The Cuckoo Feature Filtration Method for Intrusion Detection (Cuckoo-ID)

Wafa Alsharafat
Al al-Bayt University, Jordan

***Abstract*—Intrusion Detection Systems (IDSs) play a crucial role in keeping online systems secure from attacks. However, these systems usually face the challenge of needing to handle and analyze a vast volume of data in order to achieve intrusion detection. Feature filtration is a solution that overcomes this challenge by focusing on the characteristic network features that play a significant role in enabling these systems to achieve high detection rates. This paper presents an intelligent cuckoo feature filtration method that is intended to prune away insignificant network features. Then, an IDS (the Cuckoo-ID) is designed in which an eXtended Classifier System (XCS) uses the filtered features for improving the rate of detection of network intrusions. Thus, the main objective of Cuckoo-ID is to maximize the detection rate (DR) and minimize the false alarm rate (FAR). Experiments were then run on the KDDcup'99 dataset to test the intrusion detection (ID) efficiency of the proposed system. The results showed that cuckoo filtration does profoundly raise the ID rate of the entire system. Finally, the DR and FAR of Cuckoo-ID were compared with those of intrusion detection methods that depend on network feature filtration.**

Keywords—Cuckoo algorithm; feature filtration; intrusion detection; XCS; detection rate

I. Introduction

More lights have been spotted recently than before on the networks because of the sensitivity of such an environment. The networks have a vast number of resources and information. Therefore, protective solutions against possible threats and vulnerabilities of mechanisms must be implemented.

Now, an Intrusion Detection System (IDS) is one of the popular mechanisms for protecting network resources against attacks [1]. James Anderson, in 1980, published the first study of IDSs for improving the security levels of networks [2]. The IDS has been defined by Teodoro [3] as being 'a security tool, like other measures such as antivirus software and firewalls proposed for security, to enable that security to become more powerful, in terms of protecting an information and communication system'. Therefore, intrusion detection (ID) aims at achieving intelligent control of the events occurring in a. Researchers in [1,4,5] have explained that the IDSs have two major taxonomies, depending on the source of the data to collect. These are:

- Host-based Intrusion Detection System (HIDS) which are targeted to collect information about activity in a specific host [5].
- Network-based Intrusion Detection System (NIDS) which collect information from the network [5].

Different Artificial Intelligence (AI) techniques including Deep Learning, Cuckoo Algorithm, Fuzzy Logic, Genetic Algorithm, and the Artificial Neural Network have been applied and enhanced to automatically detect possible intrusions [6, 7, 8]. Furthermore, different AI techniques have been adapted to identify the key and most relevant network features that guide and lead the IDS to achieve accurate detection as in Jamali and Jafarzadeh [9]; Lee, Park, and Lee [10]; Abd Eldayem [11]; and Alsharafat [12]. Within this context, feature filtration has the crucial advantage of overcoming the conflict between network features and attacks.

Bearing this in mind, this study was initiated to assess the potential for the Cuckoo Algorithm to serve as a feature filtration method that will reduce the number of the network features needed to detect intrusion; Determine the impact of feature filtration on ID and Compare the level of ID performance of the proposed feature filtration method (Cuckoo-ID) with those of other ID methods (both the ones involving feature filtration and those which do not).

In short, the key contributions of this work are enumerated as follows.

1) Summarize a set of interrelated works related to IDS and those involving feature filtration.

2) Propose a new feature filtration method for intrusion detection system based on Cuckoo Algorithm.

3) Implement an intrusion detection model that applied the Cuckoo algorithm for feature filtration.

4) Evaluate the performance of the proposed feature filtration method and compare the result with methods involving feature filtration and those which do not.

The remainder of this paper is organized as follows. Section 2 reviews related to previous works. Section 3 describes the benchmark dataset that is widely used in testing the levels of performance of IDSs. Section 4 clarifies the proposed method for improving ID. Section 5 discusses the evaluation of the performance of the proposed ID method. Lastly, Section 6 contains a discussion of the experimental results and concludes them.

II. Related Works

A review of the published literature reveals that different researchers have employed various AI techniques for ID [6 – 20]. These techniques include Artificial Neural Networks (ANNs), the Cuckoo Algorithm, Fuzzy Logic, metaheuristic algorithm, Random forest, cuttlefish algorithm, and the Genetic Algorithm (GA), besides other new trends to be implemented in detecting network attacks, especially in the environment of the Cloud, which is regarded by intruders as being a preferred target with regard to exploiting its weak points.

Some researchers keenly delved into a search for key factors that have a positive influence on DR. In this regard, the search was guided (in some studies) by the investigation of the effect of network feature filtration on the proposed IDS [6–20]. For feature filtration, Alsharafat in 2010 [12] has developed an ID model called ANN-XCS that proceeds in two phases. The first phase concerned about feature filtration by applying ANN. Then, the filtered features will be considered in the entire work of the second phase, which applied an Extended Classifier System (XCS) for the purpose of intrusion detection. For enhancement, XCS applies a set of modifications to GA for the breeding classifier pool. As a result, the DR of ANN-XCS was 98.01%, and the concomitant FAR was0.9%.

Alzboon, Alkhaldy, and Alsharafat [13] proposed an IDS in 2017 that was based on using the Cuckoo search method integrated with GA as a classifier generator within XCS. In addition, the network features were filtered in this system using Fuzzy Clustering by the Local Approximation Membership (FLAME) method, FLAME-XCS as an abbreviation, which reduced the number of network features to track from 41 to 20 features. As a result, the DR reached 99.9% while the FAR reached 0.005%, corresponding to an outstanding ID efficiency.

A Learning Automata Intrusion Detection System (LA-IDS) was developed in 2017 by Jamali and Jafarzadeh [9]. This model applies a seven-level hierarchical structure in which each level is responsible for processing one of the network features. By reducing the number of features to trace from 41 to 7, this system (LA-IDS) proved to have a DR of 98.9% and a FAR of 1.3%. In the same year, Lee, Park, and Lee [10] focused on feature selection, which represents the first phase of the proposed work, which aimed at constructing a subset of features using a sequential, forward-floating search (SFFS) instead of the method used by Jamali and Jafarzadeh [9]. The second phase of the proposed system, however, entailed the construction of a classification model based on using a random forest classifier (RFC) to select a feature subset. Lee in his work achieved 99.9 as DR and 0.1 as FAR. In another study, an optimization technique, the Naïve Bayes (NB) classifier, was applied by Abd-Eldayem in 2014. Experimentation revealed that this optimization technique had a DR of about 99% and a FAR of nearly 1%.

In 2018, Shone and his colleagues [6] proposed a novel deep-learning (DL) classification model that was constructed using stacked, non-symmetric, deep auto-encoder a multiple, hidden-layer, unsupervised, neural network-based, feature extraction algorithm. This model had a DR of 97.9% and a FAR of 2.1%.

Also, Yan and Han [8] proposed an IDS which would use the stacked sparse auto-encoder (SSAE) for extracting the features that have a significant influence on intrusion behavior. Then, a different classifier was employed by using low-dimensional sparse features. Performance evaluation revealed that this model had a DR of 99.01% and a FAR of 0.13%.

In 2019, Sara and her colleagues [18] proposes a wrapper method for feature selection based on linear correlation coefficient (FGLCC) algorithm and cuttlefish algorithm (CFA), and the Decision tree act as a classifier in IDS. The results obtained DR equals 95.23% with a low FAR of 1.65%. Also, Boonyopakornin 2019 has applied Fuzzy logic and association with genetic network programming (GNP), FL-GNP as an abbreviation, for feature selection to create an associated rule to detect attacks [19]. Thus 24 features used instead of 41 features which produced an IDS with a 94.8 detection rate.

Convolutional neural network (CNN) has been applied by Xiao in 2019 [20] in detecting network attacks which called (CNN–IDS). The auto-encoder (AE) as a nonlinear dimension reduction technique has been used to reduce features. The overall DR and FAR were 93.0 and 0.005, respectively.

The pigeon inspired optimizer algorithm was proposed [16] by utilizing the selection process of network features. A new methodology used to binarize a continuously metaheuristic algorithm. Also, the proposed work, enternally, compared with the sigmoid function. As a result, the accuracy of detection was 0.947. While Aishwarya and his colleagues [17] examine the efficiency of J48, Naive Bayes (NB) and Random forest (RF) as a classification models. The RF reached 99.9 and 0.004 as a DR and FAR, respectively.

III. The KDD'99 Dataset

For assessing the performance of the proposed Cuckoo-ID system, there was a need to run it on actual data. For this purpose, the researcher utilized the KDD'99[21] dataset, which is (so far as the author knows) the most appropriate dataset for this purpose. KDD'99 is a benchmark dataset that is frequently used by different researchers to evaluate the levels of performance of their proposed IDSs.

The origin of KDD'99 is DARPA, which produced it in MIT Lincoln Labs. This dataset is a standard dataset that is commonly used to evaluate results in this line of research. A standard set of data needs to be audited, since it includes a huge number of intrusion records that have been simulated in a military network Laboratories [21]. In this respect, the analysis of the KDD'99 provides useful information for the expansion of IDSs. The data in this dataset are classified into normal records and attack records, and they involve mining rules. This dataset contains41 features. Hence, one of the objectives of the feature filtration method is its ability to extract the most relevant set of features. In this context, different algorithms can be applied to select the relevant features from the KDD'99 dataset, as in Jamali and Jafarzadeh [9]; Lee, Park, and Lee [10]; Abd-Eldayem[11]; and Alsharafat [12].

IV. Proposed Work

Here, a new IDS will be presented by adapting a Cuckoo Algorithm to include feature filtration, which is due to working overall the XCS steps. The Cuckoo Algorithm is used in the present study as a feature filtration method to enhance the detection of the network attacks. The motivation for performing this work emerged from the high potential of this particular algorithm for feature filtration as had been confirmed in various previous studies such as Gandomi, Yang, and Alavi [22]; Yang and Deb [23]; and Yang, Deb, Karamanoglu, and Xingshi [24]. In 2009, Yang and Deb [23] presented this meta-heuristic algorithm—namely, the Cuckoo Algorithm—which they based on a parasitic-like nesting behavior for the brooding of some cuckoo species. This algorithm works coherently and effectively with the Lévy flights (LFs). Thus, the general framework of the proposed work consists of two key processes; feature filtration using a cuckoo algorithm which specifies the key features that are considered next process which concerns about intrusion detection using XCS as illustrated in Fig. 1.

A. Cuckoo Feature Filtration

One of the critical decisions in any IDS is the selection of the critical network features. Thus, for enhancing the detection of the proposed method, the cuckoo algorithm was employed as it plays an important role in distinguishing the features that will seriously affect the performance of the system. This algorithm increases the DR and reduces the associated FAR. In addition to this, the Cuckoo Algorithm works effectively with Lévy Flight (LF) and generates new solutions around the most suitable solution obtained so far, which will speed up the process of local search [22–26].

The solution-generation process of the cuckoo search algorithm depends on three rules:

- Each cuckoo randomly chooses a nest in which to lay one egg at a time.
- The elitism nests with high-quality eggs will be transferred to the next generation.
- The number of host nests is fixed, where each host can detect a strange egg with a probability of Pa ϵ [0,1]. As well, the host bird can discard the egg or leave the nest to construct a new nest in another place [23]. For such enhancements, certain characteristics of the current solution must be modified in order to breed a new solution.

The Cuckoo Algorithm for feature filtration can be summarized in the follow Pseudo-code as in Fig. 2 [23,26]:

By incorporating the LF in the Cuckoo Algorithm, the LF will guarantee to find new solutions in the region of the best-stated solution, which will boost the speed of the local search space [23,25,26] and guarantee that the system will not be trapped in a local optimum [22,23].

B. Extended Classifier System (XCS)

In 1995, Wilson has introduced The XCS[27], which is a real (integer or binary) code one of the Learning Classifier System categories. It is a fitness classifier system in which every rule depends on a fitness value for the evaluation of this system. As such, the XCSs can be classified as a rule-based classifier system. Each rule, or classifier, is constructed from two parts:

1) The Condition Part: This part is encoded using the step size parameter (α). So, a binary code is applied by using the notion of {0, 1, #}, where the symbol # refers to a non-significant value of a feature.

2) The Action Part: This part represents the result of the selected rule that will be fired at the environment. The result can be either a normal record or an attack.

Thus, in all XCS components, the filtered features produced from applying the cuckoo algorithm will be considered in condition part in every rule(classifier) through population set [P], matching set [M], prediction set and action set [A].

The XCS concentrated on two main operations: Rinforcement Learning (RL) and GA breeding. RL is concerned with gaining criticism from the external environment about the fired result. It is also concerned with taking advantage of the selected rule in order to be useful in similar situations [28,29]. On the other hand, the GA is used for breeding new rules.

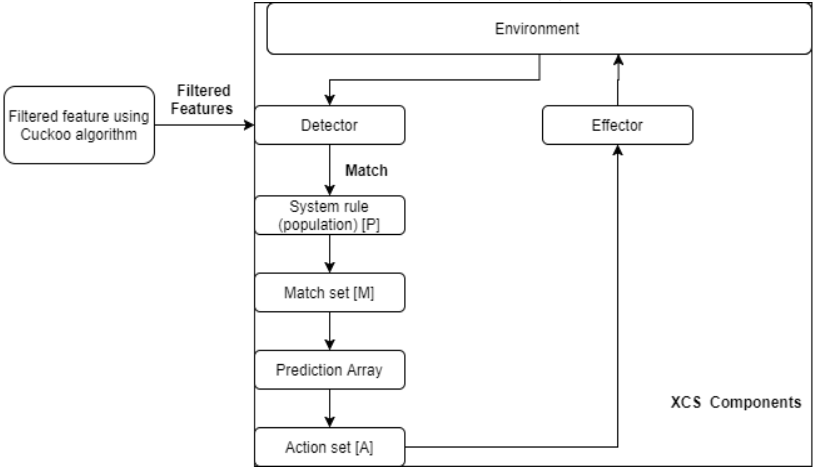
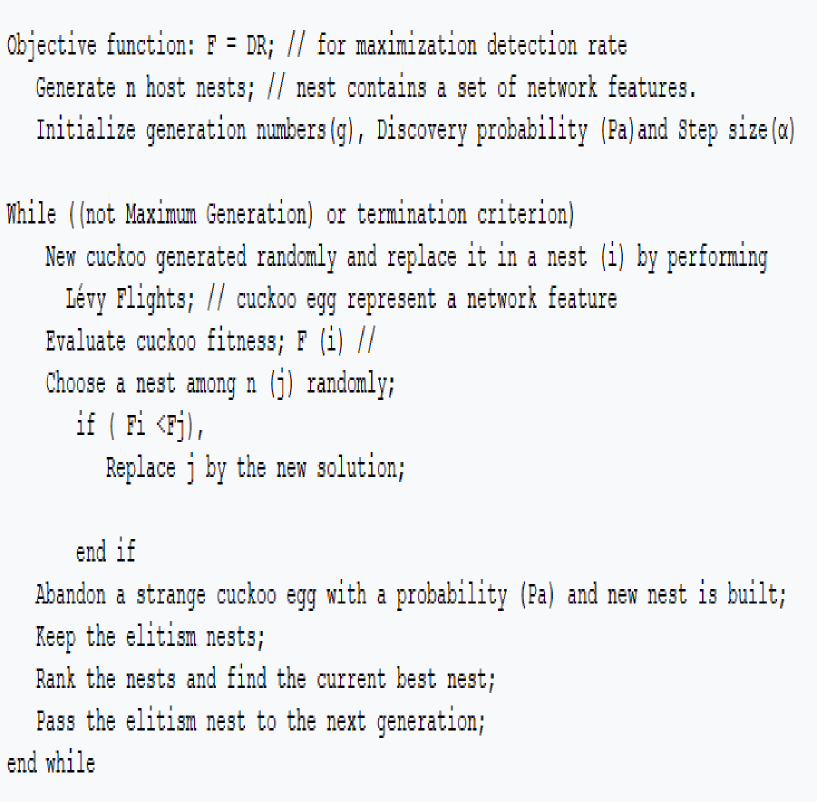


Fig. 1. The Proposed Work; Cuckoo Algorithm and XCS.



```
Objective function: F = DR; // for maximization detection rate
  Generate n host nests; // nest contains a set of network features.
  Initialize generation numbers(g), Discovery probability (Pa)and Step size(α)

While ((not Maximum Generation) or termination criterion)
   New cuckoo generated randomly and replace it in a nest (i) by performing
     Lévy Flights; // cuckoo egg represent a network feature
   Evaluate cuckoo fitness; F (i) //
   Choose a nest among n (j) randomly;
      if ( Fi <Fj),
         Replace j by the new solution;

      end if
  Abandon a strange cuckoo egg with a probability (Pa) and new nest is built;
  Keep the elitism nests;
  Rank the nests and find the current best nest;
  Pass the elitism nest to the next generation;
end while
```

Fig. 2. Cuckoo Algorithm Pseudo-Code for a Feature Filtration.

The main components of the XCSs are as follows [27–30]:

- Detector: The detector is an input gateway that considers the environment as being a traffic record to be converted into a binary code. Here, the filtered feature will be encoded using binary code while other features replaced by sign (#) to represent irrelevant features in detection.
- Match set [M]: The match set is a repository of the rules that are compiled after performing matching between system rules and records (population of rules [P]) via the detector according to the conditional part, regardless of the action result.
- Prediction Array: The prediction array is an array created from [M] according to the average weighted fitness of the prediction rules employed in an action set [A].
- Action set [A]: All the rules in [M] that support a specific action will be placed in an [A].
- Effectors: The effectors are output gateways for a rule-selected form [A]. They are intended to determine whether the traffic record is a normal record or an attack.

V. Performance Evaluation

For evaluating the performance of the proposed IDS and comparing it with levels of performance of comparable IDSs, two performance evaluation criteria were employed; the DR and the FAR.

- Detection rate (DR)

The detection rate (DR) has been defined as ‘the ratio between the number of correctly detected attacks and the total number of attacks’ [31]. This ratio is calculated as a percentage using Equation (1) [13,14]:

$$DR = ((TP)/(TP + FP)) * 100\ \% \qquad (1)$$

- False alarm rate (FAR)

The false alarm rate (FAR) has been defined as being ‘the number of “normal” patterns classified as attacks (False Positive) divided by the total number of “normal” patterns’ [31]. It is usually expressed as percentage and can be estimated using Equation (2) [13,14]:

$$FAR = ((FP) / (FP + TN)) * 100\% \qquad (2)$$

The definition of the entire parameters in equation (1) and (2) are listed in Table I.

TABLE I. Definition of the Parameters of Equations (1) and (2)

Parameter	**Definition**
True Positive (TP)	Attack records correctly classified as an attack.
False Positive (FP)	Normal record that is inaccurately classified as an attack.
True Negative (TN)	Normal record that is correctly classified as normal.
False Negative (FN)	Attack record that is inaccurately classified as normal.

VI. Experimental Results and Conclusion

One of the aims of the IDS proposed in this study is the enhancement of feature filtration in the ID process. Feature filtration aims at selecting the features that have a crucial role in the detection of each type of attack. Thus, the Cuckoo Algorithm was employed to achieve this purpose.

A comparison was held between different IDSs employing feature selection methods enhancing the efficiency of ID in terms of the DR and FAR. Comparisons in terms of the DR and FAR are shown in Table II, whereas comparisons in terms of the DR alone are illustrated by Fig. 3. It should be underscored first that the number of features identified by the different filtration methods as crucial to ID was different, varying from 7 to 41 features (Table II and Fig. 1).

In terms of the DR, it can be noticed that the IDS proposed in this study (Cuckoo-ID) has an equal performance to that LA-ID developed by Jamali [9] and a somewhat better performance (i.e. higher DR) than the ANN-XCS suggested by Alsharafat [12]. In the meantime, SFFS[10], BN in Abd-Eldayem [11], and FLAME-XCS [13] slightly outperform the system proposed in the current study (Table II and Fig. 1).

In terms of the FAR, it is found (Table II) that the IDS suggested in the present study ranks third in performance next to the system developed by Xiao[20], which had FARs of 0.09% and 0.005%, respectively (Table II and Fig. 3). The other systems included in the comparison had lower performance (that is, higher FARs) than the IDS proposed by the present study (Table II).

An issue that is worth highlighting in Fig. 3 is the effect of the number of selected features on the DR, which tends to decrease as the number of features is increased (though decreasing inconsistently). As far as the IDSs compared in Fig. 3 are concerned, it can be assumed that several features in the range of 13–20 can yield the best results. Lower DRs are likely to be obtained if the number of the employed features is lower than 13 or is higher than 20. However, this issue merits further investigation, especially since the present study used 19 features but still obtained a slightly lower DR than SFFS [10], who used 10 features.

TABLE II. Comparison between different Feature Selection Methods in Filtration Efficiency in Terms of the DR and FAR

Feature Selection method	No. of Features	DR (%)	FAR (%)
CNN-ID [20]	< 41	93	0.005
FL-GNP [19]	24	94.8	NA
FGLCC [18]	10	95.23	1.63
ANN-XCS [12]	< 41	98.01	0.09
Cuckoo-ID	19	98.9	0.09
LA-IDS [9]	7	98.9	1.3
SSAE [7 , 8]	<41	99.01	0.13
NB [11]	13	99.03	1
FLAME-XCS [13]	20	99.9	0.005
SFFS [10]	10	99.9	0.1

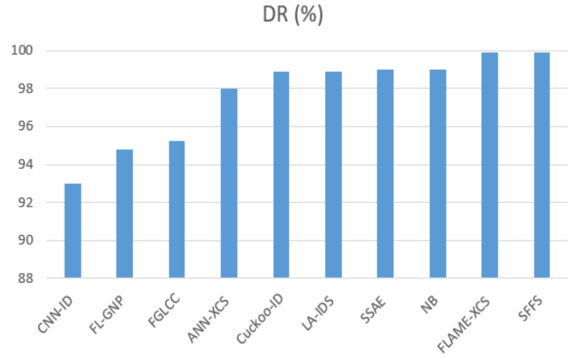


Fig. 3. A Comparison in Detection Rates (DRs) between Cuckoo-ID and IDSs that Filtered Features of the KDD'99 Dataset.

Based on her reading of Fig. 3, as discussed in the preceding paragraph, the researcher suggests using three or four sets of features in future research. These sets contain varying numbers of features in fixed combinations like the first 10 features, the first 20 features, the first 30 features, and then the whole number of features (41). Other combinations of feature sets with almost the same number of features but which involve overlaps in features are also suggested. These include features 1–12, 10–22, 20–32, and 30–41. This is due, on the one hand, to standardize the ID and performance testing processes and the comparisons between the various proposed IDSs; and, on the other hand, to specify the effect of the number of features included in performance testing on the performance of the proposed IDS itself. The researcher thinks that doing so will generate new, valuable knowledge that will contribute to the calibration of the IDS performance evaluation process and to the refinement of the ID process itself.

Given these findings (Table II and Fig. 3), the researcher concludes that her proposed IDS marks a slight improvement over one of the previously-developed IDSs called FLAME-XCS[13] in terms of the DR and varying improvements over multiple previously-developed IDSs in terms of the FAR as SFFS, LA-ID, NB, FGLCC and [8–11,18]. However, these results should be interpreted with caution for two reasons. First, as can be seen in Table II, the different researchers developed their IDSs using datasets with different numbers of features, varying from 7 to 41. Second, there is no optimal set of feature that can be applied in all these studies. Viewed from another angle, the differences between studies in the numbers of features employed in developing their suggested IDSs and evaluating their levels of performance highlights the need for standardization of the number and the type of features to use in such evaluations.

A review of the literature uncovered that there are cases when IDSs were developed using all the features (41) in the KDD'99 dataset. A list of this group of studies which the researcher knew about is given in Table III. The focus of these studies was the development of IDSs that will ensure the enhancement of the ID process in terms of the DR and FAR rather than feature filtration. Besides, a graphical comparison between these studies in the DRs associated with each of them is provided by Fig. 4. Both in Table III and Fig. 4, the researcher included her own proposed IDS (Cuckoo-ID) for comparison.

TABLE III. A COMPARISON IN PERFORMANCE BETWEEN THE PROPOSED CUCKOO-IDS AND IDSS WITH NO FEATURE SELECTION IN TERMS OF DR AND FAR

IDS	DR (%)	FAR (%)
SCDNN[33]	92.23	7.9
TLMD 4 [34]	93.11	0.761
DENDRON [35]	95.97	1.08
CNN+LSTM[36]	96.96	0.2
DEEP [6]	97.9	2.1
RF [17]	98.7	NA
Cuckoo-ID	98.9	0.09
LA-GRU[7]	98.9	0.134
ECOC[32]	99	NA
Stacked [8]	99.01	0.13

Table III and Fig. 4 points out that, in terms of the DR, Cuckoo-ID and LA-GRU[7], which both have the same DR (98.9%), rank third in performance next to the Stacked method [9] whose DR was 99.01% and ECOC method [32] whose DR was 99.0%. Again, this result supports that the researcher's own proposed IDS has noticeably good performance and is promising, owing to the fact that it performs better in terms of the DR than several previous IDSs have done (Table III).

In other respects, the comparison between the IDSs listed in Table III in terms of the FAR brings to notice that Cuckoo-ID placed in the second-lowest FAR (0.09%). Thus, the results of the performance comparison (summarized by Table III, and depicted in Fig. 5) reinforce the researcher's former conclusion (drawn from Table II and Fig. 3, Fig. 4 and Fig. 5) that the IDS proposed in this study has profoundly good performance and is quite promising as an IDS that could replace the IDSs included in the comparisons in this paper (Table II and Table III).

In other respects, the comparison between the IDSs listed in Table II and those listed in Table III underlines that, in general, the IDSs employing feature selection methods have superior performance, in terms of the DR, than do those systems which use all of the features in the KDD'99 dataset without performing feature selection. The same holds almost as true with regard to the FAR in Fig. 4, where the IDSs employing feature selection methods (Table II) generally have much lower FARs than do those IDSs which do not apply feature selection (Table III). Therefore, the researcher recommends the use of IDSs with feature selection.

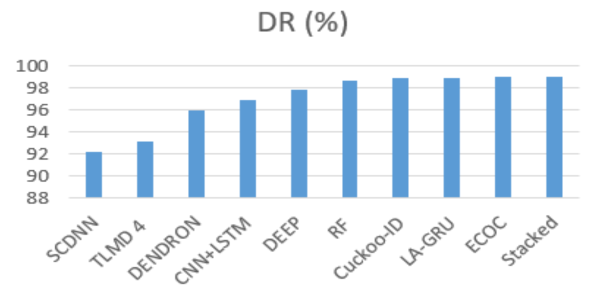


Fig. 4. A Comparison in Detection Rates (DRs) between Cuckoo-ID and IDSs that used All Features of the KDD'99 Dataset.

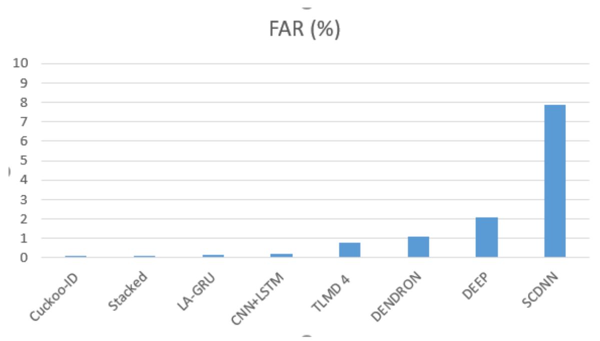


Fig. 5. A Comparison of FAR between Cuckoo-ID and IDSs that used All Features of the KDD'99 Dataset.

Fig. 3 and Fig. 4 lead the researcher to the conclusion that there is no optimal set of features for detecting network intrusions. This is because the various IDSs cited and compared in this paper (Table II and Table III, as well as Fig. 3 and Fig. 4) used different numbers of features. Accordingly, the features themselves used in these tests must be different, though there maybe common features. This is an issue that, though it cannot be negated, cannot be settled out.

The Cuckoo Algorithm was employed for feature filtration in the IDS proposed in this study. It reduced the number of features from the original 41 features down to 19 features and, in consequence, contributed to the development of a highly efficient IDS that has a high DR and a low FAR.

In view of the study's findings, the researcher maintains that it will be quite interesting for future research to develop IDSs that will produce still higher DRs for all types of attacks. Moreover, different evolutionary algorithms are already known. The use of such algorithms can improve the DR of the entire system even if sometimes using all 41 features of the KDD'99 dataset without filtration. Furthermore, another type of dataset will be examined as UNSW-NB 15 to explore new types of attacks and to test the capability of Cuckoo-ID to detect new type of attacks that not included in KDD'99.

REFERENCES

[1] Kumar DA, Venugopalan SR.Intrusion detection system: A review. Int J Adv ResComput Sci.2017;8(8):356–370.

[2] BruneauG.The history and evolution of intrusion detection. SANS Institute Reading Room whitepaper [updated 2001 Oct 13].Available from: https://www.sans.org/reading-room/whitepapers/detection/paper/344

[3] García-Teodoro P, Díaz-Verdejo J, Maciá-Fernándeza G, et al. Anomaly-based network intrusion detection: Techniques, systems and challenge. Sci Direct 2009;28(1–2):18–28.

[4] Wikimedia.Foundation. Intrusion detection system [cited 2009]. Available from: http://en.wikipedia.org/wiki/Intrusion-detection

[5] McHugh, J. Intrusion and intrusion detection. Int J InfSecur.2001;1:14–35.

[6] Shone N, Ngoc TN, Phai VD, et al.A deep learning approach to network intrusion detection. IEEE TransEmerg Topics ComputIntell. 2018;2(1):41–50.

[7] Yan B, Han, G. LA-GRU: Building combined intrusion detection model based on imbalanced learning and gated recurrent unit neural network. SecurCommunNetw.2018a;1:1 –13.

[8] Yan B, Han G. Effective feature extraction via stacked sparse auto encoder to improve intrusion detection system. IEEE Access2018 b;6:41238–41248.

[9] Jamali S,Jafarzadeh P.An intelligent intrusion detection system by using hierarchically structured learning automata. Neural ComputAppl.2017 ;28:1001–1008.

[10] Lee J, Park D, Lee C. Feature selection algorithm for intrusions detection system using sequential forward search and random forest classifier. KSII TransInternet Inf Syst. 2017;11(10):5132–5148.

[11] Abd Eldayem MM. A proposed HTTP service based IDS. Egypt Inf J.2014;15(1):13–24.

[12] Alsharafat W.Applying artificial neural network and extended classifier system for network intrusion detection. Int Arab J Inf Technol.2013;10(3):230–238.

[13] Alzboon K, Alkhaldy J, Alsharafat W. Intrusion detection model based on clustering algorithm FLAME and cuckoo search selection in genetic algorithm in XCS[master's thesis]. Jordan: Al al-Bayt University; 2017.

[14] Saeed K, KarimF.A novel classification method using hybridization of fuzzy clustering and neural networks for intrusion detection. Int J Modern EducComput Sci.2014;11:11–24.

[15] Biswajit P, Olugbenga O, PriyankaM.Training of intelligent intrusion detection system using neuro fuzzy. 15th Institute of Electrical and Electronics Engineers(IEEE)/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). 2014Jun30–Jul 2; Las Vegas, NV, USA.

[16] Alazzam H, Sharieh A, Sabri Kh, A Feature Selection Algorithm for Intrusion Detection System Based on Pigeon Inspired Optimizer. Expert Systems With Applications, https://doi.org/10.1016/j.eswa.2020.113249, 2020.

[17] Aishwarya CH, Venkateswaran N, Supriya T, et al.Intrusion detection system using KDD Cup 99 dataset. Int JInnovTechnolExplor Eng. 2020;9(4):3169–3171.

[18] Mohammadi S, Mirvaziri H, Ghazizadeh-Ahsaeea M, et al.Cyber intrusion detection by combined feature selection algorithm. J InfSecur Appl.2019;44:80–88.

[19] Boonyopakorn P. The optimization and enhancement of network intrusion detection through fuzzy association rules. 2019 6th International Conference on Technical Education (ICTechEd6).2019 March 19–20; Bangkok, Thailand.

[20] Xiao Y, Xing Ch, Zhang T. An intrusion detection model based on feature reduction and convolutional neural networks. IEEE Access2019;7:42210–42219.

[21] University of California, Irvine. KDD Cup 1999 Data [data set]. Third International Knowledge Discovery and Data Mining Tools Competition, held in conjunction with KDD-99 The Fifth International Conference on Knowledge Discovery and Data Mining [updated 1999 October 29]. Available from: http://kdd.ics.uci.edu/databases/kddcup99 /kddcup99.html

[22] Gandomi AH, YangXS, Alavi AH. Cuckoo search algorithm: a metaheuristic approach to solve structural optimization problems. EngComput.2013;29:17–35.

[23] YangXS, Deb S. Cuckoo search via Lévyflights. Proceedings of the World Congress on Nature & Biologically Inspired Computing.2009 Dec 9–11; Coimbatore, India.

[24] YangXS, Deb S, Karamanoglu M, et al. (2012). Cuckoo search for business optimization applications. National Conference on Computing and Communication Systems.2012 Nov 21–22; West Bengal, India.

[25] Yildiz AR.Cuckoo search algorithm for the selection of optimal machining parameters in milling operations. Int JAdvManuf Technol.2013;64:55–61.

[26] Santillan JH, Tapucar S, Manliguez C, et al. (2018). Cuckoo search via Lévyflights for the capacitated vehicle routing problem. J Ind Eng Int.2018;14:293–304.

[27] Wilson SW.Classifier fitness based on accuracy. EvolComput .1995;3(2):149–175.

[28] Lanzi PL. Learning classifier systems: Then and now. EvolIntell. 2008;1(1):63–82.

[29] Holmes JH, Lanzi PL, Stolzmann W, et al.Learning classifier systems: New models, successful applications.Inf Process Lett.2002;82(1):23–30.

[30] Bull L, Kovacs T, editors. Foundations of learning classifier systems. Berlin: Springer Science & Business Media; 2005.

[31] Elhamahmy ME, ElmahdyHN, SaroitIA. A new approach for evaluating intrusion detection system. CiiT International Journal of Artificial Intelligent Systems and Machine Learning2010;2(11):290–298.

[32] Zare, P. Intrusion detection system based on combination of optimized genetic and firefly algorithms in cloud computing structure.ComputEngIntell Syst.2019;10(4):6–11.

[33] Ma T, Wang F, Cheng J, et al. A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks. Sensors.2016;16(10):1701.

[34] Yuan Y, HuoL, Hogrefe D. (2017). Two layers multi-class detection method for network intrusion detection system. IEEE Symposium on Computers and Communications. 2017 Jul 3–6; Heraklion, Greece.

[35] Papamartzivanos D, Mármol FG, KambourakisG.Dendron: Genetic trees driven rule induction for network intrusion detection systems. Future GenerComputSyst.2018;79(2):558–574.

[36] Wang W, Sheng Y, WangJ, et al. (2017). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection.IEEE Access2017;6:1792–1806.