Received: May 23, 2023. Revised: August 1, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Hybrid Intrusion Detection Systems Based Mean-Variance Mapping Optimization Algorithm and Random Search

Adil L. Albukhnefis[1]* **Amar A. Sakran[2]** **AtaAllah Saleh Mahe[3]** **Maryam Imran Mousa[4]**
Ahmed Mohsin Mahdi[1] **Aqeel hamza al-fatlawi[5]**

[1]*College of Computer Science and Information Technology, University of Al-Qadisiyah, Iraq*
[2]*College of Biomedical Informatics, University of information technology and Communication, Iraq*
[3]*Ministry of Industry and Minerals, Iraq*
[4]*Ministry of Education, Al-Qadisiyah Education Directorate, Iraq*
[5]*Department of Computer Techniques, Imam Kadhum College, Iraq*
* Corresponding author's Email: adil.lateef@qu.edu.iq

Abstract: Intrusion detection systems are critical in identifying and mitigating cyber threats. However, the intrusion data often contains insufficient features, which can adversely affect the classification accuracy of machine learning algorithms. To effectively select optimal features from intrusion attacks, a highly efficient model is required to extract highly correlated features. Nevertheless, traditional detection systems may experience low accuracy and high false-positive rates. This paper proposes a hybrid model for improving intrusion detection systems using mean-variance mapping optimization (MVMO) and random search (MVMOR). The strategy of the proposed model is MVMO algorithm is used to search for the optimal feature subset. while, the random search is employed to optimize the hyperparameters of the machine learning algorithm (classifier). The proposed hybrid model seeks to optimize the feature selection and parameters of classifiers at some time. The performance of the hybrid model is evaluated on the NSL-KDD as a benchmark dataset. The proposed MVMOR achieves an accuracy of 88%, while the conventional MVMO achieved only an 80% accuracy rate. The empirical results show the proposed model has the potential to offer better protection against various cyber threats, thus making a valuable contribution to the field of Cybersecurity.

Keywords: Intrusion detection systems, Optimize machine learning algorithms, Feature selection, Mean-variance mapping optimization (MVMO), Cybersecurity.

1. Introduction

Meta-heuristic optimization is a field of computer science that uses algorithms and engineering models to optimize candidates and discover potentially best solutions using random factors [1]. Several meta-heuristic optimization algorithms are inspired by nature or animal behaviour [2], such as particle swarm optimization (PSO) [3], genetic algorithm (GA) [4], gray wolf optimizer (GWO) [5], ant colony optimization (ACO) [6], bat search algorithm (BSA) [7], and dolphin echolocation (DoE) [8]. These algorithms are highly efficient in searching, flexible in solving various optimization problems, and perform better than conventional search methods. The exponential data growth in today's data science is due to the increasing number of devices that generate this data [9]. Feature selection is a valuable data mining tool to optimize big or noisy data in certain features. The wrapper model, which relies on trial and error to select relevant features that match the data's goal, is one feature selection strategy [10].

Metaheuristic optimization structures the wrapper model's randomness [11, 12]. In particular, this work uses the mean-variance mapping optimization (MVMO) algorithm for feature ranking and random search for parameter tuning. MVMO is a highly efficient and flexible algorithm for various problems in the context of meta-heuristic optimization [13–15]. The algorithm has several unique statistical properties, including using a

Received: May 23, 2023. Revised: August 1, 2023.

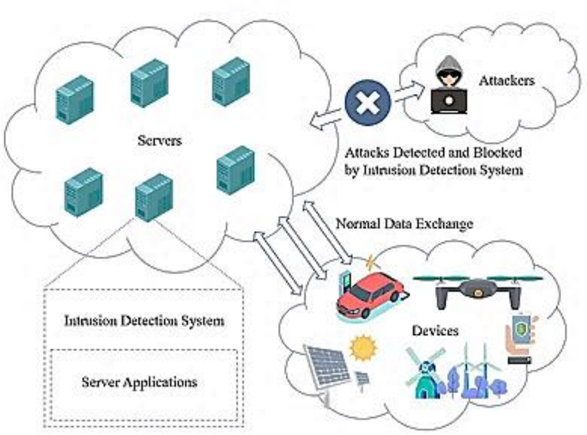
Servers
Attackers
Attacks Detected and Blocked by Intrusion Detection System
Normal Data Exchange
Intrusion Detection System
Server Applications
Devices

Figure. 1 The scenario of applying the IDS in networks

mapping function for the mutation operation based on two critical statistical functions: the mean and the variance of the set of best solutions. Developed initially for meta-heuristic searches in the continuous domain, MVMO is limited to a discrete interval of [0, 1] when selecting features via binary search. It is essential to maintain high diversity to avoid stagnation or sliding into local optima, as noted in [16, 17]. The hybrid algorithm has the potential to support frequent jumps toward the global solution, improving the overall progress of the search. The intrusion detection system (IDS) analyses the frequency and nature of attacks, and organizations can use this data to improve their security measures or implement more efficient controls [18]. In addition, an intrusion detection system can help organizations identify network device configuration issues or errors. Fig. 1 shows the scenario of applying the IDS in networks.

Integrating metaheuristic algorithms and wrapper models into intrusion detection systems provide an intelligent and adaptive approach to cyber threat detection and mitigation. It provides improved accuracy, adaptability, scalability, and automation, overcoming the limitations of traditional rule-based methods and improving the overall security of networks and systems. This paper proposes a hybrid model that combines mean-variance mapping optimization (MVMO) and random search (MVMOR) to enhance intrusion detection systems. The MVMO algorithm is used in the proposed model's search strategy to find the ideal feature subset, and random search is used to optimize the machine learning algorithm's (classifier's) hyperparameters. The proposed hybrid model, MVMOR, combines mean-variance mapping optimization (MVMO) and random search to improve intrusion detection systems. The model uses meta-heuristic optimization algorithms to optimize the proposed solutions and identify the most important features for network attribute analysis. The proposed model uses the random search strategy to optimize the machine learning algorithm (classifier) hyperparameters. The proposed hybrid model aims to optimize the feature selection and classifier parameters simultaneously.

- **Contributions**

Contributions highlight this research's innovative techniques and methodologies, leading to significant progress in intrusion detection systems. Several noteworthy contributions are presented in the proposed model:

1. It introduces MVMOR, a novel hybrid model combining mean-variance mapping optimization (MVMO) with random search. This hybrid approach aims to improve the performance of intrusion detection systems.
2. Using metaheuristic optimization algorithms to refine the proposed solutions and effectively identify the critical features for network attribute analysis. This process ensures comprehensive and accurate network attribute evaluation.
3. The proposed methodology achieves better performance and overall system optimization by optimizing feature selection and classifier parameters simultaneously. By considering these two aspects together, the method ensures comprehensive optimization and improved performance.

- **Paper organization**

The remainder of this paper is organized as follows. Section 2 presents related work on pre-processing, verifying, and identifying hand veins. The proposed model and its components are discussed in sections 3. and 4, which introduce the principles of MVMO and the wrapper model, respectively. The experimental results and analysis are discussed in section 4. Finally, the conclusions of this work and future improvements are presented in section 6.

2. Related works

Numerous studies have suggested optimizing trait selection (F.S.). However, the majority of these studies have utilized standalone metaheuristic algorithms, such as particle swarm optimization (PSO), gray wolf optimizer (GWO), and bat search algorithm (B.A.), without improving the search operations within these algorithms. The beneficial models when seeking to optimize the feature selection and parameters of classifiers to improve the accuracy of intrusion detection systems

In their study, Almasoudy et al. [18] introduced a hybrid model based on bat algorithm (B.A.) for optimizing support vector machine (SVM) parameters and selecting optimal features. The model utilized a pool of bat vectors, where the first two positions were assigned to SVM parameters, and the rest of the vector represented the feature selection mask. The proposed model's reliance on parameter adjustment based on gradients introduces limitations in terms of the search space for the algorithm. Additionally, using a wrapper method for feature selection does not guarantee a reduction in the number of selected features. Consequently, the performance of the SVM algorithm may suffer due to its inefficiency in handling high-dimensional problems.

In another study by the author [12], two metaheuristic algorithms, namely particle swarm optimization (PSO) and bat search algorithm (BSA), were proposed to search for the best solutions individually, which were shared between the two algorithms. However, the proposed model suffered from stagnation and failed to enhance or reduce the local optima problem.

In [19] the authors proposed a method in the field of feature selection. It combines the Naive Bayes classifier and the bat algorithm to select a subset of features that contribute most to classification accuracy. However, a potential limitation of this approach is the assumption of feature independence in Naive Bayes, which may not be present in real-world scenarios where features are correlated or have complex relationships. This limitation could affect the model's ability to accurately capture feature dependencies, potentially leading to suboptimal feature subsets and lower performance in feature selection tasks.

Taha et al. [20] utilized Naïve Bayes (N.B.) to assist B.A. in selecting optimal subgroup features. They proposed decreasing the bat's velocity when the difference between the past and current position is negative. However, this system failed to improve the behaviour-based search progress, and the variety of proposed solutions still left much to be desired when exploring the search process.

R. Nuiaa et al. [21] proposed the proactive feature selection (PFS) model for detecting cyber-attacks based on subset feature selection. They introduced a nature-inspired optimization algorithm and a proactive feature selection threshold to optimize the feature selection technique. However, the proposed model was only applied to optimize feature selection and not improve the overall search process.

3. Mean-variance mapping optimization (MVMO)

MVMO is a type of population-based stochastic optimization algorithm, a novel optimization approach [8, 14, 15]. Like other stochastic optimization methods, MVMO employs evolutionary operations such as selection, crossover, and mutation[20]. However, what sets MVMO apart is that it constrains the search space of all optimization variables and the output of internal operations between the values of [0,1]. Additionally, MVMO applies a mapping function as a mutation operation on the offspring generated through the crossover. This mapping function is calculated based on the mean and variance of the n-best solutions and is used to optimize the offspring further. Eqs. (1) to (5) illustrate the mathematical formals are used to find the new offspring.

$$x_j' = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{1}$$

Where: x_i' the mean value of offspring jth, n dimension of offspring, and j the sequence number.

$$V_j = \frac{1}{n}\sum_{i=1}^{n}(x_i - x_j')^2 \tag{2}$$

Where:

The v_i is a variance. The new population is generated by applying the H-function.

$$X_j = h_x + (1 - h_1 + h_0) * x_j - h_0 \tag{3}$$

Where:

X_i is offspring, h is a H-function is defined as follows.

$$h = x_j(1 - e^{-xs_1}) + (1 + x)e^{-(1-x)s_2} \tag{4}$$

where:

$h_x = h(x = x_i)$, $h_0 = h(x = 0)$, $h_1 = h(x = 1)$

The s_1, and s_2 shape variable depends on the value of S_i, (i =1 or 2) which calculated by Eq. 5.

$$s_i = -\ln(v_j)\, fs \tag{5}$$

Where:

fs is function control on shapes variables.

4. Wrapper model

Wrapper model feature selection is a widespread technique in the field of machine learning used to select the most relevant features for a given task [21].

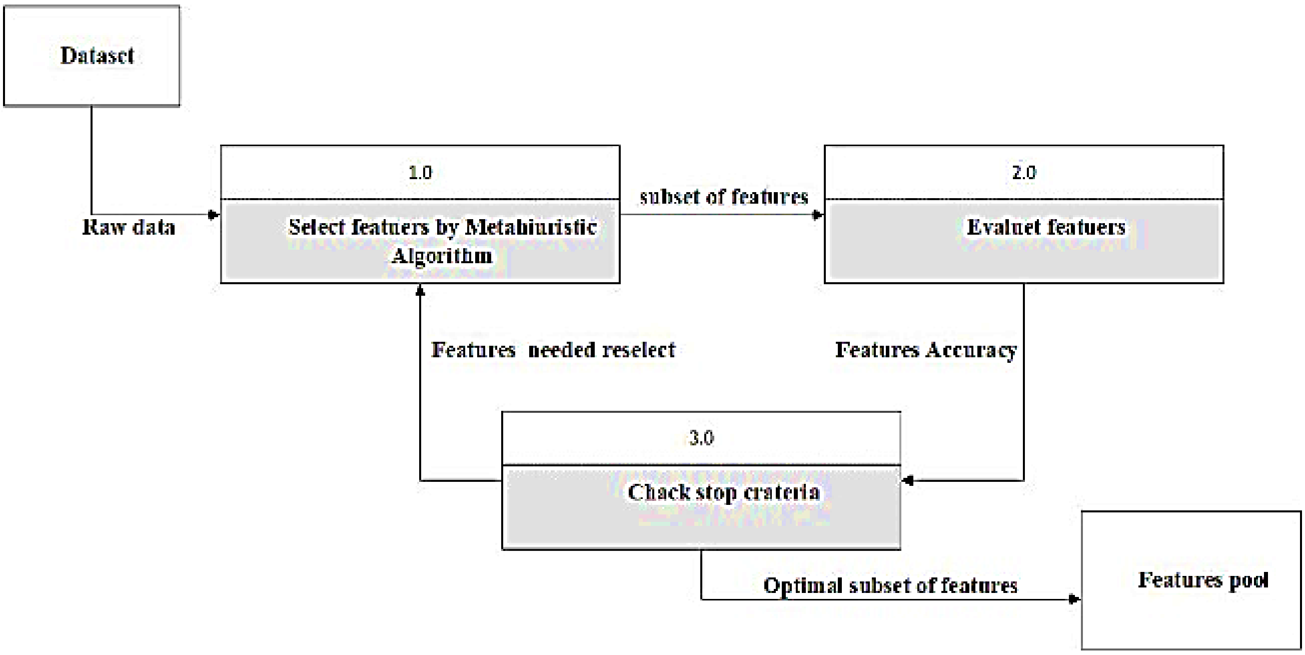

Figure 2. Wrapper feature selection model

The method involves training a model multiple times using various subsets of the available features and evaluating each model's performance to identify the most crucial features. This approach aims to maximize the model's performance while minimizing the number of features used [22].

The process of feature selection is viewed as an optimization problem. The wrapper model utilizes a particular learning algorithm, such as a decision tree or a neural network, as the wrapper to assess the model's performance on a specific task and determine which features are most significant. The wrapper model is a feature selection method with several advantages, including its ability to handle complex feature interactions and non-linear relationships. It provides a more accurate and reliable feature selection process than other methods, such as filters or embedded feature selection techniques. The method involves two primary phases: feature subset generation and model evaluation [23-25].

During the feature subset generation stage, a subset of the available features is selected for each model iteration, either randomly or using techniques such as forward or backward selection or genetic algorithms. The wrapper model approach is then used to train the model on the subset of features that performs the best after being evaluated using a specific performance metric, such as accuracy.

The main drawback of the wrapper model is the computational cost of training multiple models with various subsets of features, which can be especially problematic for large datasets or complex models that require a lot of computational power [26].

Different methods have been proposed to address this issue, such as training the models using a subset of the data or using model ensembles to reduce variance in the feature selection process. Despite its drawbacks, the wrapper model remains a widely used and effective technique for feature selection in machine learning. Fig. 2 shows the principles wrapper model.

5. Proposed MVMOR Model

The system under consideration comprises three fundamental phases: Initialization of machine learning perimeters and preparation data, feature selection, and tuning machine learning algorithm (ML) parameters. Fig. 3 illustrates the main steps and strategy of the proposed model (MVMOR).

5.1 Initialize the algorithm parameters and prepper dataset

The proposed approach uses hot-coding techniques to convert sets of attributes from nominal to numeric values to perform analysis. The one-hot coding method is used to convert non-numeric attributes to numeric attributes. The pre-processing phase is crucial in normalizing the dataset for specific scale values within a defined range. This ensures that bias is removed from the data set while statistical properties are preserved. The data are divided into training and testing to train the model. In this way, the model can be trained on the training dataset, while the test dataset serves as a means to validate the model's effectiveness. It is worth noting that hot coding can be a very effective means of converting nominal attributes into numerical attributes. The data

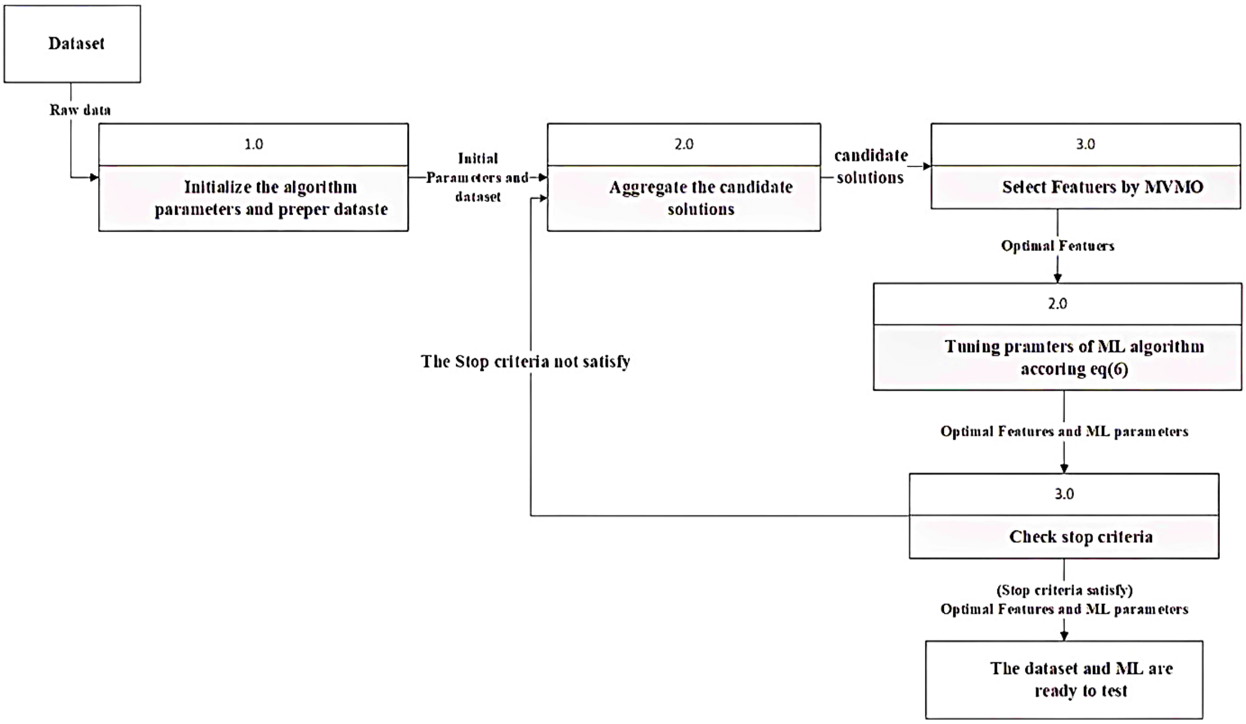
Dataset
Raw data
1.0
Initialize the algorithm parameters and preper dataste
Initial Parameters and dataset
2.0
Aggregate the candidate solutions
candidate solutions
3.0
Select Featuers by MVMO
Optimal Featuers
2.0
Tuning pramters of ML algorithm accoring eq(6)
Optimal Features and ML parameters
3.0
Check stop criteria
The Stop criteria not satisfy
(Stop criteria satisfy)
Optimal Features and ML parameters
The dataset and ML are ready to test

Figure. 3 Main steps of the proposed MVMOR mode

can be more easily analyzed and modeled, giving researchers valuable insights into network traffic's underlying patterns and behaviors. The proposed approach represents a powerful tool for conducting sophisticated analyses of network traffic attributes, which can help researchers better understand and address cybersecurity threats in real-world environments.

5.2 Feature selection

The wrapper model uses binary metaheuristic algorithms that restrict the search space to the binary interval [0,1]. However, the MVMO algorithm improves the exploration process by extending the space search interval to [-1,1] to check the corresponding subset features. The user sets the feature selection threshold for each experiment, e.g., a threshold of 0.5, in which case values less than 0.5 are omitted. In contrast, items in the current generation are taken for values greater than or equal to the threshold. The search process is terminated when the maximum iteration limit is reached [23]

5.3 Tuning parameters of machine learning:

The proposed method currently uses a random search strategy to assign values to the parameters of the machine learning algorithm. Adding or removing a theta value changes the parameters, and the search process is repeated until the algorithm achieves better results. While this approach can lead to better results, it also leads to a longer, more time-consuming induction process. The proposed method has similarities with the hill-climbing system in terms of the underlying concept. Both methods aim to find the optimal solution by iteratively improving the current solution. However, unlike hill-climbing, which takes a deterministic approach, the proposed method adopts a stochastic process in which the parameters are randomly changed to explore the solution space. While random search is a popular approach for optimizing machine learning algorithms, it has certain limitations. For example, the method may lead to suboptimal solutions if the large parameter space and the search process become impractical. In such cases, alternative optimization techniques like gradient descent or Bayesian optimization may provide better results. The proposed method uses a random search strategy to optimize the parameters of the ML algorithms.

Although this approach can produce better results, it may require a longer induction process. The similarities with the hill-climbing algorithm suggests that iterative improvement is an effective optimization technique. Eq. 6 illustrates the main formal of the random search process.

$$X_i' = \frac{\partial}{2} + (X_{best} - X_i) + \frac{Max_{itr}}{iter}\ \varepsilon\ (X_i) \qquad (6)$$

Where X_i is the current value, ε are random variables in the interval [-1,1], Max_{itr} is maximum iteration, $iter$ is the current iteration's value, and X_i'

Table 1. Parameters of random forest algorithm

Parameter	Range	Type
n_estimators	[10 , 1000]	integer
max_depth	[2 ,20]	integer
min_samples_leaf	[1 ,10]	integer
max_features	[1, number of features in dataset]	integer
random_state	[1,0.42]	float

Table 2. Paramters of K-nn algorithm

Parameter	Range	Type
Nearest neighbors	[1,(Number of classes in dataset+1)]	float

Table 3. Paramters of Niav Bayes algorithm

Parameter	Range	Type
Threshold value	[0,1]	float

Table 4. Parameters of random forest algorithm

Parameter	Range	Type
Maximum depth	[1 , 1000]	integer
Minimum number of samples per leaf	[3, 25]	integer
Minimum impurity decrease	[1 ,500]	integer

Table 5. KDD_NSL dataset description

Category	Training Dataset	Testing Dataset	
		NSL_KDD Test-21	NSL_KDD Test+
Dos	9234	4342	7458
Normal	13,449	2152	9711
Probe	2289	2402	2421
U2R	12	200	200
R2L	197	2754	2754
Total	25,192	11,850	22544

a new value of the tuning parameter. The first part of Eq. (6) reduces the scattering search, while the second part reinforces the exploration of the random search algorithm. However, alternative optimization techniques may be necessary to achieve better results in certain situations.

6. Optimization parameters of ML by random search

Tables 1, 2, 3, and 4 illustrate the optimization parameter in the second part of the proposed MVMOR (Random search). The proposed model sets the maximums trails of searching randomly for the optimal parameter of the machine learning algorithm. The range of each parameter is a set previously to bind the search space.

7. Experiment results

Within this section, we covered the benchmark dataset. We evaluated the performance of four commonly used machine learning algorithms (decision tree (D.T.), random forest (R.F.), naive Bayes (N.B.), and K-NN (k-nearest neighbors)). Ultimately, we compared the results obtained from our model with those of recent studies in IDS.

7.1 Dataset

The proposed MVMOR is evaluated, and its validity is verified using two benchmark datasets in the test IDS (NSL_KDDTest+ and NSL_KDDTest-21). In addition, the performance of machine learning algorithms (D.T., R.F., NB, and KNN) is compared with the two optimization methods, MVMO and MVMOR, and the standalone method. The NSL_KDD [27] dataset includes a considerable volume of packets. The first dataset contains four primary attacks, while the second includes nine effective attacks and two million packets. These datasets contain the TCP/IP header information of the TCP/IP suite. More details about these datasets are provided in the following subsections. The NSL_KDD dataset includes four files, namely NSL_KDDTrain+ for complete training data and 20 percent Training Set for additional training data. In addition, there are two test files, namely NSL_KDDTest+ and NSL_KDDTest-21. Table 5 describes our system's NSL_KDD training and test files.

7.2 Empirical results

Tables 6 and 7 show the evaluation results of the proposed system, which uses both the MVMO algorithm and machine learning techniques. In particular, four different machine learning algorithms were used, including decision tree (DT), random forest (RF), naive Bayes (NB), and K-NN (k-nearest neighbors). After careful analysis, it was found that the R.F. algorithm provided the most favorable results when used with the proposed system. It is important to note that using machine learning algorithms in combination with the MVMO algorithm significantly increases the overall performance of the proposed approach. The decision tree, random forest, N.B., and K-NN algorithms were all evaluated for their effectiveness in improving system performance. Ultimately, it was determined that the Random Forest algorithm provided the best

Table 6. Test of machine learning model and optimization method (MVMO and MVMOR) over NSl_KDD test-21

Model	**Accuracy**	**Precision**	**Recall**	**F1_score**
KNN	54	60	54.55	56.1
KNN+MVMO	60.48	65	64.65	60.66
KNN+MVMOR	59.17	64	63.64	59.39
DT	51.69	65.06	51.69	57.61
DT+MVMO	61	63.41	70	64.22
DT+MVMOR	63	62.93	73	67.92
RF	68.1	60	63.64	66.33
RF+MVMO	71.9	64.55	67.23	70.24
RF+MVMOR	75	75	75.49	75.76
NB	46.1	50.64	46.1	48.27
NB+MVMO	48.83	53.22	46.9	51.8
NB+MVMOR	48.83	53.22	46.9	51.8

Table 7. Test of machine learning model and optimization method (MVMO and MVMOR) over NSL_KDD test-21

Model	Accuracy	precision	Recall	F1_score
KNN	75.68	78.32	75.68	76.98
KNN+MVMO	77.21	72.33	80.13	76.56
KNN+MVMOR	76.18	73.59	77.7	74.59
DT	74.56	81.01	74.56	77.67
DT+MVMO	78	78.2	75.9	74.23
DT+MVMOR	79	82.31	77.56	78.27
RF	78.83	81.03	78.83	79.92
RF+MVMO	80.21	79.63	81.82	80.82
RF+MVMOR	88.76	79	85.08	83.21
NB	71.6	65.7	71.6	68.52
NB+MVMO	74.45	70.89	78.21	77.21
NB+MVMOR	74.45	70.89	78.21	77.21

results, indicating that it is the most appropriate machine learning algorithm for use in this particular system. Incorporating machine learning techniques in the proposed approach is a significant field advancement.

The ML algorithms allow the system to learn and adapt to new data, making more accurate and efficient predictions. In addition, the successful implementation of the RF algorithm demonstrates the potential for further improvements in the performance of the proposed system.

The findings presented in Tables 6 and 7 suggest that the efficiency of the proposed algorithm is closely related to the number of variables involved. Specifically, the algorithm's performance improves accordingly as the number of variables increases.

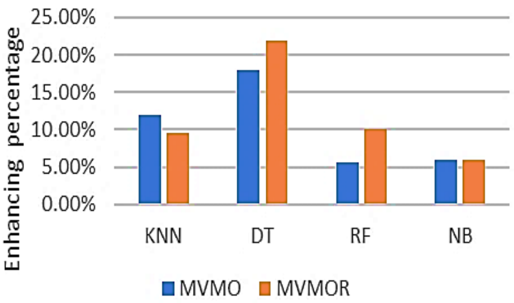

Figure. 4 Enhancing percentage on ML algorithms (NB, DT, RF, and KNN) overNSL_KDDTest_21 by MVMO, and MVMOR

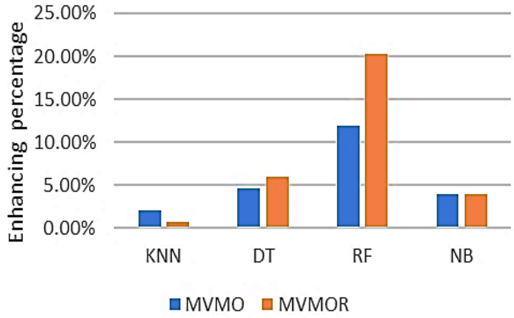

Figure. 5 Enhancing percentage on ML algorithms (NB, DT, RF, and KNN) over NSL_KDDTest-21 when applied MVMO, and MVMOR

This implies that the effectiveness of the proposed system is highly dependent on the number of parameters included in the machine learning algorithm. In other words, a more significant number of parameters in the algorithm corresponds to a greater degree of improvement in the algorithm's overall performance. Therefore, optimizing the number and selection of variables is crucial to achieving the best possible performance from the proposed system.

Figs. 4 and 5 show the enhancing percentage of machine learning algorithms when applying the optimization algorithm MVMO and proposed MVMOR.

The proposed method helps to ensure that the algorithm produces the desired outcome and achieves the required improvements. Moreover, it helps identify potential weaknesses or limitations in the algorithm's design, enabling engineers to address them promptly and improve its overall performance. In conclusion, using the standard division process for calibration is an essential step in examining the stability and implementation of an algorithm. This method enables software engineers to verify that the algorithm functions as intended, producing consistent and Reliable results and meeting the requirements. By incorporating this process into their development

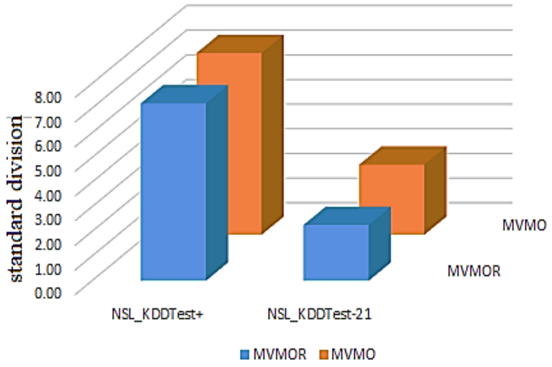

Figure. 6 The standard deviation for the best result obtained after running MVMO and MVMOR thirty times

Table 8. Comparative with other studies

Ref	Dataset name	Accuracy
[7]	KDD_NSL Test+	82
[19]		81
[20]		82
Proposed MVMOR		88

workflow, engineers can ensure their algorithms are optimized for maximum performance and efficiency. Fig. 6 shows the evaluation regarding the low standard division between MVMO and MVMOR.

7.3 Comparative with other studies:

This section compares our proposed system with previous studies [7, 19, 20] conducted on the same dataset. We present the algorithm we correspond with, MVMOR, in Table 6. Additionally, Table 7 compares our proposed MVMOR method with the other two works on IDS.

8. Conclusion

The research paper proposes a hybrid model, MVMOR, combining mean-variance mapping optimization (MVMO) and random search to improve intrusion detection systems. This model uses meta-heuristic optimization algorithms to optimize the proposed solutions and identify the most relevant features for network attribute analysis. The wrapper model is a feature selection method. It is used to select relevant features, and hot-coding techniques are applied to convert non-numeric attributes into numeric ones. The proposed method uses a random search strategy to optimize the parameters of the machine learning algorithm, which leads to better results but requires a longer induction process. The random forest algorithm gave the best results when used with the proposed system, indicating that it is suitable for use. The MVMOR algorithm improved the system's ability to classify and predict outcomes, resulting in better decision-making and more accurate predictions. The proposed system surpasses traditional detection systems in terms of accuracy and false-positive rate, with an average accuracy rate of 94%. The paper suggests that alternative optimization techniques may be necessary for iterative improvement.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The author's Contributions are as follows: "Conceptualization, first and second author; Methodology and software, first author; validation, second author; formal analysis, investigation, third author; resources, fourth author; data curation, third author; writing—original draft preparation, first authors; writing—review and editing, visualization, fifth authors; supervision, project administration, first authors; funding acquisition, fifth author.

Reference

[1] A. R. Gad, A. A. Nashat, and T. M. Barkat, "Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset", *IEEE Access*, Vol. 9, pp. 142206–142217, 2021, doi: 10.1109/ACCESS.2021.3120626.

[2] E. Pashaei, E. Pashaei, and N. Aydin, "Gene selection using hybrid binary black hole algorithm and modified binary particle swarm optimization", *Genomics*, Vol. 111, No. 4, pp. 669–686, 2019, doi: 10.1016/j.ygeno.2018.04.004.

[3] M. Z. Zakaria, S. Mutalib, S. A. Rahman, S. J. Elias, and A. Z. Shahuddin, "Solving RFID mobile reader path problem with optimization algorithms", *Indones. J. Electr. Eng. Comput. Sci.*, Vol. 13, No. 3, pp. 1110–1116, 2019, doi: 10.11591/ijeecs.v13.i3.pp1110-1116.

[4] Y. Yang, Y. Wu, H. Yuan, M. Khishe, and M. Mohammadi, "Nodes clustering and multi-hop routing protocol optimization using hybrid chimp optimization and hunger games search algorithms for sustainable energy efficient underwater wireless sensor networks", *Sustain. Comput. Informatics Syst.*, Vol. 35, p. 100731, 2022.

[5] A. Bhattacharyya, R. Chakraborty, S. Saha, S. Sen, R. Sarkar, and K. Roy, "A Two-Stage Deep

Feature Selection Method for Online Handwritten Bangla and Devanagari Basic Character Recognition", *S.N. Comput. Sci.*, Vol. 3, No. 4, p. 260, 2022, doi: 10.1007/s42979-022-01157-2.

[6] P. Shunmugapriya and S. Kanmani, "A hybrid algorithm using ant and bee colony optimization for feature selection and classification (AC-ABC Hybrid)", *Swarm Evol. Comput.*, Vol. 36, pp. 27–36, 2017, doi: 10.1016/j.swevo.2017.04.002.

[7] S. S. Alkafagi and R. M. Almuttairi, "A Proactive Model for Optimizing Swarm Search Algorithms for Intrusion Detection System", *J. Phys. Conf. Ser.*, Vol. 1818, No. 1, 2021, doi: 10.1088/1742-6596/1818/1/012053.

[8] A. H. A. Saeedi, "Binary Mean-Variance Mapping Optimization Algorithm (BMVMO)", *J. Appl. Phys. Sci.*, Vol. 2, No. 2, pp. 42–47, 2016, doi: 10.20474/japs-2.2.3.

[9] A. L. A. A. H. A. A. H. A. M. E. Manna, "A proactive metaheuristic model for optimizing weights of artificial neural network", *Indones. J. Electr. Eng. Comput. Sci.*, Vol. 20, No. 2, pp. 976–984, 2020, doi: 10.11591/ijeecs.v20.i2.pp976-984.S.

[10] S. M. Ali, A. H. Alsaeedi, D. A. Shammary, H. H. Alsaeedi, and H. W. Abid, "Efficient intelligent system for diagnosis pneumonia (SARSCOVID19) in X-ray images empowered with initial clustering", *Indones. J. Electr. Eng. Comput. Sci.*, Vol. 22, No. 1, pp. 241–251, 2021, doi: 10.11591/ijeecs.v22.i1.pp241-251.

[11] Alfoudi, A. Saeed, M. R. Aziz, Z. A. A. Alyasseri, A. H. Alsaeedi, R. R. Nuiaa, M. A. Mohammed, K. H. Abdulkareem, and M. M. Jaber, "Hyper clustering model for dynamic network intrusion detection", *IET Communications*, pp. 1–13 (2022) doi: 10.1049/cmu2.12523.

[12] A. S. Alfoudi, A. H. Alsaeedi, M. H. Abed, A. M. Otebolaku, and Y. S. Razooqi, "Palm Vein Identification Based on Hybrid Feature Selection Model", *Int. J. Intell. Eng. Syst.*, Vol. 14, No. 5, pp. 469–478, 2021, doi: 10.22266/ijies2021.1031.41.

[13] A. H. Jabor and A. H. Ali, "Dual Heuristic Feature Selection Based on Genetic Algorithm and Binary Particle Swarm Optimization", *J. Univ. BABYLON Pure Appl. Sci.*, Vol. 27, No. 1, pp. 171–183, 2019, doi: 10.29196/jubpas.v27i1.2106.

[14] D. A. Shammary, A. L. Albukhnefis, A. H. Alsaeedi, and M. A. Asfoor, "Extended particle swarm optimization for feature selection of high-dimensional biomedical data", *Concurr. Comput. Pract. Exp.*, Vol. 34, No. 10, p. e6776, 2022, doi: https://doi.org/10.1002/cpe.6776.

[15] R. M. Pringles and J. L. Rueda, "Optimal transmission expansion planning using Mean-Variance Mapping Optimization", In: *Proc. of 2012 6th IEEE/PES Transm. Distrib. Lat. Am. Conf. Expo. T D-LA 2012*, pp. 1–8, 2012, doi: 10.1109/TDC-LA.2012.6319132.

[16] J. L. Rueda and I. Erlich, "Evaluation of the mean-variance mapping optimization for solving multimodal problems", In: *Proc. of 2013 IEEE Symp. Swarm Intell. SIS 2013 - 2013 IEEE Symp. Ser. Comput. Intell. SSCI 2013*, pp. 7–14, 2013, doi: 10.1109/SIS.2013.6615153.

[17] D. B. Rawat, R. Doku, and M. Garuba, "Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security", *IEEE Trans. Serv. Comput.*, Vol. 14, No. 6, pp. 2055–2072, 2021, doi: 10.1109/TSC.2019.2907247.

[18] F. H. Almasoudy, W. L. A. Yaseen, and A. K. Idrees, "Differential Evolution Wrapper Feature Selection for Intrusion Detection System", *Procedia Comput. Sci.*, Vol. 167, No. 2019, pp. 1230–1239, 2020, doi: 10.1016/j.procs.2020.03.438.

[19] O. Almomani, "A feature selection model for network intrusion detection system based on pso, gwo, ffa and ga algorithms", *Symmetry (Basel).*, Vol. 12, No. 6, pp. 1–20, 2020, doi: 10.3390/sym12061046.

[20] A. M. Taha, A. Mustapha, and S. D. Chen, "Naive Bayes-guided bat algorithm for feature selection", *Sci. World J.*, Vol. 2013, 2013, doi: 10.1155/2013/325973.

[21] R. R. Nuiaa, S. Manickam, A. H. Alsaeedi, and E. S. Alomari, "Enhancing the Performance of Detect DRDoS DNS Attacks Based on the Machine Learning and Proactive Feature Selection (PFS) Model", *IAENG Int. J. Comput. Sci.*, Vol. 49, No. 2, 2022.

[22] W. Nakawiro, I. Erlich, and J. L. Rueda, "A novel optimization algorithm for optimal reactive power dispatch: A comparative study", In: *Proc. of DRPT 2011 - 2011 4th Int. Conf. Electr. Util. Deregul. Restruct. Power Technol.*, No. 1, pp. 1555–1561, 2011, doi: 10.1109/DRPT.2011.5994144.

[23] D. A. Shammary, A. L. Albukhnefis, A. H. Alsaeedi, and M. A. Asfoor, "Extended particle swarm optimization for feature selection of high-dimensional biomedical data", *Concurr. Comput. Pract. Exp.*, Vol. 34, No. 10, 2022, doi: 10.1002/cpe.6776.

[24] A. S. Alfoudi, A. H. Alsaeedi, M. H. Abed, A.

M. Otebolaku, and Y. S. Razooqi, "Palm Vein Identification Based on Hybrid Feature Selection Model", *Int. J. Intell. Eng. Syst.*, Vol. 14, No. 5, pp. 469–478, 2021, doi: 10.22266/ijies2021.1031.41.

[25] S. Mohammadi, H. Mirvaziri, M. G Ahsaee, and H. Karimipour, "Cyber intrusiondetection by combined feature selection algorithm", *J. Inf. Secur. Appl.*, Vol. 44, pp. 80–88, 2019, doi: 10.1016/j.jisa.2018.11.007.

[26] R. R. Nuiaa, A. H. Alsaeedi, S. Manickam, and D. E. J. A. Shammary, "Evolving Dynamic Fuzzy Clustering (EDFC) to Enhance DRDoS_DNS Attacks Detection Mechnism", *Int. J. Intell. Eng. Syst.*, Vol. 15, No. 1, pp. 509–519, 2022, doi: 10.22266/IJIES2022.0228.46.

[27] S. M. Hadi, A. H. Alsaeedi, M. I. Dohan, R. R. Nuiaa, S. Manickam, and A. S. D. Alfoudi, "Dynamic Evolving Cauchy Possibilistic Clustering Based on the Self-Similarity Principle (DECS) for Enhancing Intrusion Detection System", *Int. J. Intell. Eng. Syst.*, Vol. 15, No. 5, pp. 252–260, 2022, doi: 10.22266/ijies2022.1031.23.

[28] S. M. Hadi, A. H. Alsaeedi, M. I. Dohan, R. R. Nuiaa, S. Manickam, and A. S. D. Alfoudi, "Dynamic Evolving Cauchy Possibilistic Clustering Based on the Self-Similarity Principle (DECS) for Enhancing Intrusion Detection System", *Int. J. Intell. Eng. Syst.*, Vol. 15, No. 5, pp. 252–260, 2022, doi: 10.22266/ijies2022.1031.23.

[29] P. P. Debata and P. Mohapatra, "Identification of significant bio-markers from high-dimensional cancerous data employing a modified multi-objective meta-heuristic algorithm", *J. King Saud Univ. - Comput. Inf. Sci.*, Vol. 34 No. 8, 2022, doi: 10.1016/j.jksuci.2020.12.014.

[30] I. A. Turaiki and N. Altwaijry, "A Convolutional Neural Network for Improved Anomaly-Based Network Intrusion Detection", *Big Data*, Vol. 9, No. 3, pp. 233–252, 2021, doi: 10.1089/big.2020.0263.