated as$\omega_j(u)$.
Transmission phase: The unaffected person enhances their communal space from the infected person to avoid the occurrence of COVID-19 infection. The symptoms of the COVID are not produced immediately once affected so the person is requested to quarantine for a particular time period.

$$y_j(u+1) = T\big(y_j(u)\big) \tag{5}$$

$$T\big(y_j(u)\big) = \begin{pmatrix} y_j(u) + \xi_j(u) \bullet \omega_j(u) \bullet s(u) \\ \bullet\ ||y_j(u) - y_r(u)|| \end{pmatrix} \bullet \frac{o^{(\varepsilon/\varphi+1)}-1}{o-1} \tag{6}$$

Here, the time of the communal behavior and the dispersion of the virus are represented as$\boldsymbol{\varepsilon}$, and$\boldsymbol{\varphi}$correspondingly, the infection factor is represented as$\boldsymbol{o}$. In social interaction$\boldsymbol{u}$, the confrontation of the person $\boldsymbol{j}$is denoted as$\xi_j(u)$ and the location of the invulnerable person is$y_r(u)$.
Invulnerable stage: The communal distance is the most important factor since the person can be easily affected by the COVID-19 infection. The autoimmune system of the human body lowers the impact of the virus if the communal distance stumbles in the region of$\left(\frac{2}{3}s_t, s_t\right)$. The immune condition of the human body is elucidated in Eq. (7).

$$y_j(u+1) = S\big(y_j(u)\big) \tag{7}$$

$$S\big(y_j(u)\big) = y_j(u) + \omega_j(u) * s(u) * ||y_j(u) - y_c(u)|| * \rho e^{v} \tag{8}$$

Here, the happiness index is represented as$v$, and the physical coefficient index is represented asρ. At the explore space, the arbitrary individual is selected to maintain the population in a stable manner.
The random individual is used instead of the dead individual and it is presented in Eq. (9).

$$y_j(u+1) = bol + rndn * (uol - bol) \tag{9}$$

Here, the lower bound is indicated asbol, and the upper bound is indicated asuol. The replacement of the dead individual is done using Eq. (10).

$$y_j(u+1) = -(1 - rndn) \bullet \big(y_j(u) - medi(Y)\big) + y_c(u) \tag{10}$$

Here, for the existing iteration, the excellent solution is elucidated as$y_c(u)$, the usual distribution is developed by the random number$rndn$, and for the present population, the median is denoted as$medi(Y)$.
Algorithm 1 elucidates the pseudocode of the explored FE-CMPA.

Algorithm 1: Explored FE-CMPA

Fix the required attributes such as number of population$O$ and maximum iteration $itermxi$
Fix the lower and the upper limit values
While the termination condition is not satisfied
Update the random number using the developed concept in Eq. (1)
    For individual populations do
        If $0 < s \leq \frac{1}{3}s_t$then
            Find $y_j(u+1) = J\big(y_j(u)\big)$
        Else if $\frac{1}{3}s_t < s \leq \frac{2}{3}s_t$
            Calculate $y_j(u+1) = T\big(y_j(u)\big)$
        Else if $\frac{2}{3}s_t < s \leq s_t$
            Find $y_j(u+1) = S\big(y_j(u)\big)$
        Else
            Evaluate $y_j(u+1) = \big(y_j(u)\big)$
        End if
    End for
    If the individual surpasses the explore space, the fresh individual is arbitrarily developed
        Upgrade the size of the population using Eq. (10).
    Else
        Verify and correct the new position using the borders of variables

End

$u = u + 1$

End while

4.3. Feature extraction using RBM

The preprocessed data$S_l^{OUT}$is given to the RBM for retrieving the features. The RBM (Cai et al. 2012) is an energy-based neural network that uses unsupervised learning to extract features by analyzing the distribution of input data. The RBM is sometimes described as an energy-aided stochastic neural network. In the conventional artificial neural network, arbitrary variations are introduced to develop the stochastic neural network. The hidden and the visible units are available in the RBM. The data distribution is done by the hidden unit of the RBM and the inputs are given to the discernible units of the RBM. The Gibbs sampling is used as the transition operator and it is used to scamper the Monte Carlo Markov Chain (MCMC) towards the direction of union. This process may be used to obtain the samples of the RBM. The visible units of the RBM are not dependent on each other. Further, in each layer of the RBM, the Gibbs sampling is executed. In the RBM, the energy function is illustrated in Eq. (11).

$$F(w, i|\Xi) = \frac{1}{2}(w^T Xi + c^T w + d^T i) \tag{11}$$

$$\Xi \equiv (X, c, d) \tag{12}$$

Here, the hidden units of the RBM are represented as$i$, the visible units are elucidated as$w$, the bias of the invisible and the visible unit is offered as$d$, and c correspondingly, the visible and the invisible units are attached by the weight$X$.
The partition function $A(\Xi)$ is signified in Eq. (13).

$$A(X) = \sum_y EXP[-F(y|\Xi)] \tag{13}$$

For the state$y$, the probability value is indicated in Eq. (14).

$$Q(w, i|\Xi) = \frac{1}{A(\Xi)} exp\{-F(w, i|\Xi)\} \tag{14}$$

For the visible unit and the hidden unit, the restricted probability is signified in Eq. (15) and Eq. (16).

$$q(w_j = 1|i) = \sigma(c_j + X_j i) \tag{15}$$

$$q(w_j = 1|w) = \sigma(d_j + X_k w) \tag{16}$$

$$\sigma(y) = \frac{1}{1+exp(-y)} \tag{17}$$

Here, for the weight matrix$X$, the k^{th}column vector is represented asX_k, j^{th}row vector is denoted asX_j. The features retrieved from the RBM are indicated asG_h^{RBM} .

4.4. Optimal weighted feature selection

The optimal weighted feature selection is carried out by FE-CMPA. Here, the FE-CMPA is initially used to optimally pick the specific set of features retrieved from the RBM. Similarly, the weight values in related to the features are optimized by the same FE-CMPA. These optimized features and the weights are multiplied with each other in the weighed fused feature and it is given in Eq. (18).

$$G_w^{FW} = G_w^{OPT} \times W^{OPT} \tag{18}$$

Here, the weighted fused feature is represented asG_w^{FW}, the optimally selected feature is indicated asG_w^{OPT} , and the optimally selected weight is signified asW^{OPT}.
As a result of the optimization approach, the relief score value is significantly maximized. The optimal weighted feature selection is adopted to reduce the prediction error in the attack detection process. Additionally, irrelevant data is removed during the optimal weighted feature selection process. The objective function of the FE-CMPA-HD-AN is examined in Eq. (19). The objective function (Eq. 19) defines how optimal features (f_opt) and weights (w_e) are selected to maximize the relief score (R_relf), thereby minimizing prediction error.

$$h_{obj} = \arg\min_{\{f_{opt}, we\}} \left(\frac{1}{relf}\right) \tag{19}$$

Here, the optimally chosen feature is indicated asf_{opt} in$[1 to 200]$, the optimized weight is termed aswe and it lies in between$[0.01,0.99]$ and the term $relf$indicates the relief score. The weighted fused feature is represented asG_w^{FW}. The relief score (Eq. 20) measures how well a feature distinguishes between different classes by comparing its values in similar vs. dissimilar instances.
Relief score: The relief score is identified using Eq. (20).

$$Relf = R(EB|D) - Q(EB|S) \tag{20}$$

Here, the relief score is indicated as$Relf$, the diverse value of feature is expressed asEB, the adjacent instance of the same and diverse class are elucidated as$S$, and Drespectively. The pictorial illustration of the optimal weighted feature selection is signified in Fig. 3.

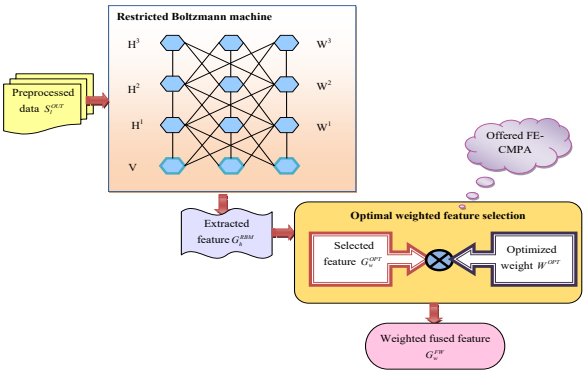


Fig. 3: Pictorial Representation of the Optimal Weighted Feature Selection.

5. An Intelligent Spoofing Attack Detection Framework Using Dilation and Attention-Based Hybrid Deep Learning Network

5.1. DTCN model

The temporal associations in the data are captured by the convolutional layers of the DTCN (Pham et al. 2021). The final layer of the DTCN takes the sequence of data as the input. Some of the layers of DTCN have a high dilation rate so it leads to the expansion of the receptive field of the higher layer. The depth of the network is increased to enlarge the receptive field of higher layers. The zero padding is applied to achieve the usual constraint in the DTCN. The padding dimension in the DTCN is identified by Eq. (21).

$$padd(j) = (l-1) \times e(j) \tag{21}$$

Here, the layer index is denoted as$j$, the dilation is signified as$e$, and the size of the kernel is specified as$l$.
The time step of the input data is covered if the receptive field of the layer is large. The DTCN is composed of a residual block in which the convolutional layers are available. In the DTCN, the amenable field is identified using Eq. (22).

$$recpfield = 1 + O \bullet (l-1) \bullet (2^C - 1) \tag{22}$$

Here, the number of convolutional layers is represented as$O$, the kernel size of all layers is illustrated as$l$, and the total number of the residual block is portrayed as$C$.

5.2. Residual LSTM model

Recently, the development of deep learning models has emerged to detect spoofing attacks effectively. CNNs cannot effectively identify unknown attack types and patterns, and thus fail when handling larger or more diverse attack datasets. Also, it requires a larger amount of labeled network traffic data and it takes more time during the implementation process. Real-time attack detection using CNN consumes high computational and more processing power. On the other hand, the traditional DTCNN is difficult to effectively recognize the attacks in real-world scenarios especially when dealing with several changes in attack types. Also, the gradient vanishing and imbalance issues are generated in existing classifier models. To address these issues, a Residual LSTM [19] is incorporated into our framework. It has the ability to effectively identify and solve the complex and long-term dependencies attacks in earlier stages and provides better generalization performance in unseen attack data. The vanishing issue is solved by the residual LSTM, which helps to enhance performance in the detection model. In the residual LSTM, the output layer $i_u^m$is amalgamated with the shortcut lane, and the internal memory cell of residual LSTM is indicated asd_u^m. The forget gate$g_u^m$is regularly maintained to control the temporal flow of the gradient usingd_u^m. The protrusion output$n_u^m$is incorporated with the shortcut lanei_u^{m-1}, which is developed from the $(l-1)^{th}$output layer. The expression involved in the residual LSTM is offered as follows.

$$j_u^m = \chi\left(X_{yj}^m y_u^m + X_{ij}^m i_{u-1}^m + x_{dj}^m d_{u-1}^m + c_j^m\right) \tag{23}$$

$$g_u^m = \chi\left(X_{yg}^m y_u^m + X_{ig}^m i_{u-1}^m + x_{dg}^m d_{u-1}^m + c_g^m\right) \tag{24}$$

$$d_u^m = g_u^m \bullet d_{u-1}^m + j_u^m \bullet tanh\left(X_{yd}^m y_u^m + X_{id}^m i_{u-1}^m + c_g^m\right) \tag{25}$$

$$p_u^m = \chi\left(X_{yp}^m y_u^m + X_{ip}^m i_{u-1}^m + X_{ip}^m i_{u-1}^m + c_d^m\right) \tag{26}$$

$$s_u^m = tanh(d_u^m) \tag{27}$$

$$n_u^m = X_q^m \bullet s_u^m \tag{28}$$

$$i_u^m = p_u^m \bullet (n_u^m + X_i^m y_u^m) \tag{29}$$

Here, the input gate is represented asj_u^m, the forget gate is signified asg_u^m, and the layer index is illustrated as$m$, the output gate is elucidated asp_u^m. The input given to the residual LSTM is signified asy_u^m, the internal cells of the residual LSTM is showcased asd_{u-1}^m, the m^{th}output layer is represented asi_{u-1}^m, and the protuberance matrix is acted asX_q^m.

If the size of y_u^m seems like ai_u^m, then the identity matrix is replaced instead of $X_i^m$and it is offered in Eq. (30).

$$i_u^m = p_u^m \bullet (n_u^m + y_u^m) \tag{30}$$

Thus, the result of the LSTM is scaled using the protuberance matrixX_q^m.

5.3. Detection of spoofing attacks using proposed HD-AN

The traditional DTCN method can effectively capture and analyze the complex attack patterns to enhance the detection accuracy with low false positive values. Additionally, the prescribed field of DTCN is enlarged through the structure of dilation. So, the precision of the spoofing attack detection is greatly increased. Yet, it needs large labeled attack datasets for the process of training and it impacts the model's performance. The residual LSTM method can significantly improve evaluation performance in long-range attack patterns with network traffic. The training process of the residual LSTM is very simple to provide better accurate results. Yet, it fails to identify attack types effectively and it requires larger training data. It takes more time for processing performance and needs high computational resources. To overcome these challenges, DTCN and Residual LSTM are integrated to form the proposed HD-ANet model. Further, the detection value in the DTCN and the residual LSTM are employed to generate the final detected result. The implemented HD-ANet-based structure is used to identify falsely data inserted by the spoofer on the signal of the vehicular network. Here, the attention mechanism is used to analyze huge amounts of input data with low memory space and the dilation structure reduces the cost required for the spoofing attack detection process. Therefore, traffic congestion can be effectively prevented using the developed model. The developed FE-CMPA-HD-ANet model also prevents spoofing attacks that mislead drivers by providing false navigation signals, since the attack can be identified at an early stage. From the weighted fused feature, the most important feature is processed by the attention mechanism and the dilation model requires a very minimal amount of parameter in the attack detection process. The weighted fused feature$G_w^{FW}$is given to the HD-ANet for the spoofing attack detection process. Moreover, the lightweight design of HD-ANet with dilation and attention mechanisms makes it more suitable for real-time deployment in vehicular environments where ECUs have limited computational resources and strict latency requirements.

Dilation (Zhang et al. 2019): The dilation is designed to be managed with the convolution mechanism. The extension of the amenable field does impact the amount of parameters in the network. The dilation rate is used to restrict the prescribed field of the dilated structure. The down-sampling process is used by most of the network to increase the receptive field. Moreover, the loss of pixel-level data can be prevented by the dilation network. The dilation network is used to confine the feature maps from the several receptive fields. The dilation structure may reduce the cost of the spoofing attack detection process because it enlarges the receptive field so the accuracy of the spoofing attack detection is maximized [42].

Attention (Fazil et al. 2021): The attention mechanism is used in the HD-ANet to effectively analyze the weighted fused feature. Here, the features are ranked based on their significance. The attention weight, context vector, and alliance layers are present in the attention structure. The alliance score between the summit vector$w$and fixed vector $i = \{i_1, i_2 \ldots i_o\}$ is identified by the alliance layer. The intact elements of the fixed vector are normalized to find the prospect distributionκ_j, here [11]$j = \{j_1, j_2 \ldots o\}$. The prospect distribution is identified by Eq. (31).

$$\kappa_j = \frac{exp(i_j^{'} w)}{\sum_{k=1}^{o} exp(i_j^{'} w)} \tag{31}$$

The summation of weighted essentials in the fixed vector$w$ is measured as output of the attention mechanism and it is denoted by Eq. (32).

$$P = \sum_{j=1}^{o} \kappa_j i_j \tag{32}$$

Here, the output of the attention network is represented as$P$and the most important information is passed to the summit vector$w$with the fixed vectori_j. This can be done if the value of prospect distribution$\kappa_j$is high. The attention system is used to handle a huge number of input data with minimal memory space. The semantic view of the HD-ANet for the spoofing attack detection is indicated in Fig. 4.

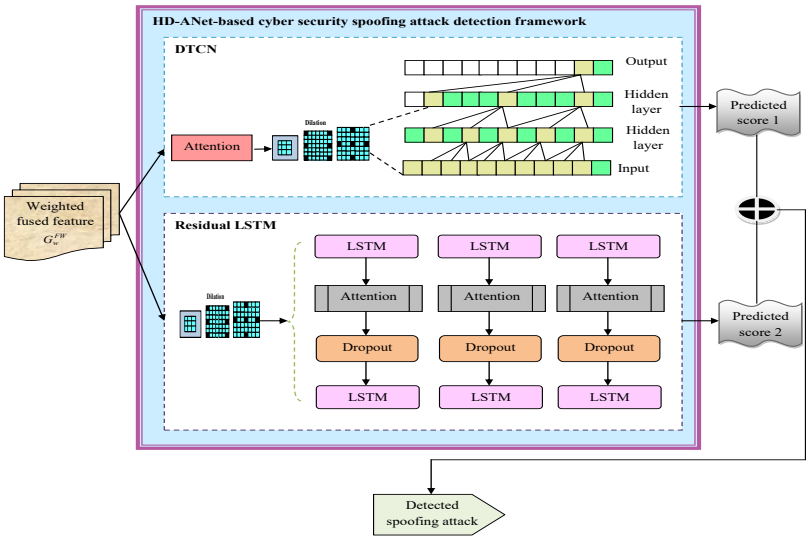


Fig. 4: Detailed View of the HD-Anet for the Spoofing Attack Detection Result and Discussion.

5.4. Experimental settings

Python software was utilized to test the explored HD-ANet-based cyber security spoofing attack detection framework. The process of experimentation was executed by considering the amount of population as 10, the total iteration as 50, and the chromosome length as 200. Conventional algorithms like Eurasian Oystercatcher Optimization (EOO), Water Strider Algorithm (WSA), Garter Snake Optimization (GSO), CMPA, and traditional prediction techniques like MobileNet, LSTM, DTCN and Bi-LSTM were taken to examine the efficacy of the HD-ANet-based cyber security spoofing attack discovery framework. Table 3 shows the parameters used in the developed FE-CMPA Technique.

Table 3: Parameters Used in This Developed ICMPA Method

Parameters	Values
No. of population	10
Chromosome Length	200
First100 features	1- no. of extracted features
Second 100 weights	0.01-0.99
Maximum Iteration	50
Proposed (ICMPA) parameters	
Safe Social Distance	1.0
Physical Fitness Coefficient	0.8
Happiness Index	0.7

5.5. Performance indices

In this research, diverse positive and negative measures are used to validate the overall performance These evaluation metrics provide accurate outcomes that enhance decision-making and security management performance. Also, these metrics allow for tracking and analysing the attack detection at an earlier stage based on its effective outcomes in the developed model. The performance enhancement in attack detection can easily mitigate the occurrence of falsely outcomes that can be used to fine-tune the detection process to enhance its accuracy and efficiency. This helps to identify the particular areas for improvement and potential attacks earlier stage to minimize the system damage. The below performance indices are used in the HD-ANet-based cyber security spoofing attack detection framework for validating the effectiveness of the planned scheme.

$$accurcay = \frac{m1+m2}{m3+m4+m1+m2} \tag{33}$$

$$precision = \frac{m2}{m1+m3} \tag{34}$$

$$MCC = \frac{m1*m2-m3*m4}{\sqrt{(m1+m3)(m1+m4)(m2+m3)(m2+m4)}} \tag{35}$$

$$FNR = \frac{m2}{m2+m4} \tag{36}$$

$$FDR = \frac{m3}{m3+m2} \tag{37}$$

$$FPR = \frac{m1}{m3+m2} \tag{38}$$

$$NPV = \frac{m2}{m2+m4} \tag{39}$$

$$sensitivity = \frac{m1}{m1+m3} \tag{40}$$

$$specificity = \frac{m2}{m2+m3} \tag{41}$$

$$F1score = \frac{2m1}{2m1+m3+m4} \tag{42}$$

Thus, the true negative and true positive are represented as$m2$, and $m1$ respectively, the false negative and false positive are indicated as$m4$, and $m3$correspondingly.

5.6. Roc curve analysis for two datasets over conventional techniques

The developed spoofing attack detection model analyzed using the ROC curve is revealed in Fig. 5. For the first dataset, the HD-ANet-based cyber security spoofing attack detection approach achieves higher true positive rates of 11.11%, 9.75%, 8.43%, and 4.65% for MobileNet, LSTM, DTCN, and Bi-LSTM when the false positive is taken as 0.4. These results confirm that the proposed HD-ANet-based spoofing attack detection approach outperforms traditional methods.

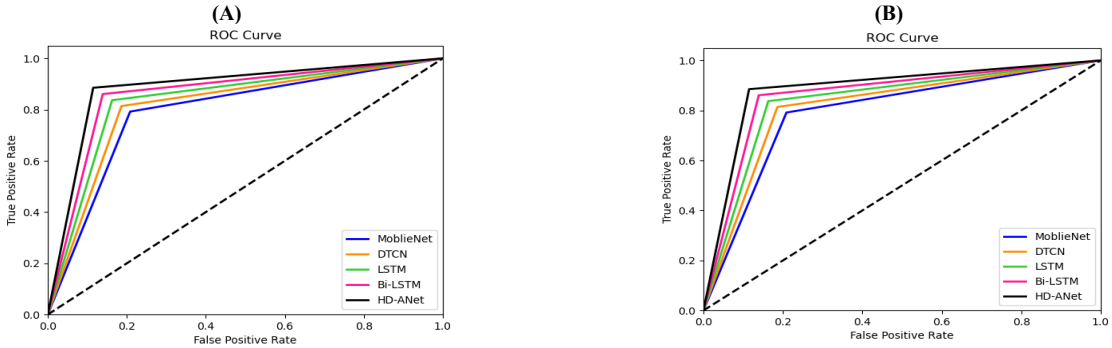


Fig. 5: ROC Curve Investigation of the Deep Model-Based Cyber Security Spoofing Attack Detection Model Over Various Techniques for (A) Dataset 1, (B) Dataset 2

5.7. Convergence analysis for two datasets over various algorithms

The convergence analysis of the HD-ANet-based cyber security spoofing attack detection framework among diverse frameworks is portrayed in Fig. 6. From the Fig. 5 (b), the convergence of the HD-ANet-based cyber security spoofing attack detection framework is reduced than the EOO, WSO, GSO, and CMPAS with 60%, 80%, 68% and 60% at the 20th iteration. Thus, the graphical results showed that the convergence function of the HD-ANet-based cyber security spoofing attack discovery framework is considerably reduced than the conventional models.

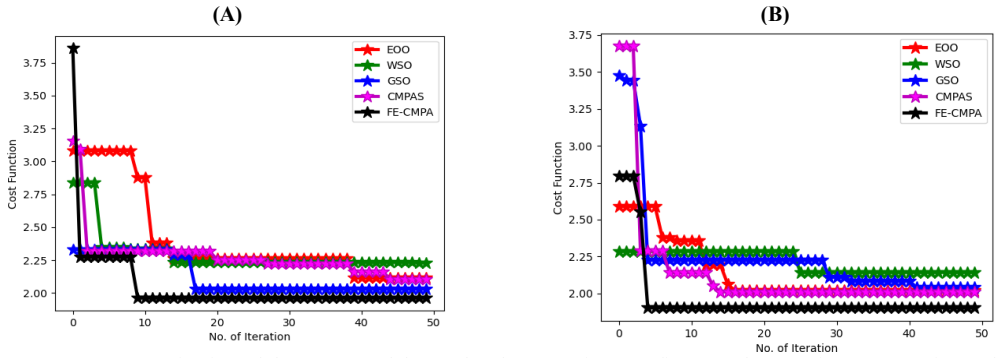
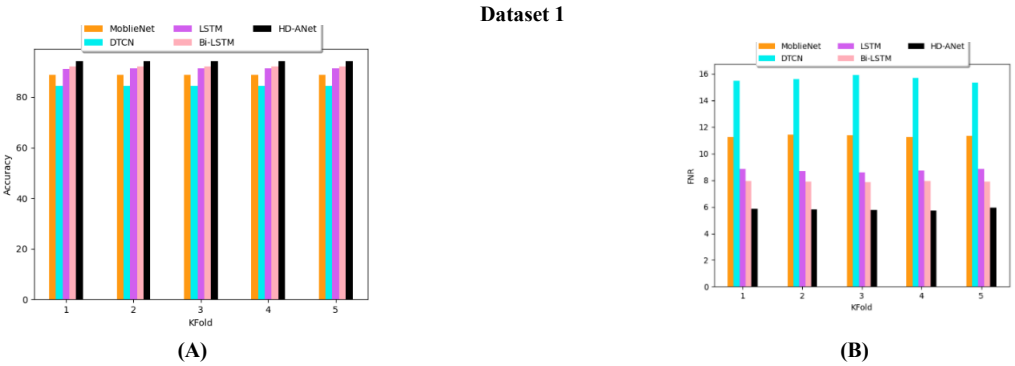
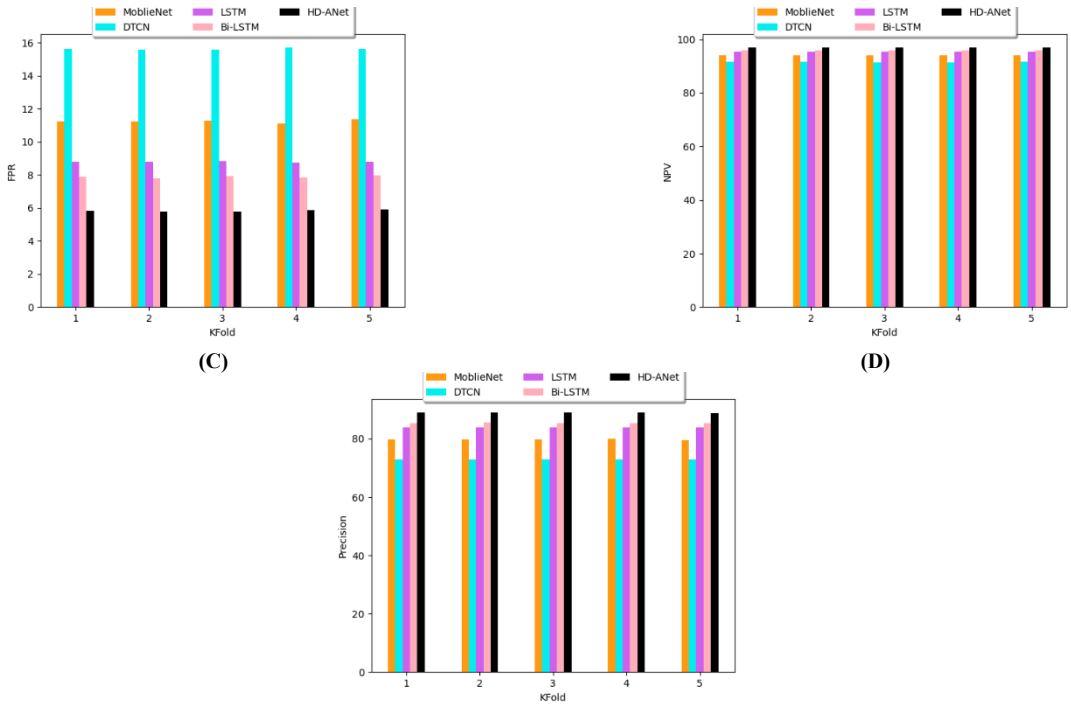


Fig. 6: ROC Curve Investigation of the Deep Model-Based Cyber Security Spoofing Attack Detection Over Various Algorithms for (A) Dataset 1, (B) Dataset 2.

5.8. Performance judgment of the implemented method using k-fold metrics

The performance comparison of the explored HD-ANet-based cyber security spoofing attack recognition model using the K-fold metrics is indicated in Fig. 7. The suggested HD-ANet-based cyber security spoofing attack discovery model obtains 8.23% enhanced accuracy than the MobileNet, 6.97% enhanced than the DTCN, 12.19% enhanced than the LSTM and 5.74% enhanced than the Bi-LSTM for the 1st dataset. So, the performance of the HD-ANet-based cyber security spoofing assault detection is better over the conventional techniques.

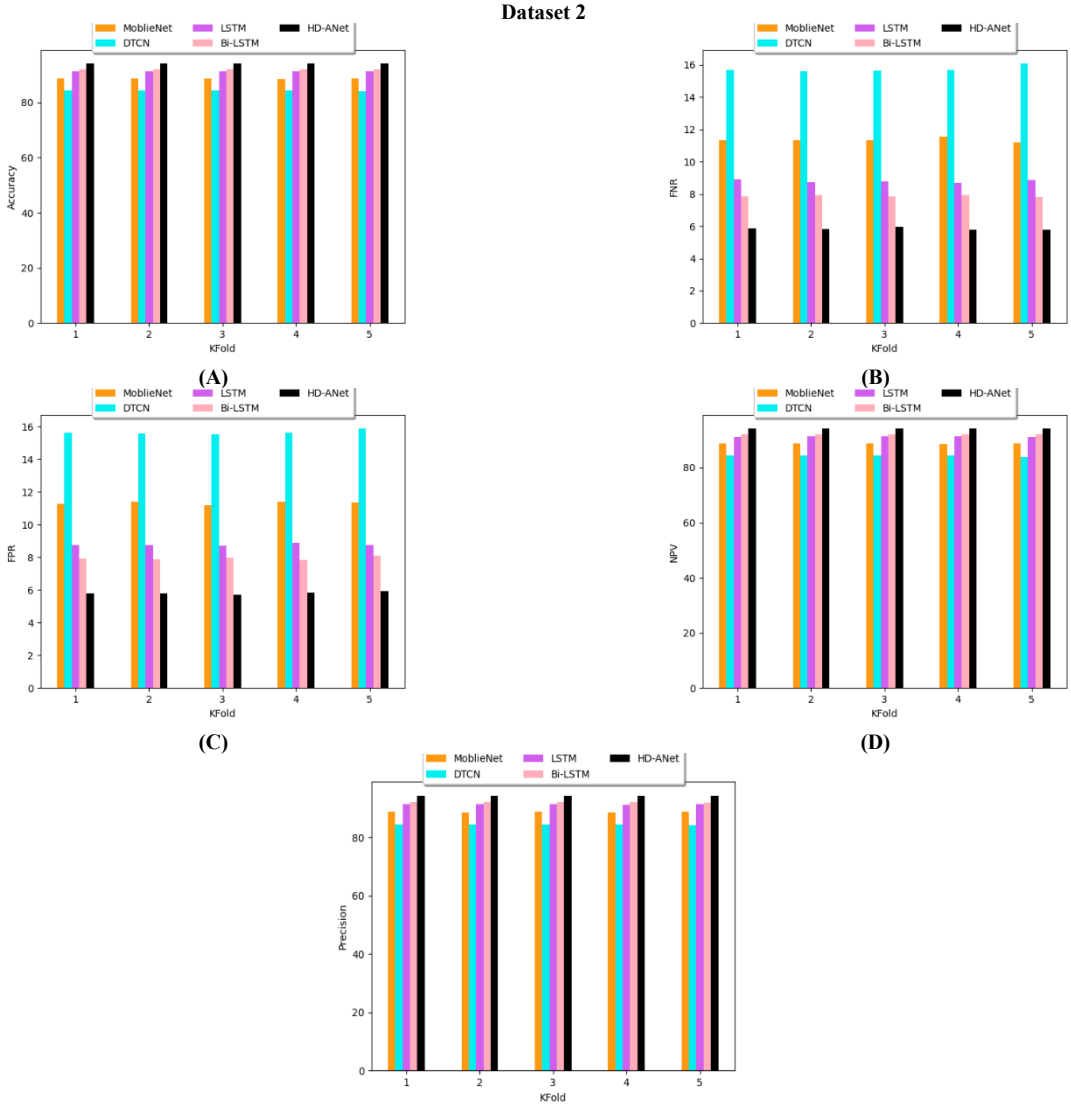




(C) (D)

(E)

Dataset 2



(A) (B)

(C) (D)

(E)

Fig. 7: Performance Investigation of the Deep Model-Based Cyber Security Spoofing Attack Detection Over Diverse Techniques for (A) Accuracy, (B) FNR, (C) FPR, (D) NPV, (E) Precision.

5.9. Performance assessment on various feature approaches

The performance comparison of the FE-CMPA-RBM-based feature selection approach is given in Table 4. From the table results, the accuracy of the FE-CMPA-RBM-based feature selection approach is better than the Mobile Net, LSTM, DTCN, and RBM with 6.11%, 11.67%, 3.18%, and 2.22% for the first dataset. Thus, the feature selection performance of the RBM with optimization is superior to the without optimization techniques.

Table 4: Performance Analysis on Deep Model-Baed Feature Selection Over Different Techniques

Dataset 1 TERMS	MobileNet (Li et al. 2022)	LSTM (Gers et al. 2002)	DTCN (Pham et al. 2021)	RBM (Without optimization)	FE-CMPA-RBM (with optimization)
Accuracy	88.77249	84.35538	91.29101	92.1552	94.20899
Sensitivity	88.77513	84.16402	91.54762	92.19841	94.2328
Specificity	88.77116	84.45106	91.1627	92.1336	94.19709
Precision	79.81021	73.01981	83.81776	85.42331	89.03442
FPR	11.22884	15.54894	8.837302	7.866402	5.80291
FNR	11.22487	15.83598	8.452381	7.801587	5.767196
NPV	94.05359	91.42788	95.56951	95.93813	97.02969
FDR	20.18979	26.98019	16.18224	14.57669	10.96558
F1-Score	84.0543	78.19686	87.51233	88.68165	91.55989
MCC	75.68265	66.49874	81.03176	82.83341	87.23898
Dataset 2					
Accuracy	88.628	84.347	91.09	92.094	94.062
Sensitivity	88.624	84.222	91.108	92.044	94.06
Specificity	88.632	84.472	91.072	92.144	94.064
Precision	88.63109	84.43308	91.07521	92.13614	94.06376
FPR	11.368	15.528	8.928	7.856	5.936
FNR	11.376	15.778	8.892	7.956	5.94
NPV	88.62491	84.26135	91.1048	92.05195	94.06024
FDR	11.36891	15.56692	8.924787	7.863864	5.936237
F1-Score	88.62755	84.32741	91.0916	92.09005	94.06188
MCC	77.256	68.69421	82.18001	84.18804	88.124

5.10. Statistical results over various algorithms

Table 5 indicates the statistical outcome of the developed HD-ANet-based cyber security spoofing attack detection model. When considering the first dataset, the best statistical measure of the HD-ANet-based cyber security spoofing attack discovery model is increased than the EOO, WSO, GSO, and CMPAS with 11.05%, 16.84%, 6.84%, and 10.52%. Hence, the performance of the HD-ANet-based cyber security spoofing attack discovery model is better compared to other conventional techniques.

Table 5: Statistical Analysis on Deep Model-Based Cybersecurity Spoofing Attack Detection Model Over Different Algorithms

Dataset 1 TERMS	EOO (Salim et al. 2022)	WSO (Kaveh and Eslamlou 2020)	GSO (Naghdiani et al. 2023)	CMPAS (Yuan et al. 2023)	HD-ANet
BEST	2.114435	2.229939	2.032005	2.105529	1.960964
STANDARD DEVIATION	0.346989	0.164473	0.139023	0.187093	0.282598
MEAN	2.408413	2.301953	2.131549	2.276166	2.048776
WORST	3.082415	2.840482	2.332396	3.154449	3.858832
MEDIAN	2.261225	2.231731	2.032005	2.252637	1.960964
Dataset 2					
BEST	2.018517	2.142208	2.04007	2.010289	1.901316
STANDARD DEVIATION	0.201755	0.071424	0.342472	0.393814	0.228247
MEAN	2.139993	2.213852	2.251227	2.148764	1.968378
WORST	2.59043	2.285276	3.477595	3.673704	2.797339
MEDIAN	2.018517	2.213857	2.224808	2.010289	1.901316

5.11. Performance analysis over several approaches

The performance assessment of the HD-ANet-based cyber security spoofing attack detection model over numerous techniques is presented in Table 6. For the initial dataset, the specificity of the HD-ANet-based cyber security with spoofing attack detection model is increased than MobileNet, LSTM, and DTCN with 6.16%, 11.49%, 3.14%, and 2.21%. Finally, the specificity of the HA-ANet-based cyber security spoofing attack detection process is superior to the existing techniques.

Table 6: Performance Analysis on Deep Model-Baed Cybersecurity Spoofing Attack Detection Model Over Various Techniques

TERMS	MobileNet (Li et al. 2022)	LSTM (Gers et al. 2002)	DTCN (Pham et al. 2021)	Bi-LSTM (Jang et al. 2020)	HA-ANet
Accuracy	88.6358	84.47002	91.18783	92.05996	94.07055
Sensitivity	88.67725	84.65344	91.1455	92.11905	94.05556
Specificity	88.61508	84.37831	91.20899	92.03042	94.07804
Precision	79.56892	73.04207	83.82929	85.24947	88.81589
FPR	11.38492	15.62169	8.791005	7.969577	5.921958
FNR	11.32275	15.34656	8.854497	7.880952	5.944444
NPV	93.99492	91.66415	95.37074	95.89409	96.93744
FDR	20.43108	26.95793	16.17071	14.75053	11.18411
F1-Score	83.87654	78.42027	87.33444	88.55123	91.36066
MCC	75.40504	66.834	80.76186	82.63285	86.93532
Dataset 2					
Accuracy	88.717	84.007	91.193	92.061	94.145
Sensitivity	88.786	83.904	91.15	92.202	94.226
Specificity	88.648	84.11	91.236	91.92	94.064
Precision	88.66364	84.0772	91.22846	91.94272	94.0736
FPR	11.352	15.89	8.764	8.08	5.936
FNR	11.214	16.096	8.85	7.798	5.774
NPV	88.7705	83.93709	91.1576	92.17995	94.21663
FDR	11.33636	15.9228	8.771544	8.057278	5.926399
F1-Score	88.72478	83.99051	91.18921	92.07218	94.14974
MCC	77.43407	68.01414	82.38603	84.12233	88.29012

5.12. Computational time analysis of the developed method

Table 7 shows the computational time analysis of the implemented method over existing algorithms and classifiers. Considering Table 7, the traditional GSO algorithm shows a high time as 19.9343 (secs). This maximum computation time potentially degrades the system performance and fails to detect the attacks at an earlier stage. Also, it fails to detect complex anomalies in network events. The developed HD-ANet model shows a minimum computational time of 14.0021 (secs) than the other traditional models. It has the ability to identify a spoofing attack very quickly with limited time. The implemented approach can significantly enhance the detection process effectively to maximize the developed framework.

Table 7: Computational Time Analysis: Proposed Model vs. Traditional Algorithms and Classifiers

Algorithms	Time (seconds)
EOO (Salim et al. 2022)	16.9655
WSO (Kaveh and Eslamlou 2020)	17.65694
GSO (Naghdiani et al. 2023)	19.9343
CMPAS (Yuan et al. 2023)	16.9494
Developed HD-ANet	14.002160
Classifier analysis	
MobileNet (Li et al. 2022)	15.6495
DTCN (Pham et al. 2021)	17.5956
LSTM (Gers et al. 2002)	19.4657
Bi-LSTM (Jang et al. 2020)	15.6254
Proposed FE-CMPA-RBM	14.002160

5.13. Sensitivity analysis of the developed framework

Table 8 shows the sensitivity analysis of the developed model with diverse performance parameters such as safe social distance, physical fitness, and happiness index. By analyzing safe social distance, the various distance such as 0.25, 0.35, 0.50, 0.75, and 1.0 are validated using statistical measures like worst, best, mean, median, and standard deviation. The physical fitness coefficient has analyzed with different values like, 0.15, 0.3, 0.45, 0.6, and 0.75. Also, the happiness index has been evaluated with diverse interval of 0.12, 0.25, 0.35, 0.55, 0.65 values. Utilizing the sensitivity analysis helps the developed model to provide better performance in spoofing attack detection model.

Table 8: Sensitivity Analysis of the Implemented Method

Variations by Safe Social Distance					
TERMS	0.25	0.35	0.50	0.75	1.0
Worst	0.4498	0.4706	0.4933	0.5237	0.3941
Best	0. 3989	0. 3925	0.3951	0. 4029	0. 3832
Mean	0. 4094	0.4047	0.4051	0. 4146	0. 3840
Median	0. 3987	0. 3925	0.3951	0. 4092	0. 3832
Standard deviation	0.0201	0.0207	0. 0204	0. 0199	0.0025
Variations by Physical Fitness Coefficient					
TERMS	0.15	0.3	0.45	0.6	0.75
Worst	0. 4744	0. 4477	0. 5317	0. 4330	0.4146
Best	0. 3906	0. 3916	0. 3903	0. 3924	0. 3797
Mean	0. 3986	0. 3967	0.3994	0. 3975	0. 3825
Median	0. 3906	0. 3916	0. 3935	0. 3925	0.3797
Standard deviation	0. 0134	0. 0088	0. 0243	0. 0116	0. 0054
Variations by Happiness Index					
TERMS	0.12	0.25	0.35	0.55	0.65
Worst	0.4564	0.4532	0.497	0.4654	0.4133
Best	0.4031	0.3975	0.3908	0.3936	0.3804
Mean	0.4174	0.4088	0.4052	0.3950	0.3827
Median	0.4154	0.3994	0.4082	0.3936	0.3804
Standard deviation	0.0151	0.0128	0.0175	0.0100	0.0057

6. Conclusion

In this paper, the novel spoofing attack detection model was developed by combining FE-CMPA with the HD-ANet model. The FE-CMPA was applied for the optimal weighted feature selection process, reducing dimensionality and maximizing the relief score. Next, the HD-ANet model was utilized for effective spoofing attack recognition by integrating DTCN and Residual LSTM with dilation and attention mechanisms. The proposed FE-CMPA-HD-ANet model exhibited better outcomes than other conventional techniques in terms of classification accuracy, recall, precision, F-measure, training loss, and execution time. These improvements confirm that the fitness-entrenchment strategy in FE-CMPA provides more robust feature optimization than conventional CMPA, while the hybrid HD-ANet framework enhances temporal pattern learning and improves overall detection performance. Importantly, the lightweight design of the proposed framework makes it suitable for real-time deployment in vehicular environments where ECUs have limited computational resources and CAN bus compatibility must be maintained. In the future, this work can be extended by validating the model on larger vehicular datasets and testing under diverse attack scenarios to further strengthen its robustness.

References

[1] Baldini, G. 2022. “Detection of cybersecurity spoofing attacks in vehicular networks with recurrence quantification analysis.” *Computer Communications* 191:486-499. https://doi.org/10.1016/j.comcom.2022.05.021.

[2] Baldoni, S., Battisti, F., and Neri. A. 2020. “On the Use of Differential Correction Clustering for Facing Spoofing Attacks to GNSS Augmentation Networks.” *IEEE Access* 8 :219903-219922. https://doi.org/10.1109/ACCESS.2020.3042469.

[3] Cai, X., Hu, S., and Lin, X. 2012. “Feature extraction using Restricted Boltzmann Machine for stock price prediction.” *IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China,* 2012:80-83. https://doi.org/10.1109/CSAE.2012.6272913.

[4] Chang, J., Zhang, L., Hsu, L. -T., Xu, B., Huang, F and Xu. D. 2022. “Analytic Models of a Loosely Coupled GNSS/INS/LiDAR Kalman Filter Considering Update Frequency Under a Spoofing Attack.” *IEEE Sensors Journal* 22(23):23341-23355. https://doi.org/10.1109/JSEN.2022.3212977.

[5] Chauhan S. V. S., and Gao. G. X. 2021. “Synchrophasor Data Under GPS Spoofing: Attack Detection and Mitigation Using Residuals.” *IEEE Transactions on Smart Grid* 12(4):3415-3424. https://doi.org/10.1109/TSG.2021.3051926.

[6] Dasgupta, S., Ghosh, T and Rahman. M. 2022b. “A Reinforcement Learning Approach for Global Navigation Satellite System Spoofing Attack Detection in Autonomous Vehicles.” arXiv pre print 2676 12. https://doi.org/10.1177/03611981221095509.

[7] Dasgupta, S., Rahman, M., Islam, M and Chowdhury. M. 2022a. “A Sensor Fusion-Based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles.” *IEEE Transactions on Intelligent Transportation Systems* 23(12):23559-23572. https://doi.org/10.1109/TITS.2022.3197817.

[8] Demir, M. Ö., Kurt, G. K., and Pusane, A. E. 2023. “A Pseudorange-Based GPS Spoofing Detection Using Hyperbola Equations.” *IEEE Transactions on Vehicular Technology* 72(8):10770-10783. https://doi.org/10.1109/TVT.2023.3257228.

[9] Dora, V.R.S and Naga Lakshmi, V. 2024. ORCID Icon "Smart network security using advanced ensemble-DDoS attack detection and hybrid JA-SLOA-linked optimal routing-based mitigation", *Australian Journal of Electrical and Electronics Engineering* 21. doi: https://doi.org/10.1080/1448837X.2024.2335797.

[10] Fan, Y., Zhang, Z., Trinkle, M., Dimitrovski, A. D., Song, J. B., and Li, H. 2015. “A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids.” *IEEE Transactions on Smart Grid* 6(6):2659-2668. https://doi.org/10.1109/TSG.2014.2346088.

[11] Fazil, M., Sah, A.K and Abulaish, M. 2021.“DeepSBD: A Deep Neural Network Model With Attention Mechanism for SocialBot Detection.” *IEEE Transactions on information forensics and security* 4211-4223 16. https://doi.org/10.1109/TIFS.2021.3102498.

[12] Gers, Felix, A., Nicol, N. Schraudolph, and Schmidhuber, J. 2002."Learning precise timing with LSTM recurrent networks." *Journal of machine learning research* 3:115-143.

[13] Hoang, T. M., van Chien, T., van Luong, T., Chatzinotas, S., B. Ottersten and L. Hanzo. 2022. “Detection of Spoofing Attacks in Aeronautical Ad-Hoc Networks Using Deep Autoencoders.” *IEEE Transactions on Information Forensics and Security* 17:1010-1023, https://doi.org/10.1109/TIFS.2022.3155970.

[14] Jang, Beakcheol, Kim, M., Harerimana, G., Kang, S and Kim, J. W. 2020 . "Bi-LSTM model to increase accuracy in text classification: Combining Word2vec CNN and attention mechanism." *Applied Sciences* 10:5841: 17. https://doi.org/10.3390/app10175841.

[15] Jannu, C and Vanambathina, S.D. 2023a. “An Overview of Speech Enhancement Based on Deep Learning Techniques", *International Journal of Image and Graphics.* https://doi.org/10.1142/S0219467825500019.

[16] Jannu, C., and Vanambathina, SD. 2023b. “An attention based densely connected U-NET with convolutional GRU for speech enhancement.” 2023 3rd International conference on Artificial Intelligence and Signal Processing (AISP)):1-5. https://doi.org/10.1109/AISP57993.2023.10134933.

[17] Kaveh, A and Eslamlou, A.D. 2020. "Water strider algorithm: A new metaheuristic and applications." *In Structures* 25:520-541. Elsevier, https://doi.org/10.1016/j.istruc.2020.03.033.

[18] Kim, C., Chang, S. -Y., Lee, D., Kim, J., Park, K and Kim, J. 2023. “Reliable Detection of Location Spoofing and Variation Attacks.” *IEEE Access* 11:10813-10825. https://doi.org/10.1109/ACCESS.2023.3241236.

[19] Kim, J., El-Khamy, M., Lee, J. 2017. “Residual LSTM: Design of a Deep Recurrent Architecture for Distant SpeechRecognition.” arXiv:1701.03360v3 [cs.LG]. https://doi.org/10.21437/Interspeech.2017-477.

[20] Kumari, T.L and Babu, A.R. 2024. “Genetic fuzzy rules and hybrid QDCNN-F-DSAE for detecting attacker behavior with tuning of firewall", *Australian Journal of Electrical and Electronics Engineering*. https://doi.org/10.1080/1448837X.2024.2373528.

[21] Li, N., Xia, S., Tao, X., Zhang, Z & Wang, X. 2020. “An area-based physical layer authentication framework to detect spoofing attacks.” *Science China Information Sciences* 63 222302. https://doi.org/10.1007/s11432-019-2802-x.

[22] Li, W., Wang, N., Jiao, L., and Zeng. K. 2021. “Physical Layer Spoofing Attack Detection in MmWave Massive MIMO 5G Networks.” *IEEE Access* 9:60419-60432. https://doi.org/10.1109/ACCESS.2021.3073115.

[23] Li, Yanyu, Yuan, G., Wen, Y., Hu, J., Evangelidis, G., Tulyakov, S., Wang, Y and Ren, J. 2022. "Efficientformer: Vision transformers at mobilenet speed." *Advances in Neural Information Processing Systems* 35 12934-12949.

[24] Liu, X., Li, B., Chen, H., Sun, Z., Liang, Y. C and Zhao C. 2019. “Detecting Pilot Spoofing Attack in MISO Systems With Trusted User.” *IEEE Communications Letters* 23(2):314-317. https://doi.org/10.1109/LCOMM.2018.2889491.

[25] Naghdiani, Maryam, Jahanshahi, M and Matin, R.K. 2023. "A Garter Snake Optimization Algorithm for Constrained Optimization." *Research square.* https://doi.org/10.21203/rs.3.rs-2899298/v1.

[26] Pham, C., Nguyen, L., Nguyen, A., Nguyen, N., Van-Toi, Nguyen. 2021. “Combining skeleton and accelerometer data for human fine-grained activity recognition and abnormal behavior detection with deep temporal convolutional networks.” *Multimedia Tools and Applications* 80:28919–28940. https://doi.org/10.1007/s11042-021-11058-w.

[27] Pinto, A., Schwartz, W. R., Pedrini, H., and Rocha, A. d. R. 2015. “Using Visual Rhythms for Detecting Video-Based Facial Spoof Attacks.” *IEEE Transactions on Information Forensics and Security* 10(5):1025-1038. https://doi.org/10.1109/TIFS.2015.2395139.

[28] Qiu, W., Li, C., Tang, Q., Sun, K., Liu, Y., and Yao. W. 2022. “Attack Detection for Spoofed Synchrophasor Measurements Using Segmentation Network.” *CSEE Journal of Power and Energy Systems* 8(5):1327-1337. https://doi.org/10.17775/CSEEJPES.2021.02780.

[29] Qiu, W., Tang, Q., Wang, Y., Zhan, L., Liu, Y and Yao. W. 2020. “Multi-View Convolutional Neural Network for Data Spoofing Cyber-Attack Detection in Distribution synchrophasors.” *IEEE Transactions on Smart Grid* 11(4):3457-3468. https://doi.org/10.1109/TSG.2020.2971148

[30] Rattani, A., Scheirer, W. J., and Ross, A. 2015. "Open Set Fingerprint Spoof Detection Across Novel Fabrication Materials." *IEEE Transactions on Information Forensics and Security* 10(11):2447-2460. https://doi.org/10.1109/TIFS.2015.2464772.
[31] Salim, A., Jummar, W.K., Jasim, F.M and Yousif, M. 2022. "Eurasian oystercatcher optimiser: New meta-heuristic algorithm." *From the journal Journal of Intelligent System.* https://doi.org/10.1515/jisys-2022-0017
[32] Sanders, C and Wang, Y. 2020. "Localizing Spoofing Attacks on Vehicular GPS Using Vehicle-to-Vehicle Communications." *IEEE Transactions on Vehicular Technology* 69(12):15656-15667. https://doi.org/10.1109/TVT.2020.3031576.
[33] Schmidt, E., Gatsis, N., and Akopian, D. 2020. "A GPS Spoofing Detection and Classification Correlator-Based Technique Using the LASSO." *IEEE Transactions on Aerospace and Electronic Systems* 56(6):4224-4237. https://doi.org/10.1109/TAES.2020.2990149.
[34] Shabbir, M., Kamal, M., Ullah, Z and Khan M. M. 2023. "Securing Autonomous Vehicles Against GPS Spoofing Attacks: A Deep Learning Approach." *IEEE Access* 11:105513-105526. https://doi.org/10.1109/ACCESS.2023.3319514.
[35] Shiaeles S. N., and M. Papadaki. 2015. "FHSD: An Improved IP Spoof Detection Method for Web DDoS Attacks." *the Computer Journal* 58(4):892-903. https://doi.org/10.1093/comjnl/bxu007.
[36] Theyazn, H., Aldhyani, H and Alkahtani. H. 2022. "Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity" 22(360). doi: https://doi.org/10.3390/s22010360.
[37] Valderrama, W., Magadán, A., Vergara, O. O., Ruiz, J., Pinto, R and Reyes, G. 2022. "Detection of Facial Spoofing Attacks in Uncontrolled Environments Using ELBP and Color Models." *IEEE Latin America Transactions* 20(6):875-883. https://doi.org/10.1109/TLA.2022.9757369.
[38] Vitale, C., Piperigkos, N., Laoudias, C., Ellinas, G., Casademont, J., Escrig, J, Kloukiniotis, A., Lalos, A.S., Moustakas, K., Rodriguez, R.D., Baños. D., Crusats, G.R., Kapsalas, P., Hofmann, K & Khodashenas, PS. 2021. "CARAMEL: results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks." *EURASIP Journal on Wireless Communications and Networking* 115, https://doi.org/10.1186/s13638-021-01971-x.
[39] Xiong, Q., Liang, Y. -C., Li, K. H and Gong, Y. 2015. "An Energy-Ratio-Based Approach for Detecting Pilot Spoofing Attack in Multiple-Antenna Systems." *IEEE Transactions on Information Forensics and Security* 10(5):932-940. https://doi.org/10.1109/TIFS.2015.2392564.
[40] Yang, Y., Duan, Z and Tehranipoor, M. 2020. "Identify a Spoofing Attack on an In-Vehicle CAN Bus Based on the Deep Features of an ECU Fingerprint Signal." *Smart Cities* 3(1):17-30. https://doi.org/10.3390/smartcities3010002
[41] Yuan, Y., Shen, Q., Wang, S., Ren, J., Yang, D., Yang, Q., Fan, J & Mu. X. 2023. "Coronavirus Mask Protection Algorithm: A New Bio-inspired Optimization Algorithm and Its Applications." *Journal of Bionic Engineering* 20:1747–1765. https://doi.org/10.1007/s42235-023-00359-5
[42] Zhang, J ., Lu, C., Wang, J., Wang, L and Yue X. 2019 . "Concrete Cracks Detection Based on FCN with Dilated Convolution." *Applied Science* 9:2686. https://doi.org/10.3390/app9132686
[43] D. Y. Bhadane, I. S. Borse, "An Intelligent Ensemble Deep Learning Techniques with Improved Owl Search Algorithm-Aided Optimal Feature Selection for Predicting the Presence of Heart Diseases", International Journal of Image and Graphic, 2025 https://doi.org/10.1142/S0219467827500215
[44] R. V. Patil, R. M. Patil, D. Y. Bhadane, G. M. Poddar, A. L. Wakekar, & S. R. Patil, "Adaptive Cheetah Optimization-Driven CNN: A Hybrid Approach for Robust Image Segmentation.", International Journal of Basic and Applied Sciences, 14(2), 691-702, Aug. 2025. https://doi.org/10.14419/c62avh78.
[45] Chetan Gode, Bhushan Marutirao Nanche, Dharmesh Dhabliya, Rahul Dnyanoba Shelke, , Rajendra V Patil. & Shushma Bhosle, "Dynamic neural architecture search : A pathway to efficiently optimized deep learning models" , Journal of Information and Optimization Sciences, 46:4-A, 1117–1127, 2025, https://doi.org/10.47974/JIOS-1896.
[46] A. Hidayat, A. Nurfikri, D. V. Priya, R. V. Patil, V. R. Hire and N. S, "Statistical Methods for Big Data Analysis in Technological Systems," 2025 International Conference on Frontier Technologies and Solutions (ICFTS), Chennai, India, 2025, pp. 1-7, https://doi.org/10.1109/ICFTS62006.2025.11031562.
[47] J. S. R, R. V. Patil, Y. S, P. M, S. S and R. Maranan, "Spilled Deep Capsule Neural Network with Skill Optimization Algorithm for Breast Cancer Recognition in Mammograms," *2025 International Conference on Inventive Computation Technologies (ICICT)*, Kirtipur, Nepal, 2025, pp. 632-637, https://doi.org/10.1109/ICICT64420.2025.11004784
[48] B. Gudivaka, N. Anute, Y. Ramaswamy, V. N. Sankaran, R. V. Patil and J. N, "Fog and Edge Computing: Bridging the Gap Between Cloud and IoT," 2025 International Conference on Frontier Technologies and Solutions (ICFTS), Chennai, India, 2025, pp. 1-7, https://doi.org/10.1109/ICFTS62006.2025.11031558.