Indonesian Journal of Electrical Engineering and Computer Science
Vol. 24, No. 1, October 2021, pp. 590~599
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v24.i1.pp590-599

Optimized machine learning algorithm for intrusion detection

Royida A. Ibrahem Alhayali[1], Mohammad Aljanabi[2], Ahmed Hussein Ali[3], Mostafa Abdulghfoor Mohammed[4], Tole Sutikno[5]
[1]Department of Computer Engineering, College of Engineering, University of Diyala, Diyala, Iraq
[2,3]Department of computer, College of Education, Al-Iraqia University, Baghdad, Iraq
[2,3]Department of Computer Science, Al Salam University College, Baghdad, Iraq
[4]Imam Aadham University College, Baghdad, Iraq
[5]Department of Electical Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Article Info

Article history:

Received Jul 9, 2021
Revised Sep 2, 2021
Accepted Sep 4, 2021

Keywords:

Extreme learning machine
Feature subset selection
Intrusion detection system
Logistic regression
Machine learning
Rao optimization algorithm
Support vector machine

ABSTRACT

Intrusion detection is mainly achieved by using optimization algorithms. The need for optimization algorithms for intrusion detection is necessitated by the increasing number of features in audit data, as well as the performance failure of the human-based smart intrusion detection system (IDS) in terms of their prolonged training time and classification accuracy. This article presents an improved intrusion detection technique for binary classification. The proposal is a combination of different optimizers, including Rao optimization algorithm, extreme learning machine (ELM), support vector machine (SVM), and logistic regression (LR) (for feature selection & weighting), as well as a hybrid Rao-SVM algorithm with supervised machine learning (ML) techniques for feature subset selection (FSS). The process of selecting the least number of features without sacrificing the FSS accuracy was considered a multi-objective optimization problem. The algorithm-specific, parameter-less concept of the proposed Rao-SVM was also explored in this study. The KDDCup 99 and CICIDS 2017 were used as the intrusion dataset for the experiments, where significant improvements were noted with the new Rao-SVM compared to the other algorithms. Rao-SVM presented better results than many existing works by reaching 100% accuracy for KDDCup 99 dataset and 97% for CICIDS dataset.

Corresponding Author:

Ahmed Hussein Ali
Department of Computer Science
Al Salam University College
Baghdad, 98182, Iraq
Email: msc.ahmed.h.ali@gmail.com

1. INTRODUCTION

The need for network information security has increased recently due to the advancements and popularization of information and network technologies [1]-[12]. Human-based IDSs can either warn or intercept network intrusion, but this is not the case for the traditional network defense mechanisms. The focus of most studies in this field has been on the improvement of the performance of smart network intrusion detection systems (IDSs) [13]-[17] as they are considered an effective solution to network security. Considering the low detection rate (DR) of the existing IDSs in the presence of new attacks, coupled with the high overhead associated with audit data, efforts are being channeled to machine learning-based methods and optimization algorithms for network intrusion detection [18]-[29].

This era of big data is associated with issues on the security of network system. Intrusion detection is receiving much attention due to the need for better security of network infrastructure in recent times. Different machine learning (ML) methods have been combined with optimization algorithms for efficient intrusion detection; for instance, some of the current combinations include fuzzy logic, k-nearest neighbors (KNN), artificial neural network (ANN), particle swarm optimization (PSO), support vector machine (SVM), Cuttlefish optimization algorithm, and artificial immune system (AIM) approaches [30]-[36]. Most of the approaches that combine ML with optimization algorithms have shown better performance as compared to the traditional classification techniques [37]-[40]. Various ML and optimization-based IDS have been proposed in the literature [41]-[43]; for instance, a combination of K-means clustering, NB, C4.5, and Kruskal-Wallis has been proposed by Louvieris *et al.* [44] for the detection of network intrusion with high accuracy. This approach can be used to classify relevant feature sets as it includes a statistical tool for validity.

A study by Črepinšek *et al.* [45] proposed a self-organizing map (SOM) and principal component analysis (PCA)-based IDS that filters noise in dataset and low-variance features using the PCA and fisher discriminant ratio (FDR). It relies on the most discriminative projections that do not depend solely on the explained variance by the prototypes of the eigenvectors generated by the SOM process. However, the major problem of this system is low detection rate (DR) [15]. A time-varying chaos-PSO method has been provided by Bamakan [14] as a new ML-based IDS; the proposed method is based on 2 conventional optimizers which are multiple criteria linear programming (MCLP) and SVM. The parameters of these optimizers were set using the proposed method; it was also used to select the most appropriate feature subsets [46]-[49]. The only problem of this new method is the prolonged training period which needs to be improved. Although these combinations can improve IDS performance in terms of DR and learning speed, further improvement is still needed [50]. Rao and Fatel *et al.* [51] proposed Rao-SVM algorithm that requires no user-defined parameter during the optimization process for mechanical design problems. The new method was evaluated on different benchmark functions and found to perform better than some pf the existing ones. The potential of a new Rao-SVM algorithm in optimal free parameters selection for SVM regression models has been reported by [30] using multi-commodity futures index data retrieved from multi-cut crossover (MCX). From the results, SVM-Rao-SVM performed well in finding the optimal parameters compared to the classical SVM.

The hybrid SVM-Rao-SVM model was presented by Das *et al.* [52] via introduction of a dimension-reduction approach that allows the reduction of the number of input variables using PCA, kernel principal component analysis (KPCA), and independent component analysis (ICA). The study also investigated the possibility of using the multi-commodity futures index data extracted from the MCX in the proposed model. The performance of the proposed model was confirmed to be superior to that of some existing population-inspired models. In another study, the effect of number of generations and sample size on the performance of optimization frameworks was evaluated by Rao and Patel [50] while Crepinšek *et al.* [45] focused on using Rao-SVM to solve the exact problems highlighted in [42] and [53]. A multi-objective Rao-SVM was developed by Nayak and Rout [47] where a matrix of solutions was developed for each objective. For the Rao-SVM model, the teacher selection process was reliant on the best-found solution in the search space while the learners are taught just to maximize that objective. The available solutions in the search space were arranges to arrive at a set of optimal solutions. The study by Shukla *et al.* [54] relied on different teaching methods to present a multi-objective Rao-SVM in which the crossover operator (instead of using a scaler function) was utilized in-between solutions in the teaching & learning phases. Kiziloz *et al.* [40] presented 3 multi-objective Rao-SVM frameworks for FSS-BCP. Among the presented methods, a multi-objective Rao-SVM with scalar transformation (MRao-SVM-ST) was the fastest despite providing a limited number of non-dominated solutions. Regarding the multi-objective Rao-SVM with non-dominated selection (MRao-SVM-NS), it searches the solution space, generate a set of non-dominated solutions, and requires much implementation time. Multi-objective Rao-SVM with minimum distance (MRao-SVM-MD) generates similar solutions to that of MRao-SVM-NS; yet, in a significantly lesser amount of time. The proposed Rao-SVM were evaluated for performance using LR, SVM, and ELM. Sultana and Jabbar [55] stated that FSS in the Wrapper method is made as a black box, meaning that there is no knowledge of the underlying algorithm. The selection of feature subsets is done using inductive algorithms and the selected feature subset are used to estimate the accuracy of the training model. The accuracy level will guide the model in deciding whether features can be added or removed from the selected subset. Hence, the Wrapper methods are considered more computationally complex [56]-[58]. The Filter method is another method where the model initiates with all the available features before selecting the best feature subset based on certain statistical metrics, such as Pearson's correlation [59], ANOVA, LDA, Chi square, and mutual information [60], [61]. These statistical metrics are based on the feature and response variables in the dataset; however, the commonly used statistical metrics are pearson's correlation (PC) and mutual Information methods [61]-[64].

Most of the feature selection methods earlier discussed are dependent on feature subset at the preprocessing level; hence, the methods to be discussed here are the embedded methods as they work in a way allows the selection of the best features during the learning phase [65]-[67]. The advantages of incorporating the feature selection process in the learning process include improved computational cost, better classification accuracy, and avoidance of the need to retrain models whenever new features are added. The embedded method performs feature subset selection, and the learning algorithm interacts in a different manner compared to other feature selection methods. Filter-based learning algorithms are not commonly employed for feature selection, but the Wrapper method tests the quality of the selected features using the learning algorithm [68]. For the embedded method, it addresses the issue of computational complexity as it performs the appropriate model learning and feature selection at the same time; feature selection is done during the model training stage, thereby reducing the computational cost compared to that of the Wrapper method.

When the accuracy of detection is increased, the execution time will sometimes increase by a substantial amount. On the other hand, there may be reduction in the execution time, leading to low accuracy. Hence, the FSS problem can be seen as a multi-objective optimization (MOO) problem that requires more than one solution [45], [52], [69]. For some, accuracy is very important; the solution that offers accuracy is chosen. Meanwhile, for others, the best solution is the one that reduces the execution time even if accuracy is compromised. Rao was developed as a new metaheuristic for various intractable optimization problems and has performed well in such applications compared to other frameworks, such as genetic algorithms (GA), PSO, and ant colony optimization (ACO). The combination of the new multi-objective Rao-SVM framework with supervised machine learning (ML) techniques is proposed in this paper for FSS in binary classification problems. While trying to select the least number of features without impacting the accuracy of FSS problems, the first objective should be the selection of the right number of features, while the second concern should be the accuracy of the detection. The performance of Rao-SVM has been reported as remarkable when compared to other metaheuristics algorithms. The new teaching-learning-based optimization (Rao-SVM) and a set of supervised ML techniques were employed for optimal features subset selection in this study. This work contributes the following to literature: i) the utilization of the Rao-SVM algorithm for feature selection in IDS for the first time; ii) the new Rao-SVM algorithm proposed in this study. The rest of this article is arranged as follows: introduction of the FSS problem presented in section 2; the proposed Rao-SVM presented in section 3; introduction of the machine learning techniques applied with Rao-SVM and experimental setup presented in section 4; the results of the Rao-SVM algorithm in comparison to Rao-SVM presented in section 5; and the conclusion o the study presented in section 6.

2. FEATURE SUBSET SELECTION PROBLEM

Feature subset selection is the process of selectin feature subsets from a large set of features. It is aimed at reducing the complex calculations by relying on fewer number of features to achieved improved performance of classifiers. Various scholars have provided different definitions of FSS [62]; for instance, some defined it as the reduction of the size of the selected feature subset while some considered it a way of improving the prediction accuracy of classifiers. FSS is regarded as a way of establishing the effective subsets that captures the information hidden in a dataset by removing the irrelevant and redundant features. Hence, the aim of FSS is to find the least number of features without significantly affecting the classification accuracy. Extraction of optimal feature subsets is a complex task that currently has no polynomial time algorithm to address it; this implies that FSS is an NP-hard problem [63]. A typical FSS involves 4 typical steps [64]-[67]: i) a search for the selection of individual features that will make up the subsets; ii) evaluation of the subsets and their comparison with each other; iii) determination of whether the termination condition has been met; and iv) check for the establishment of the optimal feature subset based on pre-knowledge.

Problem definition: this study involves two major parts: best feature subset selection, and performance evaluation. Since there are two major objectives, FSS is considered a multi-objective problem. A formal definition of finding optimal solutions through meeting both objectives is provided in (1) and (2).

$$f1 = |k| \quad (1)$$

$$f2 = accuracy\,(k)\ where\ k \subseteq K \quad (2)$$

Where k represents the subset of the original dataset (K) that optimizes f1 and f2 (the objectives). The second part involves the evaluation of the selected feature subsets based on accuracy (an established performance evaluation metric), as provided in (3). Accuracy calculation requires the division of the instances that are classified correctly by all instances.

$$Accuracy = (TP + TN) / (TP + FP + FN + TN) \quad (3)$$

Where TP = true positive, TN = true negative, FP = false positive, and FN = false negative.

The proposed Rao-SVM algorithm was implemented at the FSS phase. It was initialized via random generation of an initial population called the Teacher and a set of Students. The features were represented in the Rao-SVM by combining Rao-SVM with GA, and the features were represented as a chromosome as this is one of the features of GA. The chromosomes were updated by applying crossover and mutation parameters of GA and each solution in the population is considered a chromosome or an individual, as shown in Figure 1. Chromosomes that have a feature gene with a value of 1 are considered selected while those with a value of 0 are not selected. The Rao-SVM executed various iterations ad the teacher is considered the best individual in the population while the rest are the students. After selecting the teacher, the three phases of Rao-SVM are initiated which are the Teacher, Best Classmates (Learner Phase 1), and Learner Phase 2. The Teacher Phase involves the teacher sharing knowledge with each student to improve their understanding while the Best Classmate Phase involves selection of two best students that will interact with the other students. Learner Phase 2 involves random interaction among the each to enhance their understanding. The generation of new chromosomes in the new Rao-SVM was done using special crossover operators called half-uniform crossover and bit-flip mutation operators, as shown in Figure 1 and Figure 2. The crossover operator needs two parent chromosomes (may be a teacher and a student, or two students). The crossover operator depends on the information of the two parent chromosomes. So, if the same gene is present in both parents, the gene is kept; but when the parents feature different genes, the gene of either parent is chosen randomly [32]. This operation results in the generation of one new chromosome. The bit-flip mutation operates on a single chromosome to alter a single gene using a probabilistic ratio; if the gene has a value of zero, it will be updated as one, or vice versa.

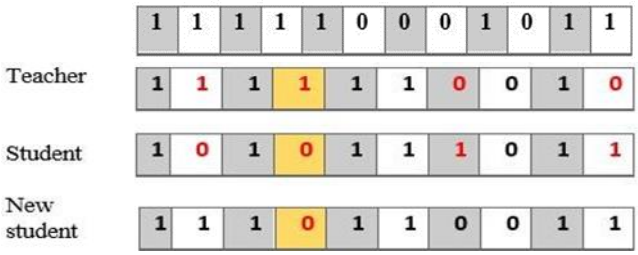

Figure 1. Schematic representation of a chromosome

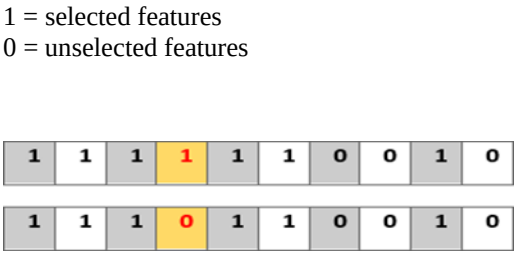

Figure 2. Mutation operator

3. PROPOSED RAO-SVM METHOD

In the proposed algorithm, Rao was implemented at the FSS phase; it was initialized via random generation of the initial population called the Teacher and a set of Students (these represent the potential solutions). Then, the crossover and mutation operators of GA was borrowed to represent the features in the Rao via the representation of the features as chromosomes. Crossover was used to update the chromosome. Each solution in the population is considered an individual/chromosome, as shown in Figure 1. Chromosomes that have a feature gene with a value of 1 are considered selected while those with a value of 0 are not selected. Details of the proposed method are presented in Algorithm 1 and Figure 3.

Algorithm 1: Details of the Rao-SVM algorithm

Step 1: Initialize the population randomly with each population having different set of features

Step 2: Based on the accuracy of the classification for each set of features, specify best and worst set (population)

Step 3: Modify solutions based on the best and worst solutions and random interactions based on New_set= random_set crossover with (best_set crossover with worst_set)

Step 4: If the new set of features better than the old best set (in term of accuracy of classification) then keep the new set else keep the old set

Step 5: Is the termination criteria satisfied or not? if yes report the best set of features, else go to step 3

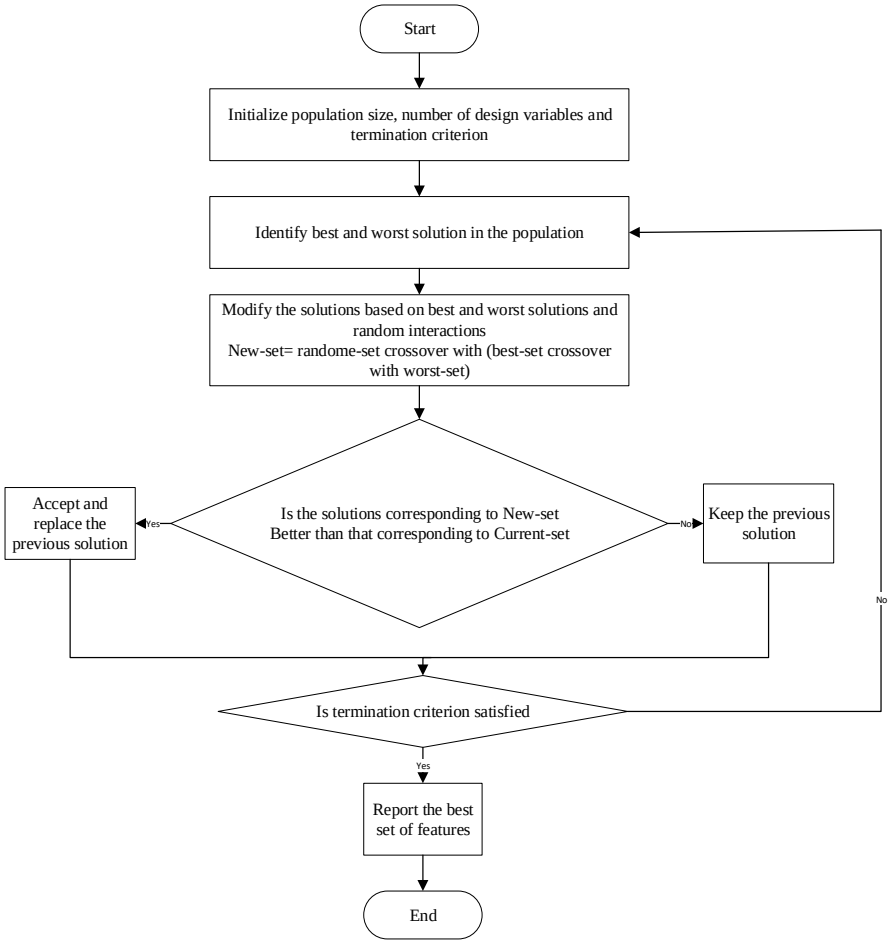

Figure 3. Rao-SVM algorithm

4. EXPERIMENTAL SETUP

The present study evaluated the solutions achieved using Rao-SVM by deploying three ML techniques (LR, SVM, and ELM). LR is a common, fast, and easily implemented classifier; SVM is well-known for its effectiveness in binary classification; whereas ELM is a newly introduced but promising classifier. LR: classification with LR is performed by estimating an event's occurrence probability based on the similarity of given data points. It finds the probability of the event occurrence by employing a sigmoid function. If the occurrence probability of an event is >0.5, then the LR predicts the event as "occurred" or "not occurred", as the case may be. SVM: classification tasks using SVM are performed through the construction of a separating line between the given data points [37]. The data points closest to this line are designated as support vectors (SVs). This line is iteratively constructed through the maximization of the margin between the SV and the line of the classes. This idea originates from the assumption that an increase in the margin can reduce the generalization error. ELM: ELM is built as a feed forward neural network (FFNN) with a hidden layer, an input layer, and an output layer. The training data are fed into the model through the input layer, where they are then weighted and forwarded to the hidden layer via a function. A similar transformation is executed between the hidden and output layers. The FFNN requires iterative tuning of its parameter; however, no parameter tuning occurs in the ELM. Therefore, the learning time of ELM is lower as compared to those of conventional FFNNs.

The experimental scenario, problem instances, and the outcome of the experiments are all presented in this section. In this study, the experiments were performed on two intrusion datasets (KDDCup 99 and CICIDS), which were reduced, because of the focus on binary classification to accommodate only two classes (normal and intrusion). To ensure fair validation, K-fold validation was used, where the value of K is set to 10 [39].

KDDCup 99 dataset was first used to build an IDS at the 3rd international knowledge discovery and data mining tools competition [50]. The defense advanced research projects agency (DARPA) intrusion detection evaluation program was set up in 1998 by the MIT Lincoln Laboratory as a simulated environment

for gathering raw transmission control protocol/internet protocol (TCP/IP) dump data for a local area network (LAN) [46]. It was set up with the aim of comparing various intrusion detection methods based on their performance. A version of the DARPA'98 dataset was used in the KDDCup 99 dataset [31]. The DARPA'98 dataset consists of compressed raw TCP dump data of 7 weeks of network pattern. It is approximately4 gigabytes in size and can be processed into about 5,000,000 connection records, each of about 100 bytes [33]. In the dataset, the two weeks' test data contains approximately 2,000,000 connection records. The KDD training dataset is comprised of about 4,900,000 single connection vectors of 41 features each, which are labeled either as normal or an attack of a specific type [1].

The attack types in the dataset were categorized into four major categories:

a) Probing attack: this is an effort by an attacker to gain network information simply to circumvent the network's security controls. The CICIDS dataset contains both benign and the recent forms of attacks that mimic real-world data principal component analysis of proteomics (PCAPs). The dataset also contains data from network traffic analysis which was performed using a CIC flowmeter. The labeling of the flows is based on the timestamp, the source port, the destination port, the source IP, the destination IP, attack, and protocols.
b) Denial-of-service (DoS) attack: in this type of attack, the intruder intentionally denies legitimate network access by making the system too busy to process legitimate requests.
c) User-to-root (U2R) attack: the attacker gains access to the network by accessing the system as a legitimate user, before exploiting the lapses in some systems to gain root access.
d) Remote-to-user (R2L) attack: this is a form of attack where an invader exploits vulnerability in machines by sending packets to them over a network in a bid to gain local access as a legal user.

Although several types of R2U attacks exist, the most common types are those executed via social engineering. These attacks (DoS, U2R, R2L, and probing) are classified into 22 different attack types in the KDDCup 99 dataset, as shown in Table 1. These do not only refer to the specific case of KDDCup 99 dataset; additionally, several known classifications and taxonomies of computer system attacks were also analyzed in this study [37].

The CICIDS 2017 dataset [18], [43] satisfies the 11 mandatory attributes of a true IDS dataset, which are available protocols, feature set, complete interaction, anonymity, complete capture, attack diversity, complete traffic, metadata, complete network configuration, labeling, and heterogeneity [1], [18], [38]. The dataset contains 3,057,503 rows (devised on 8 files) and each row contains 79 features. Each row is either labeled as benign or as any of the 14 types of attack. Table 2 summarized the types of attack distribution in the benign rows.

In this study, the experiments were performed on a computer running an Intel Core i7-4810 processor with a CPU clock rate of 2.80 GHz and an 8 GB main memory. The classification aspect of the algorithms was done using MATLAB 2017a. The two important parameters that must be decided prior to running Rao-SVM were population size and number of generations. A higher value of these parameters ensures a higher result of accuracy, even though the computation time will be increased. An investigation of a new individual is time inefficient.

Table 1. KDD dataset

Attack class	Types of attacks
DoS	smurt, neptune, pod, teardrop, back, land,
R2L	phf, ftp-write, imap, multihop, warezclient, warezmaster, spy, guess password
U2R	perl, loadmodule, buffer-overflow, rootkit
Probing	portsweep, ipsweep, satan, nmap

Table 2. CICIDS dataset

Attack class	Types of attacks
DOS	DDoS, slowloris, Heratbleed, Hulk, GoldenEye, Slowhttptest
PortScan	Portscan
Bot	Bot
Brute-Force	FTP-Patator, SSH-Patator
Web Attack	Web attack XSS, web attack SQL injection, web attack brute force
Infiltration	Infiltration

5. RESULTS AND DISCUSSION

The parameters used in this study are shown in Table 3. The accuracy result of the KDDCup 99 dataset is presented in Table 4, and the results of the CICIDS 2017 dataset are presented in Table 5. The Tables 4 and 5 present the accuracy results for both datasets. From Table 4, both Rao-SVM and Rao-SVM

offered the same execution time for each ML technique. For each ML, the number of features, accuracy, and execution time were calculated. The numbers in red suggest the best results for both Rao-SVM and Rao-SVM. Rao-SVM consistently presented better accuracies as compared to Rao-SVM using the three ML techniques. It also presented better time accuracy using LR and SVM ML techniques. However, Rao-SVM provided a better execution time with ELM as compared to Rao-SVM. With the CICIDS 2017 dataset, Rao-SVM consistently showed better accuracy than many other algorithms using the three ML techniques. With the LR technique, Rao-SVM presented a better execution time compared to the SVM and ELM techniques, as shown in Table 5.

The detection rate (DR) as shown in (4) refers to the percentage of the correctly classified samples by the classifier into their correct class.

$$Detection\ rate\ = \frac{TP}{TP+FP} \tag{4}$$

Another statistical test is the error rate, which is the proportion of patterns that have been incorrectly classified by the model. ER is calculated based on (5).

$$Error\ Rate\ = \frac{FP+FN}{TP+FP+FN+TN} \tag{5}$$

Table 6 illustrates the results of (4) and (5). Another statistical test (T-test) was applied to demonstrate the superiority of Rao-SVM over Rao-SVM. Table 7 shows the p-values and t-values where the small values portrayed the significance of the new Rao-SVM algorithm. Comparison results with existing works showed that the proposed model performed better than many existing works in terms of accuracy as shown in Table 8.

Table 3. Parameters used in this study

Parameter	Value
Population size for Rao	40
Number of generations for Rao	60
Crossover type	Half-uniform
Mutation type	Bit-flip

Table 4. Accuracy result of KDDCup 99 dataset

Classifier	**Rao**	
LR	No. of features	Accuracy
	2	0.992
	4	0.994
Total time	11.4023	
SVM	3	0.97
	4	0.998
	5	1.00
Total time	1305.0355	
ELM	2	0.993
	3	0.995
	4	0.999
Total time	4.4261	

Table 5. Accuracy result of CICIDS 2017 dataset

Classifier	**Rao**	
LR	No. of features	Accuracy
	8	0.94
	9	0.954
	14	0.9552
	15	0.96
	23	0.976
Total time	29.089	
SVM	14	0.90
	17	0.922
	22	0.93
Total time	5484.097	
ELM	6	0.901
	7	0.92
Total time	6.5312	

Table 6. Results of (4) and (5)

	KDDCup 99	CICIDS 2017
Detection Rate	0.999	0.990
Error Rate	0.00445	0.0267

Table 7. T-Test

	KDDCup 99	CICIDS 2017
P-Value	0.0157	0.00678
T-Value	3.175	4.051

Table 8. Comparison with existing works

Ref.	Dataset	Accuracy
[47]	CICIDS	97.90 %
[2]	CICIDS	97.08 %
[41]	KDD	99.75 %
[49]	KDD	99.89 %
Proposed method	CICIDS	97.6 %
Proposed method	KDD	100 %

6. CONCLUSION

This paper proposes a new (Rao-SVM) for feature subset selection problems in intrusion detection. The performance of the new algorithm was demonstrated to be superior to many other algorithms in FSS problems on two large intrusion datasets. The proposed Rao-SVM consistently presented better accuracy in the execution time. On the statistical tests (confusion matrix) applied to the Rao-SVM detection rate and error rate extracted from the confusion matrix, Rao-SVM showed a higher detection rate for both the KDDCup 99 and ICIDS2017 datasets. It showed a low error rate for the two datasets. As a recommendation, the proposed Rao-SVM should be applied to multi-class classification problems, and more ML techniques could be used for evaluating its performance.

ACKNOWLEDGEMENTS

The authors would like to thank University of Diyala and Al Salam University College for their facilities and support; and Universitas Ahmad Dahlan to support this collaborative research.

REFERENCES

[1] I. Aljarah and S. A. Ludwig, "MapReduce intrusion detection system based on a particle swarm optimization clustering algorithm," *2013 IEEE Congress on Evo. Comp.*, 2013, pp. 955-962, doi: 10.1109/CEC.2013.6557670.

[2] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *Journal of Computational Science*, vol. 25, pp. 152–160, 2018, doi: 10.1016/j.jocs.2017.03.006.

[3] I. Idrissi, M. Boukabous, M. Azizi, O. Moussaoui, and H. E. Fadili, "Toward a deep learning-based intrusion detection system for iot against botnet attacks," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 1, pp. 110–120, 2021, doi: 10.11591/ijai.v10.i1.pp110-120.

[4] A. M. Al-Ghaili *et al.*, "A review of anomaly detection techniques in advanced metering infrastructure," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 266–273, 2021, doi: 10.11591/eei.v10i1.2026.

[5] B. Altay, T. Dokeroglu, and A. Cosar, "Context-sensitive and keyword density-based supervised machine learning techniques for malicious webpage detection," *Soft Computing - A Fusion of Foundations, Methodologies and Applications*, vol. 23, no. 12, pp. 4177–4191, 2019, doi: 10.1007/s00500-018-3066-4.

[6] P. Wanda, M. E. Hiswati, and H. J. Jie, "DeepOSN: Bringing deep learning as malicious detection scheme in online social network," *IAES International Journal of Artificial Intelligence*, vol. 9, no. 1, pp. 146–154, 2020, doi: 10.11591/ijai.v9.i1.pp146-154.

[7] A. W. Muhammad, C. F. M. Foozy, and K. M. B. Mohammad, "Multischeme feedforward artificial neural network architecture for ddos attack detection," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 458–465, 2020, doi: 10.11591/eei.v10i1.2383.

[8] V. Mach, M. Adamek, J. Valouch, and K. Barcova, "Control and indicating equipment communicating via the peripheral component interconnect express bus," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 2, pp. 729–738, 2020, doi: 10.11591/eei.v9i2.1753.

[9] M. S. I. Sharifuddin, S. Nordin, and A. M. Ali, "Comparison of CNNs and SVM for voice control wheelchair," *IAES International Journal of Artificial Intelligence*, vol. 9, no. 3, pp. 387-393, 2020, doi: 10.11591/ijai.v9.i3.pp387-393.

[10] A. Boukhalfa, N. Hmina, and H. Chaoui, "Parallel processing using big data and machine learning techniques for intrusion detection," *IAES International Journal of Artificial Intelligence*, vol. 9, no. 3, pp. 553–560, 2020, doi: 10.11591/ijai.v9.i3.pp553-560.

[11] A. J. Mohammed, M. H. Arif, and A. A. Ali, "A multilayer perceptron artificial neural network approach for improving the accuracy of intrusion detection systems," *IAES International Journal of Artificial Intelligence*, vol. 9, no. 4, pp. 609–615, 2020, doi: 10.11591/ijai.v9.i4.pp609-615.

[12] T. Ghrib, M. Benmohammed, and P. S. Pandey, "Automated diagnosis of attacks in internet of things using machine learning and frequency distribution techniques," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 2, pp. 950–961, 2021, doi: 10.11591/eei.v10i2.2766.

[13] M. Alsajri, M. A. Ismail, and S. Abdul-Baqi, "A Review on the Recent Application of Jaya Optimization Algorithm," *2018 1st Annual International Conference on Information and Sciences (AiCIS)*, 2018, pp. 129-132, doi: 10.1109/AiCIS.2018.00034.

[14] S. M. H. Bamakan, H. Wang, T. Yingjie, and Y. Shi, "An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization," *Neurocomputing*, vol. 199, pp. 90–102, 2016, doi: 10.1016/j.neucom.2016.03.031.

[15] J. Cai, J. Luo, S. Wang, and S. Yang, "Feature selection in machine learning: A new perspective," *Neurocomputing*, vol. 300, pp. 70–79, 2018, doi: 10.1016/j.neucom.2017.11.077.

[16] S. Rajagopal, P. P. Kundapur, and H. K. Siddaramappa, "A predictive model for network intrusion detection using stacking approach," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp. 2734–2741, 2020, doi: 10.11591/ijece.v10i3.pp2734-2741.

[17] S. M. Sharath, P. Manjunatha, and H. R. Shwetha, "Insights on critical energy efficiency approaches in internet-of-things application," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 4, pp. 2925–2933, 2021, doi: 10.11591/ijece.v11i4.pp2925-2933.

[18] A. Chaudhary, V. Tiwari, and A. Kumar, "A novel intrusion detection system for ad hoc flooding attack using fuzzy logic in mobile ad hoc networks," *Int. Conf. Rec. Adv. and Innov. Eng.*, 2014, pp. 1-4.
[19] M. K. Hossain and M. M. Haque, "Semi-supervised learning approach using modified self-training algorithm to counter burst header packet flooding attack in optical burst switching network," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 4, pp. 4340–4351, 2020, doi: 10.11591/ijece.v10i4.pp4340-4351.
[20] K. S. Yin and M. A. Khine, "Optimal remote access Trojans detection based on network behavior," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 3, pp. 2177–2184, 2019, doi: 10.11591/ijece.v9i3.pp2177-2184.
[21] Y. Khamayseh, M. B. Yassein, and M. Abu-Jazoh, "Intelligent black hole detection in mobile AdHoc networks," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 3, pp. 1968–1977, 2019, doi: 10.11591/ijece.v9i3.pp1968-1977.
[22] H. H. Ibrahim, *et al.*, "A comprehensive study of distributed Denial-of-Service attack with the detection techniques," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 4, pp. 3685–3694, 2020, doi: 10.11591/ijece.v10i4.pp3685-3694.
[23] A. Boukhalfa, A. Abdellaoui, N. Hmina, and H. Chaoui, "LSTM deep learning method for network intrusion detection system," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp. 3315–3322, 2020, doi: 10.11591/ijece.v10i3.pp3315-3322.
[24] P. I. Priyadarsini and G. Anuradha, "A novel ensemble modeling for intrusion detection system," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 1963–1971, 2020, doi: 10.11591/ijece.v10i2.pp1963-1971.
[25] M. Narender and B. N. Yuvaraju, "Preemptive modelling towards classifying vulnerability of DDoS attack in SDN environment," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 1599–1611, 2020, doi: 10.11591/ijece.v10i2.pp1599-1611.
[26] M. C. Belavagi and B. Muniyal, "Multiple intrusion detection in RPL based networks," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 467–476, 2020, doi: 10.11591/ijece.v10i1.pp467-476.
[27] A. Saravanan, S. Sathya Bama, S. Kadry, and L. K. Ramasamy, "A new framework to alleviate DDoS vulnerabilities in cloud computing," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 5, pp. 4163–4175, 2019, doi: 10.11591/ijece.v9i5.pp4163-4175.
[28] M. S. Vidya and M. C. Patil, "Reviewing effectivity in security approaches towards strengthening internet architecture," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 5, pp. 3862–3871, 2019, doi: 10.11591/ijece.v9i5.pp3862-3871.
[29] Y. N. Doddamani and U. C. Kapale, "A transition from manual to intelligent automated power system operation - A indicative review," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 4, pp. 2274–2280, 2019, doi: 10.11591/ijece.v9i4.pp2274-2280.
[30] S. P. Das and S. Padhy, "A novel hybrid model using teaching–learning-based optimization and a support vector machine for commodity futures index forecasting," *Int. J. Mach. Learn. Cybern.*, vol. 9, no. 1, pp. 97–111, 2018.
[31] E. De la Hoz, E. De La Hoz, A. Ortiz, J. Ortega, and B. Prieto, "PCA filtering and probabilistic SOM for network intrusion detection," *Neurocomputing*, vol. 164, pp. 71–81, 2015, doi: 10.1016/j.neucom.2014.09.083.
[32] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018, doi: 10.1016/j.neucom.2017.10.009.
[33] T. Dokeroglu, "Hybrid teaching–learning-based optimization algorithms for the quadratic assignment problem," *Computers & Industrial Engineering*, vol. 85, pp. 86–101, 2015, doi: 10.1016/j.cie.2015.03.001.
[34] J. A. Jupin, T. Sutikno, M. A. Ismail, M. S. Mohamad, S. Kasim, and D. Stiawan "Review of the machine learning methods in the classification of phishing attack," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 4, pp. 1545–1555, 2019, doi: 10.11591/eei.v8i4.1344.
[35] S. Rajagopal, K. S. Hareesha, and P. P. Kundapur, "Performance analysis of binary and multiclass models using azure machine learning," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 978–986, 2020, doi: 10.11591/ijece.v10i1.pp978-986.
[36] K. Farhana, M. Rahman, and M. T. Ahmed, "An intrusion detection system for packet and flow based networks using deep neural network approach," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, pp. 5514–5525, 2020, doi: 10.11591/ijece.v10i5.pp5514-5525.
[37] S. Dumais, J. Platt, D. Heckerman, and M. Sahami, "Inductive learning algorithms and representations for text categorization," *Proceedings of the seventh international conference on Information and knowledge management*, 1998, pp. 148–155, doi: 10.1145/288627.288651.
[38] A. S. Eesa, Z. Orman, and A. M. A. Brifcani, "A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems," *Expert Systems with Applications*, vol. 42, no. 5, pp. 2670–2679, 2015, doi: 10.1016/j.eswa.2014.11.009.
[39] C. Guo, Y. Ping, N. Liu, and S.-S. Luo, "A two-level hybrid approach for intrusion detection," *Neurocomputing*, vol. 214, pp. 391–400, 2016, doi: 10.1016/j.neucom.2016.06.021.
[40] H. E. Kiziloz, A. Deniz, T. Dokeroglu, and A. Cosar, "Novel multiobjective TLBO algorithms for the feature subset selection problem," *Neurocomputing*, vol. 306, pp. 94–107, 2018, doi: 10.1016/j.neucom.2018.04.020.
[41] M. K. Khaleel, M. A. Ismail, U. Yunan, and S. Kasim, "Review on intrusion detection system based on the goal of the detection system," *Int. J. Integr. Eng.*, vol. 10, no. 6, 2018, doi: 10.30880/ijie.2018.10.06.028.
[42] W.-C. Lin, S.-W. Ke, and C.-F. Tsai, "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors," *Knowledge-based Syst.*, vol. 78, pp. 13–21, 2015, doi: 10.1016/j.knosys.2015.01.009.
[43] Y. Li, J.-L. Wang, Z.-H. Tian, T.-B. Lu, and C. Young, "Building lightweight intrusion detection system using wrapper-based feature selection mechanisms," *Computers & Security*, vol. 28, no. 6, pp. 466-475, 2009.

[44] P. Louvieris, N. Clewley, and X. Liu, "Effects-based feature identification for network intrusion detection," *Neurocomputing*, vol. 121, pp. 265–273, 2013, doi: 10.1016/j.neucom.2013.04.038.
[45] M. Črepinšek, S.-H. Liu, and L. Mernik, "A note on teaching–learning-based optimization algorithm," *Information Sciences*, vol. 212, pp. 79–93, 2012, doi 10.1016/j.ins.2012.05.009.
[46] S. Mahdavifar and A. A. Ghorbani, "Application of deep learning to cybersecurity: A survey," *Neurocomputing*, vol. 347, pp. 149–176, 2019, doi: 10.1016/j.neucom.2019.02.056.
[47] M. A. Mohammed, *et al*., "A Focal load balancer based algorithm for task assignment in cloud environment," *2018 10th Int. Conf. Elec., Compt. Artif. Intell.*, 2018, pp. 1-4, doi: 10.1109/ECAI.2018.8679043.
[48] M. R. Nayak, C. K. Nayak, and P. K. Rout, "Application of multi-objective teaching learning based optimization algorithm to optimal power flow problem," *Pro. Tech.*, vol. 6, pp. 255–264, 2012, doi: 10.1016/j.protcy.2012.10.031.
[49] R. V. Rao, V. J. Savsani, and D. P. Vakharia, "Teaching–learning-based optimization: a novel method for constrained mechanical design optimization problems," *Computer-Aided Design*, vol. 43, no. 3, pp. 303–315, 2011.
[50] R. V. Rao, V. J. Savsani, and J. Balic, "Teaching–learning-based optimization algorithm for unconstrained and constrained real-parameter optimization problems," *Eng. Opt.*, vol. 44, no. 12, pp. 1447–1462, 2012.
[51] R. V. Rao and V. Patel, "An improved teaching-learning-based optimization algorithm for solving unconstrained optimization problems," *Scientia Iranica*, vol. 20, no. 3, pp. 710–720, 2013, doi: 10.1016/j.scient.2012.12.005.
[52] S. P. Das, N. S. Achary, and S. Padhy, "Novel hybrid SVM-TLBO forecasting model incorporating dimensionality reduction techniques," *Appl. Intell.*, vol. 45, no. 4, pp. 1148–1165, 2016, doi: 10.1007/s10489-016-0801-3.
[53] R. Sen, M. Chattopadhyay, and N. Sen, "An efficient approach to develop an intrusion detection system based on multi layer backpropagation neural network algorithm: IDS using BPNN algorithm," *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, 2015, pp. 105–108, doi: 10.1145/2751957.2751979.
[54] A. Shukla, S. Kumar, and H. Singh, "ANN based execution time prediction model and assessment of input parameters through ISM.," *Int. Arab J. Inf. Technol.*, vol. 17, no. 5, pp. 683–691, 2020, doi: 10.34028/iajit/17/5/1.
[55] A. Sultana and M. A. Jabbar, "Intelligent network intrusion detection system using data mining techniques," *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, 2016, pp. 329-333, doi: 10.1109/ICATCCT.2016.7912017.
[56] P. Tao, Z. Sun and Z. Sun, "An Improved Intrusion Detection Algorithm Based on GA and SVM," *IEEE Access*, vol. 6, pp. 13624-13631, 2018, doi: 10.1109/ACCESS.2018.2810198.
[57] Y. Tian, M. Mirzabagheri, S. M. H. Bamakan, H. Wang, and Q. Qu, "Ramp loss one-class support vector machine; a robust and effective approach to anomaly detection problems," *Neurocomputing*, vol. 310, pp. 223–235, 2018.
[58] A. H. Ali, Z. F. Hussain, and S. N. Abd, "Big Data Classification Efficiency Based on Linear Discriminant Analysis." *Iraqi Journal For Computer Science and Mathematics*, vol. 1, no. 1, pp. 7-12, 2020, doi: 10.52866/ijcsm.2019.01.01.001.
[59] S. N. Abd, M. Alsajri and H. R. Ibraheem, "Rao-SVM Machine Learning Algorithm for Intrusion Detection System." *Iraqi Journal For Computer Science and Mathematics*, vol. 1, no. 1, pp. 23-27, 2020, doi: 10.52866/ijcsm.2019.01.01.004.
[60] M. A. Mohammed, I. A. Mohammed, R. A. Hasan, N. Ţăpuş, A. H. Ali, and O. A. Hammood, "Green Energy Sources: Issues and Challenges," *2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, 2019, pp. 1-8, doi: 10.1109/ROEDUNET.2019.8909595.
[61] M. A. Mohammed, Z. H. Salih, N. Ţăpuş, and R. A. K. Hasan, "Security and accountability for sharing the data stored in the cloud," *2016 15th RoEduNet Conference: Networking in Education and Research*, 2016, pp. 1-5, doi: 10.1109/RoEduNet.2016.7753201.
[62] M. A. Mohammed and N. Ţăpuş, "A novel approach of reducing energy consumption by utilizing enthalpy in mobile cloud computing," *Studies in Informatics and Control*, vol. 26, no. 4, pp. 425–434, 2017, doi: 10.24846/v26i4y201706.
[63] N. Q. Mohammed, M. S. Ahmed, M. A. Mohammed, O. A. Hammood, H. A. N. Alshara and A. A. Kamil, "Comparative Analysis between Solar and Wind Turbine Energy Sources in IoT Based on Economical and Efficiency Considerations," *2019 22nd International Conference on Control Systems and Computer Science (CSCS)*, 2019, pp. 448-452, doi: 10.1109/CSCS.2019.00082.
[64] R. A. I. Alhayali, M. A. Ahmed, Y. M. Mohialden, and A. H. Ali, "Efficient method for breast cancer classification based on ensemble hoffeding tree and naïve Bayes," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, pp. 1074–1080, 2020, doi: 10.11591/ijeecs.v18.i2.pp1074-1080.
[65] Z. H. Salih, G. T. Hasan, and M. A. Mohammed, "Investigate and analyze the levels of electromagnetic radiations emitted from underground power cables extended in modern cities," *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2017, pp. 1-4, doi: 10.1109/ECAI.2017.8166452.
[66] Z. H. Salih, G. T. Hasan, M. A. Mohammed, M. A. S. Klib, A. H. Ali, and R. A. Ibrahim, "Study the Effect of Integrating the Solar Energy Source on Stability of Electrical Distribution System," *2019 22nd International Conference on Control Systems and Computer Science*, 2019, pp. 443-447, doi: 10.1109/CSCS.2019.00081.
[67] N. D. Zaki, N. Y. Hashim, Y. M. Mohialden, M. A. Mohammed, T. Sutikno, and A. H. Ali, "A real-time big data sentiment analysis for iraqi tweets using spark streaming," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 4, pp. 1411–1419, 2020, doi: 10.11591/eei.v9i4.1897.
[68] N. M. Hussien, Y. M. Mohialden, N. T. Ahmed, M. A. Mohammed, and T. Sutikno, "A smart gas leakage monitoring system for use in hospitals," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 2, pp. 1048–1054, 2020, doi: 10.11591/ijeecs.v19.i2.pp1048-1054.
[69] M. Dash and H. Liu, "Feature selection for classification," *Intell. data Anal.*, vol. 1, no. 1–4, pp. 131–156, 1997, doi: 10.1016/S1088-467X(97)00008-5.