Feature Selection Algorithms in Intrusion Detection System: A Survey

Sofiane MAZA and Mohamed TOUAHRIA
Department of Computer Science, University of Ferhat Abbas Setif-1, Setif 19000; Algeria
[e-mail : maza.sofiane.dz@gmail.com]
*Corresponding author: Sofiane MAZA

Received December 18, 2017; revised April 14, 2018; accepted May 5, 2018; published October 31, 2018

Abstract

Regarding to the huge number of connections and the large flow of data on the Internet, Intrusion Detection System (IDS) has a difficulty to detect attacks. Moreover, irrelevant and redundant features influence on the quality of IDS precisely on the detection rate and processing cost. Feature Selection (FS) is the important technique, which gives the issue for enhancing the performance of detection. There are different works have been proposed, but a map for understanding and constructing a state of the FS in IDS is still need more investigation. In this paper, we introduce a survey of feature selection algorithms for intrusion detection system. We describe the well-known approaches that have been proposed in FS for IDS. Furthermore, we provide a classification with a comparative study between different contribution according to their techniques and results. We identify a new taxonomy for future trends and existing challenges.

Keywords: Intrusion Detection System, Feauture Selection, Artificial Intelligence Algorithms, Deterministic algorithms, Swarm Intelligence.

http://doi.org/10.3837/tiis.2018.10.024 **ISSN : 1976-7277**

1. Introduction

Internet is considered as a virtual world which provides to the people and enterprise opportunities to exercise their activities as services like e-business, e-commerce, education, and entertainment. Furthermore, the Internet is an environment that contains a large flow of data which represents people privacy and financial transactions. Influencing on exchange data regarding Confidentiality, Integrity, and Availability (CIA) represents a dangerous impact on the networks and systems. Front of the increasing network attacks, different security tools have been developed to protect the systems against attacks such as firewalls, encryption, antivirus software, authorization mechanism, Intrusion Prevention System (IPS), and Intrusion Detection System (IDS).

IDS is very important components of the security infrastructure in any security policy. IDS secures the system against the threats by detecting all intrusions in the networks (N-IDS) and hosts (H-IDS). However, the main objective of IDS is to keep the adaptability to detect novel attacks. Regarding the methodology of detection [1], IDS uses the Misuse and Anomaly detection approach. The first one uses the signatures to find attacks, but the second one uses statistical and intelligent patterns (machine learning) to discover the normal and abnormal behavior [1-3]. The large methods have been proposed to construct IDS are based on anomaly detection, these methods have been founded on intelligent classification techniques which use artificial intelligence algorithms to recognize between the normal and abnormal behavior [1,4]. Classifier model in IDS guarantees the detection of new attacks and gives the aspect of intelligent computational to the process of detection [1, 2]. Each classifier model has its pattern, detection accuracy and error rate. Based on these three characteristics several research has been proposed to enhance the performance of intrusion detection such as: Decision Tree (DT), Support Vector Machine (SVM), and Naïve Bayesian (NB) [5-8]; k-Nearest neighbor (KNN) [9, 10]; Fuzzy Logic (FL), Genetic Algorithm (GA), and Rough Set (RS) [2, 11, 12]; Artificial Neural Network (ANN) and K-means [13, 14, 77].

Unfortunately, almost classifiers that have been developed are suffering from low attacks Detection Rate (DR) and high False Alarm (FA). Further, they still have some problems in complexity of classifier architecture and processing cost. Furthermore, the high degree of the classification, complexity, computational time, and storage of requirement influence on the quality and performance of detection [15, 16]. So, the improving of classifier performance and reducing the processing costs remain a major challenge in intrusion detection and need further investigation. For that, Reduction dataset dimensionality gives the opportunity to enhance the effectiveness of detection and avoid from the overhead classification problem. In recent years, among successful optimization process that have been used to solve such as problems is Feature Selection (FS). FS [17, 18] has been emerged to reduce the dimension data by selecting the interested attributes without redundancy (minimum redundancy) and irrelevance (maximum relevance) with the high performance of accuracy rate. Those objectives give us a good data understanding out noise, avoid about over-fitting problem, and allow to select the best feature subset of those have highly relevant relation between them and target class. Further, the large works have been proposed in this area of research needs to spot the light on them to explore and provide a new vision matching with the current challenges. Also, A new survey and classification are more incontestable to extract the different techniques which use them for enhancing the future trends. A survey with new taxonomy is very important and is a major challenge.

In this paper, we describe an overview of the most techniques have been proposed in the FS research by investigation of existing contributions. Further, we introduce the latest well-known FS algorithms for IDS which are developed to select the best feature subsets. We provide a map to understand and construct the current state of the FS in IDS by classification and comparative study. Therefore, a survey is presented to comprehension the research progress and identify the new taxonomy for future trends and existing challenges. The remainder of the paper is organized as follows. In section 2, we represent definitions, types, and topology of IDS. Mathematical definition of FS is given with their techniques and types in section 3. In section 4, data sets are described with the parameters setting. In section 5, we present a new taxonomy with different works of FS on IDS which are classified into five classes. Conclusion and future work are described in section 6.

2. Intrusion Detection System

2.1 Definitions

- Intrusion Detection process [3, 19] is an intelligent process to monitor the computer system or network events and signs the possible incidents.
- Intrusion detection model [19, 20] uses computational and intelligent methods to construct the model recognition, which is used to detect possible intrusions.
- Intrusion Detection System [1, 20] is an intelligent machine with their ability of collaboration with other IDS which automate the intrusion detection process by executing the recognition model to detect possible intrusion.

Fig. 1 illustrates the general architecture of IDS [1, 19, 20, 21] which each IDS unit has the possibility of collaboration with other IDS units.

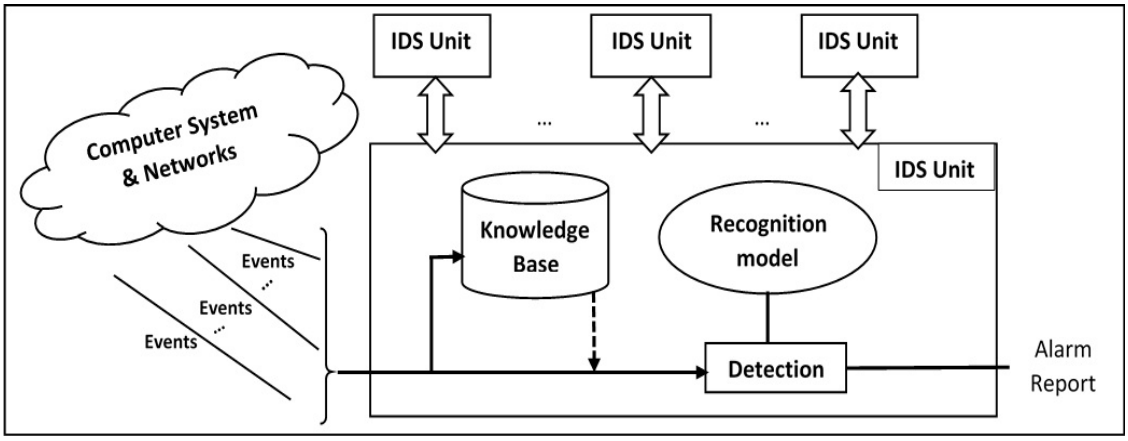

Fig. 1. General IDS Architecture.

2.2 Type

There are different classification types of IDS, which are based on their position on the system, deployment, architecture, functionality and detection methods. **Table 1** illustrates the different classification of IDS.

Table 1. IDS Classification.

Type	Name	Description
Position	HIDS NIDS	Hosts monitoring. Networks monitoring.
Deployment	WIDS NBA MIDS	Wireless traffic monitoring. Monitoring the behavior of networks. Multiple techniques.
Architecture	Centralized Hierarchical Fully distributed	Different Detection Units (DU)with one Correlation Unit (CU). Multiple communication groups for IDS. Each DU with its CU that are belonging to distributed correlation schema.
Detection	Signature (misuse) Anomaly (behavior) Stateful Protocol Anlysis	Using a knowledge base of signatures. Using behavior to detect the normal and abnormal connexion. Specific version of signature detection.

The most IDS classifications regarding position in the system are divided into the Host IDS (HIDS) and Network IDS (NIDS) [1, 3]. HIDS is placed on the host to monitor and sign intrusions. Beside, NIDS is placed on the network to control the traffic for detecting the suspicious activities. Further, another IDS classification is based on the deployment aspect that are mentioned in [3] as follows: Wireless-based IDS (WIDS), Networks, Behavior analysis (NBA), and Mixed IDS (MIDS). WIDS is specified for wireless network and the NBA is used to analyze network, protocols and application to sign the suspicious activities. MIDS is defined like an adoption of multiple technologies (hybrid techniques). Further, Wireless Sensor Networks (WSNs) intrusion detection is considered as a part of WIDS. There are several works which are proposed for intrusion prevention and detection into WSNs such as: [76, 77]. Collaboration IDS (CIDS) [20] is among IDS classification type that belongs to the architecture aspect. CIDS is based on the correlation and detection unit into each IDS. CIDS is divided into three types which as: Centralized, Hierarchical, and fully distributed. Furthermore, Detection methodology is also among the aspect of classification which Regarding the detection method of [1, 3], IDS uses the misuse detection (signature) and anomaly (behavior) detection. Misuse detection uses the pre-definition of known attacks like a knowledge base of signatures to define the possible suspicious events such as [78]. Therefore, anomaly detection has been used a statistical and machine learning pattern to build a classifier model which is used to discover the normal and abnormal behavior.

In anomaly detection, the most intelligent classification model has been used by IDS are based on artificial and computational intelligence algorithms. These classifiers models have been applied as a single or multi (hybrid) algorithms which are combined between a set of algorithms such as: DT, SVM, NB, KNN, GA, RS, FL, ANN, Swarm Intelligence (SI), and Artificial Immune System (AIS).

Despite the results of these models, they still suffer from the limitation in achieving high detection rate accuracy versus the False Positive Rate (FPS), which appears as an inability to recognize all attack attempts. Architecture complexity, processing cost, computational time, and storage requirements of the models have been influenced on the quality and detection performance. Thus, FS is presented like preprocessing optimization process to solve these problems by selecting the interesting attributes without redundancy and irrelevance.

3. Feature Selection

3.1 Definition

Feature Selection (FS) [17, 18] is a preprocessing optimization process to decrease the dimensionality of dataset by selecting the interesting features without redundancy and irrelevance. These features represent the best subset(s) which ensure [18, 26, 29, 30]:
- Increasing the performance of the classification model (Accuracy Rate), and avoid the overhead of classification problem.
- Reducing the computation time and storage requirements.
- Understanding data out noise and avoid over-fitting problem.

Mathematical definition of feature selection is presented as 6-uplet FS = { D, F, C, S, fs, E }, where: D is a dataset D= { $i_1,i_2,...,i_m$} with m instances, F is set of features F = { $f_1,f_2,...,f_n$} with n number of features, C is a target class C = {$c_1,c_2,...,c_k$} with the k label of target classes, S (search space) is a partition of set F which contains all subsets that we can construct by F where S= { $s_1,s_2,...,s_l$ } (l= 2^n - 1: NP-Hard optimization problem) with s_i = { $f_j,f_k,...,f_l$ } ($1 \leq j \neq k \neq l \leq n$), E evaluation measure, and function fs which represents the process of feature selection: fs : $F \rightarrow S$.

Furthermore, the evaluation measure (E) is used by fs to evaluate the feature subsets and gives metrics that determine the goodness of them. The evaluation measure is divided into five types according to [31] which are : Distance, Information, Dependency, Consistency, and Classifier Error Rate.

3.2 Process and Mechanisms

According to [17, 32], **Fig. 2** illustrates the most popular process that is used for FS. Subset generation is the search method, which discovers the search space for selecting the best subset(s). Subset evaluation uses the criterion measure to evaluate each subset. While, Result validation is the step of validation, which classifier algorithms are used to decide its effectiveness. Evaluation measure (Evaluation step) and search method (Subset generation) are the important steps in the feature selection, they decide effectiveness of feature subset(s) which are selected.

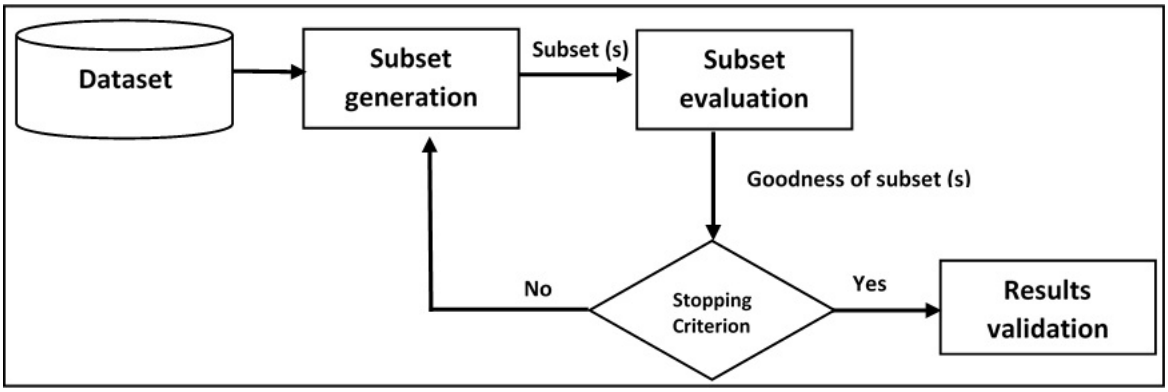

Fig. 2. Feature Selection Process.

FS process follows a mechanism of detection which is focused into three categories such as: incremental, decremental, and random selection.

Incremental mechanism, the set of features that represents the best features are selected by the process of selection is started empty. In each iteration the process adds a new feature into the set (one by one). Selection of the new feature is depending to the evaluation metrics. At the end of the process, the set of features contains the best features which represent the best feature subset. In Decremental mechanism, Set of the best features starts full with all features. When, the selection process is finished, the set of features contains just the best features that remain after removing other features one by one in each iteration. Also, Decremental mechanism uses the metric evaluation to select which feature is removed. Furthermore, Random mechanism, in each iteration, it selects a group of features like subset and evaluates it with evaluation measures. At the end of the process, it gets the best subset between all subsets selected. The manner to select the features group is depending to the techniques are used by the approach proposed.

3.3 Type

Depends on the dependency with learning/classification algorithms, the feature selection has been classified into three groups [17, 33, 34]: wrapper, filter, and hybrid approach.

Wrapper approach [2, 18, 30] uses the learning/classification algorithms to select the best features like a tool of evaluation. It uses accuracy rate (error rate) as a feedback to determine the effectiveness of feature subsets. Filter approach [2, 30, 31] uses the statistical learning data as a measure to evaluate the attributes independently of learning/classification algorithm. However, wrapper and filter approach have some advantages and inconvenients. The wrapper methods reach better classification performance than filter method, but they are more computationally expensive [2, 35]. On otherwise, filter approach has been assigned when processing has high dimensional data [18]. Hence, the hybrid approach is a combination between wrapper and filter methods, which has been emerged to cover those inconvenient and benefit from the advantages.

4. Datasets and Performance Evaluation

4.1 Datasets

Different public and private datasets are integrated as a benchmark data for IDS evaluation. Private and self-produced datasets are generated to avoid incomplete training datasets, but still inaccessible and difficult to guarantee their efficiency. Furthermore, public datasets utilise user behavior system call sequences and network traffic data source. DRAPA98-99, KDDcup99, and NSL-KDD are the famous public benchmarks which have been based on traffic network and considered useful data to evaluate IDS. DRAPA-Lincoln dataset [22] has been created by MIT's Lincoln Laboratory. DRAPA-Lincoln has two versions (DRAPA98 and DRAPA99). DRAPA98 data set is a collection of 300 instances of 38 attacks between training and test data. While, DRAPA99 dataset contains 200 instances of 58 attacks. Further, KDDcup99 [23] is considered a derivation of DRAPA98 which integrates the individual TCP packets into TCP connections. KDDcup99 is a collection of five million connections records from seven weeks of network traffic. KDDcup99 is distributed in two versions, the full data set with 4898431 records and the 10 % subset with 494307 recordings.

The new version of KDDcup99 is NSL-KDD [5, 24] that considered like a revised version. The most advantages of NSL-KDD is focused on the record number of training set and test set that minimizing the level of difficulty. At NSL-KDD, they remove all redundant records in the training set and duplicate records in the test set whose make the data set has a

reasonable record number. Both data sets (KDDcup99 and NSL-KDD) have the same problems regarding the real network representation [25]. However, Both data sets have been still used by the most research like an experimental data set. While, KDDcup99 is derived from DRAPA98 and NSL-KDD is obtained by removing the redundant and duplicate instances of KDDcup99. We focus on KDDcup99 and NSL-KDD to describe the different features which contain 41 features (32 continuous and 9 nominal attributes) with target class. The 41 features have been characterized in four categories (Basic, content and traffic (time based traffic and host based traffic)). The description of all features of KDDcup99 and NSL-KDD are shown in **Table 2.**

Table 2. KDDcup99 / NSL-KDD description.

Num	Name	Type		Description
1	duration	Continuous	Category 1	Length of the connection.
2	Protocol_type	Nominal		Connection protocol.
3	service	Nominal		Destination service.
4	flag	Nominal		Status flag of the connection.
5	Src_bytes	Continuous		Bytes sent from source to destination
6	Dst_bytes	Continuous		Bytes sent from destination to source
7	land	Nominal		1 if is from/to the same host/port; 0 otherwise
8	Wrong_fragment	Continuous		Number of wrong fragment
9	urgent	Continuous		Number of urgent packets
10	hot	Continuous	Category 2	Number of hot indicators
11	Num_failed_logins	Continuous		Number of failed login in attempts
12	Logged_in	Nominal		1 if successfully logged in; 0 otherwise
13	Num_compromised	Continuous		Number of compromised conditions
14	Root_shell	Nominal		1 if root shell is obtained; 0 otherwise
15	Su_attempted	Nominal		1 if su root command attempted; 0 otherwise
16	Num_root	Continuous		Number of root accesses
17	Num_file_creations	Continuous		Number of file creation operations
18	Num_shells	Continuous		Number of shell prompts
19	Num_access_files	Continuous		Number of operations on access control files
20	Num_outbound_cmds	Continuous		Number of outbound commands in an ftp session
21	Is_hot_login	Nominal		1 if the login belongs to the hot list; 0 otherwise
22	Is_guest_login	Nominal		1 if the login is a guest login; 0 otherwise
23	count	Continuous	Category 3	Number of connections to the same host as the current connection in the past two seconds
24	Srv_count	Continuous		Number of connections to the same service as the current connection in the past two seconds
25	Serror_rate	Continuous		% of connections that have SYN errors (same-host connections)
26	Srv_serror_rate	Continuous		% of connections that have SYN errors (same-service connections)
27	Rerror_rate	Continuous		% of connections that have REJ errors (same-host connections)
28	Srv_rerror_rate	Continuous		% of connections that have REJ errors (same-service connections)
29	Same_srv_rate	Continuous		% of connections to the same service (same service connections)
30	Diff_srv_rate	Continuous		% of connections to different services
31	Srv_diff_host_rate	Continuous		% of connections to different hosts (same-service connections)
32	dst host count	Continuous	Category 4	% Count of connections having the same destination host

33	Dst_host_srv_count	Continuous		% Count of connections having the same destination host and using the same service
34	Dst_host_same_srv_rate	Continuous		% of connections having the same destination host and using the same service
35	Dst_host_diff_srv_rate	Continuous		% of different services on the current host
36	Dst_host_same_src_port_rate	Continuous		% of connections to the current host having the same port
37	Dst_host_srv_diff_host_rate	Continuous		% of connections to the same service coming from different hosts
38	Dst_host_serror_rate	Continuous		% of connections to the current host that have an SO error
39	Dst_host_srv_serror_rate	Continuous		% of connections to the current host and specified service that have an SO error
40	Dst_host_rerror_rate	Continuous		% of connections to the current host that have an RST error
41	Dst_host_srv_rerror_rate	Continuous		% of connections to the current host and specified service that have an RST error

Each instance of KDDcup99 and NSL-KDD are classified by normal or attacks connections. KDDcup99 has 24 types of attacks that have been categorized into 4 classes with normal class, namely: DOS (Denied of Service), Probe, U2R (User to Root), and R2L (Romote to Local). These five classes define the type of connection in each instance of KDDcup99. **Table 3** gives the statistical detail about the 5 classes in KDDcup99.

Table 3. KDDcup99 detail.

	Normal	**DOS**	**Probe**	**R2L**	**U2R**	**Total**
Whole KDD	972780	3883370	41102	1126	52	4898430
10% KDDcup99 data set	97564	391458	4107	1126	52	494307

Preprocessing step is a very important to prepare the dataset for experimentation before any study or model building. It is performed to eliminate all problems concerning size, incomplete information, and duplication record. For that, different techniques have been integrated using discretization, discrimination, reduction and normalization techniques to prepare the dataset for training and test steps.

4.2 Performance Evaluation

IDS performances are measured by an evaluation metric. According to the confusion matrix (**Table 4**), we illustrate the most performance measures are used to evaluate the effectiveness of any IDS.

Table 4. Confusion Matrix.

		Predicale class	
		Normal	**Attacks**
Actual class	Normal	True Positive (TP)	False Negative (TN)
	Attacks	False Positive (TP)	True Negative (TN)

We define seven performance evaluation as follows:
- Error Rate (ER) = (FN+FP) / (TP+TN+FN+FP).
- Accuracy Rate (AR) = (TN+TP) / (TP+TN+FN+FP).
- Detection Rate (DR) = Recall = TP / (TP+FN).
- False Positive Rate (FPR) = FP / (FP+TN).
- Precision = (TP) / (TP+FP).
- F-measure = (β^2+1) (Precision.Recall) / (β^2 .Precision + Recall); where β =1.

- Time Complexity = Time taken by an algorithm to complete its tasks (for selecting the subset of features).

5. Taxonomy of Feature Selection Algorithms

In this section, we propose a new classification taxonomy for feature selection algorithms. In this taxonomy, we present the characteristics of each algorithm depending on its selection technique have been used, selection mechanism, subset solution single/multi-solution, dataset, selection approach, Mono or multi-objective aspects, and the classifiers for evaluating performances. **Fig. 3** illustrates the global taxonomy of feature selection algorithms.

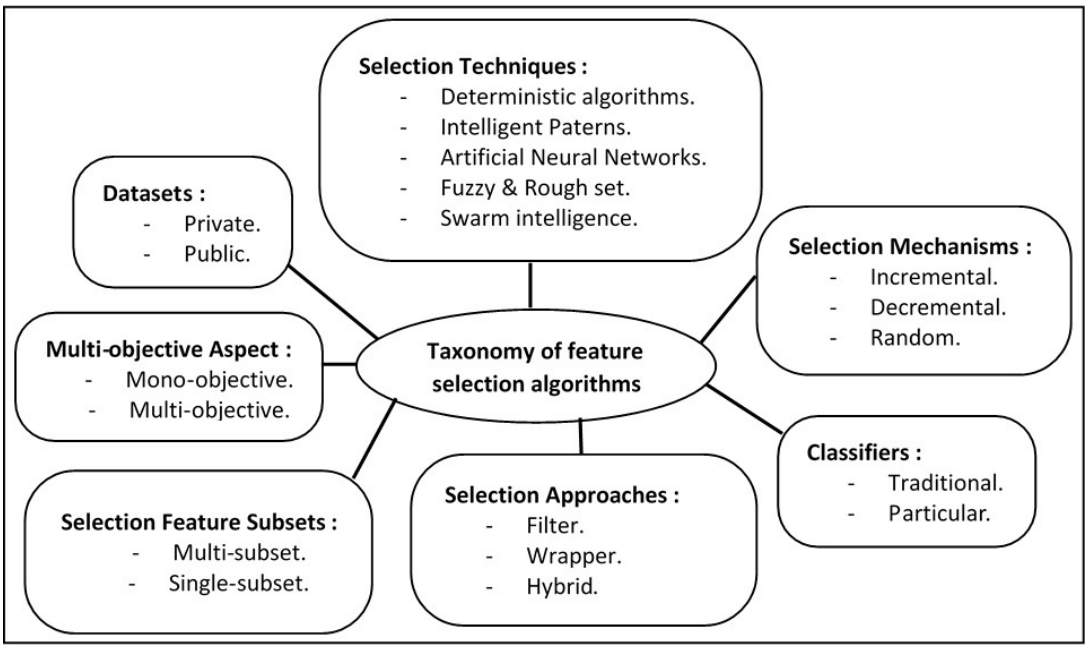

Fig. 3. Taxonomy of feature selection algorithms.

We introduce the well-known algorithms have been developed into feature selection for intrusion detection depending to this taxonomy. We classify the algorithms into five approaches according to the techniques have been integrated with them which are: Deterministic Algorithms, Intelligent Patterns, Artificial Neural Networks, Fuzzy & Rough Set and Swarm Intelligent. In each method, we define their techniques that are used with the results have been earned. Regading the results, we add a table of results that specifies the different number of subset(s) are selected, number of feature in subset(s), and accuracy rate(Mean & Max). We specify the selection approach of algorithms between filter, wrapper or hybrid. Feature selection algorithms which used filter approach has lower time complexity than the wrapper approach which is considered higher, because a filter is based on distance, information, dependency, and consistency measures instead of the wrapper which is based on classifiers error rate. Furthermore, we integrate the aspect of single and multi-solution in this classification which means the algorithm has one feature subset like a solution or multi-subset. Another aspect is integrated in these classifications which is mono or multi-objective approaches that have been used in the algorithms. On the other hand, the algorithm uses or not

the Trade-off (Pareto set) in their process of selection. In each section of our classification, we represent traditional classifier algorithms like DT, SVM, KNN, MLP, and BN which are used by Evaluation or validation steps to confirm the feature subset(s) performance. Furthermore, fewer of algorithms develop their particular classifiers to ensure the evaluation of feature subset(s).

5.1 Deterministic Algorithms

In this section, we present the algorithms that have been based on statistical, probabilistic, and similarity measures to select the best feature without redundancy and irrelevance. Among these measures, we cite Mutual Information (MI), Entropy (E), Correlation Coefficient (CC), Chi-Squared, One-R, Relief-F, and Gain Ratio,..., etc. The strategy has been supported in these algorithms is either incremental or decremental mechanism. Characteristics and results research of algorithms are presented in **Table 5** and **Table 6**.

Table 5. Deterministic feature selection algorithms.

Algorithms	Techniques	Mechanism	Single or Multi-solution	Dataset	Approach	Description
[31]	Mutual Information	Incremental	Multi	KDDcup99	Filter	Dependency and correlation analysis
[27]	Mutual Information	Incremental	Multi	KDDcup99	Filter	Using Least Square SVM classier
[36]	Correlation and consistency based FS with INTERACT algorithm	Incremental	Multi	KDDcup99	Filter	Combination between multi techniques. (Discretizer, filters and classifiers)
[37]	Least Square Regression, Maximal Information compression index, and Correlation Coefficient.	Incremental	Multi	KDDcup99	Filter	Comparison study between feature ranking techniques.
[38]	Pearson correlation coefficient	Incremental	Single	NSL-KDD	Filter	Using Correlation between features, then Correlation between selected features and classes.
[39]	Generic Feature Selection (GFS)	Incremental	Multi	KDDcup99	Filter	Using multi SVM classifier.
[26]	Visualized feature generation	Random	Multi	KDDcup99	Filter	Generation technique.
[40]	Information Gain Ratio	Incremental	Single	KDDcup99	Filter	Using SVM classifier.
[18]	Mutual Information and Binary Gravitational Search Algorithm (BGSA) with SVM.	Random	Single	NSL-KDD	Hybrid	MI integrated into BGSA with SVM classifier.
[41]	Chi-square and multi class SVM	Random	Single	NSL-KDD	Hybrid	Using multi-class SVM classifier
[42]	Chi-square and modified BN.	Decremental	Single	NSL-KDD	Hybrid	Using LDA to remove noisy attributes.
[43]	Correlation feature selection	Incremental	Single	NSL-KDD	Filter	Using BN classifier
[44]	Chi-square, One-R, Relief-F, Information Gain, Gain Ratio, and Symmetrical Uncertainty.	Incremental	Single	NSL-KDD	Filter	Comparison study between feature ranking techniques and different combination of classifiers. Feature subset not mentioned.

Table 6. Results of deterministic feature selection algorithms.

Algorithms	Number of subsets	Number of feature in the subset	Mean	Max
[31]	4	10, 10, 9, and 9	77.6	82.99
[27]	10	6, 15, 13,7,8,36,10,4(R2L),10, and 3(U2R)	96.27	97.77
[36]	9	6, 6, 7, 7, 6, 7, 7, 16, and 7	77.02	94.86
[37]	3	10, 20, and 30	81.83	98.14
[38]	1	17	/	99.1
[39]	6	13, 13, 15, 15, 20, and 29	99.4	99.94
[26]	2	4,16	93.73	94.35
[40]	1	10	/	93.34
[18]	1	5	/	88.36
[41]	1	31	/	98
[42]	1	22	/	96.8
[43]	1	12	/	65.43(U2R)
[44]	1	(not montioned)	/	/

In this section, the most researches support incremental mechanism with filter approach. According to the measure of selection have been used which are specified on ranking measure, algorithms of (Sec. 5.1) are obligated to follow the incremental mechanism with one way to arrive to the best features. They select the first feature that achieves a better criteria value and depending this feature and evaluation measure, they select the next feature until they get the final set which represents the best feature subset. Measures have been used in this section are based on ranking measurements, but, they have not prevented to achieve a good result.

5.2 Intelligent Patterns

In this section, we present different algorithms, which are based on Artificial Intelligence (AI) techniques. We focus on SVM, DT, BN, k-means, Cuttlefish, Immune Artificial System (IAS) and evolutionary algorithm which is specified on Genetic Algorithms (GA). **Table 7** and **Table 8** show the algorithms of these sections with the results that have been obtained.
Most of these researches are considered like a wrapper or hybrid approaches. On the other hand, they have been merged between techniques for extracting a new technique of selection for example SVM and DT, K-means and SVM. The strategy has been followed by these algorithms are based on random selection. In these researches, they use reduction techniques with intelligent algorithms to achieve the best features at the minimum time. Among reduction techniques are used with feature selection approaches in this section are: PCA (Principal Component Analysis), LDA (Linear Discriminant Analysis), ICA (Independent Component Analysis) and GPC (Genetic Principal Component).

Table 7. Intelligent patterns feature selection algorithms.

Algorithms	Techniques	Mechanism	Single or Multi-solution	Dataset	Approach	Description
[2]	Genetic and fuzzy rule **(Multi-objective).**	Random	Single	KDDcup99	Wrapper	Using multi-objective technique.
[45]	DT (CART), SVM-wrapper, Markov-blanket, Generic Feature Selection (GFS).	Random	Multi	KDDcup99	Hybrid	Comparison study between different wrapper methods and GFS.
[6]	SVM, DT and Simulated Annealing	Random	Single	KDDcup99	Wrapper	Hybrid approach
[46]	SVM and GPC (Genetic Principal component).	Random	Multi	KDDcup99	Hybrid	Using GPC and PCA for reducing the dimension.
[47]	Hybrid Bat algorithm and SVM.	Random	Single	NSL-KDD	Hybrid	Hybrid approach compared with PSO-SVM.

[48]	Hierarchical clustering method, Mutual information and DT.	Random	Multi	KDDcup99	Hybrid	Agglomerative hierarchical clustering with DT and Mutual information.
[49]	Artificial Immune System	Random	Single	KDDcup99	Wrapper	Compared with ANN.
[50]	K-means clustering algorithm and SVM	Random	Multi	KDDcup99	Hybrid	Using radial basis kernel function (RBF) for SVM as classification module. The selected features are different for each attack class.
[28]	K-means clustering algorithm	Random	Multi	NSL-KDD	Wrapper	Using MLP classifier
[51]	Consistency based feature selection , SVM, and LPBoost	Random	Single	NSL-KDD	Hybrid	Fusion model.
[52]	Hypergraph-Genetic algorithm and SVM. **(Multi-objective)**	Random	Single	NSL-KDD	Hybrid	Using a weighted objective function (trade-off) between the max detection rate and min false alarm rate.
[53]	Vote algorithm with Information Gain	Random	Single	NSL-KDD	Hybrid	Estimate the intrusion scope threshold degree. Using different classifiers: DT, Meta Pagging, RandomTree, REPTree, AdaBoostM1, DecisionStump, and BN.
[54]	Genetic algorithm and logistic regression	Random	Multi	KDDcup99	Wrapper	Using different DT like classifiers,

Table 8. Results of Intelligent patterns feature selection algorithms.

Algorithms	Number of subsets	Number of feature in the subset	Mean	Max
[2]	1	25	/	92.76
[45]	5	17, 18, 17, 12, 4, and 5	98.22	99.6
[6]	1	23	/	99.96
[46]	2	10 and 12	99.95	99.96
[47]	1	23	/	99.28
[48]	7	8, 10, 9, 11, 13, 12, and 14	93.35	93.8
[49]	1	21	/	99.1
[50]	5	41, 30, 26, 29, and 35	91.02	/
[28]	20	Between 16 to 26	96.93	99.73
[51]	1	10	/	96.2
[52]	1	35	/	96.72
[53]	1	8	/	99.81
[54]	8	18, 15, 20, 17, 16, 18, 22, and 18	99.34	99.5

5.3 Artificial Neural Networks

Artificial Neural Networks (ANN) [15, 39, 55] are an interesting technique which is inspired from the neurons of the human brain. It is an interconnecting neurons that each neural represents a processor unit. These collections of processor units have the ability of learning to solve problems. There are different types of ANN that are classified into different categories according to Supervised or Unsupervised learning, and Feed-forward or Recurrent architecture. Different research works have been proposed on feature selection for IDS which integrate ANN into their solutions. **Table 9** and **Table 10** represent the different algorithms which are based on ANN to solve the problem of feature selection for IDS.

Table 9. ANN feature selection algorithms.

Algorithms	Techniques	Mechanism	Single or Multi-solution	Dataset	Approach	Description
[56]	Hybrid flexible neural tree	Random	Single	DRAPA98	Wrapper	Using an evolutionary algorithm and parameters by PSO. For each class has its feature subset.
[55]	Back-propagation neural network.	Random	Single	KDDcup99	Wrapper	Using ICA (Independent Component Analysis) to eliminate insignificant and/or useless inputs.
[57]	Back-propagation neural network and genetic algorithm.	Random	Single	KDDcup99	Wrapper	Multi class classification process
[15]	Hierarchical self-organizing maps. **(Multi-objective)**	Random	Multi	KDDcup99	Wrapper	Multi-objective approach.
[58]	Hybridization of Neural Network and K-Means Clustering.	Random	Single	NSL-KDD	Hybrid	Using PCA to reduce the computational complexity.
[59]	Artificial neural network	Incremental	Single	KDDcup99	Hybrid	Using information gain and correlation.

Table 8. Results of ANN feature selection algorithms.

Algorithms	Number of subsets	Number of feature in the subset	Mean	Max
[56]	5	4, 13, 12, 8, and 10	99.02	99.75
[55]	1	8	/	99.5
[57]	23 (for each attack its subset)	Between 10 to 17	58.39	86
[15]	5	22, 29, 25, 25, and 29	98.13	99.12
[58]	1	23	/	97.63
[59]	1	25	/	97.91

ANN is integrated into the process of feature selection, such as a classifier in validation step, but different works have been used like an algorithm of feature selection. Back-propagation Neural Network and Self-Organization Maps are the most type of ANN are used in FS area. According to **Table 10**, we confirm the efficiency of ANN which their accuracy rate is between 99 % and 97.9 % in each research. ANN is used with other techniques like GA and K-means, for that, the most algorithms of ANN use random mechanism with wrapper and hybrid approaches.

5.4 Fuzzy & Rough Set

Fuzzy Logic (FL) [60, 61] and Rough Set (RS) [62, 63] are two techniques of artificial intelligence that are used to solve the problems for uncertain, inconsistent and incomplete datasets. Fuzzy logic is an extension of the classical logic and set theory. It has the ability to define decision rules using vague concepts to solve the different real problems. Further, Rough set is a formal framework which is useful for knowledge discovered and analyze data for NP-Hard problems. FS is among a field that have been interested to integrate Fuzzy Logic and Rough Set. **Table 11** and **Table 12** illustrate the recent works that have been developed into feature selection for IDS using FL and RS.

Table 11. Fuzzy & Rough set feature selection algorithms.

Algorithms	Techniques	Mechanism	Single or Multi-solution	Dataset	Approach	Description
[62]	Rough set and fuzzy	Random	Single	KDDcup99	Wrapper	Combination approach.
[64]	Multicriterion fuzzy classification method.	Random	Single	KDDcup99	Wrapper	Combined with a greedy attribute selection.
[65]	Fuzzy control language	Random	Multi	KDDcup99	Wrapper	Integrating Entropy-based feature selection.
[63]	Rough set and NetFlow/IPFIX	Random	Multi	KDDcup99	Wrapper	Using KNN classifier.
[66]	Rough set and Hypergraph Technique	Random	Single	KDDcup99	Filter	Using minimal transversal and vertex linearity for the identification of the optimal feature subset.

Table 12. Results of fuzzy & rough set feature selection algorithms.

Algorithms	Number of subsets	Number of feature in the subset	Mean	Max
[62]	4 (for each attacks its subset)	5, 5, 4, and 4	94.15	99.75
[64]	1	11	/	99.96
[65]	3	14, 17, and 21	99.24	99.66
[63]	6	11, 16, 16, 16, 16, and 17	90.33	98
[66]	1	23	/	96.63

FL and Rough Set have been mostly integrated into feature selection for obtaining the minimal feature from all possible feature set. Almost research of FL and RS are associated under the wrapper approach and random mechanism of selection. We remarked that the research of the FL and RS for feature selection is merged with other techniques like a fusion for more precision or like a classification algorithm to evaluate their effectiveness.

5.5 Swarm Intelligence

In this section, we present Swarm Intelligence (SI) technique [1, 32], which is an artificial intelligence technique. It is inspired from the emergent behavior of social insects and swarms. SI is based on individuals that are interacted between them and environments to optimize objectives by a collaborative search. It is used to solve the complex problems by applying a sophisticated collective intelligence. Each individual represents a potential solution and all of them present the population of solutions. Two famous techniques of SI are presented in this section, which are: Ant Colony Optimization (ACO) and Particle Swarm optimization (PSO). The ACO and PSO have been used to solve the problem of feature selection for IDS.

5.5.1 Ant Colony Optimization

ACO [1, 32, 67] is an inspiration from the real behavior of ants, which want to find the shortest path between the colony and food sources. Each individual of the population is presented by ants with its pheromones. ACO is based on their pheromone and ants to find the optimal solution of search space. The ACO have been applied to solve the discrete optimization problems. Further, it is used in feature selection for IDS with interesting approach, but it is still limited. In this section, we present three improving works which are [67- 69]. **Table 13** and **Table 14** illustrate the different proposed approach of ant colony for feature selection and their results.

Table 13. ACO feature selection algorithms.

Algorithms	Techniques	Mechanism	Single or Multi-solution	Dataset	Approach	Description
[68]	Ant colony optimization	Random	Single	KDDcup99	Wrapper	Using SVM for detection.
[67]	Ant colony optimization, K-means and SVM	Decremental	Multi	KDDcup99	Wrapper	Combination between Techniques.
[69]	ACO and fuzzy entropy	Random	Single	Private	Wrapper	Combination approaches.

Table 14. Results of ACO feature selection algorithms.

Algorithms	Number of subsets	Number of feature in the subset	Mean	Max
[68]	1	32	/	97.76
[67]	4	10, 10, 10, and 19	96.78	98.62
[69]	1	13	/	99.69

5.5.1 Particle Swarm Optimization

PSO [32] is among techniques are used in feature selection for IDS. It is inspired on simulation of social behavior of birds flocking. PSO has been used to solve the global no linear optimization problem with constraints. PSO is based on the fitness, velocity, and position of each particle to get the optimal solution. In PSO, each partial solution (individual) is encoded by a vector. PSO has two versions, which are: discrete and continuous depending on the problem, data type and population. Based on the mechanisms that have been integrated into PSO, different researches have been proposed to search about the best feature subset(s) for intrusion detection system. **Table 15** and **Table 16** show different works have been based on PSO and their results.

Table 15. PSO feature selection algorithms.

Algorithms	Techniques	Mechanism	Single or Multi-solution	Dataset	Approach	Description
[70]	PSO and rough set.	Random	Single	KDDcup99	Wrapper	Rough-DPSO algorithm between RS and PSO
[71]	PSO. **(Multi-objective)**	Random	Single	KDDcup99	Wrapper	**Multi-objective approach.**
[72]	PSO and Random forest.	Random	Multi	KDDcup99	Wrapper	**Multi-objective approach.**
[16]	PSO and Genetic algorithm	Random	Multi	NSL-KDD	Hybrid	Using PCA.
[73]	Multi-objective PSO. **(Multi-objective)**	Random	Single	KDDcup99	Wrapper	Deal with Real time attacks
[74]	PSO with tree-based classifiers	Random	single	NSL-KDD	Wrapper	Using three types of Decision tree (CART, Random forest, and C4,5).
[75]	PSO and Bat algorithm	Random	Multi	NSL-KDD	Wrapper	Comparative study on FS based swarm intelligence. Using two versions of the Bat algorithm (BAL and BAE).

Table 16. Results of PSO feature selection algorithms.

Algorithms	Num of subsets	Number of feature in the subset	Mean	Max
[70]	1	6	93.40	95.35
[71]	1	6	/	94.15
[72]	9 for PROB attck	7, 13, 20, 15, 13, 30, 17, 14, and 3	85	100
[16]	2	8 and 10	98.8	99.4
[73]	1	11	/	98
[74]	3	11, 9, and 6	99.47	99.8
[75]	20	Between 13 to 22	93.63	97.17

We remarked that the ACO and PSO works have been integrated into wrapper with hybrid approaches. They use either incremental or random mechanism into their feature selection algorithms. ACO and PSO need an orientation techniques to guide their exploration of the search space. For that, ACO and PSO are combined with other techniques to orient their research into the search space. Deffirent classifiers have been used with ACO and PSO to calculate performnaces of each feature subset(s).

5. Conclusion

IDS is an important tool in any security infrastructure, which is used to protect a system against attacks. Further, it is suffer of computational complexity, response time, and storage requirements. FS is among preprocessing step, which searches to decrease the degree of these problems by reducing the number of features. Thus, FS selects the best feature subset(s), which avoid over-head classification problem. In this paper, we represented a survey of feature selection for intrusion detection systems. We explored the most contributions in applying FS to the problem of IDS by an overview of different works. A new taxonomy was proposed, which focused on the techniques of selection, mechanisms of selection, single or multi-solution of subset, dataset experimentation, approaches type, and mono-or multi-objective aspect. The different feature selection algorithms are classified into five classes depending on their techniques, which are used in each works. We presented their characteristics according to the new taxonomy, and we illustrated their results that were obtained by showing their number of subsets, number of features in the subset, and Accuracy Rate (Mean, Max)). We considered this survey like a map to understand the current state and future trends challenges.

References

[1] Wu. S.X., Banzhaf. W, "The use of computational intelligence in intrusion detection systems: A review," *Applied soft computing*, Vol. 10, No. (1), PP. 1-35, 2010. Article (CrossRef Link)

[2] Tsang. C.-H, Kwong. S, Wang. H, "Genetic-fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection," *Pattern Recognition*, Vol. 40, No. (9), PP. 2373-2391, 2007. Article (CrossRef Link)

[3] Liao. H.-J., Lin. C.-H.R., Lin, Y.-C., Tung, K.-Y. "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, Vol. 36, No. (1), PP. 16-24, 2013. Article (CrossRef Link)

[4] Ganapathy, S., Kulothungan, K., Muthurajkumar, S., Vijayalakshmi, M., Yogesh, P., Kannan. A, "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey," *EURASIP Journal on Wireless Communications and Networking*, Vol. 2013, No. (1), PP. 271, 2013. Article (CrossRef Link)

[5] Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A, "A detailed analysis of the KDD CUP 99 data set," *In: Computational Intelligence for Security and Defense Applications*, CISDA 2009. IEEE Symposium on 2009, pp. 1-6. IEEE, 2009. Article (CrossRef Link)

[6] Lin, S.-W., Ying, K.-C., Lee, C.-Y., Lee, Z.-J, "An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection," *Applied Soft Computing*, Vol. 12, No. (10), PP. 3285-3290, 2012. Article (CrossRef Link)

[7] Kim, G., Lee, S., Kim. S, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Systems with Applications*, Vol. 41, No. (4), PP. 1690-1700, 2014. Article (CrossRef Link)

[8] Goeschel, K, "Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis," in *Proc. of SoutheastCon, 2016*, pp. 1-6. IEEE, 2016. Article (CrossRef Link)
[9] Aburomman, A.A., Reaz, M.B.I, "A novel SVM-kNN-PSO ensemble method for intrusion detection system," *Applied Soft Computing*, Vol. 38, PP. 360-372, 2016. Article (CrossRef Link)
[10] Jaiswal, S., Saxena, K., Mishra, A., Sahu, S.K, "A KNN-ACO approach for intrusion detection using KDDCUP'99 dataset," in *Proc. of Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on 2016*, pp. 628-633. IEEE
Article (CrossRef Link)
[11] Dhopte, S., Chaudhari, M, "Genetic Algorithm for Intrusion Detection System," *IJRIT International Journal of Research in Information Technology*, Vol. 2, No. (3), PP. 503-509, 2014.
Article (CrossRef Link)
[12] Sengupta, N., Sen, J., Sil, J., Saha. M, "Designing of on line intrusion detection system using rough set theory and Q-learning algorithm," *Neurocomputing*, Vol. 111, PP. 161-168, 2013.
Article (CrossRef Link)
[13] Raman, M.G., Somu, N., Kirthivasan, K., Sriram, V.S, "A hypergraph and arithmetic residue-based probabilistic neural network for classification in intrusion detection systems," *Neural Networks*, Vol. 92, PP. 89-97, 2017. Article (CrossRef Link)
[14] Subba, B., Biswas, S., Karmakar. S, "A Neural Network based system for Intrusion Detection and attack classification," in *Proc. of Communication (NCC), 2016 Twenty Second National Conference on 2016*, pp. 1-6. IEEE. Article (CrossRef Link)
[15] De la Hoz, E., de la Hoz, E., Ortiz, A., Ortega, J., Martínez-Álvarez. A, "Feature selection by multi-objective optimisation: Application to network anomaly detection by hierarchical self-organising maps," *Knowledge-Based Systems*, Vol. 71, PP. 322-338, 2014.
Article (CrossRef Link)
[16] Ahmad. I, "Feature selection using particle swarm optimization in intrusion detection," *International Journal of Distributed Sensor Networks*, Vol. 11, No. (10), PP. 806954, 2015.
Article (CrossRef Link)
[17] Liu, H., Yu. L,"Toward integrating feature selection algorithms for classification and clustering," *IEEE Transactions on knowledge and data engineering*, Vol. 17, No. (4), PP. 491-502, 2005.
Article (CrossRef Link)
[18] Bostani, H., Sheikhan. M, "Hybrid of binary gravitational search algorithm and mutual information for feature selection in intrusion detection systems," *Soft computing*, Vol. 21, No. (9), PP. 2307-2324, 2017. Article (CrossRef Link)
[19] Kolias, C., Kambourakis, G., Maragoudakis. M, "Swarm intelligence in intrusion detection: A survey," *computers & security*, Vol. 30, No. (8), PP. 625-642, 2011. Article (CrossRef Link)
[20] Zhou, C.V., Leckie, C., Karunasekera. S, "A survey of coordinated attacks and collaborative intrusion detection," *Computers & Security*, Vol. 29, No. (1), PP. 124-140, 2010.
Article (CrossRef Link)
[21] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., Vázquez. E, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security*, Vol. 28, No. (1-2), PP. 18-28, 2009. Article (CrossRef Link)
[22] *The drapa dataset*. 1998. Article (CrossRef Link)
[23] *The kdd cup 1999 dataset*. 1999. Article (CrossRef Link)
[24] *The nsl-kdd dataset*. 2009. Article (CrossRef Link)
[25] McHugh. J, "Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory," *ACM Transactions on Information and System Security (TISSEC)*, Vol. 3, No. (4), PP. 262-294, 2000.
Article (CrossRef Link)
[26] Luo, B., Xia. J, "A novel intrusion detection system based on feature generation with visualization strategy," *Expert Systems with Applications*, Vol. 41, No. (9), PP. 4139-4147, 2014.
Article (CrossRef Link)

[27] Amiri, F., Yousefi, M.R., Lucas, C., Shakery, A., Yazdani. N,"Mutual information-based feature selection for intrusion detection systems," *Journal of Network and Computer Applications*, Vol. 34, No. (4), PP. 1184-1199, 2011. Article (CrossRef Link)
[28] Kang, S.-H., Kim, K.J, "A feature selection approach to find optimal feature subsets for the network intrusion detection system," *Cluster Computing*, Vol. 19, No. (1), PP. 325-333, 2016. Article (CrossRef Link)
[29] Qin, Z., Feng, C., Wang, Y., Li. F, "Conditional Mutual Information-Based Feature Selection Analyzing for Synergy and Redundancy," *Etri Journal*, Vol. 33, No. (2), PP. 210-218, 2011. Article (CrossRef Link)
[30] Xue, B., Cervante, L., Shang, L., Browne, W.N., Zhang. M, "A multi-objective particle swarm optimisation for filter-based feature selection in classification problems," *Connection Science*, Vol. 24, No. (2-3), PP. 91-116, 2012. Article (CrossRef Link)
[31] Qu, G., Hariri, S., Yousif. M, "A new dependency and correlation analysis for features," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 17, No. (9), PP. 1199-1207, 2005. Article (CrossRef Link)
[32] Xue .B, "Particle swarm optimisation for feature selection in classification," *A thesis submitted to the Victoria University of Wellington in fulfilment of the requirements for the degree of Doctor of Philosophy in Computer Science*. Victoria University of Wellington, 2014. Article (CrossRef Link)
[33] Chen, Y., Li, Y., Cheng, X.-Q., Guo. L, "Survey and taxonomy of feature selection algorithms in intrusion detection system," in *Proc. of International Conference on Information Security and Cryptology 2006*, pp. 153-167. Springer, 2006. Article (CrossRef Link)
[34] Salappa, A., Doumpos, M., Zopounidis. C, "Feature selection algorithms in classification problems: An experimental evaluation," *Optimisation Methods and Software*, Vol. 22, No. (1), PP. 199-212, 2007. Article (CrossRef Link)
[35] Xue, B., Qin, A.K., Zhang. M, "An archive based particle swarm optimisation for feature selection in classification," in *Proc. of Evolutionary Computation (CEC), 2014 IEEE Congress on 2014*, pp. 3119-3126. IEEE, 2014. Article (CrossRef Link)
[36] Bolon-Canedo, V., Sanchez-Marono, N., Alonso-Betanzos. A, "Feature selection and classification in multiple class datasets: An application to KDD Cup 99 dataset," *Expert Systems with Applications*, Vol. 38, No. (5), PP. 5947-5957, 2011. Article (CrossRef Link)
[37] Parsazad, S., Saboori, E., Allahyar. A, "Fast feature reduction in intrusion detection datasets," in *Proc. of MIPRO, 2012 Proceedings of the 35th International Convention 2012*, pp. 1023-1029. IEEE, 2012. Article (CrossRef Link)
[38] Eid, H.F., Hassanien, A.E., Kim, T.-h., Banerjee. S, "Linear correlation-based feature selection for network intrusion detection model," in *Proc. of Advances in Security of Information and Communication Networks*. pp. 240-248. Springer, 2013. Article (CrossRef Link)
[39] Le Thi, H.A., Le, A.V., Vo, X.T., Zidna. A, "A filter based feature selection approach in msvm using dca and its application in network intrusion detection," in Proc. of *Asian Conference on Intelligent Information and Database Systems 2014*, pp. 403-413. Springer, 2014. Article (CrossRef Link)
[40] Balakrishnan, S., Venkatalakshmi, K., Kannan. A, "Intrusion detection system using Feature selection and Classification technique," *International Journal of Computer Science and Application (IJCSA)* Vol. 3, No. (4), November 2014, 2014. Article (CrossRef Link)
[41] Thaseen, I.S., Kumar, C.A, " Intrusion detection model using fusion of chi-square feature selection and multi class SVM," *Journal of King Saud University-Computer and Information Sciences*, Vol. 29, No. (4), PP. 462-472, 2017. Article (CrossRef Link)
[42] Thaseen, I.S., Kumar, C.A, "Intrusion Detection Model Using Chi Square Feature Selection and Modified Naïve Bayes Classifier," in *Proc. of Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC–16') 2016*, pp. 81-91. Springer. Article (CrossRef Link)

[43] Bahl, S., Sharma, S.K, "A minimal subset of features using correlation feature selection model for intrusion detection system," in *Proc. of Proceedings of the Second International Conference on Computer and Communication Technologies 2016*, pp. 337-346. Springer, 2016. Article (CrossRef Link)
[44] Panigrahi, A., Patra, M.R, "Performance Evaluation of Rule Learning Classifiers in Anomaly Based Intrusion Detection," in *Proc. of Computational Intelligence in Data Mining*. Vol 2. pp. 97-108. Springer, 2016. Article (CrossRef Link)
[45] Nguyen, H.T., Petrović, S., Franke. K, "A comparison of feature-selection methods for intrusion detection," in *Proc. of International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security 2010*, pp. 242-255. Springer, 2010. Article (CrossRef Link)
[46] Ahmad, I., Hussain, M., Alghamdi, A., Alelaiwi. A, "Enhancing SVM performance in intrusion detection using optimal feature subset selection based on genetic principal components," *Neural computing and applications*, Vol. 24, No. (7-8), PP. 1671-1682, 2014. Article (CrossRef Link)
[47] Laamari, M.A., Kamel. N, "A hybrid bat based feature selection approach for intrusion detection," in *Proc. of Bio-Inspired Computing-Theories and Applications*. pp. 230-238. Springer, 2014. Article (CrossRef Link)
[48] Song, J., Zhu, Z., Price. C, "Feature grouping for intrusion detection system based on hierarchical clustering," in *Proc. of International Conference on Availability, Reliability, and Security 2014*, pp. 270-280. Springer, 2014. Article (CrossRef Link)
[49] Yin, C., Ma, L., Feng. L, "Towards accurate intrusion detection based on improved clonal selection algorithm," *Multimedia Tools and Applications*, Vol. 76, No. (19), PP. 19397-19410, 2017. Article (CrossRef Link)
[50] Ravale, U., Marathe, N., Padiya. P, "Feature selection based hybrid anomaly intrusion detection system using K means and RBF kernel function," *Procedia Computer Science*, Vol. 45, PP. 428-435, 2015. Article (CrossRef Link)
[51] Thaseen, I.S., Kumar, C.A, "An integrated intrusion detection model using consistency based feature selection and LPBoost," in *Proc. of Green Engineering and Technologies (IC-GET), 2016 Online International Conference on 2016*, pp. 1-6. IEEE, 2016. Article (CrossRef Link)
[52] Raman, M.G., Somu, N., Kirthivasan, K., Liscano, R., Sriram, V.S, "An efficient intrusion detection system based on hypergraph-Genetic algorithm for parameter optimization and feature selection in support vector machine," *Knowledge-Based Systems*, Vol. 134, PP. 1-12, 2017. Article (CrossRef Link)
[53] Aljawarneh, S., Aldwairi, M., Yassein, M.B, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *Journal of Computational Science*, 2017. Article (CrossRef Link)
[54] Khammassi, C., Krichen. S, "A GA-LR wrapper approach for feature selection in network intrusion detection," *Computers & Security*, Vol. 70, PP. 255-277, 2017. Article (CrossRef Link)
[55] Sun, N.-Q., Li. Y, "Intrusion detection based on back-propagation neural network and feature selection mechanism," in *Proc. of International Conference on Future Generation Information Technology 2009*, pp. 151-159. Springer, 2009. Article (CrossRef Link)
[56] Chen, Y., Abraham, A., Yang. J, "Feature selection and intrusion detection using hybrid flexible neural tree," in *Proc. of International Symposium on Neural Networks 2005*, pp. 439-444. Springer, 2009. Article (CrossRef Link)
[57] Subbulakshmi, T., Ramamoorthi, A., Shalinie, S.M, "Feature Selection and Classification of Intrusions Using Genetic Algorithm and Neural Networks," *Recent Trends in Networks and Communications*. pp. 223-234. Springer, 2010. Article (CrossRef Link)
[58] Biswas, N.A., Shah, F.M., Tammi, W.M., Chakraborty. S, "FP-ANK: An improvised intrusion detection system with hybridization of neural network and K-means clustering over feature selection by PCA," in *Proc. of Computer and Information Technology (ICCIT), 2015 18th International Conference on 2015*, pp. 317-322. IEEE, 2015. Article (CrossRef Link)
[59] Manzoor, I., Kumar. N, "A feature reduced intrusion detection system using ANN classifier," *Expert Systems with Applications*, Vol. 88, PP. 249-257, 2017. Article (CrossRef Link)

[60] Reardon, B.J, "Fuzzy logic versus niched Pareto multiobjective genetic algorithm optimization," *Modelling and Simulation in Materials Science and Engineering*, Vol. 6, No. (6), PP. 717, 1998. Article (CrossRef Link)
[61] El Ougli. A, "Intégration des techniques floues à la synthèse de contrôleurs adaptatifs," 2009. Article (CrossRef Link)
[62] Muthurajkumar, S., Kulothungan, K., Vijayalakshmi, M., Jaisankar, N., Kannan. A, "A Rough Set based feature Selection Algorithm for Effective Intrusion Detection in Cloud Mode," in *Proc. of Proceedings of the international conference on advances in communication, network, and computing 2013*, pp. 8-13, 2013. Article (CrossRef Link)
[63] Beer, F., Bühler. U, "Feature selection for flow-based intrusion detection using Rough Set Theory," in *Proc. of Networking, Sensing and Control (ICNSC), 2017 IEEE 14th International Conference on 2017*, pp. 617-624. IEEE, 2017. Article (CrossRef Link)
[64] El-Alfy, E.-S.M., Al-Obeidat, F.N, "A multicriterion fuzzy classification method with greedy attribute selection for anomaly-based intrusion detection," *Procedia Computer Science*, Vol. 34, PP. 55-62, 2014. Article (CrossRef Link)
[65] Ramakrishnan, S., Devaraju. S, "Attack's feature selection-based network intrusion detection systzm using fuzzy control language," *International Journal of Fuzzy Systems*, Vol. 19, No. (2), PP. 316-328, 2017. Article (CrossRef Link)
[66] Raman, M.G., Kirthivasan, K., Sriram, V.S, "Development of Rough Set–Hypergraph Technique for Key Feature Identification in Intrusion Detection Systems," *Computers & Electrical Engineering*, Vol. 59, PP. 189-200, 2017. Article (CrossRef Link)
[67] Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., Dai. K, "An efficient intrusion detection system based on support vector machines and gradually feature removal method," *Expert Systems with Applications*, Vol. 39, No. (1), PP. 424-430, 2012. Article (CrossRef Link)
[68] Gao, H.-H., Yang, H.-H., Wang, X.-Y, "Ant colony optimization based network intrusion feature selection and detection," in *Proc. of Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference on 2005*, pp. 3871-3875. IEEE, 2005. Article (CrossRef Link)
[69] Varma, P.R.K., Kumari, V.V., Kumar, S.S, "Feature Selection Using Relative Fuzzy Entropy and Ant Colony Optimization Applied to Real-time Intrusion Detection System," *Procedia Computer Science*, Vol. 85, PP. 503-510, 2016. Article (CrossRef Link)
[70] Zainal, A., Maarof, M.A., Shamsuddin, S.M, "Feature selection using Rough-DPSO in anomaly intrusion detection," in *Proc. of International Conference on Computational Science and Its Applications 2007*, pp. 512-524. Springer. Article (CrossRef Link)
[71] Zhou, L.-H., Liu, Y.-H., Chen, G.-L, "A feature selection algorithm to intrusion detection based on cloud model and multi-objective particle swarm optimization," in *Proc. of Computational Intelligence and Design (ISCID), 2011 Fourth International Symposium on 2011*, pp. 182-185. IEEE, 2011. Article (CrossRef Link)
[72] Malik, A.J., Khan, F.A, "A Hybrid Technique Using Multi-objective Particle Swarm Optimization and Random Forests for PROBE Attacks Detection in a Network," in *Proc. of Systems, Man, and Cybernetics (SMC), 2013 IEEE International Conference on 2013*, pp. 2473-2478. IEEE, 2013. Article (CrossRef Link)
[73] Sujitha, B., Kavitha. V, "Layered Approach For Intrusion Detection Using Multiobjective Particle Swarm Optimization," *International Journal of Applied Engineering Research*, Vol. 10, No. (12), PP. 31999-32014, 2015. Article (CrossRef Link)
[74] Tama, B.A., Rhee, K.H, "A combination of PSO-based feature selection and tree-based classifiers ensemble for intrusion detection systems," in *Proc. of Advances in Computer Science and Ubiquitous Computing*. pp. 489-495. Springer, 2015. Article (CrossRef Link)
[75] Enache, A.-C., Sgârciu, V., Togan. M, "Comparative Study on Feature Selection Methods Rooted in Swarm Intelligence for Intrusion Detection," in *Proc. of Control Systems and Computer Science (CSCS), 2017 21st International Conference on 2017*, pp. 239-244. IEEE, 2017. Article (CrossRef Link)

[76] Wazid, M., Das, A.K, "A Secure Group-Based Blackhole Node Detection Scheme for Hierarchical Wireless Sensor Networks," *Wireless Personal Communications*, Vol. 94, No. (3), PP. 1165-1191, 2017. Article (CrossRef Link)
[77] Wazid, M., Das, A.K, "An efficient hybrid anomaly detection scheme using K-means clustering for wireless sensor networks," *Wireless Personal Communications*, Vol. 90, No. (4), PP. 1971-2000, 2016. Article (CrossRef Link)
[78] Wazid, M., Sharma, R., Katal, A., Goudar, R., Bhakuni, P., Tyagi. A, "Implementation and Embellishment of Prevention of Keylogger Spyware Attacks," in *Proc. of International Symposium on Security in Computing and Communication 2013*, pp. 262-271. Springer, 2013 Article (CrossRef Link)

SOFIANE Maza received his ENGINEER degree in Computer Science from University of Mohamed Boudiaf- M'Sila, Algeria in 2007. He received his MAGISTER degree in Computer Science from University of Mohamed Khider Biskra, Algeria in 2010. Currently, he is a PhD Student candidate in the Computer Science Department, University of Ferhat Abbas Setif-1, Setif 19000; Algeria. He is an assistant professor at University of Mohamed El Bachir El Ibrahimi Bordj Bou Arréridj 34000. His main research focuses on Artificial Intelligence and Security Networks.

Mohamed Touahria Appointed in 2014 as Professor in the Computer Science Department of Ferhat Abbas University in Setif, Algeria. For the last fifteen years, he has been in charge of computer science research teams in the field of artificial intelligence and knowledge engineering. He is the author of numerous publications and a member of international conference program committees. His fields of research are artificial intelligence, web applications and automatic translation of natural languages.