Enhancing Intrusion Detection System Performance Using a Hybrid of Harris Hawks and Whale Optimization Algorithms

Mosleh M. Abualhaj
Department of Networks and Cybersecurity, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan
m.hyari@ammanu.edu.jo (corresponding author)

Sumaya N. Al-Khatib
Department of Computer Science, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan
sumayakh@ammanu.edu.jo

Mahran Al Zyoud
Department of Networks and Cybersecurity, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan
m.zyoud@ammanu.edu.jo

Iyas Qaddara
Department of Computer Science, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan
i.qaddara@ammanu.edu.jo

Mohammed Anbar
Cybersecurity Research Centre (CYRES), Universiti Sains Malaysia (USM), Penang, Malaysia
anbar@cyres.usm.my

Received: 11 March 2025 | Revised: 5 April 2025 and 20 April 2025 | Accepted: 23 April 2025

 DOI: https://doi.org/10.48084/etasr.10919

ABSTRACT

Intrusion Detection and Prevention Systems (IDPSs) play a crucial role in safeguarding online connections against unauthorized access and malicious activities. To enable efficient and effective detection and mitigation, IDPSs must continuously improve their performance due to the constantly developing nature of cyber threats. However, an IDPS is more difficult to use and less reliable when it deals with huge amounts of data. This study aimed to improve the performance of IDPSs by employing optimization algorithms to reduce the data size. Particularly, the Harris Hawks Optimization (HHO) and Whale Optimization Algorithm (WOA) were combined for feature selection. The experimental results showed that the performance of the proposed IDPS was greatly improved by combining the HHO and WOA algorithms. Combining a Random Forest classifier with the suggested HHO/WOA feature selection method achieved very high results in accuracy (99.17%), recall (98.76%), precision (98.76%), and F1-score (98.43%).

Keywords-feature selection; Harris hawks optimization algorithm; intrusion detection; machine learning; whale optimization algorithm

I. INTRODUCTION

Cybercrime costs are increasing, with some projections indicating that by 2025 they could reach $10.5 trillion [1]. Depending on the type of attack and the security mechanisms to prevent it, this can happen in different ways. Malware infections, DoS attacks, phishing scams, ransomware attacks, and other cyberattacks are just a few examples of the many different types of cyberattacks that can occur [2, 3]. Strong security measures should be implemented to stop the spread of

cyberattacks, including firewalls, antivirus software, Intrusion Detection and Prevention Systems (IDPSs), and routine security updates [3, 4].

The purpose of IDPSs is to monitor network traffic for indications of malicious behavior. They can be configured to provide alerts depending on predetermined criteria, such as a predetermined threshold for failed login attempts, and can be configured to monitor various network components, such as servers, endpoints, or network devices, as shown in Figure 1. IDPSs often employ Machine Learning (ML) and Artificial Intelligence (AI) techniques to offer efficient defense against a variety of cyber threats while also being responsive and agile to changing security requirements [5-7].

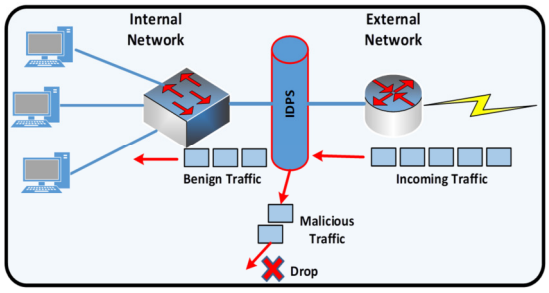

Fig. 1. IDPS function.

ML involves algorithms that can find patterns in large datasets and make predictions based on them. With the use of historical data learning, IDPS-based ML can offer a more effective defense against a variety of security threats. However, false alerts are a problem that ML-based IDPSs frequently face, and optimized feature selection can be used to reduce them. Metaheuristic algorithms can be used to find the most useful among a set of features [8-10]. Metaheuristic algorithms have been shown to be effective in solving optimization problems, demonstrating high efficiency in scientific, real-world, and engineering issues [11]. The advantage of these algorithms is their ability to find nearly optimal solutions in a relatively short time, which is important for solving problems. Accordingly, these algorithms can be applied to feature selection in the case that the number of features is high [11-13]. The Harris Hawks Optimization (HHO) and the Whale Optimization Algorithm (WOA) are two of the common metaheuristic algorithms that imitate the behavior of wolves and whales, respectively, in nature [14, 15]. This study combines these two methods to select features for an ML-based IDPS.

Several methods have been proposed to improve intrusion detection. In [16], an AI-IDS was presented to detect web intrusions in real-time. This system used deep learning to learn from web traffic data and classify patterns into normal and abnormal behaviors, employing a Convolutional Neural Network and a Long Short-Term Memory (CNNL-STM) model based on Spatial Feature Learning (SFL). The CNN-LSTM model was based on SFL-extracted features of real-time HTTP traffic without encryption, calculating entropy, or compression. The experimental results showed that this system outperformed other solutions in terms of accuracy (98.07%), precision (97.06%), and recall (98.13%).

In [17], a method was proposed to deal with the issue of processing similar features that provide redundant information and increase computational time. This feature selection technique minimized the input data features. To improve the possibility of them participating in different groups, features were initially randomly grouped and sorted by accuracy score. The packets received by the network nodes were classified using only the highest-ranked features, which were saved as part of the node's previous performance. The ML technique incorporated the past behavior of the node to estimate classification decisions, achieving an accuracy of 91%.

In [18], an effective Network-based IDS (NIDS) system was developed using an ensemble ML classifier with a newly proposed feature selection technique that used the Double Particle Swarm Optimization (DPSO). DPSO uses two fitness functions to control the relevance and redundancy of the selected features. The selected features were then fed to the ensemble ML classifiers. The proposed NIDS system was evaluated on the NSL-KDD dataset to detect attacks. Simulations were carried out to test the performance of the suggested NIDS system with the existing PSO model. The proposed DPSO achieved 98.30% accuracy, while PSO achieved 92.05% accuracy. In addition, the WOA was tested in the same environment, achieving an accuracy of 94.90%.

In [19], two IDS models were introduced, which employed a Backpropagation Neural Network (BPN) and a Multilayer Perceptron (MLP) to detect attacks based on the NSL-KDD dataset. These models used a hybrid optimization algorithm from the HHO and PSO optimizers to decrease the dataset size by selecting relevant features that represent anomalies in network traffic. This hybrid algorithm also tuned the selected features assigned as initial weight vectors for both the BPN and MLP IDS models. The HHO-PSO/BPN achieved a detection accuracy of 97.08% with an F1 score of 0.9743. The HHO-PSO/MLP achieved a detection accuracy of 97.74% with an F1 score of 0.9800.

In [15], an IDS was introduced that featured an innovative attack detection method. This method leveraged an Elevated HHO (EHHO) variant, modifying the internal operations of the original HHO to enhance anomalous detection within network traffic. Performance evaluation of the suggested IDS model using the new EHHO optimizer was performed with the Gated Recurrent Unit (GRU) neural network mechanism. The results were then compared with the original HHO and WOA optimizers. Notably, the EHHO-GRU achieved the highest accuracy at 82.47%, surpassing the HHO-GRU and WOA-GRU, which attained 79.97% and 79.77%, respectively.

In [8], an IDS model used several algorithms to select key features for attack detection. In particular, several metaheuristic algorithms were hybridized to build an efficient feature selection method for the IDS. The proposed IDS adopted the AdaBoost ensemble method to classify attacks, which was chosen because it is cost-sensitive and enhances attack detection for minority classes. The NSL-KDD dataset was used to evaluate the proposed hybridized feature selection method with the AdaBoost classifier. Error rate, execution time, and detection accuracy were improved in the test dataset, achieving 81.1% accuracy for minority classes.

Several IDS models have been introduced to improve the accuracy of attack detection. Notable works, such as [16] and [17], leverage diverse techniques, including deep learning, ML, and feature selection, to optimize IDS performance. Moreover, in [8, 15, 18, 19], the integration of metaheuristic optimization algorithms was explored to reduce data size, improving the attack detection rate and speed in IDS models. Various metaheuristic algorithms, such as PSO, WOA, and HHO, have been employed, demonstrating promising results, as summarized in Table I. However, there is still room for innovation to further enhance attack detection accuracy. This work proposes a novel hybrid technique that combines the HHO and WOA optimizers to increase IDS performance and attack detection accuracy [20].

TABLE I. COMPARISON OF EXISTING IDPS MODELS

Ref.	Year	Algorithm	Optimizer	Accuracy
[18]	2022	Ensemble	PSO	92.05%
			DPSO	98.30%
			WOA	94.90%
[19]	2023	BPN	HHO-PSO	97.08%
		MLP	HHO-PSO	97.74%
[15]	2024	GRU	HHO	79.97%
			EHHO	82.47%
			WOA	79.77%
[8]	2023	AdaBoost	PSO	81.1%

II. BACKGROUND

A. NSL-KDD dataset

Although the NSL-KDD dataset has significant issues, it is regarded as a sufficient benchmark dataset that assists security engineers in investigating various IDPSs. The dataset contains 148517 samples and 40 features, excluding the output column. Table II shows the primary characteristics of the dataset, which has four main attack types: DoS, Probe, User to Root (U2R), and Remote to Local (R2L). The dataset also contains a fifth category called "Normal," which represents normal network traffic without any attacks [21, 22].

TABLE II. THE NSL-KDD DATASET

No.	Feature Name	No.	Feature Name
1	protocol_type	21	is_guest_login
2	service	22	Count
3	flag	23	srv_count
4	src_bytes	24	serror_rate
5	dst_bytes	25	srv_serror_rate
6	land	26	rerror_rate
7	wrong_fragment	27	srv_rerror_rate
8	urgent	28	same_srv_rate
9	hot	29	diff_srv_rate
10	num_failed_logins	30	"rv_diff_host_rate
11	logged_in	31	dst_host_count
12	num_compromised	32	dst_host_srv_count
13	root_shell	33	dst_host_same_srv_rate
14	su_attempted	34	dst_host_diff_srv_rate
15	num_root	35	dst_host_same_src_port_rate
16	num_file_creations	36	dst_host_srv_diff_host_rate
17	num_shells	37	dst_host_serror_rate
18	num_access_files	38	dst_host_srv_serror_rate
19	num_outbound_cmds	39	dst_host_rerror_rate
20	is_host_login	40	dst_host_srv_rerror_rate

B. Supervised ML Classifiers

In supervised ML, the model is trained on a labeled dataset, picking up knowledge from a set of input/output pairings (also referred to as labeled instances) to build a model that can be applied to predict the outcome of unobserved data. Table III shows the main aspects of the SVM, KNN, and RF supervised ML classifiers that were investigated in the proposed IDPS [22-29].

TABLE III. MAIN ASPECTS OF SVM, KNN, AND RF

Aspect	RF	KNN	SVM
Learning approach	Ensemble learning	Instance-based learning	Supervised learning
Working mechanism	Constructs multiple decision trees and aggregates their results for classification	Assigns labels based on the majority vote of the K-nearest training samples	Finds an optimal hyperplane that maximizes class separation
Strengths	High accuracy, handles high-dimensional data, resistant to overfitting	Simple and effective, non-parametric	Effective in high-dimensional spaces, robust to outliers
Performance on attack detection	High accuracy and robustness, effective in detecting complex attacks	Effective, but may struggle with high-dimensional data	Works well with structured attack data, good at detecting anomalies
Computational complexity	Moderate to high (depends on the number of trees)	High (distance calculation for every prediction)	High (especially with complex kernels)

C. Feature selection

The accuracy and effectiveness of ML models can be improved by choosing a suitable feature selection algorithm that depends on the nature of the problem to be addressed. In this study, two well-known optimization algorithms, HHO and WOA, were employed to select relevant features for the IDPS system, which is called Hybrid IDPS (H-IDPS). HHO and WOA are renowned for their efficacy and efficiency in feature selection.

1) HHO Algorithm

HHO is a cutting-edge optimization technique that was motivated by Harris Hawks' hunting practices. It starts by initializing a collection of potential solutions known as hawks. Each hawk, represented by a collection of feature weights or coefficients, is one potential solution to the optimization problem. After initialization, the algorithm simulates hawk hunting techniques to obtain the best solution. The algorithm divides the hawk population into smaller groups or hunting parties during the simulation. Algorithm 1 shows a pseudocode for the HHO algorithm [14, 30].

```
Algorithm 1: HHO Algorithm
  psn is position, hk is hawk, a is alpha
  hawk, b is beta hawk
  Initialize population of hk randomly
  Calculate fitness of each hk
  Set best solution (global best) as hk
  with highest fitness
  Repeat until # of iteration is met:
```

```
    Sort hk based on fitness in descending
    order
    Update psn of a (leader):
      Generate random number x1 between 0
      and 1
      Update psn of a using the formula:
      a.psn = a.psn + x1 * (globalBest.psn
      - a.psn)
    For each remaining hk (b):
      Generate random number x2 between 0
      and 1
      Update psn of b using the formula:
      b.psn = (b.psn+a.psn)/2 + x2 *
      (globalBest.psn - b.psn)
    Perform exploration:
    For each hk (except a and b):
      Generate random number x3 between 0
      and 1
      Update position of hk using the
      formula:
        hk.psn = hk.psn + x3 *
        (globalBest.psn - hk.psn)
    Calculate fitness of new psn
    Update global best solution if hk has
    better fitness
  Return best solution found
```

2) WOA Algorithm

WOA is an optimization method that draws inspiration from nature and is based on how humpback whales hunt. Exploration, exploitation, and convergence are the three primary activities that the WOA performs to find the best solution. Based on the location of the whale and the distance to the ideal solution, a random vector and a distance factor determine the movement for each of the three activities. The a parameter of the WOA is used to regulate the ratio of exploration to exploitation. As time goes on, the value of a drops, eventually changing the algorithm's emphasis from exploration to exploitation. Algorithm 2 displays the pseudocode for the WOA [31].

```
Algorithm 2: WOA Algorithm
  psn is position, wh is whale
  Initialize a population of wh randomly
  Calculate fitness of each wh
  Set the best solution (global best) as
  the wh with the highest fitness
  Repeat until # of iteration is met:
    Update a (decreasing linearly) from 2
    to 0 over iterations
    For each wh:
      Generate a random number x1 between
      0 and 1
      Generate a random number x2 between
      0 and 1
      If x2 < 0.5:
        Update the psn of the wh using the
        formula:
          wh.psn =globalBest.psn-
          (x1*distanceToGlobalBest)
      Else if x2 >= 0.5 and absolute
      value(a) < 1:
        Select a random wh (wh_j)
        Update the psn of the wh using
        the formula:
        wh.psn = wh_j.psn - (x1 *
        distanceToWhale_j)
      Else if x2 >= 0.5 and absolute
      value(a) >= 1:
        Generate a random number x3
        between 0 and 1
        Update the psn of the wh using the
        formula:
        wh.psn = (globalBest.psn - wh.psn)
        * (x3 * a)
      Check the whale's psn based on the
      constraints
      Calculate fitness of new psn
      Update the global best solution if a
      wh has a better fitness
  Return the best solution found
```

III. HYBRID IDPS (H-IDPS) MODEL

A. Data Preprocessing

1) Transformation Operation

The NSL-KDD dataset includes preprocessed network traffic that has been transformed into numerical values. However, some features in the dataset are categorical, demanding transformation into numerical values for use in ML models. A typical method of transforming categorical features into numerical values is label encoding, which allocates a unique integer value in sequence to each category [3, 21]. The NSL-KDD dataset contains three features with a text data type. These features are *protocol_type*, *service*, and *flag*. The label-encoding method was used to encode the text values within these three features into numerical values. The *protocol_type* feature contains three different text values: tcp, udp, and icmp. The label-encoding method replaced these three text values with 0, 1, and 2, respectively. The *service* feature contains 65 different text values: auth, bgp, ..., X11, and Z39_50. The label-encoding method replaced these 65 text values by 0, 1, …, 63, and 64, respectively. The flag feature contains ten different text values: OTH, REJ, …, SF, and SH. The label-encoding method replaced these ten text values with 0, 1, …, 8, and 9, respectively.

2) Normalization Operation

Normalization is an important preprocessing step in ML to scale features to a consistent range, ensuring that the sizes and magnitudes of the numerical features in the NSL-KDD dataset are comparable, preventing one feature from overpowering others during model training. Min-max scaling, which scales values to a range between 0 and 1, is a well-liked normalization method. For features with known minimum and maximum values, the Min-Max scaling method is very suitable [3, 21].

3) Hybrid Feature Selection Method

A hybrid feature selection approach selects the key features from a set based on two or more feature selection techniques. Using two or more techniques can increase the accuracy and efficiency of the feature selection process. Hybrid feature selection approaches have the potential to be more successful than single ones. This happens because they take advantage of many methods while compensating for their shortcomings. By combining various techniques to provide a thorough and accurate selection of features, hybrid feature selection can improve the performance of ML models and prevent overfitting.

As mentioned earlier, HHO and WOA were chosen for several reasons. The integration of WOA and HHO can achieve a harmonious global exploration and efficient exploitation, capitalizing on their strengths in diverse search mechanisms and collaborative search behavior. This integration achieves the main goal of feature selection, which is to find the most relevant attack features that can be used to identify the attack accurately, increase the detection rate and speed, and improve the performance of the IDPS [8, 14, 15, 19, 30].

The proposed H-IDPS model utilized hybrid feature selection by combining HHO and WOA optimizers. The HHO and WOA optimizers were applied to the NSL-KDD dataset in parallel. The number of selected features when using HHO was 13 and when using WOA was 16, as shown in Table IV. The mutual features from the two optimizers were combined to form a new reduced subset of 25 features, rather than the 40 features in the NSL-KDD dataset, as shown in Table IV. Figure 2 illustrates the feature selection process. The resulting reduced subset of features was used in the H-IDPS model to improve performance.

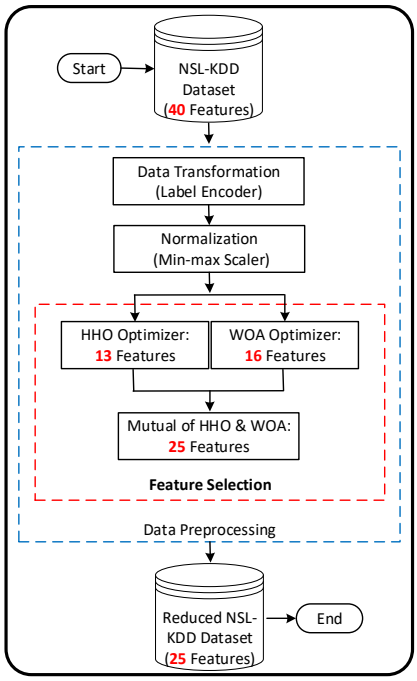

Fig. 2. Feature selection process.

TABLE IV. SELECTED FEATURES PER OPTIMIZER

Optimizer	Selected features (feature #)
WOA	2, 3, 4, 10, 15, 18, 19, 20, 21, 23, 24, 25, 28, 30, 35, 39
HHO	1, 3, 4, 5, 8, 9, 18, 22, 29, 31, 32, 34, 35
HHO and WOA	1, 2, 3, 4, 5, 8, 9, 10, 15, 18, 19, 20, 21, 22, 23, 24, 25, 28, 29, 30, 31, 32, 34, 35, 39

B. Attack Detection

The proposed model used the NSL-KDD dataset for training and testing the ML classifiers, after using the hybrid feature selection method discussed above (25 of 40 features). Finally, the H-IDPS model implemented the KNN, SVM, and RF classifiers to identify attacks. The performance of the three classifiers was evaluated using several metrics based on the K-fold cross-validation method with a k equal to 5. Figure 3 describes the proposed H-IDPS model.

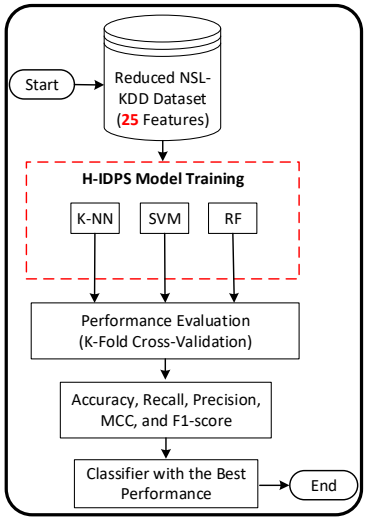

Fig. 3. H-IDPS model.

IV. PERFORMANCE EVALUATION OF THE H-IDPS MODEL

A. Implementation Environment

The proposed H-IDPS model was tested on a desktop PC with 64-bit Microsoft Windows, Intel Core i7 13700K (up to 5.4 GHz, 16 cores, and 30 MB Intel Smart Cache), 32 GB 3600 MHz DDR4 RAM, Nvidia GeForce RTX 4090 24GB GDDR6X GPU, and M.2 1TB SSD (UP TO 5000 MB/s). Python was utilized to implement the proposed H-IDPS model, as it contains a large number of libraries and tools to develop ML models, such as NumPy and Pandas.

B. Performance Evaluation Criteria

The performance of the H-IDPS model was evaluated using a confusion matrix, which is a four-cell matrix containing the actual and predicted classes. Typically, the rows of the confusion matrix represent the actual classes, and the columns represent the predicted classes. The four cells of the matrix are True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). The confusion matrix can be used to

calculate various metrics that measure the performance of the classification model, including accuracy (3), recall (4), precision (5), and F1-score (7) [32-34].

$$Accuracy = \frac{(TP+TN)}{(TP+TN+FP+FN)} \quad (1)$$

$$Recall = \frac{TP}{(TP+FN)} \quad (2)$$

$$Precision = \frac{TP}{(TP+FP)} \quad (3)$$

$$F1-score = \frac{Precision \times Recall}{Precision + Recall} \quad (4)$$

C. Results and Discussion

The proposed H-IDPS model was implemented, tested, and evaluated using three feature selection techniques: HHO, WOA, and mutual selection of the features selected by HHO and WOA (HHO/WOA). The best-performing feature selection method will be used with the H-IDPS model. Accuracy, recall, precision, and F1-score were measured for each of these feature selection techniques using SVM, KNN, and RF. Figures 4, 5, 6, and 7 show the accuracy, recall, precision, and F1-score metrics, respectively. Each metric was used to evaluate the proposed H-IDPS with the above-mentioned classifiers and feature selection methods.

As shown in Figure 4, all three classifiers in combination with the three feature selection methods achieved high accuracy. However, the accuracy using the HHO/WOA method outperformed both HHO and WOA with all classifiers. In addition, among the three classifiers, RF achieved the highest accuracy with the three feature selection methods. Therefore, the combination of the RF classifier and HHO/WOA method achieved the highest accuracy of 99.17%. As shown in Figures 5 and 6, both recall and precision were almost identical with all combinations of the three classifiers and three feature selection methods. In general, all three classifiers in combination with the three methods achieved acceptable or high recall and precision results. However, the recall and precision of the HHO/WOA method outperformed both HHO and WOA with all classifiers. In addition, the RF classifier achieved the highest recall and precision with all three feature selection methods. Therefore, the combination of RF classifier and HHO/WOA method achieved the highest recall and precision of 98.76%.

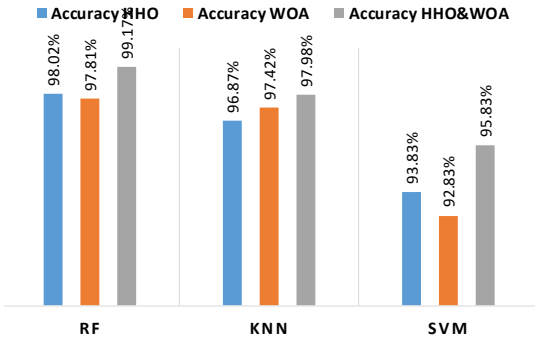

Fig. 4. Accuracy of the proposed H-IDPS model.

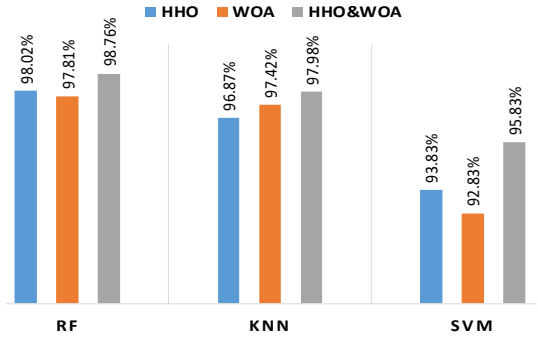

Fig. 5. Recall of the proposed H-IDPS model.

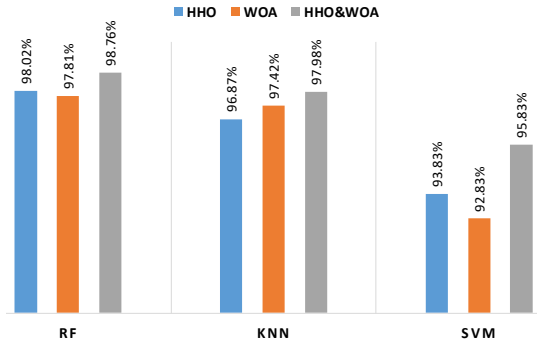

Fig. 6. Precision of the proposed H-IDPS model.

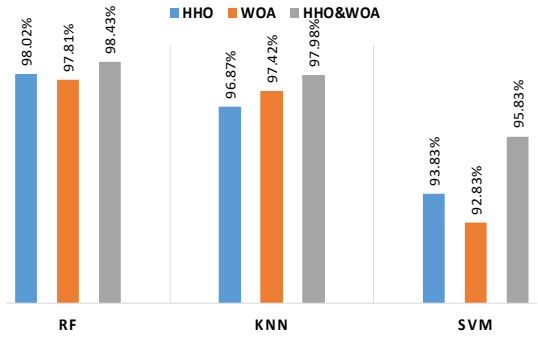

Fig. 7. F1-score of the proposed H-IDPS model.

As shown in Figure 7, the F1 scores were between acceptable and high with all combinations of the three feature selection methods and the three classifiers. However, similar to the previous metrics, the combination of the RF classifier and the HHO/WOA method achieved the highest F1-score of 98.43%. In summary, the combination of the RF classifier and the HHO/WOA method achieved the best results in all four metrics: accuracy (99.17%), recall (98.76%), precision (98.76%), and F1-score (98.43%). Therefore, the proposed H-IDPS model will employ HHO/WOA as a feature selection method and RF as an ML classifier.

The proposed H-IDPS model was benchmarked against other IDS models utilizing metaheuristic algorithms in terms of accuracy, as shown in Figure 8. Notably, the H-IDPS model incorporating HHO/WOA and RF achieved the highest accuracy at 99.17%. In contrast, the closest competing model [18] achieved an accuracy of 98.30%, demonstrating an

improvement of 0.87%. The proposed HHO/WOA hybrid feature selection method outperformed existing approaches by effectively reducing irrelevant features while preserving critical information, resulting in higher classification accuracy and faster computation, and demonstrating its robustness and suitability for network intrusion detection tasks.

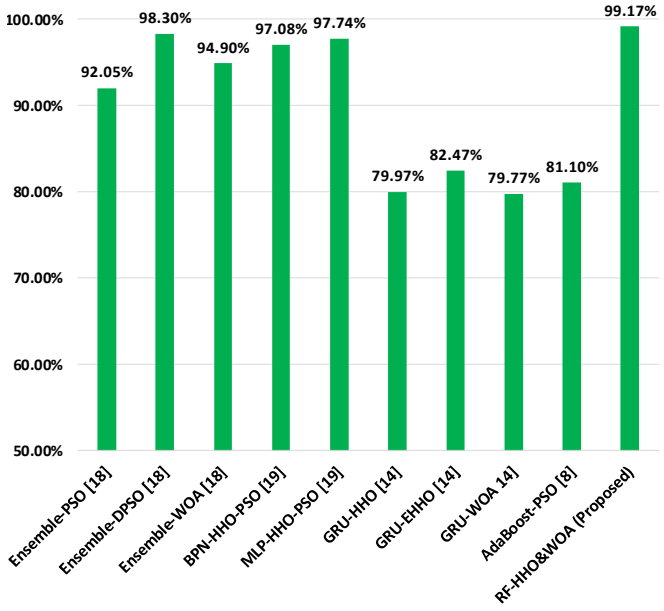

Fig. 8. Accuracy of the proposed H-IDPS against other IDS models.

V. CONCLUSION

This study introduced a hybrid feature selection approach based on HHO and WOA to improve the effectiveness of network IDPSs in securing network communications. The proposed method demonstrated its ability to reduce feature space while maintaining or enhancing classification accuracy, offering both computational efficiency and high detection performance. This highlights the practical relevance of the method for real-time security applications, where quick and accurate identification of threats is critical. By leveraging the complementary strengths of two bioinspired optimization algorithms, the proposed approach provides a robust and generalizable solution for processing high-dimensional network traffic data, offering a valuable contribution to the field of intelligent network communication security.

REFERENCES

[1] "Global cybercrime estimated cost 2029," *Statista*. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.

[2] H. Al-Mimi, N. A. Hamad, and M. M. Abualhaj, "A Model for the Disclosure of Probe Attacks Based on the Utilization of Machine Learning Algorithms," in *2023 10th International Conference on Electrical and Electronics Engineering (ICEEE)*, Istanbul, Turkiye, May 2023, pp. 241–247, https://doi.org/10.1109/ICEEE59925.2023.00051.

[3] M. M. Abualhaj, A. A. Abu-Shareha, M. O. Hiari, Y. Alrabanah, M. Al-Zyoud, and M. A. Alsharaiah, "A Paradigm for DoS Attack Disclosure using Machine Learning Techniques," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 3, 2022, https://doi.org/10.14569/IJACSA.2022.0130325.

[4] M. Ren, W. Zhang, S. Kong, D. Zhou, D. Li, and Y. Tian, "Research on abnormal traffic diagnosis based on deployment mode of firewall," in *2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, Chongqing, China, Dec. 2020, pp. 2286–2291, https://doi.org/10.1109/ITAIC49862.2020.9339189.

[5] Z. S. Malek, B. Trivedi, and A. Shah, "User behavior Pattern -Signature based Intrusion Detection," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, London, UK, Jul. 2020, pp. 549–552, https://doi.org/10.1109/WorldS450073.2020.9210368.

[6] A. Grzech, "Intelligent Distributed Intrusion Detection Systems of Computer Communication Systems," in *2009 First Asian Conference on Intelligent Information and Database Systems*, Dong hoi, Quang binh, Vietnam, Apr. 2009, pp. 1–6, https://doi.org/10.1109/ACIIDS.2009.87.

[7] P. Widulinski and K. Wawryn, "A Study of Detection Probabilities and Real-World Testing of a Human Immunity Inspired Intrusion Detection System," in *2021 28th International Conference on Mixed Design of Integrated Circuits and System*, Lodz, Poland, Jun. 2021, pp. 261–264, https://doi.org/10.23919/MIXDES52406.2021.9497536.

[8] R. Kaur and N. Gupta, "Network intrusion detection using meta-heuristic feature selection and cost-sensitive learning," *International Journal of Internet Technology and Secured Transactions*, vol. 13, no. 2, 2023, Art. no. 105, https://doi.org/10.1504/IJITST.2023.129572.

[9] G. Yedukondalu, G. H. Bindu, J. Pavan, G. Venkatesh, and A. SaiTeja, "Intrusion Detection System Framework Using Machine Learning," in *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, Sep. 2021, pp. 1224–1230, https://doi.org/10.1109/ICIRCA51532.2021.9544717.

[10] J. A. Abraham and V. R. Bindu, "Intrusion Detection and Prevention in Networks Using Machine Learning and Deep Learning Approaches: A Review," in *2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, Coimbatore, India, Oct. 2021, pp. 1–4, https://doi.org/10.1109/ICAECA52838.2021.9675595.

[11] H. Mendes, S. E. Quincozes, and V. E. Quincozes, "A Web User Interface Tool for Metaheuristics-Based Feature Selection Assessment for IDSs," in *2022 6th Cyber Security in Networking Conference (CSNet)*, Rio de Janeiro, Brazil, Oct. 2022, pp. 1–5, https://doi.org/10.1109/CSNet56116.2022.9955616.

[12] A. Almomani, "Ensemble-Based Approach for Efficient Intrusion Detection in Network Traffic," *Intelligent Automation & Soft Computing*, vol. 37, no. 2, pp. 2499–2517, 2023, https://doi.org/10.32604/iasc.2023.039687.

[13] S. M. Kasongo and Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *Journal of Big Data*, vol. 7, no. 1, p. 105, Nov. 2020, https://doi.org/10.1186/s40537-020-00379-6.

[14] M. Alazab, R. Abu Khurma, P. A. Castillo, B. Abu-Salih, A. Martín, and D. Camacho, "An effective networks intrusion detection approach based on hybrid Harris Hawks and multi-layer perceptron," *Egyptian Informatics Journal*, vol. 25, Mar. 2024, Art. no. 100423, https://doi.org/10.1016/j.eij.2023.100423.

[15] Y. Xiao, C. Kang, H. Yu, T. Fan, and H. Zhang, "Anomalous Network Traffic Detection Method Based on an Elevated Harris Hawks Optimization Method and Gated Recurrent Unit Classifier," *Sensors*, vol. 22, no. 19, Jan. 2022, Art. no. 7548, https://doi.org/10.3390/s22197548.

[16] A. Kim, M. Park, and D. H. Lee, "AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection," *IEEE Access*, vol. 8, pp. 70245–70261, 2020, https://doi.org/10.1109/ACCESS.2020.2986882.

[17] Z. Chkirbene, A. Erbad, R. Hamila, A. Mohamed, M. Guizani, and M. Hamdi, "TIDCS: A Dynamic Intrusion Detection and Classification System Based Feature Selection," *IEEE Access*, vol. 8, pp. 95864–95877, 2020, https://doi.org/10.1109/ACCESS.2020.2994931.

[18] P. S. Deshpande, S. R. Jondhale, M. D. Jakhete, and S. A. Panwar, "Double Particle Swarm Optimization based Ensemble ML Technique for detecting the intrusion in Networks," *Bulletin of Environment, Pharmacology and Life Sciences*, no. special issue 1, pp. 915–923, 2022.

[19] S. Sumathi and R. Rajesh, "A Dynamic BPN-MLP Neural Network DDoS Detection Model Using Hybrid Swarm Intelligent Framework," *Indian Journal Of Science And Technology*, vol. 16, no. 43, pp. 3890–3904, Nov. 2023, https://doi.org/10.17485/IJST/v16i43.1718.

[20] A. A. Othman, T. M. Hasan, and S. O. Hasoon, "Impact of Dimensionality Reduction on The Accuracy of Data Classification," in *2020 3rd International Conference on Engineering Technology and its Applications (IICETA)*, Najaf, Iraq, Sep. 2020, pp. 128–133, https://doi.org/10.1109/IICETA50496.2020.9318955.

[21] Ü. Çavuşoğlu, "A new hybrid approach for intrusion detection using machine learning methods," *Applied Intelligence*, vol. 49, no. 7, pp. 2735–2761, Jul. 2019, https://doi.org/10.1007/s10489-018-01408-x.

[22] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, ON, Canada, Jul. 2009, pp. 1–6, https://doi.org/10.1109/CISDA.2009.5356528.

[23] A. H. Efat *et al.*, "Inquisition of The Support Vector Machine Classifier in Association with Hyper-parameter Tuning: A Disease Prognostication Model," in *2022 4th International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE)*, Rajshahi, Bangladesh, Dec. 2022, pp. 131–134, https://doi.org/10.1109/ICECTE57896.2022.10114543.

[24] C. Liu, Z. Gu, and J. Wang, "A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning," *IEEE Access*, vol. 9, pp. 75729–75740, 2021, https://doi.org/10.1109/ACCESS.2021.3082147.

[25] R. Wazirali, "An Improved Intrusion Detection System Based on KNN Hyperparameter Tuning and Cross-Validation," *Arabian Journal for Science and Engineering*, vol. 45, no. 12, pp. 10859–10873, Dec. 2020, https://doi.org/10.1007/s13369-020-04907-7.

[26] T. Markovic, M. Leon, D. Buffoni, and S. Punnekkat, "Random Forest Based on Federated Learning for Intrusion Detection," in *Artificial Intelligence Applications and Innovations*, 2022, pp. 132–144, https://doi.org/10.1007/978-3-031-08333-4_11.

[27] A. K. Balyan *et al.*, "A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method," *Sensors*, vol. 22, no. 16, Jan. 2022, Art. no. 5986, https://doi.org/10.3390/s22165986.

[28] A. Pathak and S. Pathak, "Study on Decision Tree and KNN Algorithm for Intrusion Detection System," *International Journal of Engineering Research and*, vol. V9, no. 05, May 2020, Art. no. IJERTV9IS050303, https://doi.org/10.17577/IJERTV9IS050303.

[29] M. Mohammadi *et al.*, "A comprehensive survey and taxonomy of the SVM-based intrusion detection systems," *Journal of Network and Computer Applications*, vol. 178, Mar. 2021, Art. no. 102983, https://doi.org/10.1016/j.jnca.2021.102983.

[30] B. S. Bhati and C. S. Rai, "Analysis of Support Vector Machine-based Intrusion Detection Techniques," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 2371–2383, Apr. 2020, https://doi.org/10.1007/s13369-019-03970-z.

[31] B. D. Shivahare, M. Singh, A. Gupta, S. Ranjan, D. Pareta, and B. M. Sahu, "Survey Paper: Whale optimization algorithm and its variant applications," in *2021 International Conference on Innovative Practices in Technology and Management (ICIPTM)*, Noida, India, Feb. 2021, pp. 77–82, https://doi.org/10.1109/ICIPTM52218.2021.9388344.

[32] H. M. Al-Mimi, N. A. Hamad, M. M. Abualhaj, S. N. Al-Khatib, and M. O. Hiari, "Improved intrusion detection system to alleviate attacks on DNS service," *Journal of Computer Science*, vol. 19, no. 12, pp. 1549–1560, 2023.

[33] R. Basfar, M. Y. Dahab, A. M. Ali, F. Eassa, and K. Bajunaied, "Enhanced Intrusion Detection in Software-Defined Networking using Advanced Feature Selection: The EMRMR Approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 19001–19008, Dec. 2024, https://doi.org/10.48084/etasr.9256.

[34] O. Almomani, A. Alsaaidah, A. A. Abu-Shareha, A. Alzaqebah, M. A. Almaiah, and Q. Shambour, "Enhance URL Defacement Attack Detection Using Particle Swarm Optimization and Machine Learning," *Journal of Computational and Cognitive Engineering*, Feb. 2025, https://doi.org/10.47852/bonviewJCCE52024668.