Many-Objective Optimization Based Intrusion Detection for In-Vehicle Network Security

Jiangjiang Zhang, Bei Gong, Muhammad Waqas, *Senior Member, IEEE*, Shanshan Tu, *Member, IEEE*, and Sheng Chen, *Fellow, IEEE*

***Abstract*— In-vehicle network security plays a vital role in ensuring the secure information transfer between vehicle and Internet. The existing research is still facing great difficulties in balancing the conflicting factors for the in-vehicle network security and hence to improve intrusion detection performance. To challenge this issue, we construct a many-objective intrusion detection model by including information entropy, accuracy, false positive rate and response time of anomaly detection as the four objectives, which represent the key factors influencing intrusion detection performance. We then design an improved intrusion detection algorithm based on many-objective optimization to optimize the detection model parameters. The designed algorithm has double evolutionary selections. Specifically, an improved differential evolutionary operator produces new offspring of the internal population, and a spherical pruning mechanism selects the excellent internal solutions to form the selected pool of the external archive. The second evolutionary selection then produces new offspring of the archive, and an archive selection mechanism of the external archive selects and stores the optimal solutions in the whole detection process. An experiment is performed using a real-world in-vehicle network data set to verify the performance of our proposed model and algorithm. Experimental results obtained demonstrate that our algorithm can respond quickly to attacks and achieve high entropy and detection accuracy as well as very low false positive rate with a good trade-off in the conflicting objective landscape.**

***Index Terms*— Many-objective optimization, intrusion detection, information entropy, in-vehicle network.**

I. Introduction

With the rapid development of vehicle communication technology and computer network, in-vehicle information system [1] is widely deployed on vehicles with abundant applications, including intelligent navigation and intelligent parking [2]. In-vehicle network is an automobile internal data interaction network composed of electronic control unit (ECU) and communication bus, which integrates computer network, communication, electronics and other technologies [3], [4]. These system applications require various vehicle external interfaces, which also increase the attack path of hackers. Therefore, it is very necessary to install intrusion detection system (IDS) to ensure the safety of in-vehicle network [5]. IDS monitors the system and network transmission in real time. It determines whether there is abnormal behavior by collecting and analyzing the security log, audit data and other available key point information in the whole communication network [6]. If abnormal behavior is found, the system will send an alarm or take other relevant defense measures. Different from the traditional network security technology, IDS is an active security defense technology [7]. As the most widely used in-vehicle bus in automobile, vehicle controller area network (CAN) bus is liable to many types of attacks. Without the relevant information security mechanism and protection means in the in-vehicle CAN bus network, any in-vehicle ECU in the network may access other in-vehicle ECUs on CAN bus, and the attacker may modify the source code of any ECU to achieve the vehicle full control, which can seriously threaten the driving safety of vehicles [8]. Therefore, the research on CAN bus data anomaly detection is critical.

Recently, researchers have proposed a variety of intrusion detection methods for CAN bus attacks [9]. Javed et al. [10] provided a novel approach based on convolutional attention incorporated with gated recurrent neural network to improve the accuracy of detecting CAN bus attacks. Yu and Wang [11] presented an intrusion detection method based on network topology verification to improve the security of CAN bus network. Olufowobi et al. [7] described a method for extracting real-time model parameters from observations of CAN bus and presented an IDS based on CAN bus real-time scheduling capability and response time analysis. Derhab et al. [12] designed an intrusion detection and filtering framework based on histogram. It assembles CAN packets into windows and calculates their corresponding histograms, which are used to assist multi-class classifier to identify and filter the normal CAN packets in the malicious traffic window. Choi et al. [6] implemented an IDS mechanism that can monitor information transmission in real time to protect the security of the CAN bus. This IDS mechanism can detect the malicious CAN bus messages that are transmitted in the in-vehicle network with

Manuscript received 6 February 2023; revised 31 May 2023; accepted 12 July 2023. Date of publication 25 July 2023; date of current version 29 November 2023. This work was supported in part by the National Key Research and Development Project of China under Grant 2019YFB2102300 and in part by the National Natural Science Foundation of China under Grant 61971014. The Associate Editor for this article was M. Bilal. *(Corresponding author: Muhammad Waqas.)*

Jiangjiang Zhang, Bei Gong, and Shanshan Tu are with the Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China (e-mail: zhangjiangjiang@emails.bjut.edu.cn; gongbei@bjut.edu.cn; sstu@bjut.edu.cn).

Muhammad Waqas is with the Department of Computer Engineering, Faculty of Information Technology, University of Bahrain, Sakhir 32038, Bahrain, and also with the School of Engineering, Edith Cowan University, Perth, WA 6027, Australia (e-mail: engr.waqas2079@gmail.com).

Sheng Chen is with the School of Electronics and Computer Science, University of Southampton, SO17 1BJ Southampton, U.K. (e-mail: sqc@ecs.soton.ac.uk).

Digital Object Identifier 10.1109/TITS.2023.3296002

high accuracy according to the difficult forgery of electrical characteristics. Ying et al. [13] developed a vehicle intelligent decision support system based on clock deviation for CAN bus data to predict stealth attacks. Groza and Murvay [14] proposed an intrusion detection mechanism based on CAN bus data using Bloom filtering to help improve the accuracy of detecting potential replay or modification attacks.

However, these existing detection methods only target on one or few individual detection performance indicators, such as accuracy, false positive rate and response time, and rarely they address all the major factors that impact on the detection performance [15]. In fact, the factors affecting the intrusion detection performance of the CAN bus data for in-vehicle network security come from many aspects [16]. Moreover, these factors are inextricably linked and they influence each other [17]. Therefore, there exist multiple conflicting detection performance metrics. Generally, the shorter the response time of detection, the poorer the detection accuracy and the false positive rate may increase. On the other hand, lower the real-time requirements allows the IDS with more detection time to improve the accuracy [15], [18]. How to comprehensively address the impact of these factors on CAN bus data intrusion detection performance and effectively balance the conflicting metrics is very challenging. Meanwhile, the multi knowledge fusion decision-making learning usually shows better detected intrusion behavior performance than individual learning, which can make the learning mechanisms with different abilities support each other, improve the reliability of prediction and reduce the risk of classification errors [17]. Implementing multi knowledge fusion is of great significance for improving correct classification and accurately identifying intrusion behavior performance, which motivates our work.

Against this background, in this paper we formulate the in-vehicle bus data of CAN anomaly detection problem as a complex many-objective optimization problem (MaOP) [17]. The main contributions of this paper are listed as follows.

1) Considering that the vehicle is affected by many uncertain factors, the information entropy theory is applied [18]. A many-objective CAN bus data anomaly detection optimization model is built to reflect detection performance of in-vehicle network, and we adopt the information entropy measurement, accuracy, false positive rate and response time of anomaly detection as the four objectives to be optimized, which comprehensively describe the underlying detection process.
2) We design a many-objective based algorithm with double evolutionary selections, called MaOEA-ID, to optimize the intrusion detection model decision-making solution. We also introduce the idea of multi knowledge fusion in the design of intrusion detection algorithm [36], and the algorithm performance is greatly improved through the evolutionary fusion of internal and external population knowledge. An improved differential evolutionary (DE) operator produces new offspring of the internal population, and a spherical pruning mechanism selects the excellent internal solutions to form the selected pool of the external archive. Then the second evolutionary selection produces new offspring of the updated archive, and an archive selection mechanism for the external archive selects and stores the optimal solution in the whole detection process.
3) An extensive simulation experiment is performed using a real-world dataset to validate our proposed model and algorithm. We also discuss and analyze some key parameters of the model design. The experimental results demonstrate that our algorithm can respond quickly to attacks and obtain high entropy and detection accuracy as well as very low false positive rate with a good trade-off in the conflicting objective landscape. In particular, our method achieves better IDS performance for in-vehicle network than existing state-of-the-art algorithms.

The paper is organized as follows. Section II reviews the related work, which naturally leads to what motivates our work, namely, the intrusion detection for in-vehicular network is a complicated MaOP problem. In Section III, the in-vehicle network security problem is detailed, and the many-objective intrusion detection model is constructed. To optimize this model, a many-objective evolutionary algorithm design is proposed in Section IV, which is referred to as MaOEA-ID. In Section V, an experiment is carried out using a real-world in-vehicle network data set to validate our model and algorithm. The paper is concluded in Section VI.

II. Related Work

With the development of modern Internet, in-vehicle network system has integrated a variety of emerging technologies to provide more comfortable services, such as assisted driving and entertainment facilities [16], [19]. This however has dramatically increased the potential attacks and securing the in-vehicle network becomes critically important. Fig. 1 depicts the abnormal detection process of common in-vehicle network. The CAN bus data active transmission message has a stable characteristic state when the vehicle is in the normal working mode. Under stable conditions, the collected normal vehicle behavior data are processed to obtain vehicle related knowledge for reference. With the help of an efficient intrusion detection algorithm, knowledge features are extracted, and the vehicle normal behavior feature database is established. When the CAN bus transmits the mixed data of the current vehicle behavior again, the aforementioned data processing method is used to obtain the test data that can be recognized by the detection algorithm. To judge whether the vehicle behavior is normal at the moment, the currently obtained data features are extracted and compared with the feature base of the vehicle normal behavior. If the evaluation result is within the threshold range, the vehicle behavior is regarded as a normal working state, otherwise it is regarded as abnormal [20].

A. Review of Existing Anomaly Detection Methods

Various CAN bus data anomaly detection methods can be divided into three classes: statistics-based, rules-based and machine learning based methods.

1) Statistics-Based Anomaly Detection: Alotibi et al. [21] performed the anomaly detection for cooperative adaptive cruise control in autonomous vehicles using statistical learning

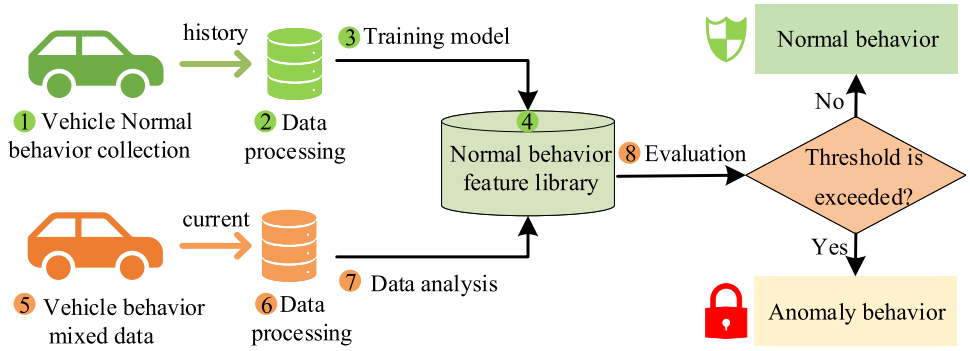


Fig. 1. Common anomaly detection process.

and kinematic model. This class of methods capture CAN data flow by counting a large number of historical message records, so as to establish a summary model that can model the random behaviors of CAN data [21]. The summary model is typically gone through three stages of development, namely, univariate probability model based on independent Gaussian variables, multi-variable model considering the correlation between multi-variables, and time series model analyzing the law of data changing with time [22]. The advantage of this class of methods is that the detection system does not need to have prior knowledge of the attack, and it can detect the latest attack behavior in real time [23]. However, the detection performance of high-dimensional data based on statistics is poor, and the choice of abnormal threshold will affect the detection performance [18], [21].

2) Rules-Based Anomaly Detection: Han et al. [24] designed and performed the one-way analysis of variance test on CAN traffic data to distinguish the abnormal status of the connected cars in IoT environment. This types of detection methods divide the CAN data patterns into normal data and abnormal data, under the guidance of known prior or expert knowledge [15], [25]. These methods can achieve good classification effect with high robustness, but the detection decision-making process is extremely complex [15]. In particular, the detection conclusion often depends on the expert's ability and competent, and it consumes a lot of manpower [25].

3) Machine Learning Based Anomaly Detection: Through learning, the machine learning based methods can reconstruct the existing knowledge structure, acquire new knowledge and hence improve the detection performance [18], [20]. These methods can be further divided into different categories.

a) Method based on bayesian network: It requires fewer parameters and is easy to construct an uncertainty model with good performance [26]. In [27], hardware security modules and Bayesian algorithms were used to improve the security of CAN networks. But the network feature variables are selected based on experience. If the parameters are selected improperly, it will cause a large false detection rate [15], [26].

b) Method based on neural network: Through training, it can predict whether there is anomaly behavior according to the known behavior data of vehicles [28]. In [29], a graph neural network and a two-stage classifier cascade is described to developed the CAN bus IDS and detect all attacks simultaneously. The method is highly adaptive and has strong parallel processing and fault tolerance capability. However, it imposes high computational complexity when generating the training model [30].

c) Method based on fuzzy theory: Fuzzy theory has some advantages in anomaly detection, as it does not require detailed derivation and its decision-making process is similar to human thinking mode. Yu et al. [31] proposed the use of time interval conditional entropy fuzzy method to detect intrusion attacks suffered in automotive CAN networks, which distinguishes and detects attacks by collecting and utilizing the conditional entropy values of conventional communication messages. It is effective in the field of port scanning and detection but the resource consumption is high [32].

d) Method based on genetic algorithm (GA): The anomaly detection performance can be improved by applying GA in an iteration process to evolve towards a better solution [33]. Xi et al. [33] described a multisource genetic immune detector adaptive model in neighborhood shape-space and applies it to anomaly detection. GA include operations such as gene encoding and decoding, and their involved crossover and mutation probability parameter settings may require prior experience to determine, which may affect the quality of the initial population decision solution to some extent.

e) Method based on density: Tang and He [34] presented an effective density-based outlier detection method where a relative density-based outlier score is assigned to observations as a means of distinguishing major clusters in a dataset from outliers. The algorithm, called the local anomaly factor algorithm, assigns an anomaly degree to the object to be detected relative to its local neighborhood, and it is advantageous in detecting local anomaly data [15]. Due to the need to traverse the entire data to calculate the distance, this algorithm is not suitable for applications requiring short response times in detection systems. In addition, it is necessary to manually adjust parameters during the outlier clustering process.

f) Method based on clustering: Indirect clustering based on similarity measurement between samples can be used to perform anomaly detection. Zhang et al. [17] designed a novel weight-based ensemble classifier algorithm to identify abnormal messages of vehicular CAN bus network. Similarly, the one-class SVM and isolation forest can

also be used for anomaly detection [21]. These methods rely heavily on the effectiveness of clustering algorithms, which may be a bottleneck in improving detection performance.

B. Essence of Anomaly Detection Process

There are many factors that affect the intrusion detection performance of the CAN bus data for in-vehicle network security, and the key factors include information entropy measurement reflecting the uncertainty of vehicle behavior, detection accuracy, false positive rate, and response time of anomaly detection. These factors are inherently linked and they influence each other [17]. In other words, there exist multiple conflicting key detection performance metrics. For example, the shorter the response time of detection, the lower the detection accuracy and higher the false positive rate. On the other hand, the lower the real-time requirements, the intrusion detection system may impose higher detection time, so as to improve the detection accuracy. Consequently, the anomaly detection problem of CAN bus data for in-vehicle network security should be viewed as a MaOP, in order to effectively balance the multiple conflicting metrics [35].

To better describe the problem, therefore, the generic CAN bus data intrusion detection optimization can be formulated as the following MaOP [17]

$$\min_{X\in\Phi} f(X) = \min_{X\in\Phi} \left\{f_1(X), f_2(X), \cdots, f_M(X)\right\}, \tag{1}$$

$$\text{s.t.} \quad \begin{cases} g_i(X) > 0, \ 1 \le i \le n_i, \\ h_j(X) = 0, \ 1 \le j \le n_e, \end{cases} \tag{2}$$

where $X = [x_1 \ x_2 \cdots x_{n_v}]^{\mathrm{T}}$ is the n_v-dimensional decision variable vector and Φ denotes the decision variable space, while $f_m(X)$ denotes the mth objective function and M is the number of objectives. $g_i(X) > 0$ is the ith inequality constraint, and $h_j(X) = 0$ is the jth equality constraint. For multi-objective optimization problems (MOPs), $M \ge 2$ should be satisfied. When $M \ge 4$, MOPs are referred as MaOPs. Furthermore, there are n_i and n_e represent upper bounds on the number of inequality and equality constraints, respectively.

Different from the previous studies, in this paper, we comprehensively address the impact of the multiple factors on the performance of CAN bus data intrusion detection to balance the conflict metrics, which is of great practical significance to the research on in-vehicle network security [15], [16], [17]. Our work first builds a many-objective CAN bus data anomaly detection optimization model by considering information entropy, accuracy, false positive rate and response time of anomaly detection as the four objectives. Then an effective many-objective optimization approach is adopted to optimize the detection model. We also introduce the idea of multi knowledge fusion in the design of intrusion detection algorithm [36], and the algorithm performance is greatly improved through the evolutionary fusion of internal and external population knowledge. The specific model construction process and algorithm optimization principle are described in the following two sections, respectively.

III. In-Vehicle Network Security Problem

A. System Description

CAN is a bus-topology communication network commonly used in the in-vehicle network environment [6], [16]. It is a non-preemptive communication network based on priority, and can meet many specific requirements of in-vehicle network environment, such as real-time processing, strong robustness and cost-effective activity [2]. In the data link layer of CAN, broadcast communication is used to transmit messages, allowing any ECU to broadcast data packets to all the connected ECUs. The smallest unit for information transmission in CAN bus is CAN frame, which can be divided into the following four types: data, remote, error and overload frame [17], each serving a specific purpose as summarized in Table I.

Each CAN message contains the following information [8], [17]: start of frame (SOF), arbitration field, control field, data field, cyclic redundancy check (CRC), acknowledge character (ACK) field and end of frame (EOF). The generic format of data frame is shown in Fig 2. SOF indicates the start of a packet and enables synchronization of all nodes on the CAN bus. Arbitration filed (12 bits) is composed of arbitration ID (11 bits) and remote transmission request (1 bit). The Arbitration ID is used as a priority during a collision between two or more CAN packets. The node who has the lowest ID has the highest priority to send packets. Control field (4 bits) provides information for the receiver to check if the packet is successfully received. Data filed (64 bits) contains the actual payload data, and it is up to 8 bytes. CRC field (16 bits) is used for error detection. ACK field (2 bits) contains 2 bits with 1 bit for the ACK and the other bit for the ACK delimiter. EOF (7 bits) indicates the end of the CAN packet.

From the above CAN network structure and message format, some security vulnerabilities of CAN bus data may be exploited by attackers to launch network attacks, which may endanger driving safety [37].

1) No Encryption: There is no inherent encryption method to ensure confidentiality, which enables intruders to interview sensitive data and cause privacy intrusion. At present, only the communication matrix provided by the manufacturer offers some confidentiality but it is not difficult to crack it [10], [38]. The current confidentiality mechanism is far from meeting the confidentiality standard required.

2) No Certification: Any device connected to the CAN bus can read and write to the bus [39]. The CAN bus protocol has no provisions on authentication or access control mechanism. In addition, the CAN message does not contain the source address and destination address [40]. The node only judges whether to receive the message according to the frame identifier, and the legitimacy of the sender cannot be verified. CAN protocol considers all data from the CAN bus to be believable. Any malicious node can forge legitimate messages to attack other nodes in the in-vehicle network.

3) Authenticity of the Message Cannot be Distinguished: CAN protocol cannot distinguish the real error message from the error message crafted by the attacker [41]. It cannot know whether the device is indeed faulty or has been attacked, which may result in the device in the bus off state.

TABLE I
TYPES AND FUNCTIONS OF CAM FRAMES

Types	Purpose
Data frame	Transmission data sent by the sender
Remote frame	Receiving direction requests data from the sender with the same ID
Error frame	When an error occurs, notify other units of the error
Overload frame	Receiver sends it to the sender, indicating that it is not ready for reception

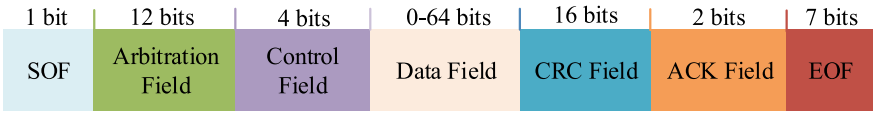


Fig. 2. CAN data frame standard format.

TABLE II
CONFUSION MATRIX

Type	Predicted normal	Predicted attack
True normal	TN	FP
True attack	FN	TP

4) Vulnerable to Denial of Service (DoS) Attacks: CAN bus adopts the broadcast communication mechanism and priority of ID based message transmission. If the message with the highest priority is sent, the node with lower priority will not be able to access the network [42]. Attackers can continue to send high-frequency messages, which will lead to the occupation of CAN bus resources and the delay of signal transmission and response of other nodes, resulting in node communication failure in the vehicle and endangering driving safety.

B. Anomaly Detection Model Construction

It is important to evaluate network vulnerabilities and highlight the security issues faced by CAN networks in the process of constructing an intrusion detection model. To improve the detection performance of an IDS, it is necessary to discover as many attacks as possible, in real-time and with high precision. For this purpose, we adopt the information entropy, accuracy, false positive rate and response time of anomaly detection are the four objectives to be optimized. To describe the process of anomaly detection, the key is to analyze and find the possible abnormal behavior in the IDS network through the description of the normal behavior of network traffic, and the core problem of anomaly detection is to realize the description of normal traffic behavior, real-time detection, comprehensiveness of information and sensitivity of response [17]. Generally, the truth positive (TP), truth negative (TN), false positive (FP) and false negative (FN) are employed to express the IDS detection performance, and they can be intuitively displayed by employing the confusion matrix shown in Table II.

1) Information Entropy (Obj_1): Whether the CAN bus data has the internal characteristics and rules consistent with the behavior can be audited to determine if it has been invaded. In the case of an intrusion, the proportion of high priority instructions in the CAN bus will increase in a short time, while the proportion of low priority messages will decrease [18], [42]. This behavior will lead to abnormal change of the CAN bus information entropy. Therefore, by using the information entropy to describe the characteristics of CAN bus data, we can analyze and audit the CAN bus data log to distinguish between normal and abnormal vehicle behavior.

Specifically, let the average value and standard deviation of information entropy in the CAN bus be avg and σ, respectively. The predicting decision condition interval of normal behavior is $(avg - k\sigma,\ avg + k\sigma)$, where $k \in [0.001,\ 2]$ is a sensitive factor controlling the decision variables [18], [42]. Under normal circumstances, the decision variable value of information entropy should be within the decision range. The stronger the regularity of the CAN bus data, the higher the information entropy value will be and vice versa. When the information entropy value is lower than the preset threshold, i.e., smaller than $avg - k\sigma$, the in-vehicle network behavior is regarded as an abnormal situation under attack. Assume that the CAN bus data model can be represented as $\Psi = (D, W)$, where $D = \{d_1, d_2, \cdots, d_n\}$ is the state set of the in-vehicle IDS with n different states, appearing within the sliding window of size W. The information entropy of the CAN bus data in sliding window W can be expressed as follows

$$H(D) = -\sum_{i=1}^{n} P_{d_i} \log P_{d_i}, \tag{3}$$

where P_{d_i} is the probability of D in state d_i.

The network state can be determined by detecting and monitoring the in-vehicle network, and the number of message or state d_i appearing in sample window W can be obtained by counting. Let the number of state d_i appearing in W be $Count_{d_i}$. Then the probability of d_i appearing in sample window W can be calculated as $P_{d_i} = \frac{Count_{d_i}}{\sum_{j=1}^{n} Count_{d_j}}$, which satisfies $\sum_{i=1}^{n} P_{d_i} = 1$ and $P_{d_i} \geq 0,\ \forall i$. Therefore, the information entropy measurement of the IDS in sampling window W for the in-vehicle network is obtained as

$$Obj_1 = H(D) = -\sum_{i=1}^{n} \left(\frac{Count_{d_i}}{\sum_{j=1}^{n} Count_{d_j}} \right) \times \log \left(\frac{Count_{d_i}}{\sum_{j=1}^{n} Count_{d_j}} \right). \tag{4}$$

It is worth noting that for the DoS attack scenario, higher information entropy value means better system stability.

2) Accuracy (Obj_2): The accuracy rate reflects the ability of the IDS to correctly judge the overall detection samples. That is, it defines the classification ability to correctly judge the normal samples as normal and the attack samples as attacks [17], and it can be calculated according to

$$Obj_2 = \frac{TP + TN}{TP + TN + FP + FN}. \tag{5}$$

A high accuracy value indicates good detection performance.

3) False Positive Rate (Obj_3): The false positive rate reflects the ability of the IDS to correctly predict the purity of normal samples and avoid predicting attack samples as normal samples. That is, it measures the proportion of attack samples predicted as normal samples in the total attack samples [17], and it can be calculated as follows

$$Obj_3 = \frac{FP}{TN + FP}. \tag{6}$$

A small false positive rate value indicates good detection performance.

4) Response Time (Obj_4): Response time describes the time taken by a system to answer the requested message. It is usually timed from the time when the request is sent to the time when the system declares the request or reaches a answer [8]. In the IDS, the response time of attack detection is usually in the form of sliding window with a fixed number of messages to monitor the possible attacks on the bus [43], and it can be calculated as follows

$$Obj_4 = \sum_{i=1}^{n} \left(current_{d_i}^{time} - attack_{d_i}^{time} \right), \tag{7}$$

where $current_{d_i}^{time}$ and $attack_{d_i}^{time}$ are the current starting time of responding to the attack and the time of detecting the message attack, respectively. A short response time indicates good detection performance.

IV. Proposed Optimization Algorithm

Our CAN bus data intrusion detection model is a many-objective optimization design with the four objectives, information entropy, accuracy rate, false positive rate and response time of anomaly detection, to be optimized. Recently, many excellent many-objective optimization algorithms have been designed to attain balanced solutions in convergence and distribution (CaD) based on the distance or angle selection mechanism [44]. By using distance or angle selection mechanism to choose elite solution, it ensures the final population solutions distribute near the optimal Pareto-front as much as possible, and at the same time, it takes the CaD of the solutions into account to meet the needs of the actual problems [45], [46]. Different from these selection mechanisms, in our MaOEA-ID, there are two areas that are optimized separately during each iteration. Specifically, for the internal population, an improved DE operator is applied to produce new offspring, and a spherical pruning mechanism is employed to select the excellent solutions. These excellent internal solutions then form the selection pool for the external archive, and an archive selection mechanism of the external archive is adopted to select and store the optimal solutions in the whole detection process. We now detail these operations of our MaOEA-ID.

A. Improved DE Operator

Typical DE algorithm starts the operation by randomly generating the initial population and it takes the fitness value of each individual in the population as the selection standard. The main evolution process of DE includes three stages: mutation, crossover and selection [45], [47], [48]. By controlling the hybridization of parents according to the fitness value, the mutation vector of DE is generated by the parent difference vector, and is crossover with the parent vector to generate offspring vector. At each evolution iteration, the population is evolved into a better place in the objective landscape, and eventually moves towards the Pareto-front.

However, the standard DE algorithm may arrive in a non-dominated relationship between solutions in solving MaOPs [45]. With its typical method of comparing fitness values, it may be impossible to obtain the optimal individual in screening and guiding the population to evolve towards a better place. To effectively overcome this problem, an improved DE operator can be adopted to ensure that the population evolves towards a better place [49]. The tth iteration of this improved DE operator is described as follows

$$X_i(t) = \begin{cases} X_i(t) + F \cdot \left(X_j(t) - X_i(t) \right) \\ \quad + F \cdot \left(X_k(t) - X_i(t) \right), & \text{if } rand \le CR, \\ X_j(t) \text{ or } X_k(t), & \text{otherwise}, \end{cases} \tag{8}$$

where X_i is an individual randomly selected from the current population, X_j and X_k are two individuals randomly selected from the top 10 percents of the individuals in the external archive, while F is the contraction factor, $rand$ is a random number in the range of [0, 1] and CR is the crossover probability. By introducing two solutions of the external archive, the diversity of solutions is improved [49].

B. Spherical Pruning Mechanism

To ensure that excellent solutions are selected from the set of offspring solutions generated by the DE operator, the spherical pruning mechanism is used. This mechanism analyzes the current approximate Pareto-front (PF) solution set, denoted as PF^*, by normalizing all the population reference solutions to the spherical coordinates. In addition, it ensures that the size of the set of offspring solutions obtained meets the requirements [50]. Fig. 3 depicts the relationship of different solutions on the sphere. For each spherical sector, only one solution with the lowest selection norm is selected, so that the solutions are well distributed in the PF [51].

We now describe the normalization mapping relationship for solution X_i. The fitness value $f(X_i)$ in the spherical coordinate can be expressed as $E(X_i) = \left[Z(f(X_i)) \; V^{\mathrm{T}}(f(X_i)) \right]^{\mathrm{T}}$, where $V(f(X_i)) = \left[V_1(f(X_i)) \cdots V_{M-1}(f(X_i)) \right]^{\mathrm{T}}$ is the arc vector, and $Z(f(X_i))$ is the Euclidean distance from the

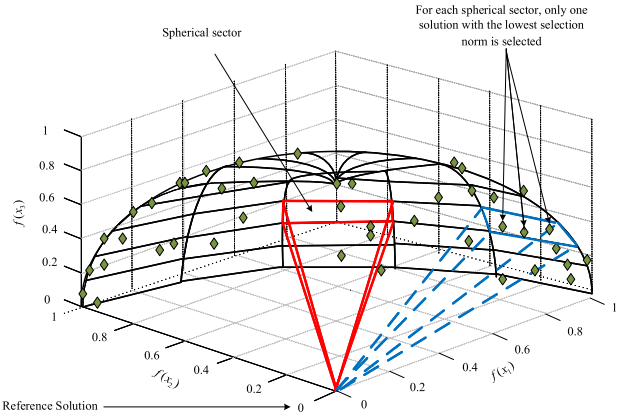


Fig. 3. Illustration of spherical relationship between different solutions.

solution $f(X_i)$ to the normalized ideal solution given by $f\left(X^{ideal}\right) = \min_{f(X)\in PF^*} \{f_1(X), \cdots, f_M(X)\}$ [52]. Given two solutions X_i and X_j, X_i has an spherical preference over X_j if and only if:

$$\left\{SP\left(X_i\right) = SP\left(X_j\right)\right\} \bigcap \left\{Z\left(f\left(X_i\right)\right) < Z\left(f\left(X_j\right)\right)\right\}. \quad (9)$$

Here $SP(X_i)$ denotes the normalized spherical sector of solution X_i and is defined by

$$SP\left(X_i\right) = \left[\frac{V_1(f(X_i))}{SP_1(PF^*)} \cdots \frac{V_{M-1}(f(X_i))}{SP_{M-1}(PF^*)}\right]^{\mathrm{T}} \quad (10)$$

in which $SP(PF^*) = \left[SP_1(PF^*) \cdots SP_{M-1}(PF^*)\right]^{\mathrm{T}}$ is the hypercone grid on the objective space in the arc increment $V^{\Delta} = \left[V_1^{\Delta} \cdots V_{M-1}^{\Delta}\right]^{\mathrm{T}}$. Define $V^U = \left\{V_1^U, \cdots, V_{M-1}^U\right\}$ and $V^L = \left\{V_1^L, \cdots, V_{M-1}^L\right\}$ as the sight range upper and lower bounds from the ideal solution to the approximation solution in PF^*, respectively, which are computed according to

$$V^U = \max_{f(X_i)\in PF^*} \{V_1(f(X_i)), \cdots, V_{M-1}(f(X_i))\}, \quad (11)$$

$$V^L = \min_{f(X_i)\in PF^*} \{V_1(f(X_i)), \cdots, V_{M-1}(f(X_i))\}. \quad (12)$$

Then $SP(PF^*)$ is computed as

$$SP\left(PF^*\right) = \left[\frac{V_1^U - V_1^L}{V_1^{\Delta}} \cdots \frac{V_{M-1}^U - V_{M-1}^L}{V_{M-1}^{\Delta}}\right]^{\mathrm{T}}. \quad (13)$$

Algorithm 1 summarizes this spherical pruning mechanism, where $\mathcal{G} = \{X_1, X_2, \cdots, X_N\}$ is the population solution set with N individuals and $\mathcal{S}$ is the excellent solution set added in each generation.

C. Archive Selection Mechanism

Generally, the fitness function can be used to guide the population toward the optimal PF in solving a MaOP [53]. Moreover, the CaD must be considered in the design of the algorithm. Therefore, when designing the solution selection mechanism of the external archive, it should ensure that the algorithm has good CaD. For the archive selection mechanism, the comprehensive fitness assessment (CFA) method [45] is employed, which is used to store the optimal solutions obtained in the whole detection process. By ensuring good

Algorithm 1 Spherical Pruning Mechanism

Input: $\mathcal{G}$ (Population solution set);
Output: $\mathcal{S}$ (Excellent solution set);
Begin
  For each solution in population set $\mathcal{G}$ **do**
    Map its normalized spherical coordinates;
  End For
  Establish spherical coordinate grid;
  For each solution in population set $\mathcal{G}$ **do**
    Calculate its spherical sector;
    Compare with the remainder solutions;
    IF there does not exist the same spherical sector
      Add the solution to $\mathcal{S}$;
    Else
      Add the solution to $\mathcal{S}$ when it has the lowest norm;
    End IF
  End For
  Return excellent solution set $\mathcal{S}$;
End

CaD, the CFA also help to overcoming the limitations of Pareto sorting and decomposition.

The CFA method $Fun(X_i, \mathcal{G})$ considers the factors of equilibrium CaD in the solution space, and it is expressed as:

$$Fun(X_i, \mathcal{G}) = w_1 \cdot D_{con}(X_i, \mathcal{G}) + w_2 \cdot D_{div}(X_i, \mathcal{G}), \quad (14)$$

where $D_{con}(X_i, \mathcal{G})$ and $D_{div}(X_i, \mathcal{G})$ denote the 'convergence' and 'diversity' distances of X_i, respectively, w_1 and w_2 are two weight factors to balance the influence of these two CaD distances. How to adjust the weight factors can be found in [54]. The calculation of $D_{con}(X_i, \mathcal{G})$ is given below

$$SDE(X_i) = \min_{X_j\in\mathcal{G}, j\neq i} \sqrt{\sum_{m=1}^{M} \left(sde\left(f_m(X_i), f_m(X_j)\right)\right)^2}, \quad (15)$$

$$D_{con}(X_i, \mathcal{G}) = Norm(SDE(X_i)), \quad (16)$$

where $SDE(X_i)$ is the distance using the shifted Euclidean distance to the nearest neighbor [45], and the definition of $sde(\bullet)$ can be found in [54], while $Norm(\bullet)$ is a normalization operation [45]. $D_{div}(X_i, \mathcal{G})$ is calculated as follows

$$D_{div}(X_i, \mathcal{G}) = 1 - \sqrt{\frac{\sum_{m=1}^{M} \left(f_m(X_i)\right)^2}{M}}. \quad (17)$$

The maximum and minimum values of the objectives should be normalized to help reducing the oscillation of the objectives in high-dimensional space. To prevent the size of the external archive from exceeding the population size, the truncation selection mechanism is used in the solution selection [55]. Algorithm 2 summarizes this archive selection mechanism, where $\mathcal{R}$ is the external archive used to store the optimal solutions generated and $\mathcal{S}$ is the new solution set added in each generation.

Algorithm 2 Archive Selection Mechanism

Input: N (size of population), $\mathcal{R}$ (current external archive), $\mathcal{S}$ (new excellent solution set);
Output: $\mathcal{R}$ (updated external archive);
Begin
  For $i = 1$ to $|\mathcal{R}|$
    For $j = 1$ to $|\mathcal{S}|$
      Check dominant relationship between two solutions $S_j \in \mathcal{S}$ and $R_i \in \mathcal{R}$;
      IF Relationship is non-dominant
        Add S_j to $\mathcal{R}$;
      Else
        Remove dominated solution R_i from $\mathcal{R}$;
      End IF
    End For
    IF $|\mathcal{R}| > N$
      Calculate and rank CFA values;
      Delete minimum CFA value until $|\mathcal{R}| = N$;
    End IF
  End For
  Return $\mathcal{R}$;
End

Algorithm 3 MaOEA-ID

Input: N (population size);
Output: $\mathcal{R}$ (external archive);
Begin
  Initialize population $\mathcal{G}$ with N individuals and external archive $\mathcal{R}$;
  While stopping criterion is not met **do**
    Generate offspring set $\mathcal{Q}$ from $\mathcal{G}$ and $\mathcal{R}$ by improved DE operator;
    $\mathcal{G} = \mathcal{G} \bigcup \mathcal{Q}$;
    Use spherical pruning mechanism to obtain excellent solution set $\mathcal{S}$;
    $\mathcal{R} =$ Archive selection mechanism$(\mathcal{R}, \mathcal{S})$;
    Obtain offspring $\mathcal{R}^*$ of external archive $\mathcal{R}$ using SBX and PM operators;
    $\mathcal{R} =$ Archive selection mechanism$(\mathcal{R}, \mathcal{R}^*)$;
  End while
  Return $\mathcal{R}$;
End

D. Algorithm Framework

As usual, our MaOEA-ID algorithm starts by initializing the population set $\mathcal{G}$ with N individuals. The fast non-dominated sorting method [45] is applied to the initial population set $\mathcal{G}$, and the non-dominated solutions of the initial population $\mathcal{G}$ are taken as the initial external archive $\mathcal{R}$. At each evolution generation or iteration, the improved DE strategy is executed to generate the offspring $\mathcal{Q}$ of the parent set $\mathcal{G}$ with the aid of the external archive $\mathcal{R}$. The new population is formed by combining the parents $\mathcal{G}$ and offspring $\mathcal{Q}$. For the newly formed internal population $\mathcal{G}$, the spherical pruning mechanism is used to select the excellent solutions $\mathcal{S}$ (Algorithm 1). Then the archive selection mechanism (Algorithm 2) is applied to the excellent solution set $\mathcal{S}$ and the current external archive $\mathcal{R}$, to generate the updated external archive $\mathcal{R}$. To improve the population diversity, the simulate binary crossover (SBX) and polynomial mutation (PM) [45] are adopted for the archive $\mathcal{R}$ in turn to select offspring $\mathcal{R}^*$ of $\mathcal{R}$. Finally, the new offspring $\mathcal{R}^*$ is fused with the external archive $\mathcal{R}$ by using the archive selection mechanism (Algorithm 2) to obtain the new external archive $\mathcal{R}$. The process continues until the stop condition is satisfied. In this paper, the evolution process is stopped when the preset maximum number of iterations are reached.

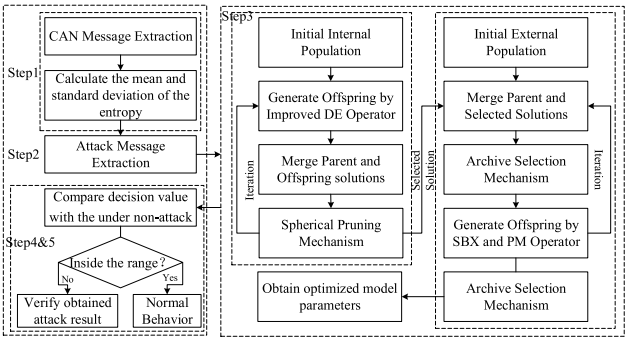


Fig. 4. Detection step process.

The pseudo code of our proposed MaOEA-ID is summarized in Algorithm 3, where $\mathcal{G}$ and $\mathcal{Q}$ are the parent and offspring sets of the internal population, respectively, while $\mathcal{R}$ and $\mathcal{R}^*$ are the parent and offspring sets of the external population, respectively. Observe that there exist double evolutions of the internal population and the external population (archive).

E. Detection Steps

The whole process for the intrusion detection of CAN bus consists of the following steps. And the corresponding detection step flow is described in Fig. 4.

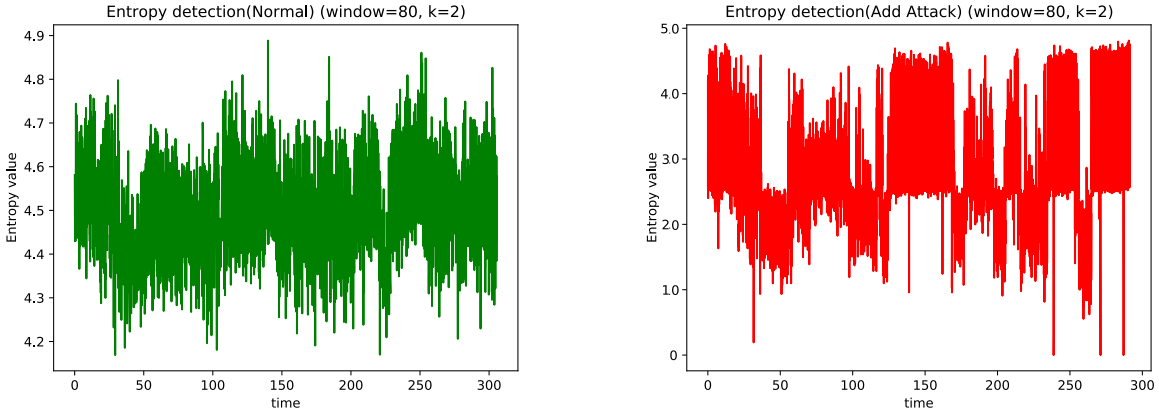
Step 1: CAN message is extracted from the normal data set, and the sliding window of size W is used as the sampling window to obtain the data information [56]. Then, the mean and standard deviation of the entropy are calculated.

Step 2: With the sliding window continuously moves forwards, the CAN message test data set containing attack is extracted to obtain attack message.

Step 3: MaOEA-ID is used to optimize the parameters of the anomaly detection model. By continuously adjusting the algorithmic parameters including sliding window size and sensitivity values, appropriate algorithmic parameter values are found to balance various conflicting objectives and obtain relatively good objective values.

Step 4: Compare the information entropy measurement decision value calculated in *Step 3* with the decision range under the non-attack condition to determine whether there is an attack block. If the value is inside the range, it is considered as normal. Otherwise, it is considered to be an attack.

Step 5: Compare the obtained attack results with the marked attack blocks to verify whether the detection is correct. By calculating the accuracy, false positive rate and response time of the test dataset message, the detection performance are visually displayed.



(a) Normal data (b) Data with attack

Fig. 5. Illustration of variations of entropy values for normal data and data with attack.

V. Simulation Experiment

A. In-Vehicle Network Security Dataset

Due to the diversity and uncertainty of attacks, there exist various in-vehicle network security data sets [10], [18]. In this paper, a real-life automotive CAN bus network dataset [57] is employed, and the CAN message block with ID $= 0 \times 000$ is added into the non-attack data set to obtain the DoS attack data set [58]. Specifically, to create a more realistic DoS scenario reflecting the uncertainty of attack, we copy the message blocks from the CAN messages sent by the legitimate ECU to the non-attack vehicle data set, and then add the DoS attack data to the test data set and further make it Gaussian distributed throughout the test data set [59].

It is widely believed that the network status changes when the CAN network is under attack, which can be reflected in the change of information entropy. To visually distinguish between no attack and DoS attack scenarios in the dataset, we take the first 320000 records of the normal dataset and the first 560000 records of the DoS attack dataset for experiments. Due to the fact that the CAN bus is an event triggered network, we use the fixed sliding window as the observation window. Fig. 5 (a) and (b) show the changes of information entropy with time in the normal data set and the data set with DoS attack blocks, respectively, with the sampling window size of 80 and sensitive value $k = 2$. As observed, the fluctuation range of the entropy is $[4.2,\ 4.9]$ for the normal data set, while in the data set with DoS attack block, the information entropy changes in the range of $(0,\ 5.0]$.

B. Parameters Settings

1) Detection Model Parameters: For the intrusion detection model, the sliding window size W and the sensitivity parameter k are among the most important parameters for the performance of IDS. The sliding window size W directly affects the detection accuracy, false positive rate and response time [18], where the maximum (Max) response time is measured from the beginning of the attack to its discovery in the sliding window [58], while the sensitivity parameter k directly affects the decision range of anomaly detection. After repeated experiments, it is found that an appropriate combination choice of the sliding window size W and the sensitivity parameter k should be selected from $W \in [20,\ 120]$ and $k \in [0.001,\ 2]$, to balance the conflicting objectives.

2) Optimization Algorithmic Parameters: To demonstrate the effectiveness of our proposed MaOEA-ID, we also employ three existing state-of-the-art many-objective optimization algorithms to optimize the anomaly detection model, and they are the NSGA-III [60], the promising region evolutionary algorithm (PREA) [61], and the hyperplane assisted evolutionary algorithm (hpaEA) [62]. These algorithms have been proved to be successful and effective in solving many practical problems [53]. The algorithmic parameters of these benchmark optimization algorithms are set according to the original literature. In particular, for the NSGA-III and PREA, the two-layer distribution method is adopted. For the MaOEA-ID, the contraction factor F and the crossover probability factor CR are chosen in the ranges of $[0.4,\ 0.95]$ and $[0.3,\ 0.9]$, respectively [45]. The population size is set to $N = 100$ for all the algorithms. SBX probability and PM probability are 1 and 1/N, respectively. And the crossover index and mutation index are uniformly set to 20. The stopping criterion for all the algorithms is the maximum number of evolution iterations, which is set to 10000. Each experiment is run independently 20 times with the test problem [63], [64].

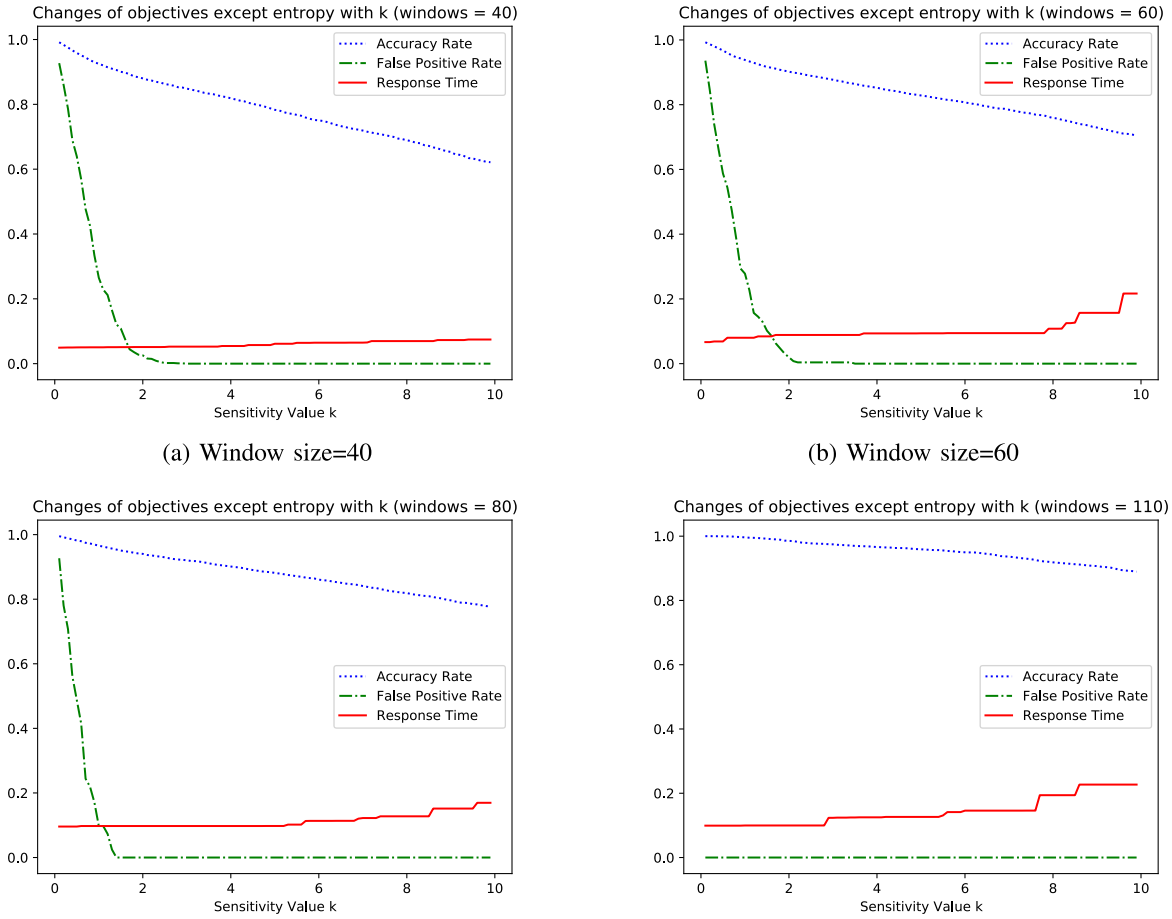
C. Experiment Resuls

1) Influence of Sliding Window Size: To investigate the impact of the sliding window size W on the performance of the detection model, we fix the other important parameter, namely, the sensitivity parameter, to $k = 2$, and conduct the experiment with different sliding window sizes on the first 560000 records of the DoS attack dataset. Table III lists the detection performance achieved by varying the sliding window size in the range of $[20,\ 120]$ with the fixed $k = 2$. It can be seen that as W increases from 20 to 120, the both average entropy and the max response time increase gradually. This means that a larger sliding window size improves the probability of detecting the attack but increases the response time of the detection. Impact of W on the false positive rate exhibits a more complex trend. As W increases from 20 to 50, the false positive rate increases but further increasing W leads

TABLE III

INFLUENCE OF SLIDING WINDOW SIZE W WITH FIXED SENSITIVITY PARAMETER $k = 2$ ON THE PERFORMANCE OF THE DETECTION MODEL

Sliding windows Size	Average Entropy	Accuracy (%)	False Positive Rate (%)	Max Response Time (ms)
20	4.02	87.96	1.49	4.73e-2
30	4.23	84.27	2.76	4.90e-2
40	4.37	83.04	2.81	5.07e-2
50	4.43	84.46	4.08	5.79e-2
60	4.48	85.62	3.64	8.00e-2
70	4.52	82.51	0	8.96e-2
80	4.54	88.22	0	8.67e-2
90	4.57	88.32	0	9.92e-2
100	4.58	91.33	0	9.94e-2
110	4.60	97.44	0	9.97e-2
120	4.61	99.28	0	9.98e-2



(a) Window size=40 (b) Window size=60

(c) Window size=80 (d) Window size=110

Fig. 6. Detection objectives (accuracy, false positive rate and response time) as the functions of sensitivity parameter k, given different sliding window sizes.

to the reduction of the false positive rate. When $W \geq 70$, the false positive rate becomes zero. For the relatively small $W \in [20, 70]$, the relationship between the accuracy and W appears slightly irregular. However, for the large sliding window size of $W \geq 80$, the accuracy increases with W, and when $W = 120$, the accuracy is 99.28%.

2) Influence of Sensitivity Value k: Because the CAN bus is an event triggered network, some subtle changes in the scene may cause huge changes in the information entropy. In particular, the decision variables controlled by the sensitivity value k have a great influence on the measurement of information entropy, and the changes in the information entropy may be irregular [10], [18]. Therefore, we concentrate on investigating the impact of the sensitivity parameter k on the three detection objectives of accuracy, false-positive rate and response time using the first 560000 records of the DoS attack dataset. Fig. 6 depicts the accuracy, false-positive rate and response time as the functions of k given four different values of the sliding window size W. It can be seen that the accuracy decreases as k increases given a fixed W, and the rate of reduction in accuracy is larger for smaller sliding window size. By contrast, the response time increases with the sensitivity parameter k given a fixed sliding window size W, and the rate of increase in response time is higher for larger W. Given $W = 40$, 60 and 80, respectively, Fig. 6(a), (b) and (c) show that the false positive rate decreases quickly as k increases in the range

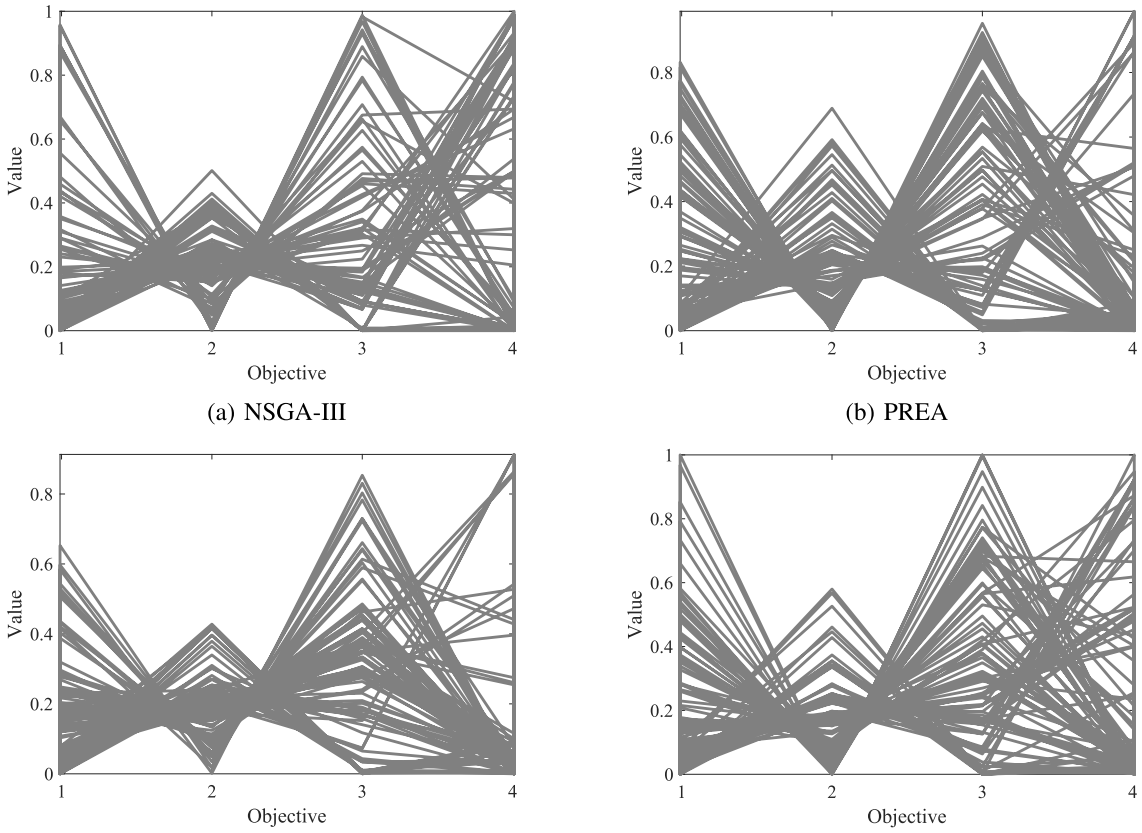


Fig. 7. Pareto solution sets found by the four algorithms, where objective 1: information entropy (Obj_1), objective 2: accuracy (Obj_2), objective 3: false positive rate (Obj_3) and objective 4: response time (Obj_4).

TABLE IV
FRIEDMAN TEST FOR COMPARISON ALGORITHMS BASED ON NHV METRIC VALUE

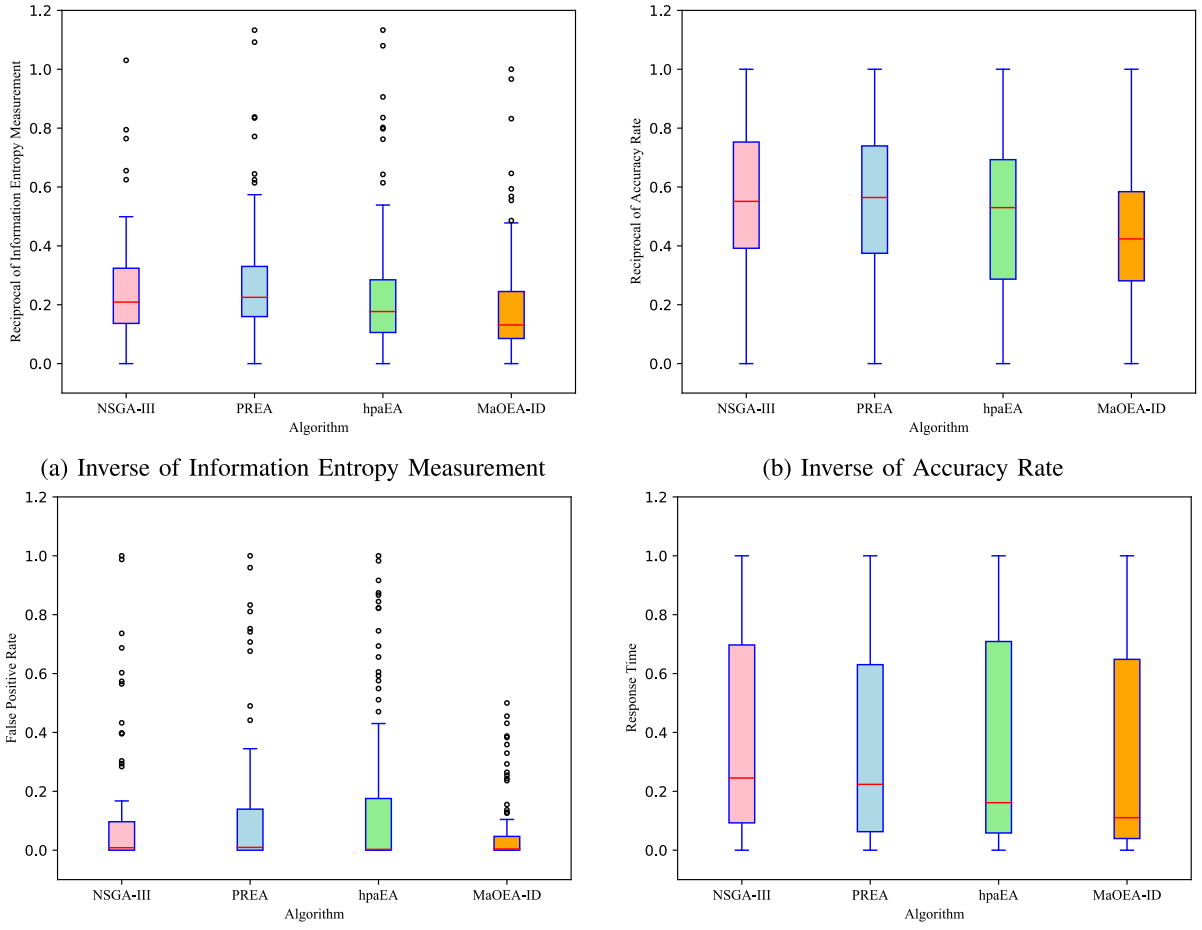
Algorithms	Ranking
NSGA-III	3.20
PREA	2.57
hpaEA	2.06
MaOEA-ID	1.42

of $k \in [0.001,\ 2]$. When the sensitivity value k exceeds this range, the false positive rate tends to zero. For very high sliding window size of $W = 110$, the false positive rate remains zero regardless the value of k, as can be seen from Fig. 6(d).

It can be seen that choosing appropriate values for the sliding window size W and the sensitivity parameter k is of great significance to improve the whole IDS performance. Therefore, in addition to the parameters involved in obtaining the information entropy and the detection classification process, W and k are also included in our decision variables to be optimized by the proposed MaOEA-ID and the benchmark algorithms in the following comparison.

3) Comparison of Different Optimization Algorithms: Table IV shows the Friedman test results of the involved algorithms based on NHV metric value with the significance difference level 0.05 [65]. And the performance ranking of the involved comparison algorithms can be followed and listed as follows: MaOEA-ID > hpaEA > PREA > NSGA-III, which means that MaOEA-ID has been proven to achieve good performance.

To vividly compare the detection performance of the four algorithms, their Pareto solution sets with the largest normalized hypervolume (NHV) metric [66] value are plotted in the parallel coordinates of the objective space, as illustrated in Fig. 7, where each solution has 4 objectives and the solution's objective values are linked by line. The intuitive correlation and conflicting relationships between the different objectives are clearly demonstrated in Fig. 7, where it can be observed that all the four algorithms converge to the PF, while they have different objective landscapes, in terms of diversity. Specifically, the solution sets of NSGA-III and MaOEA-ID have similar distribution range of $[0,\ 1]$ in Obj_3 and Obj_4. But MaOEA-ID has wider distribution ranges than NSGA-III in Obj_1 and Obj_2. More specifically, the solution ranges in Obj_1 are $[0,\ 1]$ and [0 0.95], respectively, while the distribution ranges in in Obj_2 are $[0,\ 0.6]$ and $[0,\ 0.5]$, respectively, for MaOEA-ID and NSGA-III. This indicates that the solutions obtained by MaOEA-ID in solving Obj_1 and Obj_2 have higher diversity than NSGA-III. The distribution range of PREA in Obj_2 is $[0,\ 0.7]$, which is wider than the other three algorithms. However, the values of its Pareto solution set in Obj_1 and Obj_3 distribute in the ranges of $[0,\ 0.85]$ and $[0,\ 0.95]$, respectively, which are poorer than those of NSGA-III and MaOEA-ID on the same objectives. Clearly, the quality of the solution set obtained by hpaEA, in terms of diversity, is poorer than the other three algorithms.



(a) Inverse of Information Entropy Measurement

(b) Inverse of Accuracy Rate

(c) False positive rate

(d) Response Time

Fig. 8. Objective performance comparison of different algorithms.

The results of Fig. 7 hence suggest that the quality of the solution set obtained by our MaOEA-ID, in terms of diversity, is better than the three state-of-the-art benchmark algorithms.

To compare the detection performance of different algorithms on each objective in more detail, the objective performance comparison box figure is drawn in Fig. 8. To apply the same common rule of comparison for all the four objectives, namely, the smaller the better, the inverse of the information entropy measurement, i.e., $\frac{1}{obj_1}$, and the inverse of the accuracy rate, i.e., $\frac{1}{obj_2}$, are showed in Fig. 8(a) and Fig. 8(b), respectively. As can be seen from Fig. 8(a), all the algorithms have highly similar boxes for the first objective. Based on the comparison of upper and lower quartiles and median values, a clear performance ranking for the first objective can be drawn as: MaOEA-ID $>$ hpaEA $>$ NSGA-III $\approx$ PREA, where '$>$' means 'better' and '$\approx$' indicates 'similar'. Based on the median values of Fig. 8(b), an identical ranking of MaOEA-ID $>$ hpaEA $>$ NSGA-III $\approx$ PREA is obtained for the second objective. For the objective of false positive rate depicted in Fig. 8(c), the lower quartile and median value of all the algorithms are close to 0. The box of MaOEA-ID however is more compact and concentrated. Also the upper limit value of MaOEA-ID is significantly smaller than NSGA-III, PREA and hpaEA. This means that MaOEA-ID achieves better results on false positive rate. The performance ranking for the third objective can be drawn as MaOEA-ID $>$ NSGA-III $>$ PREA $>$ hpaEA. For the objective of response time given in Fig. 8(d), MaOEA-ID has smaller median value than the other algorithms. NSGA-III and hpaEA have similar upper quartile values that are higher than the upper quartile value of PREA. In terms of response time, it may be concluded that MaOEA-ID is better than the other three algorithms.

Note that typically more evaluation time and hence higher response time is needed to attain better accuracy rate. That is, these two objectives are conflicting to each other. And it can be seen that our MaOEA-ID can not only improve the accuracy of information entropy, but also make the upper limit of false positive rate smaller and the box more compact and concentrated. This means that our MaOEA-ID can better balance these conflicting objectives and achieves superior detection performance over the existing state-of-the-art algorithms.

VI. Conclusion

We have constructed a many-objective based intrusion detection model that considers information entropy, accuracy, false alarm rate and response time of anomaly detection as the four objectives for the in-vehicle network security problem. An efficient MaOEA-ID with double evolutionary selections has been designed to optimize this many-objective intrusion detection model and hence to achieve good detection

performance that balances the conflicting objectives. The novelty of our MaOEA-ID has been its double evolutionary selections that closely link and promote each other. For the internal population, improved DE operator and spherical pruning mechanism are adopted to produce new offspring and select the excellent solutions, respectively. The excellent internal solutions are used as the selection pool of the external archive. New offspring of the external archive are generated and an archive selection mechanism is adopted to select and store the optimal solutions in the whole detection process.

To verify our intrusion detection model and optimization algorithm, an experiment has been conducted involving a a real-life automotive CAN bus network dataset. Extensive experiments have been performed to investigate the important impact of the sliding window size and the sensitivity parameter to the detection performance. Concrete experimental results have validated that our method responds quickly to attacks and is capable of obtaining high entropy and detection accuracy as well as very low false positive rate with a good balance in the conflicting objective landscape. The extensive results obtained have also demonstrated that our MaOEA-ID has superior intrusion detection performance over the three state-of-the-art benchmarks, NSGA-III, PREA and hpaEA, in terms of higher diversity and better objectives.

To further improve detection performance and service life, our future work will construct enhanced detection model by considering more influencing factors. It is also obvious that the effectiveness of MaOEA-ID is not limited to addressing the in-vehicle network problem, but can readily be applied to anomaly detection in other fields, such as medical images.

REFERENCES

[1] H. Gao and Y. Zhang, "Guest editorial optimization of electric vehicle networks and heterogeneous networking in future smart cities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1748–1751, Mar. 2021.

[2] S. Deb, D. W. Carruth, and C. R. Hudson, "How communicating features can help pedestrian safety in the presence of self-driving vehicles: Virtual reality experiment," *IEEE Trans. Hum.-Mach. Syst.*, vol. 50, no. 2, pp. 176–186, Apr. 2020.

[3] A. Grushin and W. Woods, "Anomaly detection with neural parsers that never reject," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, San Francisco, CA, USA, May 2022, pp. 88–97.

[4] Z. Peng, L. Liu, and J. Wang, "Output-feedback flocking control of multiple autonomous surface vehicles based on data-driven adaptive extended state observers," *IEEE Trans. Cybern.*, vol. 51, no. 9, pp. 4611–4622, Sep. 2021.

[5] S. Almeaibed, S. Al-Rubaye, A. Tsourdos, and N. P. Avdelidis, "Digital twin analysis to promote safety and security in autonomous vehicles," *IEEE Commun. Standards Mag.*, vol. 5, no. 1, pp. 40–46, Mar. 2021.

[6] W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Lee, "VoltageIDS: Low-level communication characteristics for automotive intrusion detection system," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2114–2129, Aug. 2018.

[7] H. Olufowobi, C. Young, J. Zambreno, and G. Bloom, "SAIDuCANT: Specification-based automotive intrusion detection using controller area network (CAN) timing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1484–1494, Feb. 2020.

[8] R. Sato and S. Fukumoto, "Response-time analysis for controller area networks with randomly occurring messages," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 3893–3902, Apr. 2020.

[9] M. R. Moore, R. A. Bridges, F. L. Combs, and A. L. Anderson, "Data-driven extraction of vehicle states from CAN bus traffic for cyberprotection and safety," *IEEE Consum. Electron. Mag.*, vol. 8, no. 6, pp. 104–110, Nov. 2019.

[10] A. R. Javed, S. u. Rehman, M. U. Khan, M. Alazab, and G. R. Thippa, "CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1456–1466, Apr. 2021.

[11] T. Yu and X. Wang, "Topology verification enabled intrusion detection for in-vehicle CAN-FD networks," *IEEE Commun. Lett.*, vol. 24, no. 1, pp. 227–230, Jan. 2020.

[12] A. Derhab, M. Belaoued, I. Mohiuddin, F. Kurniawan, and M. K. Khan, "Histogram-based intrusion detection and filtering framework for secure and safe in-vehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2366–2379, Mar. 2022.

[13] X. Ying, S. U. Sagong, A. Clark, L. Bushnell, and R. Poovendran, "Shape of the cloak: Formal analysis of clock skew-based intrusion detection system in controller area networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2300–2314, Sep. 2019.

[14] B. Groza and P.-S. Murvay, "Efficient intrusion detection with Bloom filtering in controller area networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 1037–1051, Apr. 2019.

[15] D. Chou and M. Jiang, "A survey on data-driven network intrusion detection," *ACM Comput. Surveys*, vol. 54, no. 9, pp. 1–36, Dec. 2022.

[16] Ö. F. Gemici, I. Hökelek, and H. A. Çirpan, "Modeling queuing delay of 5G NR with NOMA under SINR outage constraint," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2389–2403, Mar. 2021.

[17] Z. Zhang, Y. Cao, Z. Cui, W. Zhang, and J. Chen, "A many-objective optimization based intelligent intrusion detection algorithm for enhancing security of vehicular networks in 6G," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5234–5243, Jun. 2021.

[18] W. Wu et al., "A survey of intrusion detection for in-vehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 919–933, Mar. 2020.

[19] K. Serag, R. Bhatia, V. Kumar, Z. B. Celik, and D. Xu, "Exposing new vulnerabilities of error handling mechanism in CAN," in *Proc. 30th USENIX Secur. Symp. (USENIX)*, Aug. 2021, pp. 4241–4258.

[20] Y. Zhou, H. Ren, Z. Li, and W. Pedrycz, "Anomaly detection based on a granular Markov model," *Exp. Syst. Appl.*, vol. 187, Jan. 2022, Art. no. 115744.

[21] F. Alotibi and M. Abdelhakim, "Anomaly detection for cooperative adaptive cruise control in autonomous vehicles using statistical learning and kinematic model," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3468–3478, Jun. 2021.

[22] S. M. Djurasevic, U. M. Pesovic, and B. S. Djordjevic, "Anomaly detection model for predicting hard disk drive failures," *Appl. Artif. Intell.*, vol. 35, no. 8, pp. 549–566, Jul. 2021.

[23] L. Fang, Y. Li, Z. Liu, C. Yin, M. Li, and Z. J. Cao, "A practical model based on anomaly detection for protecting medical IoT control services against external attacks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4260–4269, Jun. 2021.

[24] M. L. Han, J. Lee, A. R. Kang, S. Kang, J. K. Park, and H. K. Kim, "A statistical-based anomaly detection method for connected cars in Internet of Things environment," in *Internet of Vehicles—Safe and Intelligent Mobility*. Cham, Switzerland: Springer, Nov. 2015.

[25] T. Cheng and B. Wang, "Total variation and sparsity regularized decomposition model with union dictionary for hyperspectral anomaly detection," *IEEE Trans. Geosci. Remote Sens.*, vol. 59, no. 2, pp. 1472–1486, Feb. 2021.

[26] O. Salem, K. Alsubhi, A. Mehaoua, and R. Boutaba, "Markov models for anomaly detection in wireless body area networks for secure health monitoring," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 526–540, Feb. 2021.

[27] W. Benrhaiem and A. S. Hafid, "Bayesian networks based reliable broadcast in vehicular networks," *Veh. Commun.*, vol. 21, Jan. 2020, Art. no. 100181.

[28] O. Rippel, P. Mertens, E. König, and D. Merhof, "Gaussian anomaly detection by modeling the distribution of normal data in pretrained deep features," *IEEE Trans. Instrum. Meas.*, vol. 70, pp. 1–13, 2021.

[29] H. Zhang, K. Zeng, and S. Lin, "Federated graph neural network for fast anomaly detection in controller area networks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1566–1579, 2023.

[30] H. Asgharzadeh, A. Ghaffari, M. Masdari, and F. S. Gharehchopogh, "Anomaly-based intrusion detection system in the Internet of Things using a convolutional neural network and multi-objective enhanced capuchin search algorithm," *J. Parallel Distrib. Comput.*, vol. 175, pp. 1–21, May 2023.

[31] Z. Yu, Y. Liu, G. Xie, R. Li, S. Liu, and L. T. Yang, "TCE-IDS: Time interval conditional entropy- based intrusion detection system for automotive controller area networks," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1185–1195, Feb. 2023.

[32] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão, and M. L. Proença, "Network anomaly detection system using genetic algorithm and fuzzy logic," *Exp. Syst. Appl.*, vol. 92, pp. 390–402, Feb. 2018.

[33] L. Xi, R.-D. Wang, Z.-Y. Yao, and F.-B. Zhang, "Multisource neighborhood immune detector adaptive model for anomaly detection," *IEEE Trans. Evol. Comput.*, vol. 25, no. 3, pp. 582–594, Jun. 2021.

[34] B. Tang and H. He, "A local density-based approach for outlier detection," *Neurocomputing*, vol. 241, pp. 171–180, Jun. 2017.

[35] A. Hafezalkotob, A. Hafezalkotob, H. Liao, and F. Herrera, "Interval MULTIMOORA method integrating interval Borda rule and interval best-worst-method-based weighting model: Case study on hybrid vehicle engine selection," *IEEE Trans. Cybern.*, vol. 50, no. 3, pp. 1157–1169, Mar. 2020.

[36] A. Kavousi-Fard, M. Dabbaghjamanesh, T. Jin, W. Su, and M. Roustaei, "An evolutionary deep learning-based anomaly detection model for securing vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4478–4486, Jul. 2021.

[37] A. d. F. Tron, S. Longari, M. Carminati, M. Polino, and S. Zanero, "CANflict: Exploiting peripheral conflicts for data-link layer attacks on automotive networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Los Angeles, CA, USA, Nov. 2022, pp. 711–723.

[38] M. E. Verma, R. A. Bridges, J. J. Sosnowski, S. C. Hollifield, and M. D. Iannacone, "CAN-D: A modular four-step pipeline for comprehensively decoding controller area network data," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 9685–9700, Oct. 2021.

[39] M. Roeschlin, G. Camurati, P. Brunner, M. Singh, and S. Capkun, "EdgeTDC: On the security of time difference of arrival measurements in CAN bus systems," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, 2023, p. 2022.

[40] S. Longari, D. H. N. Valcarcel, M. Zago, M. Carminati, and S. Zanero, "CANnolo: An anomaly detection system based on LSTM autoencoders for controller area network," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1913–1924, Jun. 2021.

[41] L. Xiao, X. Lu, T. Xu, W. Zhuang, and H. Dai, "Reinforcement learning-based physical-layer authentication for controller area networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2535–2547, 2021.

[42] Y. Tang et al., "Detection of magnetic anomaly signal based on information entropy of differential signal," *IEEE Geosci. Remote Sens. Lett.*, vol. 15, no. 4, pp. 512–516, Apr. 2018.

[43] G. Xie, R. Li, and S. Hu, "Security-aware obfuscated priority assignment for CAN FD messages in real-time parallel automotive applications," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 12, pp. 4413–4425, Dec. 2020.

[44] Z. Liang, K. Hu, X. Ma, and Z. Zhu, "A many-objective evolutionary algorithm based on a two-round selection strategy," *IEEE Trans. Cybern.*, vol. 51, no. 3, pp. 1417–1429, Mar. 2021.

[45] Z. Cui et al., "Hybrid many-objective particle swarm optimization algorithm for green coal production problem," *Inf. Sci.*, vol. 518, pp. 256–271, May 2020.

[46] J. Zhang et al., "Privacy protection based on many-objective optimization algorithm," *Concurrency Comput., Pract. Exper.*, vol. 31, no. 20, Oct. 2019, Art. no. e5342.

[47] H. Peng, Y. Han, C. Deng, J. Wang, and Z. Wu, "Multi-strategy co-evolutionary differential evolution for mixed-variable optimization," *Knowl.-Based Syst.*, vol. 229, Oct. 2021, Art. no. 107366.

[48] X. Feng, H. Muramatsu, and S. Katsura, "Differential evolutionary algorithm with local search for the adaptive periodic-disturbance observer adjustment," *IEEE Trans. Ind. Electron.*, vol. 68, no. 12, pp. 12504–12512, Dec. 2021.

[49] Q. Zhu et al., "An elite gene guided reproduction operator for many-objective optimization," *IEEE Trans. Cybern.*, vol. 51, no. 2, pp. 765–778, Feb. 2021.

[50] K. Zhang, Z. Xu, S. Xie, and G. G. Yen, "Evolution strategy-based many-objective evolutionary algorithm through Vector Equilibrium," *IEEE Trans. Cybern.*, vol. 51, no. 11, pp. 5455–5467, Nov. 2021.

[51] G. Reynoso-Meza, J. Sanchis, X. Blasco, and M. Martinez, "Design of continuous controllers using a multiobjective differential evolution algorithm with spherical pruning," in *Proc. EvoApplications*, Istanbul, Turkey, Apr. 2010, pp. 532–541.

[52] Y. Liu, N. Zhu, and M. Li, "Solving many-objective optimization problems by a Pareto-based evolutionary algorithm with preprocessing and a penalty mechanism," *IEEE Trans. Cybern.*, vol. 51, no. 11, pp. 5585–5594, Nov. 2021.

[53] X. Cai, J. Zhang, Z. Ning, Z. Cui, and J. Chen, "A many-objective multistage optimization-based fuzzy decision-making model for coal production prediction," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 12, pp. 3665–3675, Dec. 2021.

[54] Q. Lin et al., "Particle swarm optimization with a balanceable fitness estimation for many-objective optimization problems," *IEEE Trans. Evol. Comput.*, vol. 22, no. 1, pp. 32–46, Feb. 2018.

[55] R. Jiao, S. Zeng, C. Li, S. Yang, and Y.-S. Ong, "Handling constrained many-objective optimization problems via problem transformation," *IEEE Trans. Cybern.*, vol. 51, no. 10, pp. 4834–4847, Oct. 2021.

[56] J. Zhou, P. Joshi, H. Zeng, and R. Li, "BTMonitor: Bit-time-based intrusion detection and attacker identification in controller area network," *ACM Trans. Embedded Comput. Syst.*, vol. 18, no. 6, pp. 1–23, Nov. 2019.

[57] H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame," in *Proc. 15th Annu. Conf. Privacy, Secur. Trust (PST)*, Calgary, AB, Canada, Aug. 2017, pp. 5700–5709.

[58] G. Xie, L. T. Yang, Y. Yang, H. Luo, R. Li, and M. Alazab, "Threat analysis for automotive CAN networks: A GAN model-based intrusion detection technique," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4467–4477, Jul. 2021.

[59] Y. Li, F. Chu, F. Zheng, and M. Liu, "A bi-objective optimization for integrated berth allocation and quay crane assignment with preventive maintenance activities," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 4, pp. 2938–2955, Apr. 2022.

[60] K. Deb and H. Jain, "An evolutionary many-objective optimization algorithm using reference-point-based nondominated sorting approach—Part I: Solving problems with box constraints," *IEEE Trans. Evol. Comput.*, vol. 18, no. 4, pp. 577–601, Aug. 2014.

[61] J. Yuan, H.-L. Liu, F. Gu, Q. Zhang, and Z. He, "Investigating the properties of indicators and an evolutionary many-objective algorithm using promising regions," *IEEE Trans. Evol. Comput.*, vol. 25, no. 1, pp. 75–86, Feb. 2021.

[62] H. Chen, Y. Tian, W. Pedrycz, G. Wu, R. Wang, and L. Wang, "Hyperplane assisted evolutionary algorithm for many-objective optimization problems," *IEEE Trans. Cybern.*, vol. 50, no. 7, pp. 3367–3380, Jul. 2020.

[63] Z. Liang, T. Luo, K. Hu, X. Ma, and Z. Zhu, "An indicator-based many-objective evolutionary algorithm with boundary protection," *IEEE Trans. Cybern.*, vol. 51, no. 9, pp. 4553–4566, Sep. 2021.

[64] N. Elgharably, S. Easa, A. Nassef, and A. El Damatty, "Stochastic multi-objective vehicle routing model in green environment with customer satisfaction," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 1, pp. 1337–1355, Jan. 2023.

[65] J. Zhang, Z. Ning, and F. Xue, "A two-stage federated optimization algorithm for privacy computing in Internet of Things," *Future Gener. Comput. Syst.*, vol. 145, pp. 354–366, Aug. 2023.

[66] R. Cheng et al., "A benchmark test suite for evolutionary many-objective optimization," *Complex Intell. Syst.*, vol. 3, no. 1, pp. 67–81, Mar. 2017.

Jiangjiang Zhang is currently pursuing the Doctor degree with the Beijing University of Technology, China. His research interests include data security, privacy protection, computational intelligence, combinatorial optimization and modelling.

Bei Gong received the Ph.D. degree from the Beijing University of Technology in 2012. He participates in six national invention patents and one monograph textbook. In the past five years, he has published more than 30 papers in first-class SCI/EI and other famous international journals and top international conferences in relevant research fields. His research interests include trusted computing, Internet of Things security, mobile Internet of Things, and mobile edge computing. He has presided over eight national projects, such as the National Natural Science Foundation and six provincial and ministerial projects, such as the general science and technology program of the Beijing Municipal Education Commission.

Muhammad Waqas (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees from the Department of Electrical Engineering, University of Engineering and Technology Peshawar, Pakistan, in 2009 and 2014, respectively, and the Ph.D. degree from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in June 2019. From 2012 to 2015, he served Sarhad University of Science and Information Technology, Peshawar, Pakistan, as a Lecturer and Program Coordinator. From August 2019 to March 2022, he served Faculty of Computer Science and Engineering, GIK Insitute of Engineering Sciences and Technology, Pakistan, as an Assistant Professor. He was also associated with the Faculty of Information Technology, Beijing University of Technology, Beijing, China, as a Research Associate from October 2019 to September 2022. Currently, he is an Assistant Professor at the Computer Engineering Department, College of Information Technology, University of Bahrain, Bahrain. He is also an Adjunct Senior Lecturer at the School of Engineering, Edith Cowan University, Perth, Australia. His current research interests are in the areas of physical layer security, vehicular networks, mobile edge computing and the Internet of Things. He has several research publications in reputed Journals and Conferences. He is co-chair, TPC member and reviewer of several international conferences and journals. He is also an Associate Editor of the *International Journal of Computing and Digital Systems*, and received the best paper award at ASSP in 2021.

Shanshan Tu (Member, IEEE) received the Ph.D. degree from the Computer Science Department, Beijing University of Posts and Telecommunications, in 2014. From 2013 to 2014, he visited the University of Essex for National Joint Doctoral Training. He worked in the Department of Electronic Engineering at Tsinghua University, as a Postdoctoral Researcher, from 2014 to 2016. He is currently an Associate Professor in the Faculty of Information Technology, Beijing University of Technology, China. His research interests are in cloud computing, MEC and information security techniques.

Sheng Chen (Fellow, IEEE) received the Ph.D. degree in control engineering from City University of London in 1986, and the Doctor of Sciences (D.Sc.) degree from the University of Southampton, Southampton, U.K., in 2005. Since 1999, he has been with the School of Electronics and Computer Science, the University of Southampton, where he is currently a Professor in intelligent systems and signal processing. He has more than 17 700 Web of Science citations with an H-index 58 and more than 34 900 Google Scholar citations with H-index 80. His research interests include adaptive signal processing, wireless communications, modeling and identification of nonlinear systems, neural network and machine learning, intelligent control system design, and evolutionary computation methods and optimization. He is a fellow of the U.K. Royal Academy of Engineering, fellow of Asia-Pacific Artificial Intelligence Association, and fellow of IET.