Baghdad Science Journal

Volume 22 | Issue 7 Article 27

7-25-2025

Enhancing Feature Selection in Network Intrusion Detection Systems Using a Novel Hybrid Binary Swarm Algorithms

Maher Khalaf Hussein
Computer Center, Presidency of the University, University of Telafer, Mosul, Iraq,
maher.k.hussein@uotelafer.edu.iq

Asmaa Alqassab
Department of Computer Science, College of Education for Pure Science, University of Mosul, Mosul, Iraq,
asmaa_mow@uomosul.edu.iq

Lubna Thanoon ALkahla
Software Department, Information Technology College, Ninevah University, Mosul, Iraq,
lubna.thanoon@uoninevah.edu.iq

How to Cite this Article

Hussein, Maher Khalaf; Alqassab, Asmaa; and ALkahla, Lubna Thanoon (2025) "Enhancing Feature Selection in Network Intrusion Detection Systems Using a Novel Hybrid Binary Swarm Algorithms," *Baghdad Science Journal*: Vol. 22: Iss. 7, Article 27.
DOI: https://doi.org/10.21123/2411-7986.5007

BAGHDAD SCIENCE JOURNAL 2025;22(7):2429–2437

RESEARCH ARTICLE

Enhancing Feature Selection in Network Intrusion Detection Systems Using a Novel Hybrid Binary Swarm Algorithms

Maher Khalaf Hussein [1,*], **Asmaa Alqassab** [2], **Lubna Thanoon ALkahla** [3]

[1] Computer Center, Presidency of the University, University of Telafer, Mosul, Iraq
[2] Department of Computer Science, College of Education for Pure Science, University of Mosul, Mosul, Iraq
[3] Software Department, Information Technology College, Ninevah University, Mosul, Iraq

ABSTRACT

An intrusion detection system (IDS) is a system that monitors network traffic for any mistrustful activity and issues alerts when it is detected. The selection of feature stage is important in effective intrusion detection systems, as it determines the features that are most influential in detecting normal traffic and malicious traffic. In this study, new proposed hybrid method for selecting features in intrusion detection systems based on the hybrid binary Salp Swarm algorithm (SSA) and the binary Pigeon Inspired Optimizer (PIO), inspired by the collective behavior of animals. The proposed method removes unnecessary features and increases the number of features necessary, as the classification accuracy reached 99 percent. This feature selection approach increases the overall performance of intrusion detection systems by combining the strengths of binary SSA and PIO.

Keywords: Network intrusion detection systems, NIDS, Salp swarm, Pigeon inspired, SSA

Introduction

Network intrusion detection systems (NIDS) are security systems that monitor network traffic for suspicious activity, giving an alert if such activity is identified. One of the most difficult aspects of creating a successful NIDS is identifying features that can reliably distinguish between normal traffic and... Malicious Traffic,[1,2] where appropriate selection of features greatly increases the accuracy and efficiency of IDS; therefore, feature selection is crucial in building intrusion detection systems.[3,4] In the feature selection stage, a subset of relevant features is selected from a broader set of available features. In NIDS, there are several techniques for feature selection, including filtering, pooling, and embedding methods.[5,6]

To increase the accuracy and efficiency of intrusion detection systems, swarm algorithms were used in the process of selecting the most important features, as swarm algorithms are considered more effective in the feature selection process than traditional methods.[7,8] Swarm algorithms successfully deal with the high dimensions and dynamic nature of network traffic data, and in general, swarm algorithms are considered as promising algorithms to enhance the performance of intrusion detection systems and network security.[9,10]

Related works

Several studies have been carried out in order to improve the feature selection process in Intrusion

Received 21 November 2023; revised 20 April 2024; accepted 22 April 2024.
Available online 25 July 2025

* Corresponding author.
E-mail addresses: maher.k.hussein@uotelafer.edu.iq (M. K. Hussein), asmaa_mow@uomosul.edu.iq (A. Alqassab), lubna.thanoon@uoninevah.edu.iq (L. T. ALkahla).

https://doi.org/10.21123/2411-7986.5007

Detection Systems (IDS). In one study,[11] a Particle Swarm Optimization (PSO) algorithm with feature selection (FS) was implemented to improve the accuracy and detection rate (DR) of IDS. By utilizing the Random Forest (RF) algorithm, the top 10 features out of 41 were selected, and the PSO algorithm was applied to these features. The suggested algorithm exceeded of other methods, that's having higher accuracy10 features only. Another study[12] presented a new wrapper feature selection method which combined between Pearson's correlation and Whale Swarm Optimization for IDS in cloud computing environments. Compared to the K-Nearest Neighbor (KNN) algorithm, this method achieved remarkable superiority, as the accuracy reached 80% on the original dataset by selecting 8 features out of 42. Another study aims to increase efficiency and reduce complexity, another study[13] presented a majority vote system that combines three standard methods for selecting features, which leads to improving performance and building computationally effective IDS. In addition, a feature selection algorithm was proposed[14] based on the Pigeon-Inspired Optimizer to reduce the number of features while maintaining a high detection rate and accuracy, at the same time, low false alarms. The algorithm achieved high success in terms of True Positive Rate (TPR), False Positive Rate (FPR), accuracy, and F-score compared to other modern approaches. Another study,[15] explored the utilization of XGBoost and Naive Bayes (NB) classifiers to create a robust network anomaly detection model. Improved detection rate, recalls, F-measurement, and false alarm rates for the network IDS due to the benefit of Salp Swarm Algorithm (SSA). In addition, the accuracy in intrusion detection is improved and the selected features are significantly reduced when based on bio-inspired algorithms and mutual information (MI).[16] Adaptive voting was proposed in another study,[17] combining multiple machine learning techniques and wrapper feature selection methods to achieve high accuracy and suitable testing time. Various machine learning techniques, such as Decision Tree, Random Forest, and SVM, were employed in predicting prevalent attacks using feature selection techniques.[18] An Ensemble Learning algorithm-based network IDS model was proposed in another work,[19] utilizing AdaBoosting and bagging ensemble learning algorithms to modify four classifiers, resulting in high accuracy and a low false-negative rate. Finally, a hybrid intrusion detection system combining feature selection and weighted stacking classification algorithms[20] achieved improved accuracy and precision compared to traditional machine learning models. These related works collectively contribute to the advancement of IDS by offering innovative approaches to feature selection, enhancing accuracy, reducing complexity, and improving the overall performance of IDS models. By relying on various techniques in the field of machine learning and effective optimization algorithms in order to achieve further advancements in intrusion detection and network security systems.

Dataset

The NSL-KDD database shown in Table 1 is considered an improved version of the KDD'99 database. It is a good and useful benchmark that helps researchers choose different techniques for intrusion detection, despite it being limited. This dataset was developed in 2009 by Tavallaee et al.[21,22] These databases provide an evaluation of attack types for computer network intrusion systems and selection of features. They may provide a training set of up to 125,973 instances, and the testing set reaches 22,544 instances. Additionally, the feature selection integrates 41 features from the KDD Cup 1999 dataset. This dataset has been used in many research studies, adopted and published as benchmark results. It is free and available for download through many online sources.[23,24]

Table 1. List attributes of NSL-KDD dataset.[25]

Sr. No.	Feature	Sr. No.	Feature	Sr. No.	Feature
1	Duration	15	Su attempted	29	Same srv rate
2	Protocol type	16	Num root	30	Diff srv rate
3	Service	17	Num file creations	31	Srv diff host rate
4	Flag	18	Num shells	32	Dst host count
5	Source bytes	19	Num accessfiles	33	Dst host srv count
6	Destination bytes	20	Num outbound cm ds	34	Dst host same srv rate
7	Land	21	Is host login	35	Dst host diff srv rate
8	Wrong fragment	22	Is guest login	36	Dst host same src port rate
9	Urgent	23	count	37	Dst host srv diff host rate
10	Hot	24	Srv count	38	Dst host error rate
11	Number failed logins	25	Rerror rate	39	Dst host srv error rate
12	Logged in	26	Srv error rate	40	Dst host error rate
13	Num compromised	27	Rerror rate	41	Dst host srv error rate
14	Root shell	28	Srv error rate	42	Class label

Swarm optimization algorithm

Algorithm of salp swarm (SSA)

This algorithm, called SSA, was proposed by Mirjalili et al. it is considered one of the random population-based algorithms. SSA mimics the way salps swarm in the ocean to hunt food. Salps typically form a swarm known as a salp chain in heavy waters. The salp at the head of the chain is the leader in the SSA algorithm, and the salps that are left behind are referred to as followers. Similar to previous swarm-based methods, salps' position is determined inside an s-dimensional search space, where s is the problem's variable count. Thus, a two-dimensional matrix named z contains the position of every salp. As for the swarm's aim, it is also presumable that there is a food supply in the search area with the name P.[26–28] The following equation can be used to move the leader salp:[28–30]

$$z_n^1 = \begin{cases} p_n + r_1\left(\left(u_n - l_n\right) r_2 + l_n\right) & r_3 \geq 0 \\ p_n - r_1\left(\left(u_n - l_n\right) r_2 + l_n\right) & r_3 < 0 \end{cases} \quad (1)$$

The meanings of all symbols are shown in Table 2.

$$r_1 = 2e^{-\left(-\frac{4a}{A}\right)^2} \quad (2)$$

The coefficient r1 is the essential parameter in SSA because it provides a balance between exploration and exploitation capabilities.

Based on what Mirjalili et al.[28] say, Eq. (1) and Eq. (2) change the position of salps. In SSA, the most recent answer is mostly based on the most recent best solution. To make the salp swarm algorithm (SSA) better, an inertia weight ω 2[0,1] is added to SSA, just like it was done in the PSO algorithm. The new number in the SSA algorithm speeds up the speed at which the search results come together. It also strikes a balance between the abilities to exploit and explore so that it can first avoid a huge number of local solutions in feature selection tasks and then get a clear picture of the best solution.[28,29] The following equations show the new algorithm:

$$z_n^1 = \begin{cases} \omega p_n + r_1\left(\left(u_n - l_n\right) r_2 + l_n\right) & r_3 \geq 0 \\ \omega p_n - r_1\left(\left(u_n - l_n\right) r_2 + l_n\right) & r_3 < 0 \end{cases} \quad (3)$$

For more details about the algorithm, please refer to the reference.[28,31]

Pigeon-inspired optimization

An intelligent algorithm known as the Pigeon-Inspired Optimization (PIO) algorithm was developed by taking inspiration from the behavior of pigeons that had returned to their nest. An approach that is a binary variant of the PIO algorithm is known as the binary pigeon-inspired optimization (BPIO) algorithm. This algorithm can be utilized to optimize binary application problems. The algorithm operates through the iterative updating of pigeon positions, considering their individual best positions (local best) and the best position found by the entire swarm (global best).[32,33] The equations governing this process include the movement equation:

$$X_i(t+1) = X_i(t) + V_i(t) \quad (4)$$

where Xi(t) represents the current binary position of pigeon i at time t, and Vi(t) denotes the velocity term, determined by

$$V_i(t) = r_1 \cdot \left(Pbest_i(t) - X_i(t)\right) + r_2 \cdot \left(Gbest(t) - X_i(t)\right) \quad (5)$$

In equations Pbesti(t) signifies the best position that pigeon i has ever encountered while Gbest(t) represents the best position found by the entire pigeon swarm at time t. Random coefficients r1 and r2 are responsible for governing how much influence local and global bests exert.[34,35] For more information concerning Binary PIO Algorithm on Feature Selection for IDS readers are referred to go through detailed methodology outlined in.[30,31]

Table 2. The meanings of all symbols.[28]

Symbol	Meaning
Znl	leader position in nth dimension
Pn	food source position in nth dimension
Un	upper bound of nth dimension
In	lower bound of nth dimension
r1, r2, and r3	random variables uniformly produced in the interval of [0,1].
a	current iteration
A	maximum number of iterations
Z	position of mith follower salp in nth dimension
e	time

Proposed method

The research introduced SSA-PIO as a new approach to feature selection. It combines two novel algorithms that are binary Pigeon Inspired Optimizer and hybrid binary Salp Swarm algorithm for identifying features that help in enhancing the efficiency of IDS. The new method works by producing binary vectors for both algorithms where 1 represents the presence of a feature and 0 its absence. Lastly, the resultant binary vectors are combined into a bigger

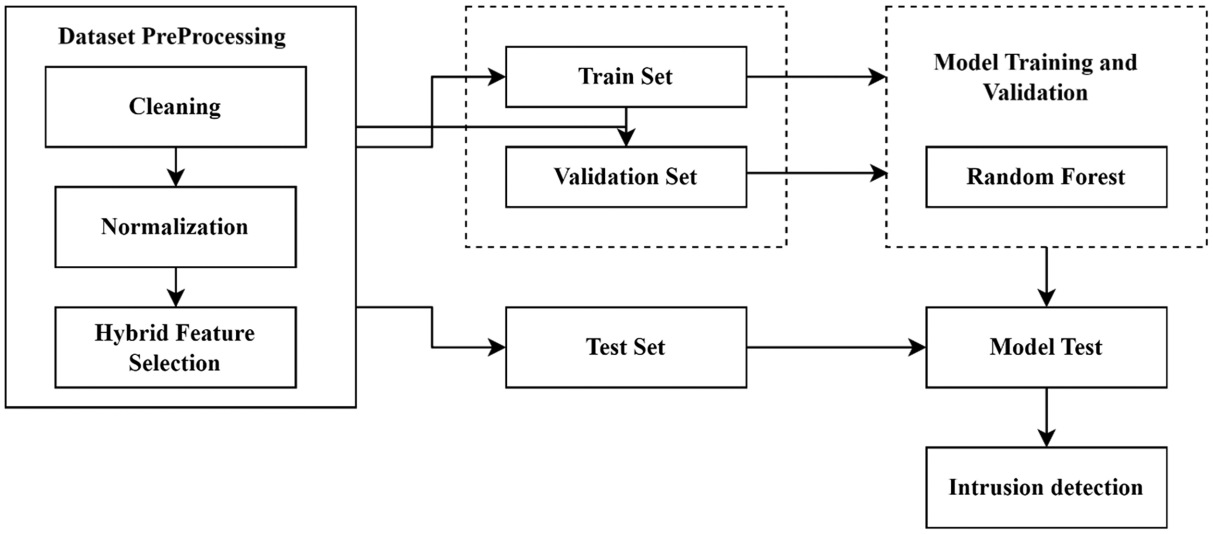

Fig. 1. Intrusion detection framework with hybrid SSA-PIO feature selection.

vector to create a final feature subset. To illustrate this technique, Fig. 1 is an example of a proposed algorithm for selecting relevant features for an intrusion detection system with respect to recognition accuracy. Its purpose is to choose features correctly, so as to improve recognition performance.

Dataset preprocessing for the NSL-KDD analysis

In order to get the data ready for classification, the first thing that has to be done is to clean up any incomplete data and transform any symbolic features into numeric features while the representation process is taking place. The second feature of the protocol, for instance, includes icmp, tcp, and udp communication protocols. For every symbol, it is possible to transform it to the values 0 and 1, and then to 2 such that the third and fourth features are used. In addition, the classes have to be transformed to a particular number when the final feature is being implemented. By way of illustration, it is a representation of the normal, DOS, PROBE, R2L, and U2R for the values 0, 1, 2, 3, and 4, respectively. Following the representation, the normalization procedure involves bringing all values into the range of 0 to 1 by employing Eq. (1). This is done in order to prevent the classifier from developing a bias toward high values. A breakdown of the preparation steps for samples taken from NSL testing data is presented in Table 1.

$$x = \frac{x - min}{max - min} \tag{6}$$

Where x represents a feature value, min represents the minimum value in the feature and max represents the maximum value in the feature.

Proposed hybrid swarm feature selection

In this study a combination of the Salp Swarm Algorithm and a binary inspired optimizer is employed to select features, for Intrusion Detection Systems (IDS) as shown in Fig. 2. To create an IDS that can accurately distinguish between malicious network traffic it is crucial to carefully choose the appropriate features. this study uses salps and pigeons' collective behavior to design these new methods to solve this problem.

The hybrid binary SSA-PIO approach generates a binary vector for each feature, where 1 indicates good features. In contrast, 0 features will be deleted. By combining these binary vectors, the largest vector represents the final subset of features.

Binary SSA-PIO randomly initializes a salp and pigeon through random binary vectors, after which the network traffic is classified as malicious or normal, in this way it is different from others.

In this study, the velocity and position of the pigeon and salp were modified by fitness evaluation, and they are quite similar to SSAs and PIOs. This technique contributes to controlling the examination of the solution space and achieving convergence with the local optimum by specifying criteria that balance between exploring the search space and exploiting it during optimization, which leads to improving the effectiveness of the algorithm.

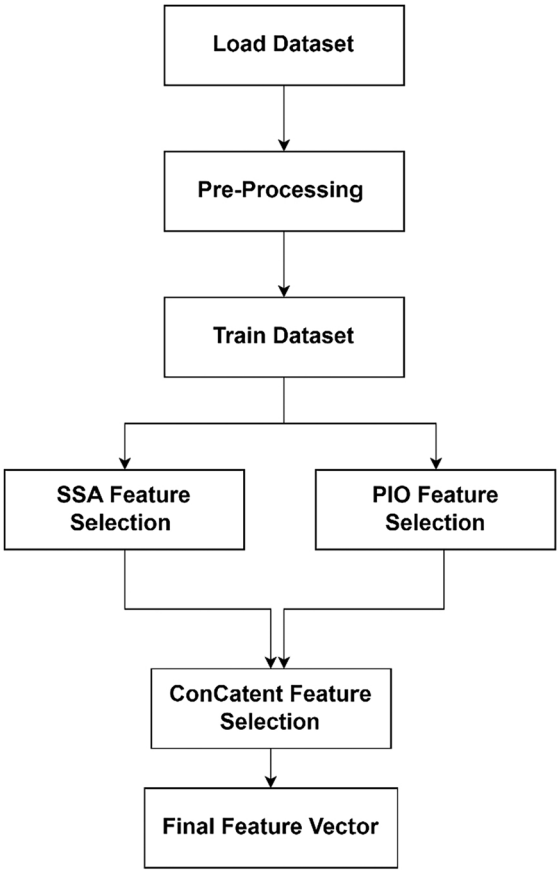

Fig. 2. Hybrid binary SSA-PIO feature selection process for IDS.

A Hybrid Binary Salp Swarm Algorithm and Pigeon Inspired Optimization (SSA-PIO) for Feature Selection in IDS:

1. Randomly populate salps and pigeons with binary vectors consisting of 0s and 1s.
2. Evaluate the usefulness of each resultant solution as a classifier for network traffic that is normal or malicious.
3. For each salp and pigeon, update position and velocity by: a. Updating the speed using SSA equation b. Updating its position using PIO equation c. Reset when it goes outside search space.
4. Re-evaluate the fitnesses of solutions after updating the positions and velocities.
5. Update personal best positions of salps and pigeons based on individual fitnesses.
6. Calculate for the whole population a new global best position according to fitness.
7. Repeat steps 3 to 6 until stopping criteria (maximum number of iterations) are met.
8. The best solution should be used to select features with a binary value of 1Here are the equations for updating the position and velocity of each salp and pigeon:

SSA equation:

$$\text{velocity} = w * \text{velocity} + c1 * r1 * (\text{pbest\_position} - \text{position}) + c2 * r2 * (\text{gbest\_position} - \text{position})$$

$$\text{position} = \text{position} + \text{velocity}$$

PIO equation:

$$\text{velocity} = w * \text{velocity} + c1 * r1 * (\text{pbest\_position} - \text{position}) + c2 * r2 * (\text{gbest\_position} - \text{position}) + c3 * r3 * (\text{migrate\_position} - \text{position})$$

$$\text{position} = \text{position} + \text{velocity}$$

Where w, c1, c2, and c3 are the parameters that control the balance between exploration and exploitation of the search space, r1, r2, and r3 are random numbers between 0 and 1, pbest_position is the personal best position of the salp or pigeon, gbest_position is the global best position, and migrate_position is the position of a randomly selected salp or pigeon.

The hyperparameter values were set after several trials as follows:

- Inertia weight (w): 0.7
- Cognitive parameter (c1): 2.0
- Social parameter (c2): 2.0
- Migration parameter (c3): 0.5

Setup and experimental environment

This work presents an algorithm method that is based on an implementation of Python that makes use of the sci-kit-learn toolkit. The purpose of this implementation is to experiment what happens in a system that has an Intel Core i7-7500u CPU at a speed of 2.70 GHz. The NSL-KDD dataset was used to test the efficiency of the model. The experimental results of this study are obtained from 5-fold cross-validation to rule out the effect of randomness ‘on the results.

Metrics of evaluation

In this particular piece of research, the evaluation criteria that were utilized were as follows: accuracy (Acc), detection rate (DR), F1 score, and false alarm rate (FAR). The Eqs. (7) to (10) is used to calculate the metrics in the appropriate manner.

$$\text{Acc} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN}) \quad (7)$$

$$\text{Precision} = \text{TP} / (\text{TP} + \text{FP}) \quad (8)$$

$$\text{DR} = \text{Recall} = \text{TP} / (\text{TP} + \text{FN}) \quad (9)$$

Table 3. Performance evaluation of feature selection models.

Model	No. of Features	Class	Precision	Recall	F1-Score	Accuracy
All Features	41	normal	0.92	0.93	0.93	0.93
		anomaly	0.94	0.93	0.93	
Binary Salp Swarm Algorithm	14	normal	0.96	0.93	0.94	0.95
		anomaly	0.94	0.97	0.95	
Binary Pigeon Inspired Optimizer	17	normal	0.98	0.95	0.97	0.97
		anomaly	0.96	0.99	0.97	
Proposed Algorithm (Binary SSA-PIO)	32	normal	0.99	0.99	0.99	0.99
		anomaly	0.99	0.99	0.99	

$$F1 = 2 * \left(\left[Precision\_Recall\right] / \left[Precision + Recall\right]\right) \quad (10)$$

Results and discussion

The efficiency of the proposed algorithm in feature selection was evaluated and compared to three other models. The comparison models used were as follows:

1. All Features: This model had all features selected.
2. Binary Salp Swarm Algorithm: This model used binary Salp Swarm Algorithm for feature selection.
3. Binary Pigeon Inspired Optimizer: The feature selection in this approach involved binary Pigeon Inspired Optimizer. The evaluation results revealed that the suggested method outperformed other methods. Table 3 summarizes the comparative findings:

According to this table, the suggested method had a highest accuracy that was at 99% and the others had a lower accuracy. It also has the topmost Precision, Recall and F1 score hence it could identify relevant features to improve classification.

These results above depict how this algorithm can reduce irrelevant features while incorporating outputs of binary Salp Swarm Algorithm and binary Pigeon Inspired Optimizer, thus enhancing feature selection to improve overall performance for other subsequent tasks or models based on these selected features.

Conclusion

This study used a new way to pick features in Network Intrusion Detection Systems (NIDS). it did this by combining a hybrid binary Salp Swarm Algorithm (SSA) and a binary-inspired optimizer (PIO). By using binary vectors, this method can pick out important features and get rid of unnecessary ones. This makes the selected features more important. When compared to other models, this approach did better in precision, recall, and F1 score. It had an outstanding accuracy rate of 99%. Using the hybrid binary SSA-PIO strategy improved the overall effectiveness of different tasks or models that rely on the chosen features and feature selection. When use Random Forest as a classifier, it made the results more resilient and accurate. The hybrid binary SSA-PIO method in general presents a potentially effective strategy for feature selection in Network Intrusion Detection Systems (NIDS), with increased accuracy and less complexity, leading to better performance of the entire system. An extensive inquiry into this method and its examination would contribute significantly to advancing network security and intrusion detection systems.

Author's declaration

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Furthermore, any Figures and images, that are not ours, have been included with the necessary permission for republication, which is attached to the manuscript.
- No animal studies are present in the manuscript.
- No human studies are present in the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee at University of Telafer.

Author's contribution statement

The authors, M. K. H, A. A, and L. T. A, helped in planning and carrying out the study, as well as analyzing the data and writing the paper.

References

1. Ahmad Z, Shahid Khan A, Wai Shiang C, Abdullah J, Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Trans Emerg Telecommun Technol. 2021;32(1):e4150. https://doi.org/10.1002/ett.4150.

2. Mebawondu JO, Alowolodu OD, Mebawondu JO, Adetunmbi AO. Network intrusion detection system using supervised learning paradigm. Sci Afr. 2020;9:e00497. https://doi.org/10.1016/j.sciaf.2020.e00497.
3. Sarhan M, Layeghy S, Portmann M. Towards a standard feature set for network intrusion detection system datasets. Mob Netw Appl. 2022;27(1):357–370. https://doi.org/10.1007/s11036-021-01843-0.
4. Young C, Zambreno J, Olufowobi H, Bloom G. Survey of automotive controller area network intrusion detection systems. IEEE Design Test. 2019;36(6):48–55. https://doi.org/10.1109/mdat.2019.2899062.
5. Mulyanto M, Faisal M, Prakosa SW, Leu JS. Effectiveness of focal loss for minority classification in network intrusion detection systems. Symmetry. 2020;13(1):4. https://doi.org/10.3390/sym13010004.
6. Zhou X, Liang W, Li W, Yan K, Shimizu S, Wang KI-K. Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system. IEEE Internet Things J. 2022;9(12):9310–9319. https://doi.org/10.1109/jiot.2021.3130434.
7. Kunhare N, Tiwari R, Dhar J. Particle swarm optimization and feature selection for intrusion detection system. Sadhana. 2020;45(1). https://doi.org/10.1007/s12046-020-1308-5.
8. Almomani O. A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms. Symmetry. 2020;12(6):1046. https://doi.org/10.3390/sym12061046.
9. Ogundokun RO, Awotunde JB, Sadiku P, Adeniyi EA, Abiodun M, Dauda OI. An enhanced intrusion detection system using particle swarm optimization feature extraction technique. Procedia Comput Sci. 2021;193:504–512. https://doi.org/10.1016/j.procs.2021.10.052.
10. Kunhare N, Tiwari R, Dhar J. Intrusion detection system using hybrid classifiers with meta-heuristic algorithms for the optimization and feature selection by genetic algorithm. Comput Electr Eng. 2022;103:108383. https://doi.org/10.1016/j.compeleceng.2022.108383.
11. Ahmadi SS, Rashad S, Elgazzar H. Efficient feature selection for intrusion detection systems. In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, 2019. https://doi.org/10.1109/uemcon47517.2019.8992960.
12. Ravindranath V, Ramasamy S, Somula R, Sahoo KS, Gandomi AH. Swarm intelligence based feature selection for intrusion and detection system in cloud infrastructure. In 2020 IEEE Congress on Evolutionary Computation (CEC), IEEE, 2020. https://doi.org/10.1109/cec48606.2020.9185887.
13. Alazzam H, Sharieh A, Sabri KE. A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer. Expert Syst Appl. 2020;148:113249. https://doi.org/10.1016/j.eswa.2020.113249.
14. Alsaleh A, Binsaeedan W. The influence of salp swarm algorithm-based feature selection on network anomaly intrusion detection. IEEE Access. 2021;9:112466–112477. https://doi.org/10.1109/access.2021.3102095.
15. Mahmood RAR, Abdi A, Hussin M. Performance evaluation of intrusion detection system using selected features and machine learning classifiers. Baghdad Sci J. 2021;18(2(Suppl.)):0884. https://doi.org/10.21123/bsj.2021.18.2(suppl.).0884.
16. Hamdan Mohammad A, Alwada'n T, Almomani O, Smadi S, ElOmari N. Bio-inspired hybrid feature selection model for intrusion detection. Comput Mater Continua. 2022;73(1):133–150. https://doi.org/10.32604/cmc.2022.027475.
17. Mhawi DN, Aldallal A, Hassan S. Advanced feature-selection-based hybrid ensemble learning algorithms for network intrusion detection systems. Symmetry. 2022;14(7):1461. https://doi.org/10.3390/sym14071461.
18. Zhao R, Mu Y, Zou L, Wen X. A hybrid intrusion detection system based on feature selection and weighted stacking classifier. IEEE Access. 2022;10:71414–71426. https://doi.org/10.1109/access.2022.3186975.
19. Ogundokun RO, Awotunde JB, Sadiku P, Adeniyi EA, Abiodun M, Dauda OI. An enhanced intrusion detection system using particle swarm optimization feature extraction technique. Procedia Comput Sci. 2021;193:504–12. doi: http://dx.doi.org/10.1016/j.procs.2021.10.052.
20. Magdy ME, Matter AM, Hussin S, Hassan D, Elsaid SA. Anomaly-based intrusion detection system based on feature selection and majority voting. Indones J Electr Eng Comput Sci. 2023;30(3):1699. https://doi.org/10.11591/ijeecs.v30.i3.pp1699-1706.
21. Bala R. A review on KDD CUP99 and NSL-KDD dataset. Int J Adv Res Comput Sci. 2019;10(2):64–67. https://doi.org/10.26483/ijarcs.v10i2.6395.
22. Meena G, Choudhary RR. A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA. In 2017 International Conference on Computer, Communications and Electronics (Comptelix). IEEE, 2017. https://doi.org/10.1109/comptelix.2017.8004032.
23. Ingre B, Yadav A, Soni AK. Decision tree based intrusion detection system for NSL-KDD dataset. In: Information and Communication Technology for Intelligent Systems (ICTIS 2017), Sharma H, Govardhan A, editors, 2, Cham: Springer International Publishing. 2018;207–218. https://doi.org/10.1007/978-3-319-63645-0_23.
24. Protić DD. Review of KDD Cup '99, NSL-KDD and Kyoto 2006+ datasets. Vojnoteh Glasn. 2018;66(3):580–596. https://doi.org/10.5937/vojtehg66-16670.
25. Singh R, Kumar H, Singla RK. A reference dataset for network traffic activity based intrusion detection system. Int J Comput Commun Control. 2015;10(3):390. https://doi.org/10.15837/ijccc.2015.3.1924.
26. Rizk-Allah RM, Hassanien AE, Elhoseny M, Gunasekaran M. A new binary salp swarm algorithm: Development and application for optimization tasks. Neural Comput Appl. 2019;31(5):1641–1663. https://doi.org/10.1007/s00521-018-3613-z.
27. Faris H, Mafarja MM, Heidari AA, Aljarah I, Al-Zoubi AM, Mirjalili S, *et al.* An efficient binary salp swarm algorithm with crossover scheme for feature selection problems. Knowl-Based Syst. 2018;154:43–67. https://doi.org/10.1016/j.knosys.2018.05.009.
28. Hegazy AE, Makhlouf MA, El-Tawel GS. Improved salp swarm algorithm for feature selection. J King Saud Univ Comput Inf Sci. 2020;32(3):335–344. https://doi.org/10.1016/j.jksuci.2018.06.003.
29. Goswami N, Raj S, Thakral D, Arias-Gonzáles JL, Flores-Albornoz J, Asnate-Salazar E, *et al.* Intrusion detection system for IoT-based healthcare intrusions with lion-salp-swarm-optimization algorithm: Metaheuristic-enabled hybrid intelligent approach. Eng Sci. 2023;25:933. https://doi.org/10.30919/es933.
30. Kumar N, Kumar S. A salp swarm optimization for dynamic resource management to improve quality of service in cloud computing and IoT environment. Int J Sens Wirel.

Commun Control. 2022;12(1):88–94. https://doi.org/10.2174/2210327911666210126122119.
31. Zivkovic M, Stoean C, Chhabra A, Budimirovic N, Petrovic A, Bacanin N. Novel improved salp swarm algorithm: An application for feature selection. Sensors (Basel). 2022;22(5):1711. https://doi.org/10.3390/s22051711.
32. Pan JS, Tian AQ, Chu SC, Li JB. Improved binary pigeon-inspired optimization and its application for feature selection. Appl Intell. 2021;51(12):8661–8679. https://doi.org/10.1007/s10489-021-02302-9.
33. Rani KV. Content based image retrieval using hybrid feature extraction and HWBMMBO feature selection method. Multimed Tools Appl. 2023;82:47477–47493. https://doi.org/10.1007/s11042-023-15716-z.
34. Kulhare R, Veenadhari DS, Sharma N. Study on multi-objective bio-inspired algorithms for feature selection. Smart Moves J Ijoscience. 2021;5–8. https://doi.org/10.24113/ijoscience.v7i7.394.
35. Abu Alghanam O, Almobaideen W, Saadeh M, Adwan O. An improved PIO feature selection algorithm for IoT network intrusion detection system based on ensemble learning. Expert Syst Appl. 2023;213(118745):118745. https://doi.org/10.1016/j.eswa.2022.118745.

تحسين اختيار الميزات في أنظمة كشف التطفل على الشبكة باستخدام خوارزميات سرب ثنائية هجينة جديدة

ماهرخلف حسين [1]، اسماء موفق محمد [2] ، لبنى ذنون احميدي[3]

[1]مركز الحاسبة، رئاسة الجامعة، جامعة تلعفر، الموصل، العراق.
[2]تربية حاسبات، كلية التربية الصرفة، جامعة الموصل، الموصل، العراق.
[3]البرمجيات، كلية تكنولوجيا المعلومات، جامعة نينوى، الموصل، العراق

الخلاصة

تعتبر أنظمة كشف التسلل إلى الشبكة ضرورية في مراقبة حركة مرور الشبكة واكتشاف الأنشطة الضارة. يعد اختيار الميزات جانبًا مهمًا في تصميم انظام كشف تسلل فعالاً، لأنه يتيح اختيار الميزات ذات الصلة التي تميز بدقة بين حركة المرور العادية والخبيثة. تقدم هذه الدراسة طريقة جديدة لاختيار الميزات تدمج بين خوارزميتين الاولى مستوحاة من سلوك الاحتشاد في المحيطات Salp Swarm Algorithm (SSA) و الثانية مستوحاة من اسراب الحمام Pigeon Inspired Optimizer (PIO) , ويتفوق المنهج المقترح على النماذج السابقة من حيث التقييم والمقارنة.حيث تعمل الخوارزمية المقترحة على إزالة الميزات غير الضرورية و زيادة عدد الميزات ذات الاهمية الاعلى ، اثبتت الخوارزمية المقترحة كفاءة عاليا حيث بلغت دقة التمييز99%

الكلمات المفتاحية: انظمة كشف التطفل، حماية، اختيار ميزات، اسراب الحمام ، الاحتشاد في المحيطات.