ISSN (Online): 2350-0530
ISSN (Print): 2394-3629

International Journal of Research -GRANTHAALAYAH
August 2020, Vol 8(08), 217 – 225
DOI: https://doi.org/10.29121/granthaalayah.v8.i8.2020.1031

OPTIMIZATION ALGORITHMS FOR INTRUSION DETECTION SYSTEM: A REVIEW

Sheren Sadiq Hasan [*1]✉, Adel Sabry Eesa [2]

[*1] Information Technology Management Department, Duhok Poly Technique University, Duhok City, KRG, Iraq

[2] Computer Science Department, Zakho University, Duhok City, KRG, Iraq

DOI: https://doi.org/10.29121/granthaalayah.v8.i8.2020.1031

Article Type: Research Article

Article Citation: Sheren Sadiq Hasan, and Adel Sabry Eesa. (2020). OPTIMIZATION ALGORITHMS FOR INTRUSION DETECTION SYSTEM: A REVIEW. International Journal of Research -GRANTHAALAYAH, 8(8), 217-225. https://doi.org/10.29121/granthaalayah.v8.i8.2020.1031

Received Date: 09 August 2020

Accepted Date: 29 August 2020

Keywords:
Intrusion Detection
Anomaly Detection
Misuse Detection
Optimization Algorithms

ABSTRACT

With the growth and development of the Internet, the devices and the hosts connected to the Internet have become the target for attackers and intruders. Consequently, the integrity of systems and data has become more sophisticated. Meanwhile, many institutions suffer from money-losing or other losses due to attacks on computer systems. Accordingly, the detection of intrusion and attacks has become a challenge and a vital necessity at the same time. Many different methods were used to build intrusion detection systems (IDSs), and all these methods seek to a plus the efficiency of intrusion detection systems. This paper is a survey which tries to covers some of the optimization algorithms used in the field of intrusion detection in past ten years such as Artificial Bee Colony (ABC), Genetic Algorithm (GA), Cuttlefish Algorithms (CFA), and Particle Swarm Optimization (PSO). It is hoped that this review will provide useful insights about the intrusion detection literature and is a good source for anyone interested in applying one of the used optimization algorithms in the field of intrusion detection.

1. INTRODUCTION

In any information system, intrusions can be defined as activities that break and violate the security policy of that system, intrusions can be identified by intrusion detection [1]. since the evolution of the internet, intrusion detection systems (IDS) are one of the most important types of the security software that has been used to deal with the intrusions [2]. Intrusion detection systems are among the necessary systems within the information security system [3].

IDS are hardware or software that observe the processes of the computer network, waiting for any violation of network management policies, or monitors any change such as modification, files addition, or files deletion on the host device [3]. Intrusion is indicated as any types of unauthorized activity that results in corrupted to the information system. Whereas, any attack that poses a potential threat to the integrity and confidentiality of the information is considered intrusion. For example, When computer services do not respond to legitimate users [4]. In the past and to this day, Cyber criminals have focused on stealing from banks and credit card customers or robbing bank account. Therefore, it is of vital importance to have IDS for detecting various attacks [5]. The goal of IDS is identifying all sorts of different attacks as soon as possible, which a traditional firewall cannot be achieved. Besides,

to distinguished between the system activities which are normal and behaviors which be classified as suspicious or intrusions.

To secure important data several methods have been used like encryption and firewall etc. Firewall acts as a defense but it reduces exposure of intrusions instead of monitors or remove the computer systems vulnerabilities [5]. So, it is necessary for finding a detecting and monitoring system to protect important data. For this reason, the methods of introns detection in the computer have attracted the attention of many researchers [6] [3].

2. TYPES OF INTRUSION DETECTION

IDSs are categorized into two types: Signature-based Intrusion Detection System (SIDS) and Anomaly-based Intrusion Detection System (AIDS). The following is a brief explanation of each one [1] [5].

- Signature intrusion detection systems (SIDS)
  SIDS is based on the techniques which depend on the principle of matching patterns for finding a known attack; these are also known as Knowledge-based Detection or Misuse Detection. In another meaning, when a signature of an intrusion matches with the intrusion signature which previously existing, the alarm signal is given.
- Anomaly-based intrusion detection system (AIDS)

This type attracted the attention of many scholars because of its superiority over SIDS in terms of its ability to beat of the limitations of SIDS. In AIDS, using machine learning, a model of normal system behavior is created. Any deviation from the normal behavior of the model is deeming an anomaly. All techniques which use this type assume that any behavior that differs from the typical behavior is considered as intrusion. The classification of the intrusion detection system is showed in "Fig.1"

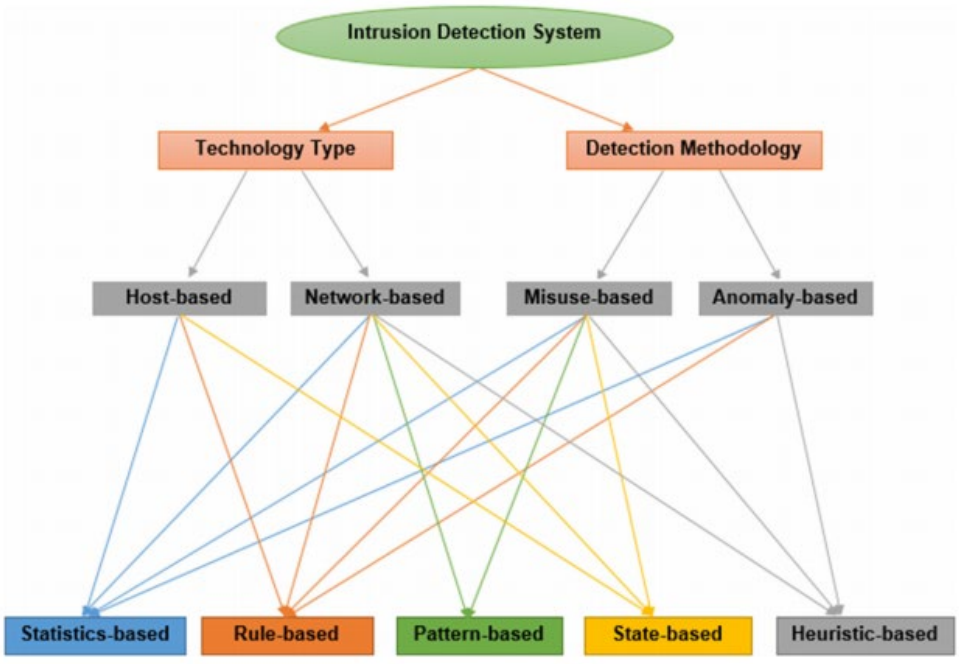

Figure 1: The taxonomy of the intrusion detection system

3. TYPES OF ATTACKS

Attacks can be classified into four types [7], [8], [9] , and [10].

- User to Root Attack (U2R): The attacker exploits the normal user of the system, where he enters the system with the powers of the regular user by obtaining the password and then exploiting some weaknesses to gain access to the system root.

- Probing**:** It is an attempt to collect information from a computer device to identify weaknesses in the computer.
- Denial-of-Service Attack (DoS): It is for the attacker to do some accounts and make the resources too busy, make the memory full, or prevent legal users from accessing the computers.
- Remote to local Attack (R2L): The attacker can send packets to the device through the network without having any account in that device and then exploits the weaknesses to enter that device as a normal user for it.

4. OPTIMIZATION ALGORITHM WITH INTRUSION DETECTION

ID is a wide field of research area, so there are many common algorithms that have been used in field of the intrusion problems such as evolutionary algorithms this include biology inspired algorithms such as Genetic algorithm [11], [12], Practical Swarm Optimization PSO [13], [14], [15], [16], [17], [18] Cuttlefish CFA [19], [20], [21], [2], Artificial Bee Colony [22], [23], [24] and Ant Colony [25], [26]. The paper provides an overview of applying some optimization algorithms to the problem of intrusion detection in past ten years.

4.1. PRACTICAL SWARM OPTIMIZATION PSO

Authors in [27]proposed an ID approach using k-means clustering algorithm and practical swarm optimization (PSO). PSO has been applied to select the cluster centers. KDD-cup 99 dataset was utilized for evaluating the approach performance. The obtained results showed high detection rate and low false alarm rate, and the method has been achieved faster processing time.

Authors in [30] proposed an approach for ID based on practical swarm optimization (PSO) and support vector machine (SVM). PSO was applied for both selecting the SVM parameters and feature selection. NSL-KDD datasets was used and the method gave good results in term of performance with accuracy rate equal to 81.8%.

While authors in [31] Proposed an approach for IDS based on feature selection using particle swarm optimization (PSO). PSO was used to select the features from the principal components. Simulated dataset was used for evaluating this method and the results showed the ability of the method for detecting intrusion with DR = 99.4% and FAR = 0.6%.

While, in [33] the authors design a new method for IDS based on (MCLP-PSO) multiple criteria linear programming and practical swarm optimization for intrusion detection. KDD datasets has been used. The approach gives good results in term of DR = 0.9913, FAR = 0.01947 and running time.

While, authors in [39] proposed a method based on NN and PSO algorithm for improving the performance of ID. The proposed method seeks to detect various kinds of attacks with high accuracy as possible. The data goes through the feature selection stage in order to keep the appropriate features for ID. This data was used to train and test the neural networks. Then optimal weights have been extracted using PSO in order to classify the data as normal or attacks. The results illustrates that this approach provides high accuracy and performance for detecting various types of attacks.

Authors in [37] proposed an IDS based on fast learning network and particle swarm optimization (FLN-PSO) for improving the intrusion detection. By applying KDD datasets the performance of the method was evaluated. The results illustrate that the accuracy of DoS and Probe attack improved when PSO optimized the parameters of the FLN. While, the accuracy of R2L and U2R attack was low and it is due to the limitation amount of training data.

4.2. ARTIFICIAL BEES COLONY (ABC)

Authors in [13] Proposed a method depended on the bees algorithm for improving the IDS. The honeybee approach is consisting of three basic components named, Undesirable-Absent (UA), Desirable-Present (DP), and Filtering-Decision (FD). Predefined attacks were detected using the UA detector. The responsibility of detecting anomalous behaviors lies with DP detector. While the FD was applied for training the UA detector in real time, it is purposed to discover new interventions. Patterns of attacks were learned in the training dataset by NN which trained by the BA to identify the attacks characteristics then classify these characteristics as unwanted characteristics during the test phase. KDD cup 99 dataset has been used for evaluating the method performance. The obtained results

showed that the method has been applied successfully and it is able to detect different kinds of attacks and it can be learned the misuse attacks characteristics and determine instances that did not notice during the train phase.

In addition, authors in [24] proposed a novel anomaly network intrusion detection system using ABC algorithms. First for each feature in the datasets, upper bound (UB) and lower bound (LB) has been determined. Then it was used to infer the classification rule. Then the ABC algorithm has been applied to recognize patterns from the network traffic. KDD datasets was used and the obtained results illustrate the ability of the method for retaining the robustness of the system with different population sizes.

Authors in [32] proposed a hybrid IDS based on artificial bee colony (ABC) algorithm and multi-layer perceptron (MLP). ABC algorithm was used for optimizing weights of MLP for getting better results in term of detection rate. NSL-KDD datasets was used and the accuracy obtained by using ABC = 87.27% while error rate= 0.126%.

Authors in [35] proposed an approach to detect Denial-of-Service Attack (Dos) in Cloud computing based on bees algorithm. The work steps are depending on selected the basic feature for each record in datasets then the ABC was applied for constructing a normal profile in training step. In testing phase centroids classifiers was applied to detect the DoS attacks. ABC gives good results for detecting attacks and is useful in handling denial-of-service attacks.

Additionally, the authors in [36] proposed a novel hybrid IDS based on (ABC-AFS) which combining the Artificial Bees Colony and Artificial Fish Swarm for ID the purpose of the approach was distinguished between normal behavior and abnormal. The approach tries to enhancing the accuracy detection of ID by taking advantage of the properties of the two algorithms after they are combined. The proposed method has been applied using UNSW-NB15 and NSL-KDD datasets. Fuzzy C Means (FCM) was used to divide train datasets, whiles for removing the irrelevant features Correlation-based feature selection (CFS) was used. In addition, classification and regression tree (CART) was used as a rules generator to separate normal behaviors from the abnormal. At last the hybrid ABC-AFS identifies the type of attacks. The approach showed good results in terms of performance measures.

Authors in [38] proposed a network ID based on modified Naive Bayes algorithm and Artificial Bee Colony Algorithm (ABC). The approach can effectively improve the network intrusion detection rate, which can well detect different kinds of network intrusion and greatly improve the security performance of the network.

4.3. CUTTLEFISH ALGORITHM

Authors in [20] Present an approach for intrusion detection systems which combines the cuttlefish algorithm CFA and Decision Tree (DT). CFA was used as a feature selection method and it searched for the optimal subset of features. The DT classifier was used as a verdict on the selected features that are produced by the CFA. By applying the feature selection using CFA on the KDD Cup 99 datasets, the acquired results were better.

In like manner, authors in [21] proposed a distributed intrusion detection system (DIDS) based on cuttlefish optimization algorithm (CFA) and decision tree DT. The system used an agent called rule and feature generator agent (RFGA) which is used for generating a subset of features by using CFA. CFA produced the best five features, and then it built a decision tree. Generated DT has been used as a judgment on the selected features. KDD dataset has been applied for testing the system. The five selected features performance compared with the completed 41 features performance and the results illustrated that with 5 features, the system performed better than the completed 41 features.

Authors in [2] proposed an intrusion detection system based on feature selection algorithm and clustering algorithm by use filter and wrapper method. The proposed method combines feature grouping based on linear correlation coefficient (FGLCC) and CFA algorithm. FGLCC filter has been applied to ranking the primary features and choose the best one among them. In this proposed system the work goes through several stages, starting with calculating the correlation coefficient between the features and classes to choose the features that have the highest correlation, then the FGLCC calculates the evolution function for the chosen features and introduces the features that have the highest rank to the CFA to start the second stage, which is choosing the best subset of initial features, the groups of features has been selected depending on the high speed of FGLCC and the high accuracy of CFA. CFA dependent on DT as a classifier to classify the features after they were selected. The results show that DR was increased while FPR was reduced.

4.4. GENETIC ALGORITHM (GA)

Authors in [28] designed an approach for intrusion detection based on genetic algorithm GA to detect different kinds of network intrusions efficiently. The systems work was divided into (1) precalculation (train) phase: depending on train data, groups of chromosomes for each attack and normal types have been made". And in (2) detection (test) phase: initial population for each test data has been made. Then population was compared with each chromosomes prepared in training phase and Portion of population were deleted in order to filter the traffic data. According to this process, the data was classified as normal or attacks. KDD data set was used and the method gave good results in term of ID with DR equal to 0.95 and FPR equal to 0.30.

In like manner, authors in [29] proposed a new IDS (PSO-GA) for malicious traffic by complain particle swarm optimization with genetic algorithm. KDD Cup datasets was used for evaluate the approach. The source of parameters was selected using PSO while GA got the normal and abnormal data from network traffic. The proposed method achieved good results in term ID with very low FAR and High DR.

What is more, authors in [11] proposed an anomaly detection system to discover anomalies in a computer network. This method depends on using retrieved information from IP flows, and it combines the genetic algorithm (GA) and a Fuzzy Logic together for getting better results in term of ID. GA was applied for generating a digital signature of network segment. Network flows extract information to be utilized for predicting the behavior of network traffic. The instances are determined by applying the fuzzy logic scheme to determine if the instance exemplifies an anomaly or not. The proposed approach was applied in real network traffic flows and achieved good results.

At last, authors in [40] developed a hybrid intrusion IDS which able to handle the large volume of NSL-KDD datasets based on the genetic algorithm and Fuzzy (GA-Fuzzy). GA has been used in order to train the Fuzzy classifier in efficient way by generating new rules. Principle Component Analysis (PCA) was used as a feature selection method to get rid of irrelevant features and for choose the appropriate features. Then the dataset was classified as normal or attack efficiently in term of accuracy. The proposed method demonstrated its ability to reduce the time spent detecting intrusion and reduce misclassification alarm rate.

In this review paper, different optimizations algorithms are illustrated and summarized in the term of intrusion detection. Table 1 exemplifies the summarization of the reviewed related works.

Table 1: The summarization of the reviewed related works

No.	Ref.	Years	Algorithm	results	summary
Practical Swarm Optimization (PSO)					
1	[27]	2011	PSO+ k-means	DR= 74.43% FAR: 1.86%	KDD datasets was used and The obtained results illustrated good results in term of DR and FAR. In addition, the method has been achieved faster processing time.
2	[30]	2014	PSO+SVM	Accuracy: 81.8%	NSL-KDD datasets was used. PSO was used for both feature selection and selecting the SVM parameters, As for computation time, this method is rather expensive.
3	[31]	2015	NN-PSO	DR = 99.4% FAR = 0.6%	Simulated Dataset has been used. In the proposed method PSO has been applied for features selection.
4	[33]	2015	PSO+ MCLP	accuracy= 0.9913 False Alarm Rate= 0.01947	KDD datasets has been used. The approach gives good outcomes in term of DR, FAR and running time.
5	[37]	2018	FLN-PSO	Accuracy with 25 neurons= 0.98 Accuracy with 200 neurons= 0.99	KDD was used. PSO has been applied for optimizing the FLN weight, and this led to improve the accuracy of the classifier performance. The results illustrated that the accuracy of the method was increased when the number of neurons increased.
6	[39]	2019	PSO + neural network	Accuracy = 98.08 using NSL-KDD.	KDD and NSL-KDD dataset has been applied for evaluating the performance of the method. The results

				Accuracy = 99.66 using KDD.	illustrates that this approach provides high accuracy and performance for detecting various types of attacks.
Artificial Bees Colony (ABC)					
7	[13]	2011	ABC	DR= 99.4 FPR= 0.5	KDD cup 99 dataset was used for evaluating the performance of the method. The results indicated the ability of the proposed method to detect different types of attacks.
8	[24]	2012	ABC	Avg. accuracy = 98.5 Best accuracy = 99.5 SD = 0.004	KDD datasets was used, the outcomes illustrate that the approach accuracy not changed when the maximum generation number increased.
9	[32]	2015	ANN-ABC	Accuracy= 87.27 Error rate= 0.126	For evaluating the approach performance NSL-KDD datasets was utilized. ABC was applied to improve the weights of the MLP. All the features in the dataset were used and the results showed that accuracy is somewhat low.
10	[35]	2016	ABC	Accuracy= 72.4%	ABC was considered as a useful algorithm for detecting Denial-of-Service (Dos) attack in the cloud environment. And it was able to detect attack in short time.
11	[36]	2018	ABC+AFS algorthims	Detection Rate= 99% False Positive Rate= 0.01%	The approach was achieved good results and tries to improve the detection accuracy in IDS.
12	[38]	2018	ABC- MNB	Accuracy= 91.08 Sensitivity= 0.86 specificity= 0.94 F-Source = 0.90	NSL-KDD datasets was used to evaluate the approach. The speed processing of the MNB algorithm increased due to the ABC algorithm capabilities, it gives varied of solutions.
Cuttlefish Algorithm					
13	[20]	2015	CFA	Using 5 features Detection Rate = 91%, FPR = 3.917 With 41 features Detection Rate = 71.087, FPR = 17.685	KDD-99 datasets was used. The study concludes that the results improve by decreasing the number of features and it gives higher DR with a lower FAR
14	[21]	2017	CFA+ DT	PSP (accuracy) = 92.17%	KDD cup99 datasets was used. This approach combine (CFA, DT, RFGA) to obtain good results for ID, the proposed system performs better when choosing 5 features instead of using all. U2R not performed well, in all cases, better results were achieved using 5 features except U2R.
15	[2]	2019	FGLCC + CFA	Accuracy= 95.03% False Positive Rate= 1.65%	KDD-CUP99 datasets has been utilized. The results obtained provide high performance accuracy.
Genetic Algorithm (GA)					

16	[28]	2012	GA	DR= 0.95 FPR= 0.30	KDD data set was used. Detect different kinds of network intrusions efficiently.
17	[29]	2013	PSO-GA	Very low FAR and High DR	KDD Cup datasets was used for evaluate the approach. Parameters source were selected using PSO and classification rules has been created, GA was used to classify datasets into attack and normal.
18	[34]	2015	GA+ FA	Accuracy= 96.1	NSL datasets was used. The results showed the ability of the method for handling large scale datasets.
19	[11]	2018	GA + Fuzzy Logic	Accuracy= 96.53% False Positive Rate= 0.56%	Provides satisfactory and high quality results in term of anomaly DR and FPA.
20	[40]	2019	GA+ Fuzzy	Accuracy = 99.96% FAR = 0.04%	NSL-KDD datasets was used. The proposed method detects attacks effectively. Added to, reduce the FAR.

5. DISSCUSION

As shown from the study, there are many optimization algorithms that have been used in the field of intrusion detection, but this study is concerned with ABC, PSO, GA, and CFA and its field for detecting attacks, whether they have been used alone or have been combined with other algorithms to increase the system performance and efficiency. It is clear that all of the mentioned algorithms contributed to the detection of attacks in new and different ways. The PSO algorithm always improves solutions to improve the problem. It can be combined with other algorithms for improving the method performance. But this algorithm does not guarantee an optimal solution. The performance of this algorithm can be affected by time and noise. According to the ABC, ABC algorithm is easy for implementing but it need high amount of evaluation functions and that may affect the ABC accuracy. While CFA was used successfully for feature selection in different study. But CFA is a mathematically complex algorithm. Last the GA is well used in term of optimizing parameters and it can be deal with large amount of datasets but GA may suffer from some restrictions.

6. CONCLUSION

It is not required that all intrusion detection systems have the same mechanism and operate in the same way. It may use different methods and strategies. Sometimes it may require a lot of monitoring and high effectiveness to reach the desired goal. In this follow up study, we concluded that there are many methods and algorithms used to detect intrusion and that each algorithm has its pros and cons. All algorithms have difficulty dealing with big data, so they always need to be combined with other algorithms or techniques to give a better performance. For this reason, many alone models fail to achieve a high detection rate with reduced false alarm rate. In this paper several optimization algorithms are described for intrusion detection that had been proposed in the past ten years. This review will be helpful to researchers for gaining a basic insight of different approaches for intrusion detection. From previous studies in related work, it is clearly that each algorithm tries to do best in a particular way but there are always some limitations that provide option for researcher to design better algorithm than existing.

SOURCES OF FUNDING

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

CONFLICT OF INTEREST

The author have declared that no competing interests exist.

ACKNOWLEDGMENT

None.

REFERENCES

[1] Ashoor, A.S., S.J.I.J.o.S. Gore, and E. Research, Importance of intrusion detection system (IDS). 2011. 2(1): p. 1-4.
[2] Mohammadi, S., et al., Cyber intrusion detection by combined feature selection algorithm. 2019. 44: p. 80-88.
[3] Khraisat, A., et al., Survey of intrusion detection systems: techniques, datasets and challenges. 2019. 2(1): p. 20.
[4] Aljawarneh, S., M.B. Yassein, and M.J.C.C. Aljundi, An enhanced J48 classification algorithm for the anomaly intrusion detection systems. 2019. 22(5): p. 10549-10565.
[5] Pradhan, M., C.K. Nayak, and S.K. Pradhan, Intrusion Detection System (IDS) and Their Types, in Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications. 2020, IGI Global. p. 481-497.
[6] Parihar, L.S., A.J.I.J.f.S. Tiwari, and A.R.i. Technology, Survey on intrusion detection using data mining methods. 2016. 3(12): p. 342-7.
[7] Tavallaee, M., et al. A detailed analysis of the KDD CUP 99 data set. in 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. 2009. IEEE.
[8] Kaushik, S.S., P.J.I.J.o.C.S. Deshmukh, and I. Technologies, Detection of attacks in an intrusion detection system. 2011. 2(3): p. 982-986.
[9] Dhanabal, L., S.J.I.J.o.A.R.i.C. Shantharajah, and C. Engineering, A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. 2015. 4(6): p. 446-452.
[10] Alharbi, A., et al., Denial-of-Service, Probing, User to Root (U2R) & Remote to User (R2L) Attack Detection using Hidden Markov Models. 2018.
[11] Hamamoto, A.H., et al., Network anomaly detection system using genetic algorithm and fuzzy logic. 2018. 92: p. 390-402.
[12] Raman, M.G., et al., An efficient intrusion detection system based on hypergraph-Genetic algorithm for parameter optimization and feature selection in support vector machine. 2017. 134: p. 1-12.
[13] Ali, G.A. and A. Jantan. A new approach based on honeybee to improve intrusion detection system using neural network and bees algorithm. in International Conference on Software Engineering and Computer Systems. 2011. Springer.
[14] Aburomman, A.A. and M.B.I.J.A.S.C. Reaz, A novel SVM-kNN-PSO ensemble method for intrusion detection system. 2016. 38: p. 360-372.
[15] Vardhini, K.K. and T. Sitamahalakshmi. Implementation of Intrusion Detection System Using Artificial Bee Colony with Correlation-Based Feature Selection. in Proceedings of the First International Conference on Computational Intelligence and Informatics. 2017. Springer.
[16] Chung, Y.Y. and N.J.A.s.c. Wahid, A hybrid network intrusion detection system using simplified swarm optimization (SSO). 2012. 12(9): p. 3014-3022.
[17] Zebari, D.A., et al., Image Steganography Based on Swarm Intelligence Algorithms: A Survey. 2020. 7(8): p. 9.
[18] Sadeeq, H., et al. A Novel Hybrid Bird Mating Optimizer with Differential Evolution for Engineering Design Optimization Problems. in International Conference of Reliable Information and Communication Technology. 2017. Springer.
[19] Eesa, A.S., et al., Cuttlefish algorithm-a novel bio-inspired optimization algorithm. 2013. 4(9): p. 1978-1986.
[20] Eesa, A.S., Z. Orman, and A.M.A.J.E.S.w.A. Brifcani, A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems. 2015. 42(5): p. 2670-2679.
[21] Eesa, A.S., A.M. Abdulazeez, and Z.J.S.J.o.U.o.Z. Orman, A DIDS Based on The Combination of Cuttlefish Algorithm and Decision Tree. 2017. 5(4): p. 313-318.
[22] Shukran, M.A.M., et al., Artificial bee colony based data mining algorithms for classification tasks. 2011. 5(4): p. 217.
[23] Ahmed, J.A., A.M.A.J.I.J.o.M. Brifcani, Aerospace, Industrial, Mechatronic, and M. Engineering, A new internal architecture based on feature selection for holonic manufacturing system. 2015. 2(8): p. 1431.

[24] Bae, C., et al., A novel anomaly-network intrusion detection system using ABC algorithms. 2012. 8(12): p. 8231-8248.
[25] Varma, P.R.K., V.V. Kumari, and S.S.J.P.c.s. Kumar, Feature selection using relative fuzzy entropy and ant colony optimization applied to real-time intrusion detection system. 2016. 85: p. 503-510.
[26] Aghdam, M.H. and P.J.I.N.S. Kabiri, Feature Selection for Intrusion Detection System Using Ant Colony Optimization. 2016. 18(3): p. 420-432.
[27] Li, Z., Y. Li, and L. Xu. Anomaly intrusion detection method based on k-means clustering algorithm with particle swarm optimization. in 2011 international conference of information technology, computer engineering and management sciences. 2011. IEEE.
[28] Hoque, M.S., et al., An implementation of intrusion detection system using genetic algorithm. 2012.
[29] Kumar, K.P.M.J.I.J.o.S., Engineering and C. Technology, Intrusion Detection system for malicious traffic by using PSO-GA algorithm. 2013. 3(6): p. 236.
[30] Manekar, V. and K.J.I.J.o.A.C.R. Waghmare, Intrusion detection system using support vector machine (SVM) and particle swarm optimization (PSO). 2014. 4(3): p. 808.
[31] Ahmad, I.J.I.J.o.D.S.N., Feature selection using particle swarm optimization in intrusion detection. 2015. 11(10): p. 806954.
[32] Mahmod, M.S., et al., Hybrid intrusion detection system using artificial bee colony algorithm and multi-layer perceptron. 2015. 13(2): p. 1.
[33] Bamakan, S.M.H., et al., A new intrusion detection approach using PSO based multiple criteria linear programming. 2015. 55: p. 231-237.
[34] Ghanem, T.F., W.S. Elkilani, and H.M.J.J.o.a.r. Abdul-Kader, A hybrid approach for efficient anomaly detection using metaheuristic methods. 2015. 6(4): p. 609-619.
[35] Sharma, S., A. Gupta, and S. Agrawal. An intrusion detection system for detecting denial-of-service attack in cloud using artificial bee colony. in Proceedings of the International Congress on Information and Communication Technology. 2016. Springer.
[36] Hajisalem, V. and S.J.C.N. Babaie, A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection. 2018. 136: p. 37-50.
[37] Ali, M.H., et al., A new intrusion detection system based on fast learning network and particle swarm optimization. 2018. 6: p. 20255-20261.
[38] Yang, J., et al. Modified naive bayes algorithm for network intrusion detection based on artificial bee colony algorithm. in 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS). 2018. IEEE.
[39] Shokoohsaljooghi, A. and H.J.I.J.o.I.T. Mirvaziri, Performance improvement of intrusion detection system using neural networks and particle swarm optimization algorithms. 2019: p. 1-12.
[40] Pradeep Mohan Kumar, K., et al., Intrusion detection system based on GA-fuzzy classifier for detecting malicious attacks. 2019: p. e5242.