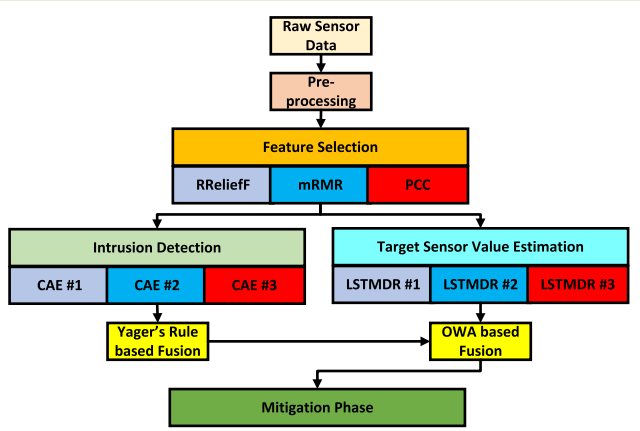
Sensor and Decision Fusion-Based Intrusion Detection and Mitigation Approach for Connected Autonomous Vehicles

Milad Moradi, *Member, IEEE*, Mojtaba Kordestani, *Senior Member, IEEE*, Mahsa Jalali, *Member, IEEE*, Milad Rezamand, Mehdi Mousavi, *Member, IEEE*, Ali Chaibakhsh, *Member, IEEE*, and Mehrdad Saif, *Fellow, IEEE*

***Abstract*—The safety of connected and autonomous vehicle (CAV) depends on the security of in-vehicle communication. The controller area network (CAN) bus holds a crucial position in ensuring in-vehicle security. Injecting attacks (e.g., increasing the speed) by hackers can affect drivers. This article proposes a fusion intrusion detection and resilient approach to maintain system performance against intrusion. The proposed system consists of two parts: sensor validation and sensor value estimation. In the sensor validation step, a new fusion approach uses three feature ranking approaches, autoencoder, and estimator-based detectors. Finally, Yager's rules are used to handle conflict between classifiers and enrich intrusion detection accuracy. Afterward, in the second part, if any intrusion is detected, the estimated values of that sensor which is under intrusion will be replaced based on estimated values by long short-term memory-based deep regressor (LSTMDR) to avoid any performance disruption of the system. The main contribution of this study is that the proposed fusion approach uses the inherent redundancy among heterogeneous sensors to create a resilient system against compromised sensors. Using Yager's rule and the ordered weighted average for information fusion significantly increases the reliability of intrusion detection systems and improves their detection rates. It also improves the performance of soft sensors and enhances the effectiveness of the mitigation phase. To evaluate the proposed approach, a real-world dataset entitled AEGIS—advanced big data value chain for public safety and personal security—is used. Test results indicate that the proposed fusion method is robust and reaches more accurate results compared with other detectors in three different considered attacks including replay, denial of service, and false data injection.**



***Index Terms*—Controller area network (CAN), information fusion, intrusion detection, resilient system, Yager's rule.**

NOMENCLATURE

1DCNN	1-D convolutional neural network.
AE	Absolute error.
Bi-LSTM	Bidirectional long short-term memory.
CAV	Connected and autonomous vehicle.
CAN	Controller area network.
CAEs	Convolutional autoencoders.
DST	Dempster–Shafer theory.
DoS	Denial of service.
ECUs	Electronic control units.
FAR	False alarm rate.
GPS	Global positioning system.
IMU	Inertial measurement unit.
IPAS	Intelligent park assist system.
ITSs	Intelligent transportation systems.
IDS	Intrusion detection system.
IVN	In-vehicle network.
LOF	Local outlier factor.

Manuscript received 29 March 2024; revised 27 April 2024; accepted 4 May 2024. Date of publication 17 May 2024; date of current version 1 July 2024. This work was supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada. The associate editor coordinating the review of this article and approving it for publication was Prof. Xintao Huan. *(Corresponding author: Mojtaba Kordestani.)*

Milad Moradi, Mojtaba Kordestani, Mahsa Jalali, Milad Rezamand, Mehdi Mousavi, and Mehrdad Saif are with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON N9B 3P4, Canada (e-mail: moradih@uwindsor.ca; kordest@uwindsor.ca; jalali3@uwindsor.ca; rezaman@uwindsor.ca; mousavi9@uwindsor.ca; msaif@uwindsor.ca).

Ali Chaibakhsh is with the Faculty of Mechanical Engineering, University of Guilan, Rasht 41996-13769, Iran (e-mail: chaibakhsh@guilan.ac.ir).

Digital Object Identifier 10.1109/JSEN.2024.3397966

LSTM	Long short-term memory.
LSTMDR	LSTM-based deep regressor.
MRMR	Minimum redundancy maximum relevance.
NN	Neural network.
OBD	On-board diagnostics.
OBUs	On-board units.
1-D	One-dimensional.
1-D Conv	1-D convolution.
OWA	Ordered weighted averaging.
PCC	Pearson correlation coefficient.
RNNs	Recurrent NNs.
RReliefF	Regressional ReliefF.
SVM	Support vector machine.

I. Introduction

CONNECTED and Autonomous Vehicles (CAVs) are known as a significant infrastructural advancement in the emerging smart world due to their real-time data transmission [1]. Some cases of CAVs' importance include their prominent role in increasing human satisfaction, decreasing the likelihood of accidents, and enhancing the effectiveness of ITSs [1]. In every vehicle, the CAN bus system acts as a fundamental mechanism for managing communication among ECUs. While the CAN bus system plays a significant role in modern automobiles, it lacks authentication and authorization mechanisms, resulting in the broadcast of messages without fundamental security features. Consequently, this vulnerability exposes it to potential attacks, making it susceptible to breach integrity, confidentiality, and availability [2].

A. Motivation

An attacker can spoof values in the CAN bus to establish incorrect or malicious behavior [3]. For instance, it can be mentioned that sending fake gear position values and speedometer on the CAN bus to trigger the IPAS to jump sporadically in the steering [3], [4]. Here, anomaly detection is defined as identifying data patterns that have a remarkable deviation from the expected behavior [5]. Hence, anomaly detection is a very important, yet essential task to detect abnormality and enhance the CAVs' reliability and security [6]. In this study, an object-oriented framework, including detection and mitigation system, is proposed to tackle this vulnerability.

B. Related Works

Hossain et al. [2] propose an intrusion detection approach using LSTM networks to identify cyber-attacks on the CAN bus. First, an attack-free dataset from an experimental car is extracted. Then, three attack types including DoS, fuzzing, and spoofing are injected into the dataset. Afterward, LSTM networks are used to detect attacks. Moreover, the best values for the hyperparameter are chosen by optimization to enhance detection accuracy. An LSTM network method is presented in [7] for a four-wheel robotic land vehicle. The results are compared with the conventional neural networks and show that higher accuracy is given by the LSTM networks.

Duan et al. [8] develop a cyber-attack detection method to diagnose data tampering attacks using anomaly score ranking and data mass through an improved isolation forest method. Using data mass in measuring local anomalies in this work leads to higher detection performance compared with other methods such as iForest, one-class SVM, and LOF. They also compare the proposed method with other anomaly detection approaches using two standard datasets and one in-vehicle simulated dataset.

He et al. [9] introduce a sensor fusion solution aimed at preventing the execution of unsafe actions by the controller due to noninvasive compromise of sensors and controller spoofing. This solution leverages the inherent redundancy among various sensors to identify abnormal sensor measurements and validate the accuracy of sensor data before the controller makes any decisions based on them. The core of this work revolves around using embedded redundancy within a deep autoencoder, with normal states serving as the benchmark for anomaly detection.

Integrated intrusion detection using LSTM and autoencoders is developed in [10]. Then, they show that the suggested approach reaches a higher accuracy in comparison to other deep learning networks. However, the integrated approach may need to be adapted to new environments.

The reviewed literature exhibits certain drawbacks that merit consideration. First, the heavy reliance on a sole source of raw data raises concerns about data availability and diversity, potentially limiting the system's ability to adapt to different scenarios and data sources. In addition, the overreliance on a single source of information and a solitary approach for anomaly detection may make the system vulnerable to evasion tactics used by sophisticated attackers not accounted for in its training data. Finally, the omission of proposals for defensive countermeasures leaves a critical gap in its comprehensive security strategy, potentially limiting its effectiveness in protecting against emerging threats.

C. Proposed Approach

This work proposes a new fusion approach based on sensor validation and sensor value estimation for intrusion detection and mitigation in CAVs. In the sensor validation, three feature selection methods, including minimum redundancy maximum relevance (MRMR), RReliefF, and PCC, are used to determine three different bunches of redundant heterogeneous sensors related to the goal sensor. Then, three CAEs are trained based on the top three obtained redundant heterogeneous sensors from each used method in the previous step. Afterward, Yager's rule as information fusion technique is used to reach a more reliable and robust intrusion detection. In the sensor value estimation phase, three deep regressors based on LSTM networks, referred to as LSTMDRs, are used to forecast the goal sensor's values before feeding to OWA as the second used fusion method.

The proposed method updates data sample-by-sample. This approach, in combination with deep CAE and LSTMDR, is crucial in real-time applications and eliminates the need for a fixed window size which is traditionally used. Moreover, this approach facilitates quicker response times to potential threats,

as it does not depend on the collection of a substantial dataset or window before initiating analysis.

D. Novelties

The main novelties are stated in the following.

1) To the best of our knowledge, this is the first time that a decision fusion approach is proposed using the Yager's rule method in the literature in this field to handle conflicts among intrusion detectors, which can enhance the robustness of the intrusion detection system and increase the cyber detection performance.
2) In addition, three distinct feature selection methods are proposed to improve the efficiency of data-driven models. These techniques address challenges such as managing multiple inputs and optimizing the selection of superior heterogeneous sensors from the initial and existing potential sensors. It reduces overfitting and enhances model generalization.
3) Distributing inputs across three sets of heterogeneous sensors makes it more challenging for attackers to compromise multiple heterogeneous sensors and enhances the system's resistance to evasion tactics.

Finally, a real-world dataset entitled AEGIS—advanced big data value chain for public safety and personal security—is used to validate the proposed intrusion detection and resilience approach. To achieve this goal, multiple replays, denial of service, and false data injection attacks are designed and implemented. The test results clearly show that the proposed fusion-based intrusion detection and resilience method is more accurate than each of the individually designed detectors.

E. Organization of This Article

The rest of this work is summarized as follows. Section II demonstrates material and methods. The experimental setup and analysis are illustrated in Section III. Section IV demonstrates results and discussion. Finally, the conclusion is given in Section V.

II. Material and Methods

A. CAN Bus

The CAN bus operates as a multi-leader, message broadcasting system, designed to function effectively in environments with high interference. CAN uses a "broadcast communication mechanism" focused on a message-based transmission approach that emphasizes the definition of message content over specifying nodes and their addresses [11]. Due to being a centralized system with a low cost, the CAN bus protocol is effective for vehicular networks. However, the CAN protocol has a security problem since nodes are all connected through the bus and take messages. CAN functions as a bus network that relies on broadcasting, and the exposure of internal data enables attackers to receive and assess the data of a targeted vehicle. Attackers, as shown in Fig. 1, can connect to the vehicles through various means, including the OBDs II port, wireless methods, or a hardwired connection [11]. A replayed message refers to a message that has been intercepted from a specific CAN bus segment or one that is already familiar.

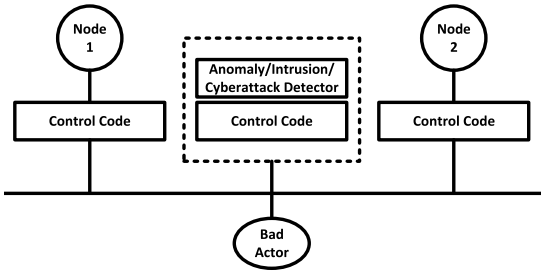


Fig. 1. Replay prevention and anomaly detection [11].

This message, containing both the arbitration identifier and data, can subsequently be used to fuzz the bus. It involves using the identifier and either sequentially cycling through the data or selecting data bits randomly [11].

B. Datasets

This study uses a research dataset called AEGIS—advanced big data value chain for public safety and personal security, which is specifically designed for the automotive domain. The dataset is part of the larger data [12] that has been supported by the European Union under Grant 732189. The dataset consists of time series data of three drivers operating the same vehicle in Austria. The AEGIS dataset, which encompasses numerous sensors, is used as a real-world dataset in this research. This dataset consists of 20-Hz sampled data from a passenger vehicle, e.g., wheel speed, accelerometer values, steer angle, and pitch. The GPS data are also included in the IMU [9].

Table I displays the sensor data used from the AEGIS dataset. It is important to emphasize that all the data included in the training set were collected during the vehicle's normal operational state.

C. Feature Reduction, Ranking, and Selection

The filter feature selection method relies on various metrics to assess the significance of features, regardless of the model used. It evaluates each feature based on its divergence or correlation and then sorts them by applying thresholds or specifying the desired number of features to be chosen [13]. In this study, we explore three feature ranking and selection methods using filter-based techniques. Continuing, a concise description of the used feature selection methods is provided.

1) *PCC:* Correlation analysis approach, such as PCC, is a common way to indicate a relationship among mathematical variables or measured data values. A static gain between -1 and $+1$ is used to show the amount of correlation between vectors X and Y as two considered variables. It is worth mentioning that the gain close to one shows a high correlation between two variables, while the gain near zero displays a weakly relationship [14].
2) *MRMR:* MRMR uses mutual information as its evaluation metric and strives to identify features that possess the highest relevance to the target variable while minimizing redundancy among them [15].

TABLE I
USED SENSOR DATA

Sensors On CAN bus		GPS Sensors	
1	Acceleration Slip Regulation	22	Current sec
2	Acceleration Pedal	23	Direction
3	Air Intake Temperature	24	Distance
4	Ambient Temperature	25	GPS fix quality
5	Boost Pressure	26	Latitude
6	Brk Voltage	27	Longitude
7	Engine Speed CAN	28	Velocity
8	Engine Temperature	IMU Sensors	
9	Kickdown	29	Accelerometer X
10	Misfiring System Tip Down	30	Accelerometer Y
11	Misfiring System Tip Up	31	Accelerometer Z
12	Steer Angle	32	Body acceleration X
13	TORQUE Friction Loss	33	Body acceleration Y
14	TORQUE Indicated	34	Body acceleration Z
15	Vehicle Speed	35	G force
16	Wheel Speed FL	36	Magnetometer X
17	Wheel Speed FR	37	Magnetometer Y
18	Wheel Speed RL	38	Magnetometer Z
19	Wheel Speed RR	39	Velocity X
20	Yaw rate	40	Velocity Y
GPS Sensors		41	Velocity Z
21	Acceleration		

3) *RReliefF:* RReliefF as an attribute ranking method ranks factors based on records and probability via the Bayes algorithm. Dealing with datasets of various classes and noise is known as this method's advantage. The RReliefF works based on feature evaluation by assigning a number to the feature to show the feature importance in the ranking [16].

D. Autoencoder

Autoencoders are known as feature extractors and are categorized as an NN model to construct a model with nonlabeled data. Autoencoder networks are versatile and applicable for anomaly detection in high-dimensional data across various data types, including images/videos, sequence data, and graph data [17].

1) Convolutional Autoencoder: The key advantage of 1DCNN, which is often used for analyzing 1-D signal data, lies in its ability to extract features from local segments of the signal at each network layer, rather than analyzing the signal as a whole. This localized analysis leads to more efficient network training by reducing the number of parameters that need to be learned [18], [19]. A CAE represents a unique variant of the autoencoder that excludes the use of fully connected neural layers. During the training phase, only normal data are used to train the CAE. The optimization process minimizes the average reconstruction error [20].

E. LSTM-Based Deep Regressor

LSTM is categorized as RNNs which due to persisting information for later use in the network are proper for temporal data analysis which changes over time [21]. The LSTM neural network amplifies its capability to extract features from time series data using threshold control mechanisms. The model undergoes training via backpropagation, where error terms are propagated through time and across the network layers, thereby significantly improving the model's capacity to handle nonlinear relationships [22].

F. Information Fusion

Generally, there are three levels in fusion approaches, which consist of data, feature, and decision level fusion. Each of them can be used for enhancing the accuracy of intrusion or fault detection [23].

1) Yager's Rule: For every piece of evidence, a mass function, which is also referred to as a basic probability assignment, is established and adheres to a specific axiom [24], [25]

$$\begin{aligned} m(\phi) &= 0 \\ m(A) &> 0 \quad \text{forall } A \in \Omega \\ \sum_{A \subseteq \Omega} m(A) &= 1. \end{aligned} \tag{1}$$

The third axiom, as presented in (1), associates unity with the sum of evidence attributed to every element within the set Ω. This leads to address ignorance directly [26]. In addition, the evidence mass allocated to a specific set is dedicated entirely to that set, rather than being distributed among the set's individual elements. Consequently, the belief function is identified as follows [24], [25]:

$$\text{Bel}(A) = \sum_{B \subseteq A} m(B). \tag{2}$$

In addition, a plausibility function is established to represent all the evidence that does not support the complement of evidence A [24], [25]

$$Pl(A) = 1 - \text{Bel}(\bar{A}) = \sum_{A \cap B \neq \emptyset} m(B). \tag{3}$$

Moreover, the Dempster rule of combination for integrating evidence can be used as follows [27]:

$$\begin{aligned} m_{1,2}(\emptyset) &= 0 \\ m_{1,2}(A) = (m_1 \oplus m_2)(A) &= \frac{1}{1-K} \sum_{B \cap C = A \neq \emptyset} m_1(B) m_2(C) \\ K &= \sum_{B \cap C = \emptyset} m_1(B) m_2(C). \end{aligned} \tag{4}$$

The conflict of evidence may occur in the Dempster rule, and therefore, Yager addresses this issue [25], [28]. In this approach, while the combination rule remains unchanged, the mass functions are modified in the following manner:

$$\begin{aligned} q(A) &= \sum_{\cap_{i=1}^{n} A_i = A} m_1(A_1) m_2(A_2), \ldots, m_n(A_n) \\ m^Y(X) &= q(X) + q(\emptyset). \end{aligned} \tag{5}$$

Because Yager's rule allocates a weight to each detector, it is more reliable than other fusion methods such as simple voting.

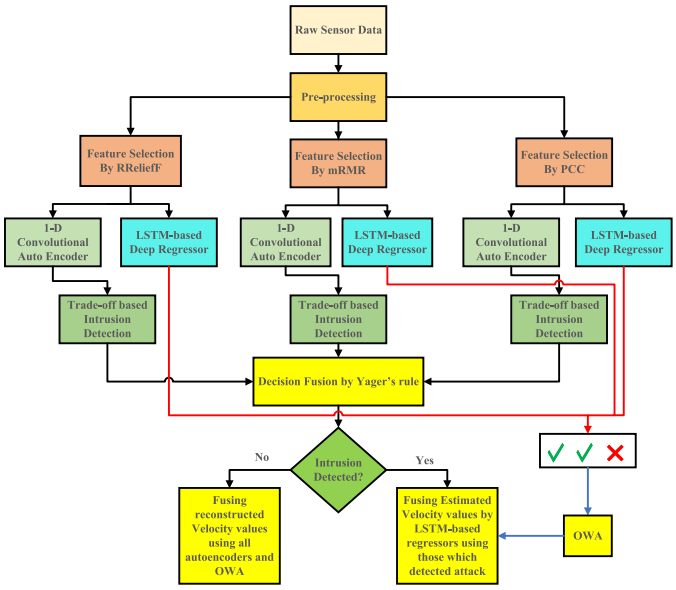


Fig. 2. Flowchart of the proposed attack resilient system, including detection and mitigation parts.

2) OWA Operator: The OWA operator assigns weights based on the order of values and allows a system to prioritize certain inputs over others irrespective of its source. An OWA operator with dimension n defines a function F: $R^n \rightarrow R$.. This function is characterized by a corresponding weight vector $W = (w_1, w2, \ldots, w_n)^T$, which must meet specific conditions [29]

$$F(a_1, \ldots, a_n) = \sum_{i=1}^{n} w_i b_i; \quad w_1 + w_2 + \cdots + w_n = 1$$
$$0 \leq w_i \leq 1, \quad i = 1, \ldots, n. \quad (6)$$

Here, b_i represents the ith largest value among $a_i, \ldots, a_n$. A key challenge in using the OWA operator is determining the appropriate weights. In this study, the gradient descent method is adopted for implementing the OWA operator.

III. Experimental Setup and Analysis

Fig. 2 illustrates the flowchart of the proposed scheme, which comprises two primary components: intrusion detection and the subsequent mitigation of intrusions through the estimation of the goal sensor's values that are affected by the intrusion or attack. The following sections provide a brief description of each of these components.

The proposed solution updates data sample-by-sample which makes it well-suited for real-time applications such as vehicle intrusion detection. The methodology involves an offline training phase where CAE and LSTM deep regressors are trained. The system then operates in real-time conditions using trained models and fusion logic to classify system conditions effectively.

A. Adversary Model

Replay and DoS attacks are common adversarial actions that are taken into account when developing an IDS, as discussed in [30], [31]. To implement and evaluate the proposed method, we use 9210 samples from the dataset for intrusion purposes. Specifically, we introduce nine distinct replay, denial of service, and false data injection attacks, totaling 927 samples for each one, which represent 10% of the entire used dataset. These attacks are applied to the normal values of the target sensor.

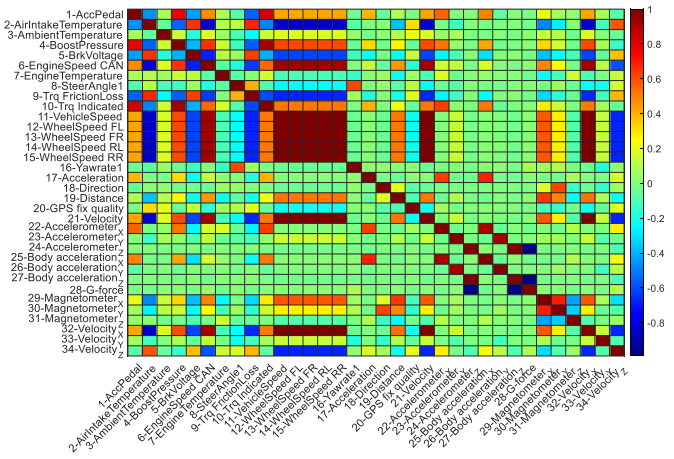


Fig. 3. PCC's analysis heatmap.

B. Preprocessing

The initial step involves rescaling the dataset to a range of [0, 1]. In addition, among the sensors listed in Table I, those with constant values of zero are removed, including rows #1, #9, #10, #11, #22, #26, and #27. Consequently, out of the original 41 sensors, only 34 remain in the dataset.

C. Feature Ranking and Selection

After the preprocessing step, each mentioned feature selection and ranking methods, including PCC, MRMR, and RReliefF, are applied to the remaining sensors to find the top redundant heterogeneous sensors related to the target sensor (velocity sensor in this case study). For example, Fig. 3 presents the heat map derived from the PCC analysis. Table II shows the result of different feature ranking and analysis methods in which the superior redundant heterogeneous sensors are put in order from top to bottom. It is worth mentioning that the reported weights have been normalized between 0 and 1 to get a better present and compare.

Furthermore, Fig. 4 presents a heatmap depicting the results obtained from all the used feature ranking methods. These results have been normalized to a range between 0 and 1, with the exception of the PCC results. In the case of PCC, its values have been mapped to the range [0.001, 1], rather than being normalized.

As previously mentioned, investigating redundant heterogeneous sensors is the goal of this step, so all redundant but not heterogeneous sensors are determined. Among the 34 remained sensors, those which are not heterogeneous with the target sensor (velocity sensor in this case) will not be entertained for the proposed scheme. These selected sensors are identified based on the information provided in Fig. 4 and Table II, and they include the following: 11—vehicle speed, 12—wheel speed FL, 13—wheel speed

TABLE II
IMPLEMENTATION RESULTS OF DIFFERENT FEATURE RANKING METHODS

	PCC		MRMR		RReliefF	
Rank	Weight	Sensor	Weight	Sensor	Weight	Sensor
1	1.00	21-Velocity	1.00	21-Velocity	1.00	21-Velocity
2	1.00	14-WheelSpeed RL	0.84	31-Magnetometer Z	0.98	11-VehicleSpeed
3	1.00	11-VehicleSpeed	0.84	28-G-force	0.98	13-WheelSpeed FR
4	1.00	12-WheelSpeed FL	0.84	34-Velocity Z	0.98	15-WheelSpeed RR
5	1.00	15-WheelSpeed RR	0.83	14-WheelSpeed RL	0.98	14-WheelSpeed RL
6	1.00	13-WheelSpeed FR	0.83	32-Velocity	0.98	12-WheelSpeed FL
7	1.00	32-Velocity	0.80	11-VehicleSpeed	0.95	32-Velocity
8	0.93	6-EngineSpeed CAN	0.80	15-WheelSpeed RR	0.67	6-EngineSpeed CAN
9	0.85	2-AirIntakeTemperature	0.78	12-WheelSpeed FL	0.38	25-Body acceleration X
10	0.68	34-Velocity Z	0.77	6-EngineSpeed CAN	0.34	2-AirIntakeTemperature
11	0.67	9-Trq FrictionLoss	0.76	26-Body acceleration Y	0.32	7-EngineTemperature
12	0.62	5-BrkVoltage	0.74	13-WheelSpeed FR	0.30	22-Accelerometer X
13	0.60	4-BoostPressure	0.70	3-AmbientTemperature	0.28	3-AmbientTemperature
14	0.57	29-Magnetometer	0.70	1-AccPedal	0.27	1-AccPedal
15	0.52	19-Distance	0.67	18-Direction	0.26	19-Distance
16	0.51	10-Trq Indicated	0.67	2-AirIntakeTemperature	0.24	4-BoostPressure
17	0.42	1-AccPedal	0.65	7-EngineTemperature	0.23	16-Yawrate1
18	0.28	30-Magnetometer Y	0.63	33-Velocity Y	0.18	34-Velocity Z
19	0.24	8-SteerAngle1	0.61	4-BoostPressure	0.16	9-Trq FrictionLoss
20	0.22	20-GPS fix quality	0.60	19-Distance	0.16	33-Velocity Y
21	0.18	3-AmbientTemperature	0.56	9-Trq FrictionLoss	0.14	29-Magnetometer
22	0.14	23-Accelerometer Y	0.53	16-Yawrate1	0.12	17-Acceleration
23	0.13	33-Velocity Y	0.51	25-Body acceleration X	0.12	26-Body acceleration Y
24	0.11	7-EngineTemperature	0.46	29-Magnetometer	0.12	10-Trq Indicated
25	0.09	31-Magnetometer Z	0.43	10-Trq Indicated	0.11	23-Accelerometer Y
26	0.04	16-Yawrate1	0.41	8-SteerAngle1	0.11	20-GPS fix quality
27	0.04	18-Direction	0.33	30-Magnetometer Y	0.08	30-Magnetometer
28	0.03	28-G-force	0.28	17-Acceleration	0.06	5-BrkVoltage
29	0.02	27-Body acceleration Z	0.23	23-Accelerometer Y	0.05	8-SteerAngle1
30	0.02	24-Accelerometer Z	0.20	20-GPS fix quality	0.05	18-Direction
31	0.01	17-Acceleration	0.18	5-BrkVoltage	0.02	27-Body acceleration Z
32	0.01	25-Body acceleration X	0.17	24-Accelerometer Z	0.02	24-Accelerometer Z
33	0.00	22-Accelerometer X	0.16	22-Accelerometer X	0.02	28-G-force
34	0.00	26-Body acceleration Y	0.00	27-Body acceleration Z	0.00	31-Magnetometer Z

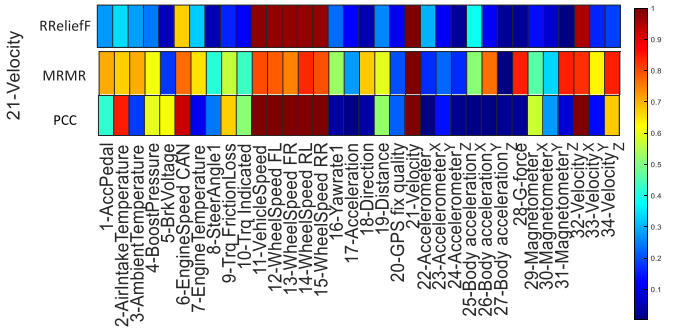


Fig. 4. Heatmap of the obtained results from each used feature ranking methods.

FR, 14—wheel speed RL, 15—wheel speed RR, 21—velocity, and 32—velocity X for elimination. These sensors are eliminated. Using three feature selection methods in the proposed structure improves detection accuracy and reduces overfitting and computational costs. By generating three unique input sets, the approach optimizes resource utilization and increases the effective anomaly detection rate, which enhances model generalization and interpretability. In addition, distributing inputs across three sets of heterogeneous sensors increases complexity for potential attackers and makes it challenging to compromise multiple sensors while reducing computational costs for health monitoring. It is worth mentioning that homogeneous sensors related to speed sensor can be quickly identified based solely on the labels in homogeneous conditions. However, the article considered heterogeneous conditions; therefore, feature selection is essential in detecting attacks.

D. CAE and Long Short-Term Memory Deep Regressor

In this section, we provide an overview of the implemented 1-D CAE.

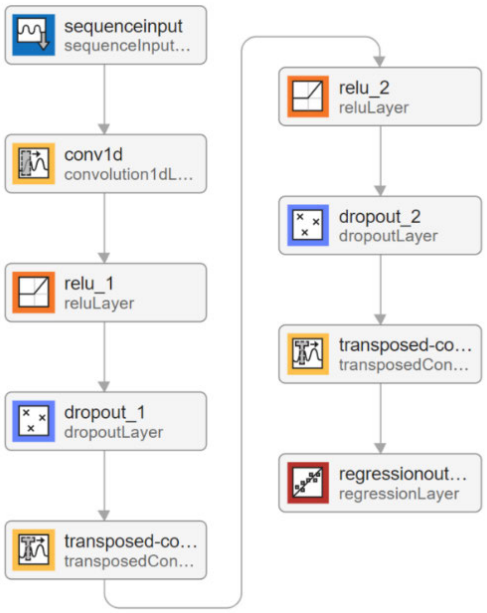


Fig. 5. Structure of used CAE for intrusion detection.

Fig. 5 illustrates the architecture of the 1-D CAE used in this study. This autoencoder, with consistent hyperparameters, is used to train all the three autoencoders. These autoencoders are trained using the selected redundant heterogeneous sensors, as determined by each feature ranking method, in addition to the velocity sensor as our considered target sensor. Table III displays the training options and filter configurations used for the CAEs.

To assess the performance of each trained deep CAE with varying numbers of top redundant heterogeneous sensors, ten repetitions of the training phase are conducted. The corresponding results are depicted in Fig. 6, which displays the performance of the three trained CAEs based on different sets of the top redundant heterogeneous sensors, ranging from two to seven sensors, in addition to the velocity sensor as target. As depicted in Fig. 6, when only two of the top redundant heterogeneous sensors are used in addition to the velocity sensor during deep CAE training, the CAE trained with the top two redundant heterogeneous sensors based on RReliefF demonstrates greater reliability compared with the others. However, as the number of redundant heterogeneous sensors used increases, deep autoencoders trained with the best features obtained through PCC exhibit enhanced reliability.

Moreover, the best trained models among the ten repetitions using different numbers of top obtained redundant heterogeneous sensors are extracted in Fig. 7. Although using a more accurate deep CAE is the preference, using more top redundant heterogeneous sensors leads to more robustness in the intrusion detection phase. Therefore, to have a tradeoff between these two criteria, those CAEs that have been trained by the top three redundant heterogeneous sensors are used for the next steps.

Fig. 8 and Table IV provide details regarding the configuration and hyperparameters used for the LSTMDR. In the second phase of the proposed approach, after an attack has

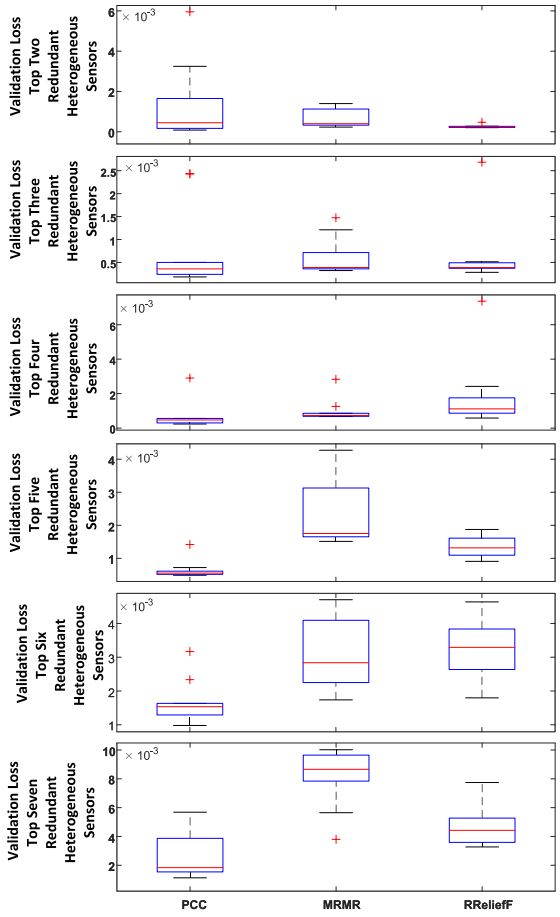


Fig. 6. Box plot of validation loss.

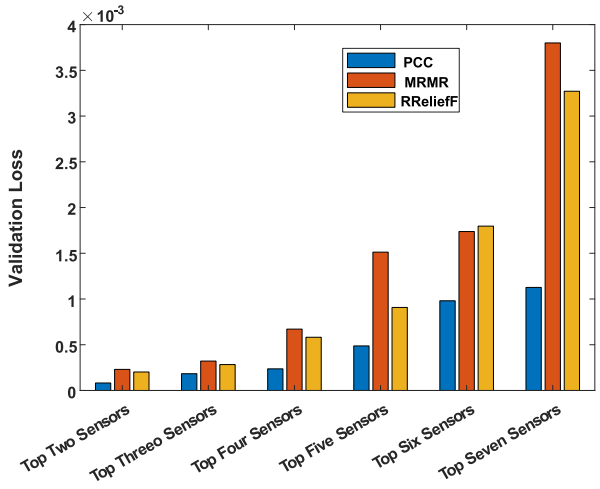


Fig. 7. Best trained models.

been detected through the CAE, the trained LSTMDR is used to estimate the values of the target sensor. This estimation is performed using the selected redundant heterogeneous sensor associated with it.

In addition, Fig. 9 displays the estimated values of the target sensor produced by each trained LSTMDR. These estimates are based on each trained LSTMDR that their inputs have been selected by each of the feature selection methods used in this study.

TABLE III
TRAINING OPTION AND USED FILTER CONFIGURATION FOR USED CAE

Optimizer	Adam
MaxEpochs	10000
MiniBatchSize	128
Outputnetwork	Best validation loss
FilterSize	7
NumFilters	16
DropoutProb	0.2

TABLE IV
CONSIDERED OPTION FOR USED LSTMDR TRAINING

optimizer	adam
MaxEpochs	3000
MiniBatchSize	128
outputnetwork	Best validation loss
InitialLearnRate	0.01
L2Regularization	1e-4

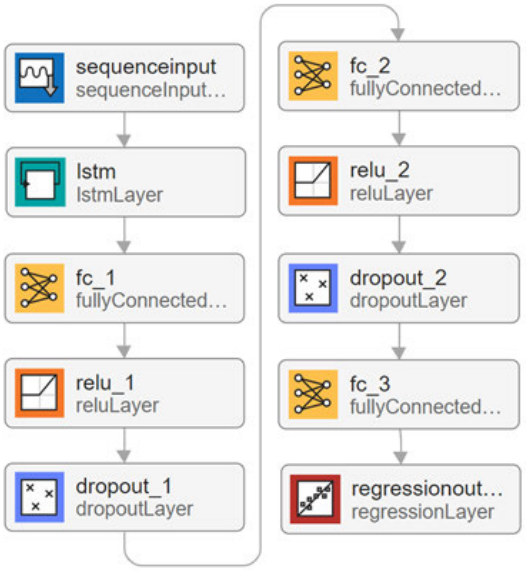


Fig. 8. Structure of the used LSTMDR for sensor value estimation phase.

Subsequently, to assess the performance of the proposed intrusion detector, various scenarios are examined in the following sections.

Scenarios: In this phase, to simulate a replay attack, we assume that the velocity sensor values have been tampered with by the attacker, who replaces them with their own previously recorded values. To achieve this, we use approximately 9210 data samples, with 10% of them (921 samples) having been substituted with the attacker's recorded values from earlier, as illustrated in Fig. 10.

E. Criterion Definition for Intrusion/Anomaly Detection

The proposed approach is analyzed in real-time conditions, and the results are indicated in Figs. 11 and 12 for the replay attack case. In addition, the article uses three

TABLE V
COMPARISON BETWEEN DIFFERENT INTRUSION DETECTORS AND THEIR FUSION RESULT

Detection Method	Attack	Feature Selection Method	Selected AE Threshold	Accuracy	Precision	Recall	F1 Score	FAR
CAE	Replay	PCC	0.0140	0.9797	0.8996	0.8986	0.8991	0.0112
		MRMR	0.0169	0.9747	0.8747	0.8738	0.8743	0.014
		RReliefF	0.0133	0.9849	0.9292	0.9202	0.9247	0.0078
		Fusion	**-**	**0.9900**	**1**	**0.9008**	**0.9478**	**0**
	DoS	PCC	0.0297	0.984	0.8631	1	0.9265	0.0177
		MRMR	0.0323	0.982	0.8481	1	0.9178	0.02
		RReliefF	0.0239	0.984	0.8631	1	0.9265	0.0177
		Fusion	**-**	**0.984**	**1**	**1**	**0.9265**	**0.0177**
	False Data Injection	PCC	0.0257	0.987	0.9343	0.9364	0.9353	0.0074
		MRMR	0.0259	0.9888	0.9213	0.972	0.9459	0.0093
		RReliefF	0.0177	0.9502	0.8162	0.6516	0.7247	0.0164
		Fusion	**-**	**0.989**	**1**	**0.9558**	**0.9461**	**0.0072**
LSTM	Replay	PCC	0.0188	0.9579	0.7926	0.7875	0.79	0.0231
		MRMR	0.0154	0.9596	0.8	0.7983	0.7991	0.0223
		RReliefF	0.0117	0.9742	0.8716	0.8716	0.8716	0.0144
		Fusion	**-**	**0.9796**	**1**	**0.8166**	**0.8895**	**0.0022**
	DoS	PCC	0.0159	0.9632	0.7322	1	0.8454	0.0409
		MRMR	0.0145	0.9693	0.7661	1	0.8676	0.0342
		RReliefF	0.0102	0.9568	0.6996	1	0.8233	0.0481
		Fusion	**-**	**0.995**	**1**	**1**	**0.9758**	**0.0056**
	False Data Injection	PCC	0.0159	0.9632	0.7322	1	0.8454	0.0409
		MRMR	0.0142	0.9643	0.7381	1	0.8493	0.0397
		RReliefF	0.0141	0.9959	0.9606	1	0.9799	0.0046
		Fusion	**0**	**0.9993**	**1**	**1**	**0.9968**	**0.0007**

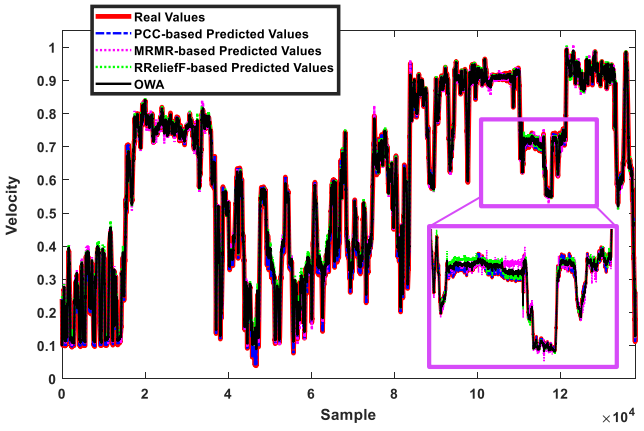


Fig. 9. Estimated values of velocity sensor.

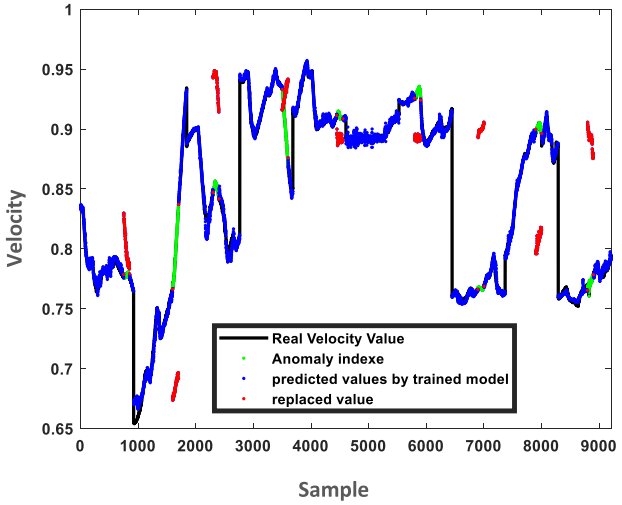


Fig. 10. Demonstration of real, estimated, and anomalous data for the replay attack scenario.

different intrusion detectors, each associated with a distinct set of selected sensors, and uses the same CAE, to make a fusion-based intrusion detector. A comprehensive comparison of these three intrusion detectors and the proposed fusion approach is presented in Table V, Figs. 11, and 12. It is worth mentioning that the same strategies have been used for denial of service and false data injection attacks too. Finally, all the mentioned scenarios for CAE evaluation are used for designed LSTM-based deep regressors as another considered intrusion detectors. To establish a criterion for intrusion detection, the AE between the input sequence and the reconstructed sequence generated by each CAE is calculated. As a criterion for intrusion detection, the maximum AE between the real velocity values and its estimated values by CAE is used as the initial baseline to set a reasonable margin for intrusion detection. The error histogram of this step for each CAE via the top three redundant heterogeneous sensors is shown in Fig. 11. The red dashed line shows the initial baseline AE value.

This value can serve as a reference point for establishing a threshold in the intrusion detection phase. However, for a more comprehensive evaluation, we explore various thresholds for each of the three CAEs. To achieve this, we use several metrics, including the FAR, accuracy, $F1$-score, precision, and recall, to assess performance [32], [33]. Fig. 12 displays the effect of applying different thresholds and margins for

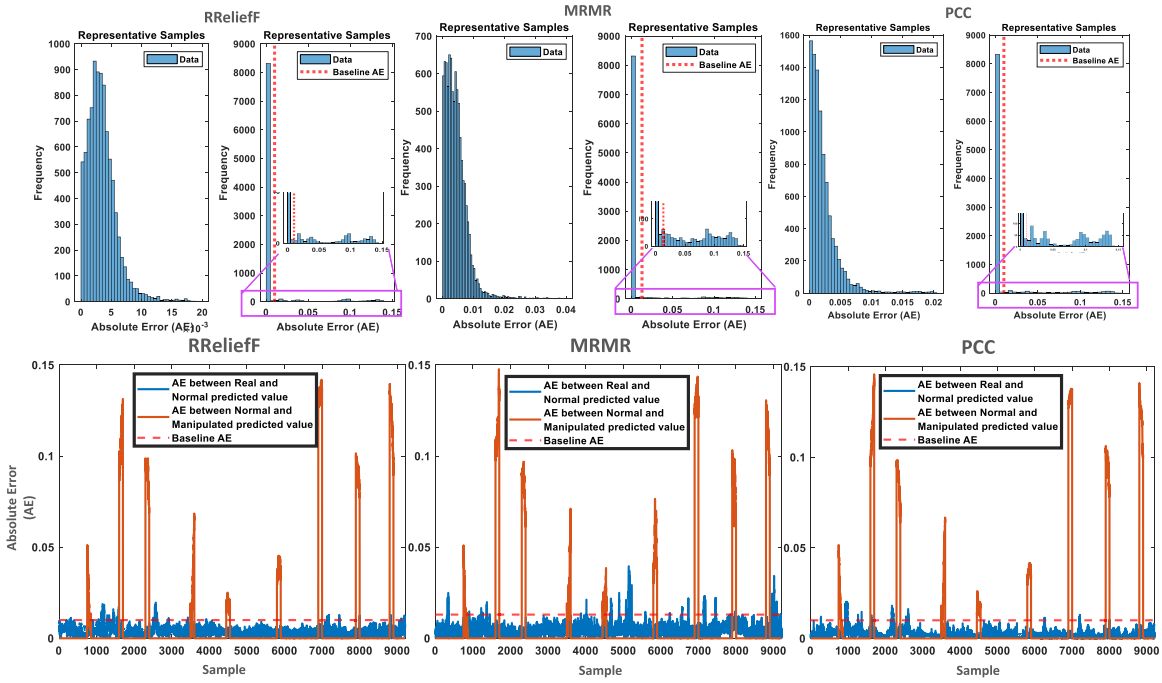


Fig. 11. Error histogram of AE in the validation step.

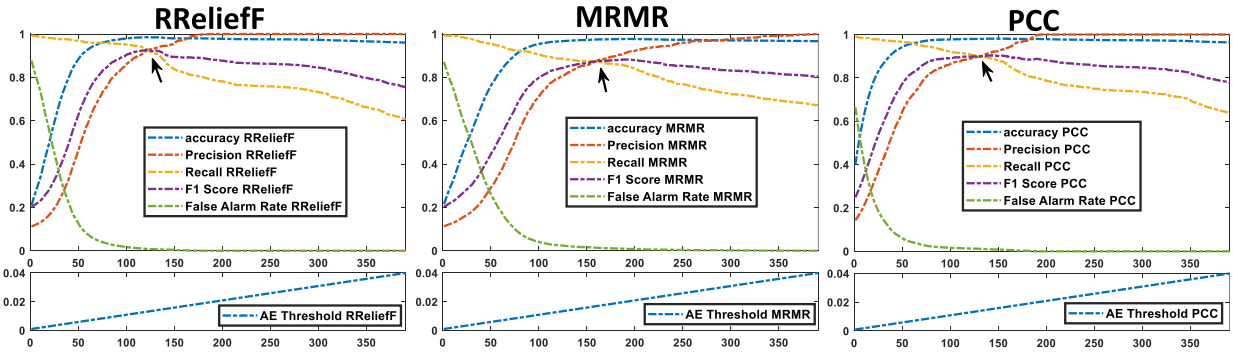


Fig. 12. Different threshold and their effects' evaluation on intrusion detector's metrics.

intrusion detection by autoencoders. The threshold range from 0.001 to 0.4 is investigated and performance metrics are evaluated in this range. Using Fig. 12, a threshold value that leads to a tradeoff between all the metrics is selected, which is shown by a black arrow.

Table V reveals the obtained results via the selected threshold, considering the tradeoff between all the metrics. Moreover, Table VI compares the results from two other studies in the literature on the same dataset with the best results obtained in this study.

F. Decision Fusion by Yager's Rule

After training the CAEs, each one exhibits its own unique performance, leading to the following scenarios for the three intrusion detectors.

1) *Scenario 1:* Three detectors show that the system works in a normal condition.
2) *Scenario 2:* Three detectors indicate that the system works in an abnormal condition.
3) *Scenario 3:* Three detectors do not act in the same way and state various conditions. Therefore, the final decision is obtained by the fusion approach via Yager's rule through a conflict of evidence at the decision level.

TABLE VI
COMPARING VARIOUS IDSS USING IDENTICAL DATASETS ACROSS LITERATURE

Reference	Attack	Detection method	Accuracy	Precision	Recall
[34]	Replay	LSTM	0.837	0.816	0.351
		MLP	0.823	0.732	0.329
		SVM	0.775	0.498	0.410
		XGBoost	0.776	0.504	0.800
		KNN	0.717	0.268	0.152
		NB	0.600	0.177	0.216
		RF	0.738	0.146	0.035
	False Data Injection (Amp.shift)	LSTM	0.838	0.812	0.595
		MLP	0.767	0.654	0.463
		SVM	0.727	0.557	0.425
		XGBoost	0.689	0.467	0.284
		NB	0.542	0.309	0.433
		RF	0.650	0.352	0.203
		KNN	0.620	0.304	0.200
[35]	Replay	LSTM	0.8370	-	-
		MLP	0.8230	-	-
	False Data Injection (Amp.shift)	LSTM	0.8380	-	-
		MLP	0.7870	-	-
The proposed method	**Replay**	**CAE**	**0.9900**	**1**	**0.9008**
		LSTM	**0.9796**	**1**	**0.8166**
	DoS	**CAE**	**0.9840**	**1**	**1**
		LSTM	**0.9950**	**1**	**1**
	False Data Injection	**CAE**	**0.9890**	**1**	**0.9558**
		LSTM	**0.9993**	**1**	**1**

Table VII presents various possible scenarios for arriving at a final detection by using all the three intrusion detectors.

TABLE VII
RESULT OF YAGER'S RULE IMPLEMENTATION IN CASE OF COMBINATION OF DIFFERENT POSSIBLE SCENARIOS

RReliefF		MRMR		PCC		Final Result		Ignorance Factor	Alarm
Normal	Abnormal	Normal	Abnormal	Normal	Abnormal	Normal	Abnormal		
1	0	1	0	1	0	0.9985	0	0.0015	0
1	0	0	1	1	0	0.9369	0.0536	0.0095	0
1	0	1	0	0	1	0.8678	0.1189	0.0132	0
1	0	0	1	0	1	0.1189	0.8678	0.0132	1
0	1	1	0	1	0	0.8678	0.1189	0.0132	0
0	1	1	0	0	1	0.0536	0.9369	0.0095	1
0	1	0	1	1	0	0.1189	0.8678	0.0132	1
0	1	0	1	0	1	0	0.9985	0.0015	1

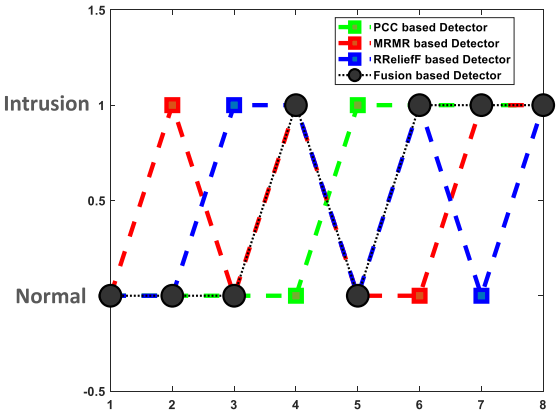


Fig. 13. Result of fusion implementation.

In this representation, normal sequences are denoted by "0" and abnormal ones by "+1." In addition, Fig. 13 provides a visual representation of the ultimate results following the application of decision fusion using Yager's rule.

Finally, upon detecting any intrusion using the detectors through the three used feature ranking methods, the LSTMDRs are deployed to estimate the velocity values during the intrusion. To enhance the robustness of the reconstructed values, we use the OWA operator to calculate the weight for each LSTMDR.

IV. RESULTS AND DISCUSSIONS

In this section, test result discussions focusing on Table V and Fig. 12 are demonstrated. First, as it is clear from Fig. 12, changing the threshold value plays a prominent role in all the metrics for performance evaluation. Therefore, in the first step, a threshold, which is a tradeoff between different metrics, is determined. Then, to evaluate the effect of the proposed fusion approach, the selected tradeoff points from each of these three feature selection methods which are shown by a black arrow in Fig. 12 are fused by Yager's rule.

To analyze the efficiency of the proposed method, other types of attacks including denial of service and false data injection are considered. Moreover, the trained LSTMDR is used as the second methodology for intrusion detection. Table V indicates the results. According to the table, in some cases, the individual methods may have a better performance in a single criterion. For example, MRMR has a higher recall rate in false injection conditions using the CAE method. However, it is important to note that the presented fusion approach overall has a better performance considering all the isolation criteria. In addition, a comparison between the obtained results from the proposed method compared with the traditional methods in other literature is presented in Table VI. According to the table, the proposed method in this article is more efficient in attack isolation in comparison to other techniques.

V. CONCLUSION

In this study, an object-oriented framework based on feature ranking, autoencoders, LSTM deep regressor, and fusion was introduced for intrusion detection and mitigation of CAVs. For this aim, three feature rankings, including PCC, MRMR, and RReliefF, were applied to determine the purest redundant heterogeneous sensors related to the target sensor. Then, three 1-D CAEs and LSTMDR networks, which were trained via three top redundant homogeneous sensors, were used for the detection and estimation phases, respectively. Moreover, information fusions were used to handle conflicts between intrusion detectors and enhance intrusion detection performance.

REFERENCES

[1] A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan, and M. S. Haghighi, "Anomaly detection in automated vehicles using multistage attention-based convolutional neural network," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4291–4300, Jul. 2021.

[2] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, "LSTM-based intrusion detection system for in-vehicle can bus communications," *IEEE Access*, vol. 8, pp. 185489–185502, 2020.

[3] A. Ganesan, J. Rao, and K. Shin, "Exploiting consistency among heterogeneous sensors for vehicle anomaly detection," SAE Tech. Paper 2017-01-1654, 2017.

[4] C. Miller and C. Valasek, "Adventures in automotive networks and control units," *Def. Con.*, vol. 21, nos. 260–264, pp. 15–31, 2013.

[5] L. Erhan et al., "Smart anomaly detection in sensor systems: A multi-perspective review," *Inf. Fusion*, vol. 67, pp. 64–79, Mar. 2021.

[6] T. Hickling, N. Aouf, and P. Spencer, "Robust adversarial attacks detection based on explainable deep reinforcement learning for UAV guidance and planning," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 10, pp. 4381–4394, Oct. 2023.

[7] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2017.

[8] X. Duan, H. Yan, D. Tian, J. Zhou, J. Su, and W. Hao, "In-vehicle CAN bus tampering attacks detection for connected and autonomous vehicles using an improved isolation forest method," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2122–2134, Feb. 2023.

[9] T. He, L. Zhang, F. Kong, and A. Salekin, "Exploring inherent sensor redundancy for automotive anomaly detection," in *Proc. 57th ACM/IEEE Design Autom. Conf. (DAC)*, Jul. 2020, pp. 1–6.

[10] V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim, "A novel two-stage deep learning model for network intrusion detection: LSTM-AE," *IEEE Access*, vol. 11, pp. 37131–37148, 2023.

[11] S. Abbott-McCune and L. A. Shay, "Intrusion prevention system of automotive network CAN bus," in *Proc. IEEE Int. Carnahan Conf. Security Technol. (ICCST)*, Mar. 2016, pp. 1–8.

[12] C. Kaiser, A. Stocker, and A. Festl, "Automotive can bus data: An example dataset from the aegis big data project," openAIRE, Tech. Rep., 2019.

[13] L. Zhang, Z. Xue, H. Liu, and H. Li, "Enhanced generalized regression neural network with backward sequential feature selection for machine-learning-driven soil moisture estimation: A case study over the qinghai-tibet Plateau," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 16, pp. 7173–7185, 2023.

[14] M. Radman, M. Moradi, A. Chaibakhsh, M. Kordestani, and M. Saif, "Multi-feature fusion approach for epileptic seizure detection from EEG signals," *IEEE Sensors J.*, vol. 21, no. 3, pp. 3533–3543, Feb. 2021.

[15] J. Wang, P. Xu, X. Ji, M. Li, and W. Lu, "Feature selection in machine learning for perovskite materials design and discovery," *Materials*, vol. 16, no. 8, p. 3134, Apr. 2023.

[16] W. Anggraeni, A. A. Wicaksono, E. M. Yuniarno, R. F. Rachmadi, S. Sumpeno, and M. H. Purnomo, "Multilevel analysis of temporal-based spatial factors impact in dengue fever forecasting using RReliefF—Deep learning," in *Proc. IEEE Int. Conf. Imag. Syst. Techn. (IST)*, Jun. 2022, pp. 1–6.

[17] N. Alkhatib, M. Mushtaq, H. Ghauch, and J.-L. Danger, "Unsupervised network intrusion detection system for AVTP in automotive Ethernet networks," in *Proc. IEEE Intelligent Vehicles Symp. (IV)*, Jun. 2022, pp. 1731–1738.

[18] T. Çavdar, N. Ebrahimpour, M. T. Kakiz, and F. B. Günay, "Decision-making for the anomalies in IIoTs based on 1D convolutional neural networks and Dempster–Shafer theory (DS-1DCNN)," *J. Supercomput.*, vol. 79, no. 2, pp. 1683–1704, Feb. 2023.

[19] F. Van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 1264–1276, Apr. 2019.

[20] Z. Chen, C. K. Yeo, B. S. Lee, and C. T. Lau, "Autoencoder-based network anomaly detection," in *Proc. Wireless Telecommun. Symp. (WTS)*, Apr. 2018, pp. 1–5.

[21] K. Zhu, Z. Chen, Y. Peng, and L. Zhang, "Mobile edge assisted literal multi-dimensional anomaly detection of in-vehicle network using LSTM," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4275–4284, May 2019.

[22] H. Pan, T. Su, X. Huang, and Z. Wang, "LSTM-based soft sensor design for oxygen content of flue gas in coal-fired power plant," *Trans. Inst. Meas. Control*, vol. 43, no. 1, pp. 78–87, Jan. 2021.

[23] M. Safizadeh and S. Latifi, "Using multi-sensor data fusion for vibration fault diagnosis of rolling element bearings by accelerometer and load cell," *Inf. Fusion*, vol. 18, pp. 1–8, Jul. 2014.

[24] G. Shafer, *A Mathematical Theory of Evidence*, vol. 42. Princeton, NJ, USA: Princeton Univ. Press, 1976.

[25] A. Iranfar, M. Soleymannejad, B. Moshiri, and H. D. Taghirad, "A modified Dempster Shafer approach to classification in surgical skill assessment," in *Proc. 31st Int. Conf. Electr. Eng. (ICEE)*, May 2023, pp. 820–825.

[26] M. Liggins II, D. Hall, and J. Llinas, *Handbook of Multisensor Data Fusion: Theory and Practice*. Boca Raton, FL, USA: CRC Press, 2017.

[27] A. P. Dempster, "A generalization of Bayesian inference," *J. Roy. Stat. Soc. B, Methodol.*, vol. 30, no. 2, pp. 205–232, 1968.

[28] R. R. Yager, "On the Dempster–Shafer framework and new combination rules," *Inf. Sci.*, vol. 41, no. 2, pp. 93–137, Mar. 1987.

[29] S. Soltani, M. Kordestani, P. K. Aghaee, and M. Saif, "Improved estimation for well-logging problems based on fusion of four types of Kalman filters," *IEEE Trans. Geosci. Remote Sens.*, vol. 56, no. 2, pp. 647–654, Feb. 2018.

[30] C. Jichici, B. Groza, R. Ragobete, P.-S. Murvay, and T. Andreica, "Effective intrusion detection and prevention for the commercial vehicle SAE J1939 CAN bus," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 17425–17439, Oct. 2022.

[31] R. Islam, R. U. D. Refat, S. M. Yerram, and H. Malik, "Graph-based intrusion detection system for controller area networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 1727–1736, Mar. 2020.

[32] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, "Multi-stage optimized machine learning framework for network intrusion detection," *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 2, pp. 1803–1816, Jun. 2021.

[33] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A multitiered hybrid intrusion detection system for Internet of Vehicles," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 616–632, Jan. 2022.

[34] Z. Khan, M. Chowdhury, M. Islam, C.-Y. Huang, and M. Rahman, "Long short-term memory neural network-based attack detection model for in-vehicle network security," *IEEE Sensors Lett.*, vol. 4, no. 6, pp. 1–4, Jun. 2020.

[35] M. Z. Khan, "Security and reliability of vehicular networks and autonomous vehicle applications using artificial intelligence and edge computing in a cyber-physical systems environment," Ph.D. dissertation, Clemson Univ., 2021.

Milad Moradi (Member, IEEE) received the bachelor's and master's degrees from the University of Guilan, Rasht, Iran, in 2013 and 2016, respectively. He is currently pursuing the Ph.D. degree in electrical engineering with the University of Windsor, Windsor, ON, Canada.

Following the completion of the master's degree, he was honored with a prestigious award from Iran's National Elites Foundation. He serves as a Research Assistant with the Laboratory for Autonomous Resilient Systems (LARS). His research interests include a wide range of fields, including deep and machine learning, condition monitoring, data-driven fault diagnosis, data mining, optimization, and their practical applications in the realms of power systems and biomedical engineering.

Mojtaba Kordestani (Senior Member, IEEE) received the bachelor's degree in electronic engineering from Malek Ashtar University, Tehran, Iran, in 2002, the master's degree in control engineering from Tehran Azad University, Tehran, in 2008, and the Ph.D. degree in electrical engineering from the University of Windsor, Windsor, ON, Canada, in 2018.

He worked as a Postdoctoral Fellow with the University of Windsor, from 2018 to 2021, and Concordia University, Montreal, QC, Canada, in 2021. His research interests include control, estimation, and observer theory, fault diagnostics and fault-tolerant control, and predictive control. He has published more than 50 refereed journal articles and conference papers in these areas.

Dr. Kordestani was a recipient of the Full Research Scholarship from the University of Windsor, in 2015. He won the Ontario Graduate Scholarship (OGS), in 2017. He was the IEEE Chair of the Young Professional Group, University of Windsor, from 2016 to 2018. He serves as the Vice-Chair and the Chair for IEEE Windsor Section from 2019 to 2020.

Mahsa Jalali (Member, IEEE) received the B.Sc. degree in robotics engineering from Shahrood University of Technology, Semnan, Iran, and the M.Sc. degree in mechatronics engineering from Islamic Azad University, Science and Research Branch, Tehran, Iran, in 2008 and 2011, respectively. She is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON, Canada.

Her current research interests include connected autonomous vehicle, diagnosis fault, control system, and machine learning methods.

Milad Rezamand received the bachelor's degree in mechanical engineering from Bahonar University, Kerman, Iran, in 2008, the master's degree in aerospace engineering from K.N.T University of Technology, Tehran, Iran, in 2012, and the Ph.D. degree in mechanical engineering from the University of Windsor, Windsor, ON, Canada, in 2019.

He is a Professor of Marketing Research and Analytics and Business Analytics and Insights with the School of Business, Centennial College, ON, Canada. His research interests include applying machine and deep learning to practical real-world applications.

Mehdi Mousavi (Member, IEEE) received the B.Sc. and M.Sc. degrees in mechanical engineering from the University of Guilan, Rasht, Iran, in 2013 and 2017, respectively. He is currently pursuing the Ph.D. degree in electrical engineering with the University of Windsor, Windsor, ON, Canada.

He was a Member of the Intelligent System and Advanced Control Laboratory (ISACLAB), University of Guilan, from 2016 to 2020. His research interests include machine learning, fault prognosis, and fault-tolerant control.

Ali Chaibakhsh (Member, IEEE) received the B.Sc. degree from the University of Guilan, Rasht, Iran, in 2002, and the M.Sc. and Ph.D. degrees in mechanical engineering from the K.N. Toosi University of Technology, Tehran, Iran, in 2004 and 2009, respectively.

He is an Associate Professor of mechanical engineering with industrial and academic research backgrounds in process control and instrumentation. His research interests include intelligent systems' design and their applications in industrial process systems.

Mehrdad Saif (Fellow, IEEE) received the B.S., M.S., and D.Eng. degrees in electrical engineering from Cleveland State University, Cleveland, OH, USA, in 1982, 1984, and 1987, respectively.

In 1987, he joined the School of Engineering Science, Simon Fraser University, Burnaby, BC, Canada. From 2011 to 2022, he was the Dean of the Faculty of Engineering, University of Windsor, Windsor, ON, Canada, where he oversaw major growth. His research interests include systems and control, estimation and observer theory, model-based fault diagnostics, condition monitoring, diagnostics, and prognostic, and application of these areas to automotive, power, autonomous systems, and other complex engineering systems. He has published more than 400 refereed journal articles and conference papers plus an edited book in these areas.

Dr. Saif is a Fellow of the Institution of Engineering and Technology (IET), the Engineering Institute of Canada (EIC), and the Canadian Academy of Engineering (CAE).