Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.016140
Article

Tech Science Press

Intrusion Detection Using a New Hybrid Feature Selection Model

Adel Hamdan Mohammad*

Computer Science Department, The World Islamic Sciences and Education University, Amman, 1101-11947, Jordan
*Corresponding Author: Adel Hamdan Mohammad. Email: adel.hamdan@wise.edu.jo

Received: 24 December 2020; Accepted: 13 April 2021

Abstract: Intrusion detection is an important topic that aims at protecting computer systems. Besides, feature selection is crucial for increasing the performance of intrusion detection. This paper employs a new hybrid feature selection model for intrusion detection. The implemented model uses Grey Wolf Optimization (GWO) and Particle Swarm Optimization (PSO) algorithms in a new manner. In addition, this study introduces two new models called (PSO-GWO-NB) and (PSO-GWO-ANN) for feature selection and intrusion detection. PSO and GWO show emergent results in feature selection for several purposes and applications. This paper uses PSO and GWO to select features for the intrusion detection system. Furthermore, in this study, a new emergent feature selection method using the interstation of (PSO and GWO) features is developed. Also, this research examines the Most frequently Repeated Features from (PSO and GWO) and gives it the name (MRF). This study runs PSO and GWO for a specific number of iterations, which the user could define. Each feature selection model runs independently, and the selected feature set is saved. PSO features, GWO features, the intersection of (PSO and GWO) features, and MRF features are tested at the next stage. This research uses the UNSW-NB15 dataset for evaluation purposes. Furthermore, experiments are implemented using two classifiers: Naïve Bayesian (NB) and Artificial Neural Networks (ANN). The results show that PSO and GWO are highly acceptable for the selection of intrusion detection features. Besides, the intersection of (PSO and GWO) features gives an emergent result with a minimum number of features. Moreover, MRF features show highly acceptable results. The evaluation process criteria are true positive, false positive, false negative, precision, and recall. The experiments demonstrate that MRF features give a good result related to precision and recall. Finally, experiments show that the performance of (PSO-GWO-NB) classifier is better than (PSO-GWO-ANN) for feature selection and intrusion detections.

Keywords: Intrusion detection; features selection; grey wolf optimizer; UNSW-NB15 dataset; particle swarm optimization; artificial neural networks; machine learning; Naïve Bayes

1 Introduction

Intrusion detection is a set of procedures and techniques used to identify an intrusion activity. As such, an intrusion detection system is any software that can detect or respond to abnormal activity. An intrusion is an illegal try to access and use a computer system and its resources [1–3]. Generally, intrusion detection is classified into two methods: misuse detection or anomaly detection [1,2]. Misuse detection systems are based on using prior knowledge of attacks to search and identify attack traces. Whereas, anomaly detection is another technique based on studying the normal activity features [2]. Furthermore, intrusion detection can be divided into three different sub-groups. Host-based intrusion detection (HBID), network intrusion detection (NIDS), and hybrid-based intrusion detection (HISD) [4–6].

Features selection is an essential factor for the success of an intrusion detection system. It is necessary for high diversity data mining, and is a fundamental data processing step in the training phase prior to moving to the next stage (testing) [7]. There are different techniques for selecting features, such as the wrapper, the filter, and the embedded methods. Other methods are bio-inspired metaheuristic [7–9]. Determining the best number of features will improve the success rate and performance. This study's outline and main contribution can be summarized with the following points: Using PSO and GWO in a new emergent method, selecting the intersection of their (PSO and GWO) features, then examining the resulting most frequently repeated features, which will represent the best set.

Intrusion detection can be implemented through several methods, such as the programmed and the self-learning methods. Fig. 1 presents several of such techniques [10]. Many studies indicate that intrusion detection systems have become one of the most recent cybersecurity research areas [5]. Additionally, recent studies demonstrate that the number of attacks on individuals and organizations tends to increase rapidly [5–7]. Intrusion detection using traditional preventions, such as firewall, encryption, and user authentication has not entirely succeeded in its mission. In other words, the need for other emergent procedures has become vital. This research focuses on using bio-inspired metaheuristic and machine learning algorithms in developing an efficient feature selection and intrusion detection system.

The rest of this paper is organized as follows: Section 2 demonstrates the proposed model. Section 3 presents feature selection. Section 4 explains particle swarm optimization. Section 5 illustrates the grey wolf optimizer. Section 6 describes machine learning algorithms. Section 7 presents related works. Section 8 introduces the dataset used in this work. Section 9 shows the proposed model experiments. Finally, Section 10 presents this research conclusion.

2 The Proposed Model

This paper proposes two hybrid models for feature selection and intrusion detection. The first model is (PSO-GWO-NB), and the second is (PSO-GWO-ANN).

Features selection is significant for the success of any classification process. As mentioned in the research, there are several techniques for feature selection. After the intensive study of the techniques, this paper gives the interest to investigate the bio-inspired techniques. Feature selection in the proposed system is as follows: The original dataset contains 49 features. The used dataset, after reduction and cleaning, has only 45 features. PSO and GWO are used to decrease the number of features. Experiments are repeated several times until getting the optimal number of features. Figs. 2 and 3 demonstrate PSO and GWO features selection models, respectively.

The process of feature selection is repeated 30 times for PSO and GWO. PSO features, GWO features, the intersection of (PSO and GWO) features, and the Most frequently Repeated Features (MRF) are used for further experiments with NB and ANN. Fig. 4 demonstrates the overall features selection model.

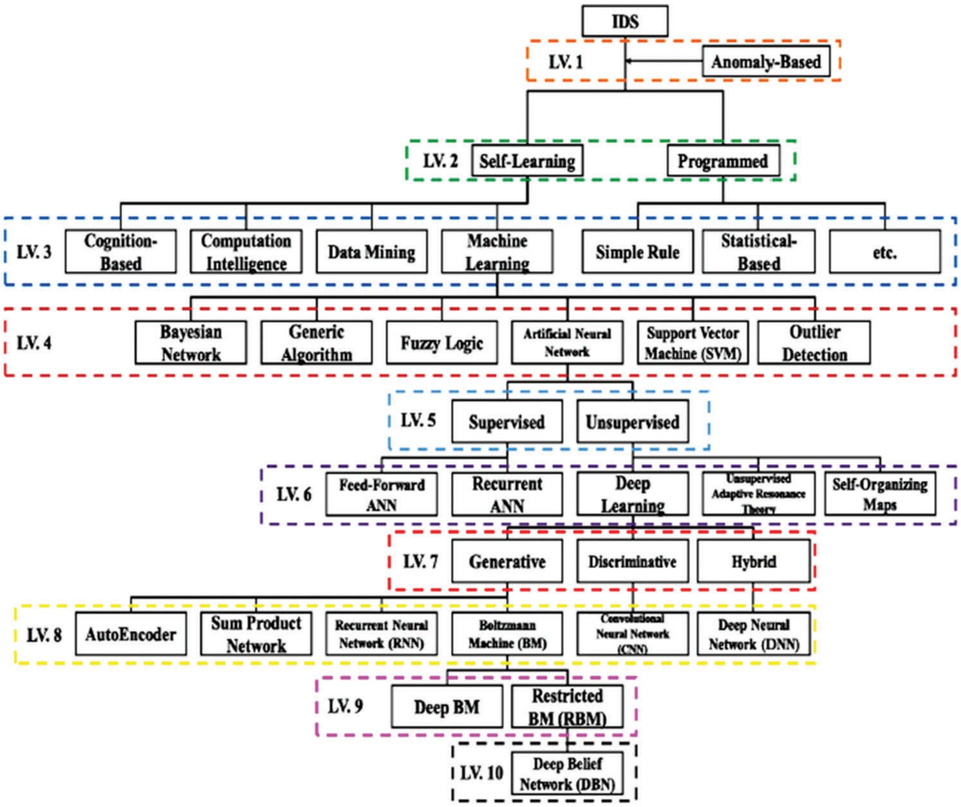

Figure 1: Classification of anomaly detection

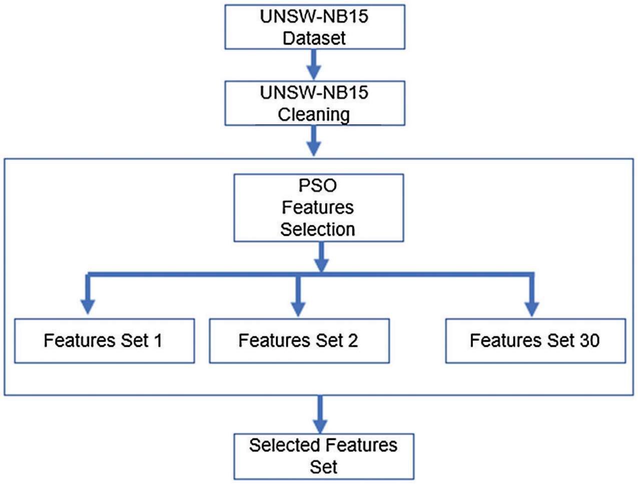

Figure 2: PSO features selection

As shown in Fig. 4, each bio-inspired algorithm used for feature selection is treated independently, and the reduced set will be used for further experiments. In the next stage, NB and ANN classifiers are used. Fig. 5 shows the overall proposed model (PSO-GWO-NB, PSO-GWO-ANN).

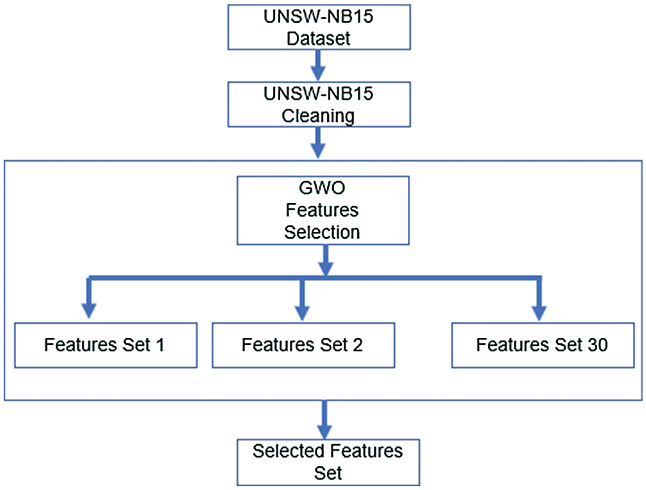

Figure 3: GWO features selection

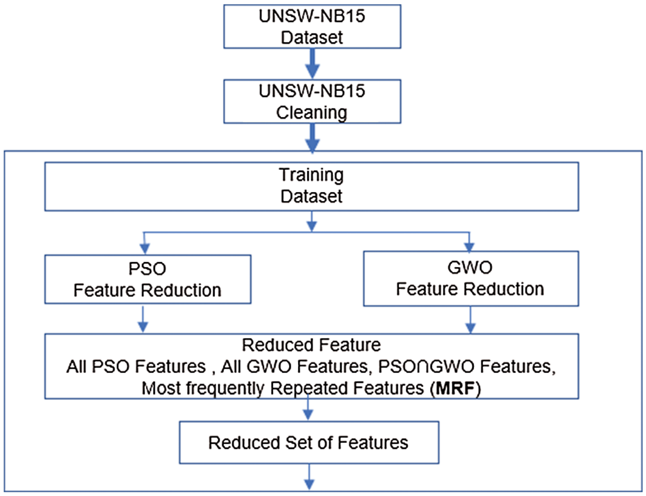

Figure 4: PSO-GWO features selection model

3 Feature Selection

Feature selection is a critical factor for the success and failure of any classification system. Many standard techniques, such as Correlation-based Feature Selection method (CFS), Gain Ratio (GR), and Information Gain (IG) [5–8]. Other types are bio-inspired algorithms, such as genetic algorithms and artificial neural networks [11,12], and new emergent algorithms should be of broad interest, such as GWO and PSO [5,13,14]. Selecting an appropriate method can be crucial for the success and failure of the overall process.

4 Particle Swarm Optimization

Particle Swarm Optimization (PSO) algorithm is a computational technique that can optimize a problem by iteratively selecting a suggestion or a candidate solution. PSO is inspired by the behavior of collective animals like fish and birds, and aims at solving the problem by having a population of appropriate solutions. Also, it can search for huge spaces of potential solutions [15]. PSO can not be guaranteed to find the best solution, and based on having a population (called swarm) of a candidate solution (called particle). Particles moved according to a few simple formulas [5], and swarms travel in the search space with the hope of finding the best solution. In addition, if a better position is discovered, the movements of the swarm will be changed; This process is repeated with the intent to find the optimal solution [16,17].

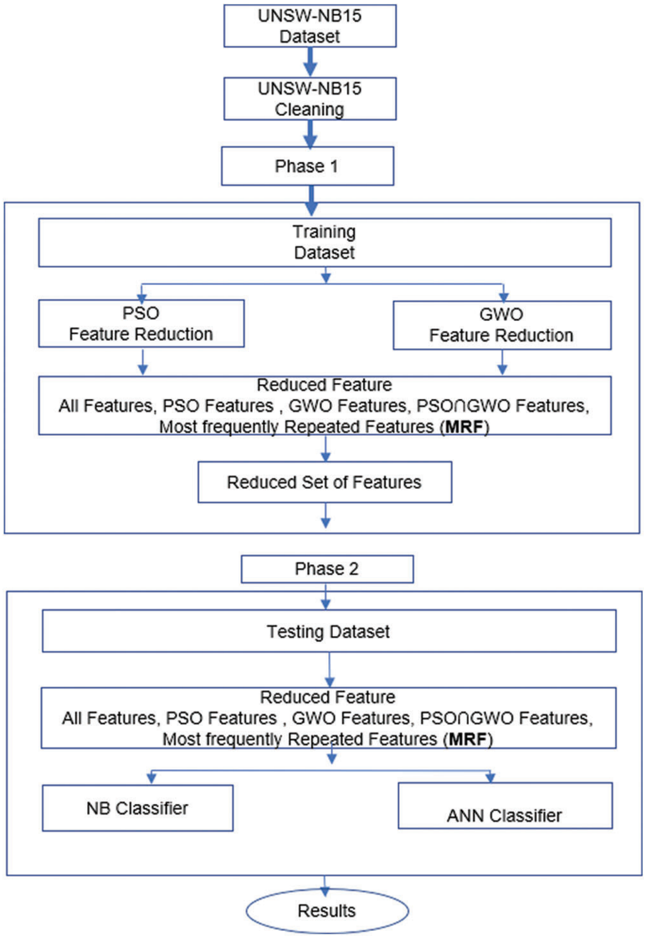

Figure 5: PSO-GWO-NB, PSO-GWO-ANN

5 Grey Wolf Optimizer

Grey Wolf Optimizer (GWO) algorithm is a swarm intelligence optimization algorithm developed by Mirjalili et al. [18] in 2014, and it emulates the leadership hierarchy and the chasing of gray wolves. Wolves are categorized into four types, as shown in Fig. 6 [18].

Wolves types are alpha, beta, delta, and omega. Alpha is the best group of individuals, and is the leader of the wolves [15,18]. The alpha type is dominant, the decision-maker, and their orders and instructions must be taken seriously by the pack. Beta is the second-best group of individuals, and acts as subsidiary wolves, which can help alpha in taking the decision. Besides, beta wolves are the candidates to be alpha in case of any problem, and play a consultant's role to alpha groups and a discipliner for the pack. The third best group of individuals is delta, and the rest of the pack is considered omega [19]. Omega is the lowest level that can eat in the groups, and is the scapegoat. It is said to be delta if a wolf does not belong to alpha, beta, or omega. Delta wolves must submit to alpha and beta, but they are dominant to omega. The first three groups guide the

GWO hunting process. In other words, alpha, beta, and delta groups lead other wolves to find the best position in the available search space [20,21].

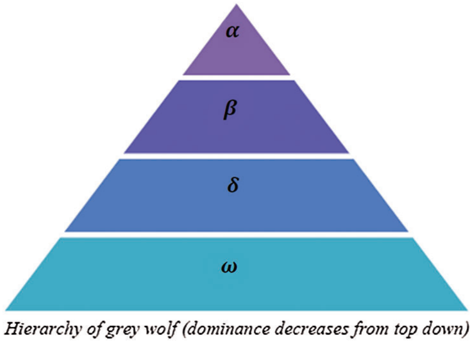

Figure 6: Wolves hierarchy

6 Machine Learning

Machine learning (ML) algorithms are used for several purposes, such as classification and prediction. Many kinds of research present several machine learning algorithms, such as Genetic Algorithm (GA), Artificial Neural Networks (ANN), Naïve Bayesian (NB), Support Vector Machines (SVM), K-Nearest Neighbors (K-NN), and decision tree in text classification, spam detection, and prediction [5,11,12,17–21]. Without a doubt, ML algorithms can be used in intrusion detection [5]. Fig. 7 presents that the machine learning process is completed into two phases: the training and the testing phases.

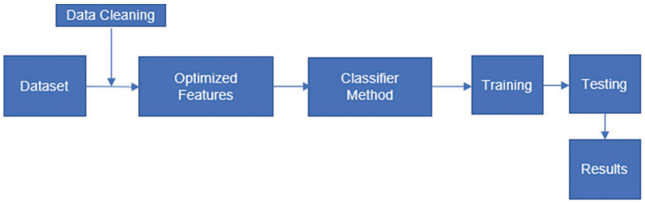

Figure 7: Machine learning process

This study applies PSO and GWO algorithms for feature reduction and selection. Also, the dataset used in this research is UNSW-NB15 [22], and ML algorithms used are NB and ANN. ML algorithms employ training of data before testing. The training is vital and aims to clean and prepare data for testing. Besides, data training is used to select the most suitable features, which will be used in the testing phase [23,24].

6.1 Naïve Bayes Classifiers

Naïve Bayes (NB) is a probabilistic classifier based on applying Bayes theorem, and is a simple and powerful algorithm that can determine the included classes using the probability theorem [25,26]. Furthermore, the NB classification hypothesis's major function is making sure that the given data belongs to a specific category. In NB, if you are given a series of x attributes, then we have 2x! independence assumptions [27]. Besides, training and data preprocessing are significant in NB since some errors, and data noise could result from unsuitable training and data variance [25–27]. Finally, the results of NB, are often correct.

6.2 Artificial Neural Networks Classifiers

Artificial Neural Networks (ANN) is considered one of the powerful learning models inspired by a biological neural network (nervous system) and emulates the human brain's role. Many studies used ANN as a classifier, especially as a text classifier [28–31]. In addition, ANN has several components, such as neurons, connections, weight, propagation function, and organization. Also, ANN has two paradigms: supervised and unsupervised learning. Besides, many researchers use ANN in intrusion detection [29,30], and numerous studies indicated that intrusion detection performance could be enhanced using neural networks. In ANN modules, the system tries to learn the pattern and make a prediction based on the learning phase, and during the training process, ANN can learn errors. Once the neural network has been trained, it can make predictions by indicating a similar pattern [31]. In this research, the Multilayer Perceptron (MLP) is used. The multilayer perceptron is a class of feed-forward ANN and employs a supervised learning method called backpropagation [32–34].

7 Related Studies

This section will demonstrate many kinds of research that illustrate intrusion detection using bio-inspired metaheuristic and machine learning algorithms.

AShahri et al. [35] proposed a hybrid model of the genetic algorithm and the support vector machine for intrusion detection. The number of features is reduced to 10 instead of 45. The authors categorize feature priorities into three levels. The highest priority is the first, and the lowest priority is the third. The distribution of features comes as follows: the first four are placed in the first priority, the other four in the second priority, and the last two are in the third priority. The overall results of this research are 0.97 true positive and 0.017 false positive.

Chung et al. [36] developed a new hybrid model for intrusion detection, and uses Intelligent Dynamic Smart swarm-based Rough-Set (IDS-RS) for feature selection. The largest number of relevant features which characterize traffic pattern must be selected by the proposed model. Also, a new weighted local search strategy is tested in simplified swarm optimization. The authors demonstrate that the proposed model can enhance performance. Besides, experiments are applied using the KDDCup99 dataset and show that the projected model can achieve an approximately 93.3% accuracy.

Çavuşoğlu [37] developed a hybrid and layered intrusion detection system, and uses a mixture of machine learning algorithms and feature selection methods to provide a maximum number of accuracies. By using two distinct features selection (CfsSubsetEval, WrapperSubsetEval), the dataset is reduced. However, in all attack types, the proposed system provides 99.7% accuracy, and the dataset used is NSL-KDD.

Buczak et al. [38] reported a survey of data mining and machine learning methods for cybersecurity and intrusion detection. The complexity of machine learning and data mining is addressed, and the crucial aspect of this study for cybersecurity is the importance of a dataset for training and testing. Also, the authors mention that machine learning and data mining cannot work without data representation, and it is difficult and time-consuming to get a dataset. Besides, recommendations on when to use a given method are provided.

Chitrakar et al. [39] proposed a hybrid learning model by joining NB with k-Medoids based clustering technique. The authors observe that the application of K-Medoids clustering techniques, followed by the NB classification method, is better for getting more accurate results. Results demonstrate that the planned model enhanced accuracy and false-positive rate.

Yin et al. [40] demonstrated how to model the intrusion detection system based on deep learning techniques, and suggest a new deep learning approach for intrusion detection using Recurrent Neural Networks Intrusion Detection System (RNN-IDS). Results are compared with J48, artificial neural networks, support vector machine, and random forest. Also, results show that RNN-IDS is very appropriate for modeling systems with high accuracy. Finally, the authors demonstrate that the model can successfully enhance intrusion detection accuracy and the ability to distinguish the intrusions types.

Almomani [5] presented several bio-inspired algorithms for feature selection, and uses the genetic algorithm, particle swarm optimization, grey wolf optimizer, and firefly optimization. Features derived from bio-inspired model evaluated using support vector machine and J48 classifiers. All experiments use the UNSW-NB15 dataset and demonstrate promising results related to false positive and accuracy.

Wang et al. [41] suggested a new approach for the artificial neural network as intrusion detection, and the recommended approach was called Fuzzy Clustering-Artificial Neural Networks (FC-ANN). The FC-ANN procedure based on using the fuzzy clustering technique to produce different training subsets. Then, based on different training subsets, different artificial neural networks are trained to express different base models. Finally, the dataset used is KDDCUP99.

Xin et al. [42] reported an important literature survey on the machine and deep learning methods for intrusion detection. The authors focused on the last three years' literature review for network security, and demonstrate that each approach used for intrusion detection has its advantages and disadvantages. The authors say that selecting a dataset is very important for training and testing. Also, they demonstrate several problems and trends in intrusion detection, such as dataset, hybrid methods, detection speed, and online learning.

Gumus et al. [43] built an online NB classifier to determine normal and unnormal activity. The classifier continually updates the mean and standard deviation of the features (IDS variables). Also, the authors compare several machine learning algorithms on the KDD99 dataset, and they mention that the proposed technique is time-efficient.

8 Dataset

Dataset used in this research is UNSW-NB15, which is complete and used for intrusion detection systems. One of the significant challenges for all researchers is the availability of a benchmark dataset, and KDD98, KDDCPU99, and NSLKDD datasets were generated a decade ago. Moustafa et al. [22] developed the UNSW-NB15 dataset for research purposes, and this dataset is hybrid and contains usual and contemporary attack events. Fig. 8 shows the UNSW-NB15 dataset [22].

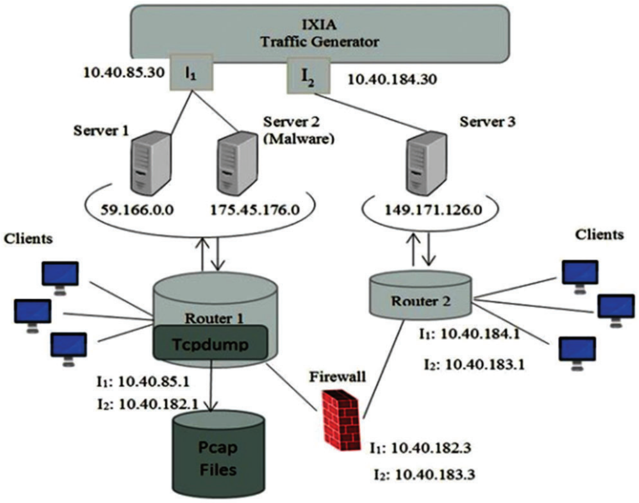

Figure 8: UNSW-NB15 Testbed

UNSW-NB15 dataset contains nine categories of attacks: fuzzers, analysis, generic, reconnaissance, shellcode, backdoors, dos, exploits, and worms. The dataset contains 49 features. Dataset record distribution is shown in Tab. 1. In UNSW-NB15, the number of records in the training set is 175,341, and the testing set is 82332. The testing and training dataset contains 45 features. Some features are missing in the training and the testing dataset, such as scrip, sport, dstip, dsport, smeansz, dmeansz, res_bdy_len, stime, and ltime. Also, few features are available in the training and the testing dataset but missing in the list of features, such as rate, smean, dmean, and response_body_len. The list of features in UNSW-NB15 is shown in Tab. 2 [22].

Table 1: Dataset record distribution in UNSW-NB15 dataset

Type	Number of records	Descriptions
Normal	2,218,761	Natural transaction data
Fuzzers	24,246	Attempting to cause a program or network suspended by feeding it the randomly generated data
Analysis	2,677	It contains different attacks of port scan, spam and html files penetrations.
Backdoors	2,329	A technique in which a system security mechanism is bypassed stealthily to access a computer or its data
DoS	16,353	A malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.
Exploits	44,525	The attacker knows of a security problem within an operating system or a piece of software and leverages that knowledge by exploiting the vulnerability.
Generic	215,481	A technique works against all blockciphers (with a given block and key size), without consideration about the structure of the block-cipher
Reconnaissance	13,987	Contains all Strikes that can simulate attacks that gather information.
Shellcode	1,511	A small piece of code used as the payload in the exploitation of software vulnerability.
Worms	174	Attacker replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it

9 Experiments and Results

This section demonstrates the experiments' phases, evaluation metrics, important features, and results.

9.1 Experiments Phases

This paper uses the Anaconda Python open-source and the Weka open-source machine learning software in carefully controlled two-phases experiments.

The first phase of the experiments starts by using the PSO and GWO algorithms. Anaconda Python open-source program is used to reduce the number of features. The results of phase 1 are PSO features, GWO features, the intersection of (PSO and GWO) features, and the MRF. The reduced set of features is selected for further experiments. Whereas in phase 2, the reduced set of features is used with NB and ANN classifiers using the Weka open-source machine learning software.

Table 2: List of features in UNSW-NB15 dataset

F No	F Name	F No	F Name	F No	F Name
1	id	16	dloss	31	Response_body_len
2	d ur	17	sinpkt	32	Ct_srv_src
3	proto	18	dinpkt	33	Ct_state_ttl
4	service	19	sjit	34	Ct_dst_ltm
5	state	20	djit	35	Ct_src_dport_ltm
6	spkts	21	swin	36	Ct_dst_sport_ltm
7	dpkts	22	stcpb	37	Ct_dst_src_ltm
8	sbytes	23	dtcpb	38	Is_ftp_login
9	dbytes	24	dwin	39	Ct_ftp_cmd
10	rate	25	tcprtt	40	Ct_flw_http_mthd
11	sitl	26	synack	41	Ct_src_ltm __
12	dttl	27	ackdat	42	Ct_srv_dst
13	sload	28	swan	43	Is_sm_ips_ports
14	dload	29	dmean	44	Attack_cat
15	sloss	30	Trans_depth	45	label

9.2 Experiments Evaluation Metrics

To accurately test the efficiency of the experiments, several criteria could be used, such as Precision (P), Recall (R), TPR (True Positive Rate), FPR (False Positive Rate), FNR (False Negative Rate), and F-measure [5,27]. See Tab. 3 and Eqs. (1)–(6).

Table 3: Confusion matrix

		Predicted	
		Normal	Attack
Actual	Normal	a (TP)	b (FN)
	Attack	c (FP)	d (TN)

TP (True Positive): The model correctly predicts the positive class.

FN (False Negative): The model incorrectly predicts the negative class.

FP (False Positive): The model incorrectly predicts the positive class.

TN (True Negative): The model correctly predicts the negative class.

TPR (True Positive Rate): Quantity of normal data identified as normal.

FPR (False Positive Rate): Quantity of attack identified as normal.

FNR (False Negative Rate): Quantity of normal identified as attack

Precision: The ratio of the numbers of decisions that are correct or relevant retrieved/total retrieved.

Recall: The ratio of total relevant results correctly classified or relevant retrieved/total relevant.

F-measure: Testing the accuracy level, and it is a single measure that balances precision and recall.

$$\mathrm{TPR} = \mathrm{a}/(\mathrm{a}+\mathrm{b}) \tag{1}$$

$$\mathrm{FPR} = \mathrm{c}/(\mathrm{c}+\mathrm{d}) \tag{2}$$

$$\mathrm{FNR} = \mathrm{b}/(\mathrm{a}+\mathrm{b}) \tag{3}$$

$$\mathrm{Precision} = \mathrm{TPR}/(\mathrm{TPR}+\mathrm{FPR}) \tag{4}$$

$$\mathrm{Recall\ or\ (Sensitivity)} = \mathrm{TPR}/(\mathrm{TPR}+\mathrm{FNR}) \tag{5}$$

$$\mathrm{F-measure} = 2 * \mathrm{Precision} * \mathrm{Recall}/(\mathrm{Precision}+\mathrm{Recall}) \tag{6}$$

All experiments were conducted using Dell Machine, Intel(R), Core i7-CPU 1.8 GHz, installed memory (RAM) 16 GB, 64 Bit Operating System, Windows10.

9.3 Experiments Important Features

Tab. 4 demonstrates the selected features using PSO, GWO, (PSO∩GWO), and MRF. For the purposes of the experiments, only one set of features will be presented.

The MRF features are selected as follows: PSO feature reduction is repeated 30 times, all features that appear more than 8 times will be selected for the MRF experiments, and this process is repeated with GWO. The result of MRF is 34 features.

Table 4: Features selected

Experiments Name	Selected Features	Number of Selected Features
ALL	f1, f2, ……………………………………f45	45
PSO	f2,f4,f5,f7,f11,f12,f16,f17,f18,f19,f20,f22,f23,f24,f25,f26,f28,f30, f31,f34,f39,f40,f41,f42	24
GWO	f1,f4,f5,f6,f13,f16,f17,f22,f23,f26,f28,f29,f34,f36,f37,f38,f40,f41, f42	19
PSO∩GWO	f4,f5,f16,f17,f22,f23,f26,f28,f34,f40,f41,f42	12
MRF	f3,f4,f6,f7,f8,f9,f10,f13,f14,f15,f16,f17,f18,f19,f20,f21,f22,f23,f24, f25,f26,f27,f28,f29,f31,f32,f34,f35,f36,f37,f41,f42,f44,f42	34

9.4 Experiments Results

The proposed (PSO-GWO-NB) and (PSO-GWO-ANN) models are evaluated and tested as shown in Tabs. 5 and 6, respectively. Experiments are conducted using NB and ANN classifiers. Tab. 5 demonstrates (PSO-GWO-NB) results, and shows TPR, FPR, FNR, precision, recall, and F-measure. MRF and (PSO∩GWO) results are highly accepted.

The second proposed system (PSO-GWO-ANN) is shown in Tab. 6. Results demonstrate that MRF and (PSO∩GWO) are promising.

Table 5: PSO-GWO-NB experiments

Experiments	TPR	FPR	FNR	Precision	Recall	F-measure
ALL Features	90.4%	8.8%	9.6%	91.2%	90.4%	90.8%
PSO	87.4%	10.7%	12.6%	89.1%	87.4%	88.2%
GWO	80.8%	14.4%	19.2%	84.9%	80.8%	82.8%
PSO∩GWO	65%	22.2%	35%	74.5%	65%	69.5%
MRF	87.7%	8.8%	12.3%	90.9%	87.7%	89.3%

Table 6: PSO-GWO-ANN experiments

Experiments	TPR	FPR	FNR	Precision	Recall	F-measure
ALL Features	82.4%	10.3%	17.6%	88.8%	82.4%	85.5%
PSO	79.4%	12.4%	20.6%	86.5%	79.4%	82.8%
GWO	76.5%	14.5%	23.5%	84.1%	76.5%	80.1%
PSO∩GWO	70.6%	16.6%	29.4%	81%	70.6%	75.4%
MRF	80.9%	11.4%	19.1%	87.7%	80.9%	84.1%

The TPR range of (PSO-GWO-NB) experiments is between 65% and 90.4%, while it is between 70.6% and 82.4% for (PSO-GWO-ANN). Also, the performance of (PSO-GWO-NB) is better than (PSO-GWO-ANN) except for (PSO∩GWO) features. See Tabs. 5 and 6 above.

The FNR range of (PSO-GWO-NB) experiments is between 9.6% and 35%, while it is between 17.6% and 29.4% for (PSO-GWO-ANN). Also, the performance of (PSO-GWO-NB) is better than (PSO-GWO-ANN) except for (PSO∩GWO) features. See Tabs. 5 and 6 above.

The FPR range of (PSO-GWO-NB) experiments is between 8.8% and 22.2%, while it is between 10.3% and 16.6% for (PSO-GWO-ANN). Also, the performance of (PSO-GWO-NB) is better than (PSO-GWO-ANN) except for (PSO∩GWO) features. Fig. 9 presents FPR results.

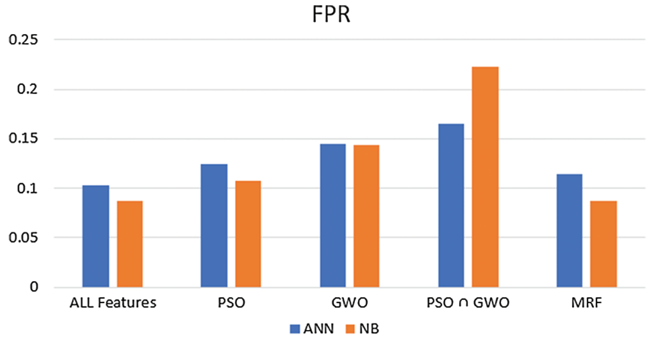

Figure 9: FPR

The precision range of (PSO-GWO-NB) experiments is between 74.5% and 91.2%, and for (PSO-GWO-ANN), is between 81% and 88.8%. Fig. 10 clearly shows precision results. Furthermore, the performance of the MRF is extremely remarkable.

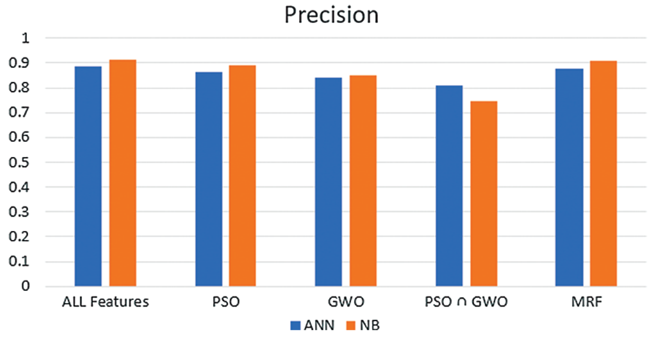

Figure 10: Precision

The recall range of (PSO-GWO-NB) experiments is between 65% and 90.4%, and for (PSO-GWO-ANN), is between 70.6% and 82.4%. Fig. 11 presents recall results. The performance of (PSO-GWO-NB) is better than (PSO-GWO-ANN) except for (PSO∩GWO) features.

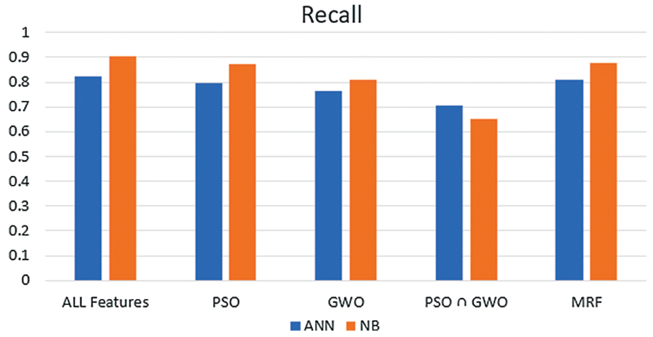

Figure 11: Recall

The F-measure range of (PSO-GWO-NB) experiments is between 69.5% and 90.8%, and for (PSO-GWO-ANN), is between 75.4% and 85.5%. Fig. 12 presents F-measure results. It is clear that the performance of (PSO-GWO-NB) is better than (PSO-GWO-ANN)) except for (PSO∩GWO) features.

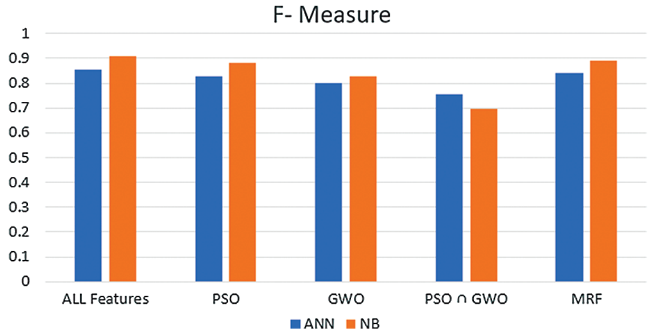

Figure 12: F-measure

10 Conclusion

Feature selection and intrusion detection are important topics, and it is crucial to improve their methods and techniques. Also, many feature selection and intrusion detection methods are available, and the traditional prevention methods have not entirely succeeded. Therefore, the need for new emergent methods is crucial. This research proposes two models for feature selection and intrusion detection in a new manner. The proposed models are (PSO-GWO-NB) and (PSO-GWO-ANN). Besides, the feature selection process is based on PSO and GWO algorithms. Anaconda Python open-source software is used in phase 1. In phase 1 of the proposed model, features are reduced using PSO and GWO. The results of phase 1 are PSO features, GWO features, the intersection of (PSO and GWO) features, and the MRF. The number of features for (PSO∩GWO) is only 12, and for MFR is 34. In phase 2, reduced sets of features are evaluated using Weka open-source machine learning software, and NB and ANN classifiers are used. Experiments using (PSO∩GWO) and MRF features are highly acceptable and promising. (PSO-GWO-NB) gives a precision range between 74.5% and 91.2% and a recall range between 65% and 90.4%, and (PSO-GWO-ANN) provides a precision range between 81% and 88.8% and a recall range between 70.6% and 82.4%.

Acknowledgement: I want to dedicate this work to my wife, father, mother, and WISE University. Further, I am very much thankful to the reviewers and Journal Authorities.

Funding Statement: The author receives funding from the World Islamic Sciences and Education University (WISE), Amman-Jordan, grant number (21/2020), www.wise.edu.jo.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] G. Kim, S. Lee and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1690–1700, 2014.

[2] O. Depren, M. Topallar, E. Anarim and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," *Expert Systems with Applications*, vol. 29, no. 4, pp. 713–722, 2005.

[3] D. P. Vinchurkar and A. Reshamwala, "A review of intrusion detection system using neural network and machine learning," *International Journal of Engineering Science and Innovative Technology*, vol. 1, no. 2, pp. 54–63, 2012.

[4] S. M. Othman, N. T. Alsohybe, B. Alwi and F. M. Zahary, "Survey on intrusion detection system types," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 4, pp. 444–463, 2018.

[5] O. Almomani, "A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA Algorithms," *Symmetry*, vol. 12, pp. 1046, 2020.

[6] B. B. Zarpelão, R. S. Miani, C. T. Kawakani and S. C. de Alvarenga , "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, 2017.

[7] E. Emary, H. M. Zawbaa and A. E. Hassanien, "Binary grey wolf optimization approaches for feature selection," *Neurocomputing*, vol. 172, pp. 371–381, 2016.

[8] Q. Al-Tashi, S. J. Kadir, H. M. Rais, S. Mirjalili and H. Alhussian, "Binary optimization using hybrid grey wolf optimization for feature selection," *IEEE Access*, vol. 7, pp. 39496–39508, 2019.

[9] A. Sahoo and S. Chandra, "Multi-objective grey wolf optimizer for improved cervix lesion classification," *Applied Soft Computing*, vol. 52, pp. 64–80, 2017.

[10] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim *et al.,* "A survey of deep learning-based network anomaly detection," *Cluster Computing*, vol. 22, pp. 949–961, 2017.

[11] S. Mukherjeea and N. Sharma, "Intrusion detection using Naive Bayes classifier with feature reduction," *Procedia Technology*, vol. 4, pp. 119–128, 2012.

[12] A. H. Mohd and R. Abu-Zitar, “Application of genetic optimized artificial immune system and neural networks in spam detection,” *Applied Soft Computing*, vol. 11, no. 4, pp. 3827–3845, 2011.

[13] F. Marini and B. Walczak, “Particle swarm optimization (PSO). A tutorial,” *Chemometrics and Intelligent Laboratory Systems*, vol. 149, pp. 153–165, 2015.

[14] J. Kennedy and R. Eberhart, “Particle swarm optimization,” in *Proceedings of ICNN’95—Int. Conf. on Neural Networks*, Perth, Australia, vol. 4, pp. 1941–1948, 1995.

[15] I. Kashif and S. Zainal, “An improved particle swarm optimization (PSO)-based MPPT for PV with reduced Steady-State oscillation,” *IEEE Transactions on Power Electronics*, vol. 27, no. 8, pp. 3627–3638, 2012.

[16] M. R. Bonyadi and Z. Michalewicz, “Particle swarm optimization for single objective continuous space problems: A review,” *Evolutionary Computation*, vol. 25, no. 1, pp. 1–54, 2017.

[17] I. Syarif, “Feature selection of network intrusion data using genetic algorithm and particle swarm optimization,” *EMITTER International Journal of Engineering Technology*, vol. 4, no. 2, pp. 277–290, 2016.

[18] S. Mirjalili, S. M. Mirjalili and A. Lewis, “Grey wolf optimizer,” *Advances in Engineering Software*, vol. 69, pp. 46–61, 2014.

[19] J. Wang and S. Li, “An improved grey wolf optimizer based on differential evolution and elimination Mechanism,” *Scientific Reports*, vol. 9, pp. 7181, 2019.

[20] D. E. Roopa and R. C. Suganthe, “Feature selection in intrusion detection Grey Wolf Optimizer,” *Asian Journal of Research in Social Sciences and Humanities*, vol. 7, no. 3, pp. 671–682, 2017.

[21] Q. M. Alzubi, M. Anbar, Z. N. Alqattan, M. A. Albetar and R. Abdullah, “Intrusion detection system based on a modified binary grey wolf optimization,” *Neural Computing and Applications*, vol. 32, pp. 6125–6137, 2020.

[22] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” in *IEEE Proc. of the 2015 Military Communications and Information Systems Conf. (MilCIS)*, Canberra, Australia, pp. 1–6, 2015.

[23] M. Saurabh and S. Neelam, “Intrusion detection using Naive Bayes classifier with feature reduction,” *Procedia Technology*, vol. 4, pp. 119–128, 2012.

[24] W. S. Al-Sharafat and R. Naoum, “Development of Genetic-based machine learning for network intrusion detection,” *World Academy of Science, Engineering and Technology*, vol. 3, no. 7, pp. 20–24, 2009.

[25] N. Naidu and R. V. Dharaskar, “An effective approach to network intrusion detection system using genetic algorithm,” *International Journal of Computer Applications*, vol. 1, no. 2, pp. 26–32, 2010.

[26] K. Aurangzeb, B. Baharum, L. H. Lee and K. Khairullah, “A Review of machine learning algorithms for text-documents classification,” *Journal of Advances in Information Technology*, vol. 1, no. 1, pp. 4–20, 2010.

[27] M. M. Al-Tahrawi and S. N. Al-Khatib, “Arabic text classification using polynomial networks,” *Journal of King Saud University-Computer and Information Sciences*, vol. 27, no. 4, pp. 437–449, 2015.

[28] P. Mrutyunjaya and M. R. Patra, “Network intrusion detection using Naïve Bayes,” *International Journal of Computer Science and Network Security*, vol. 7, no. 12, pp. 258–263, 2007.

[29] G. Poojitha, K. N. Kumar and P. J. Reddy, “Intrusion detection using artificial neural network,” in *Second Int. Conf. on Computing, Communication and Networking Technologies*, Karur, India, pp. 1–7, 2010.

[30] A. Shenfield, D. Day and A. Ayesh, “Intelligent intrusion detection systems using artificial neural Networks,” *ICT Express*, vol. 4, no. 2, pp. 95–99, 2018.

[31] B. Ingre and A. Yadav, “Performance analysis of NSL-KDD dataset using ANN,” in *IEEE Int. Conf. on Signal Processing and Communication Engineering Systems*, Guntur, India, pp. 92–96, 2015.

[32] W. H. Chen, S. H. Hsu and H. P. Shen, “Application of SVM and ANN for intrusion detection,” *Computers & Operations Research*, vol. 32, no. 10, pp. 2617–2634, 2005.

[33] S. Sunita, B. J. Chandrakanta and R. Chinmayee, “A hybrid Approach of intrusion detection using ANN and FCM,” *European Journal of Advances in Engineering and Technology*, vol. 3, no. 2, pp. 6–14, 2016.

[34] M. Madi, F. Jarghon, Y. Fazea and O. Almomani , “Comparative analysis of classification techniques for network fault management,” *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 28, no. 3, pp. 1442–1457, 2020.

[35] B. M. AShahri, R. Rahmani, M. Chizari, A. Maralani, M. Eslami *et al.,* "A hybrid method consisting of GA and SVM for intrusion detection system," *Neural Computing and Applications*, vol. 27, no. 6, pp. 1669–1676, 2016.

[36] Y. Y. Chung and N. Wahid, "A hybrid network intrusion detection system using simplified swarm optimization (SSO)," *Applied Soft Computing*, vol. 12, no. 9, pp. 3014–3022, 2012.

[37] U. Çavuşoğlu, "A new hybrid approach for intrusion detection using machine learning methods," *Applied Intelligence*, vol. 49, no. 7, pp. 2735–2761, 2019.

[38] A. L. Buczak and E. Guven, "A Survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[39] R. Chitrakar and C. Huang, "Anomaly based intrusion detection using hybrid learning approach of combining k-Medoids clustering and Naïve Bayes classification," in *8th Int. Conf. on Wireless Communications, Networking and Mobile Computing*, Shanghai, China, pp. 1–5, 2012.

[40] C. Yin, Y. Zhu, J. Fei and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[41] G. Wang, J. Hao, J. Ma and L. Huang, "A new approach to intrusion detection using artificial neural networks and fuzzy clustering," *Expert Systems with Applications*, vol. 37, no. 9, pp. 6225–6232, 2010.

[42] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li *et al.,* "Machine learning and deep learning methods for Cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.

[43] F. Gumus, C. O. Sakar, Z. Erdem and O. Kursun, "Online Naive Bayes classification for network intrusion detection," in *IEEE/ACM Int. Conf. on Advances in Social Networks Analysis and Mining*, Beijing, China, pp. 670–674, 2014.