Published by

British Journal of Contemporary Research

BEXFORD PUBLISHING

Modified Grey Wolf Optimization Algorithm (XTF-GWO) Using X Shaped Transfer Function for Feature Selection in MANET

Original Research Article | Volume 1 | Issue 4 | 2026 | Article Number: 060

Accepted: 04 September 2026 | Published: 10 September 2026 | ISSN: 2979-8582 (Online)

Crossref **: https://doi.org/10.67693/BJCR-X3BTIDNU**

Arowojolu Akindele Sunday[1], Ayeni Joshua Ayobami[1], Ipeayeda Funmilola Wumi[2]

[1]Department of Computer Sciences, Ajayi Crowther University, Oyo, Nigeria,

[2]Department of Cyber Security, Ajayi Crowther University, Oyo, Nigeria

Correspondence: Arowojolu Akindele Sunday, engrbami4real@gmail.com

Abstract

Mobile Ad Hoc Networks (MANETs) are a type of infrastructure-less network; therefore they rely on neighbour cooperation to facilitate routing of data. Such a property leaves them prone to many attacks. When intrusion detection systems are applied to MANETs; high-dimensional traffic data containing largely irrelevant or redundant features results in high computational cost and poor detection rates. Hence, feature selection becomes a crucial precursor to applying any intrusion detection algorithm to MANET environments. GWO (Grey Wolf Optimization) is popular for wrapper-based selection of features due to its simplicity and robust global search characteristics, but was designed for continuous rather than binary selection.In this study we develop an approach which applies an X-shaped transfer function on GWO's position to generate binary selected features and we guide the algorithm's initialisation based on Information Gain of the features. Named XTF-GWO, this algorithm was evaluated with network data obtained from ITU-ML5G-PS-006 (2025) repository and coded in MATLAB R2025a, classifying data with Support Vector Machine. Four levels of attack injection were analysed (25%, 50%, 75%, 100%). The experiments conclude that an improved feature exploration and exploitation of features through an X-shaped transfer function and Info Gain initialisation, led XTF-GWO to more discriminated feature subsets than GWO and hence better (on the 4 studied proportions of attack detection) results of detection rate (88.42% vs 82.10% on average, up to 96.82% vs 89.15%), with greater precise and recall values.

Keywords: Feature Selection, Grey Wolf Optimization, Transfer Function, Intrusion Detection, Mobile Ad Hoc Network

1. INTRODUCTION

A Mobile Adhoc Networks, referred to as a system of self organising wireless devices that connects nodes without the need of any pre-existing infrastructure as described by Devika et al. (2022). Mobile Ad hoc Network systems lend themselves to multiple environments such as in military communications, rescue, recovery and portable computing. Mobile Ad hoc Network systems however have inherent vulnerabilities due to the open structure, not only are MANET systems themselves mobile and readily deployable they are easy to compromise by third parties as well. Dependent on the open system with shared wireless access and routing this causes susceptibility to black hole, grey hole, wormhole and flooding attacks, as reported by Baird et al. (2024). Intrusion detection systems are thus considered to be an integral defense system which aims at distinguishing malicious intrusions and benign activities.

An inherent weakness that is consistently faced by intrusions in MANET's, due to an overabundance and variety of data generated by mobile nodes, is its dimensionality. Traffic records often have redundant, noisy attributes that add little further classification value yet increases computational burden (Theng&Bhoyar, 2024) this problem can be solved through feature selection to decrease the data by removing a certain subset of irrelevant attributes thereby increasing the performance in the classification stage. Two main types of feature selection strategies exist: filter based, and wrapper based feature selection. Wrapper based method usually achieves a better classification performance due to it imbeds the learner directly within the search but uses larger computational requirements (Theng and Bhoyar, 2024).

For the search stages in the wrapper based feature selection schemes Meta heuristic optimization algorithms are often utilized. These utilize a solution to the search space which mimics nature-inspired phenomena such as the Grey Wolf optimization algorithm proposed by Mirjalili et al. (2014). It was inspired by the hunting behaviour and leadership hierarchy characteristic of grey wolves due to its inherent simplicity, global search ability and ability to rapidly converge. Standard continuous Gray wolf Optimizer problems cannot be directly solved using such optimization techniques when the selected attributes may be assigned Binary discrete values when feature selected but can be easily approximated by mapping the continuously updated positions via aSigmoidtransformation function, giving poor performance to exploration, prematurely convergent and a poor balance between exploitation and exploration (Liu et al., 2023).

In this article, the author proposes a modified Grey Wolf optimization algorithm, known as the XTF-GWO, which overcomes the problem mentioned above by taking advantages from the dual techniques. Firstly, one X Shaped Transfer function converts the position of wolves updated through continuous search space to discrete, rather than typical Sigmoid transformation function; it offers better performance of extraction behavior in binary decision value search. Secondly, Information Gain Guided Initialization Scheme to initiate a part of the population with pre known distinctive features in the search for better solutions. Features selected from the wrapper are evaluated via Support Vector Machine classifier (which has shown great generalization performance and capability for the data sets with high dimensions).

The objective of this study is to Design an X Shaped Transfer Function based Modified Grey Wolf optimization algorithm for the feature selection in the intrusion detection systems of mobile Ad-hoc networks. A specific aim will be developed to formulate the Information Gain Guided Population Initialization Scheme; develop an X shaped transfer function that transforms continuous space searching of wolf population into feature space search, by using the proposed X Shaped Transfer function; implement the proposed feature selection algorithm and combine this feature selection with support vector machine on the real world network traffic; also to carry out standard Grey Wolf optimization based feature selection and Compare the Selected Features quality among them by providing detection metrics for classification.

2. LITERATURE REVIEW

Feature Selection for Intrusion Detection Given their crucial role in classifier performance and computational expense, feature selection for intrusion detection is a hotly pursued research area. Feature selection in intrusions can be conducted at multiple levels such as selecting the relevant feature subsets with appropriate ranking techniques, while optimizing for computational efficiency along with high accuracy for all intrusion types (Nimbalkar&Kshirsagar, 2021). Information Gain and Gain Ratio combination was utilized in Nimbalkar and Kshirsagar (2021) for selecting the most important attributes for classifying Denial of Service (DoS) and Distributed DoS (DDoS) attacks and reduce the KDDCUP99 and BOT IOT feature subsets to 19 and 16 attributes respectively prior to training a JRip classifier, yielding accuracies of ~99.99%.

Kasongo and Sun (2020) employed filter-based feature reduction using XGBoost before training multiple classifiers on UNSW NB15 dataset (including support vector machines and artificial neural networks), and noted significant accuracy improvements after the redundant features were removed. Using the UNSW NB15 and KDD99 data, Khammassi and Krichen (2017) used a wrapper method coupling a GA with logistic regression to successfully detect intrusions using only 20 and 18 attributes, respectively. Based on mean decreased impurity Sharafaldin et al. (2018) select attack-specific subsets of features in the CICIDS2017 dataset to achieve accuracy results ranging from 77% to 98% using seven different classifiers. Hota and Shrivas (2014) also found that information gain combined with C4.5 classifiers could achieve accuracy results near 99.68% with merely 17 selected features. Bio-inspired Metaheuristic Algorithms to Search The Feature Space It is widely acknowledged that Bio-inspired metaheuristic algorithms provide a good technique to search a feature space, since they can mimic evolutionary behaviours and perform effectively in dynamic, high-dimensional search environments (Xiao Xue et al., 2024).

In the application of Artificial Neural Networks to classify botnet malicious traffic with NBaIoT dataset, a novel Local Global Best Bat Algorithm is utilized to perform simultaneous feature subset selection and hyper-parameter optimization by Alharbi et al. (2021). Khare et al. (2020) employed feature dimensional reduction using Spider Monkey Optimization before feeding the selected features to a deep neural network (evaluated against NSL KDD and KDD Cup 99 data). In another work by Natesan et al. (2017), parallelized selection based on a Hadoop platform with binary Bat Algorithm and a parallel Naive Bayes classifier was applied to the KDDCUP99 dataset.

To improve performance on the KDDCUP99, NSL KDD and UNSW NB15 dataset, Alazzam et al. (2020) incorporated a Pigeon Inspired Optimizer with sigmoid transfer function for binarization but found the algorithm suffers from premature convergence (local optimal). To model the features as a graph, the intelligent water drop algorithm was used by Acharya and Singh (2018), but encountered problems with computational cost as the dimension of the graph increased. Selected GWO Approaches for Intrusion Detection Numerous studies aim at the enhancement of GWO for Feature Selection. A modified binary GWO search technique (Alzubi et al., 2020) was suggested to calculate the position of the next wolf based on four leader positions instead of the three as in conventional method, thereby reducing wolf impact on each step of the process, with the modified technique achieved on average 81.56% accuracy (with SVM) on the NSL KDD dataset with slightly improved exploration and lower convergence rates due to reliance on random initialisation.

An attempt at improving GWO was also made by Alamiedy et al. (2020), by adopting multi-objective GWO with heuristic-based population initialization to incorporate both accuracy and dimensional reduction into the fitness function, a heuristic search strategy and resulting good reduction rates on the NSL KDD, albeit at a cost of high computation load. The hybridization of feature selection approaches like PSO, GA, and Firefly Algorithm with GWO and mutual information resulted in 90.119% and 90.484% accuracies (SVM and J48) on the UNSW NB15 dataset, respectively (Al Wajih et al., 2021). Another hybrid algorithm proposed in Al Wajih et al. (2021), combines GWO and Harris Hawks Optimization algorithm to address more effective exploration-exploitation trade-off. GWO was also combined with Particle Swarm Optimization, Genetic Algorithm, and Artificial Bee Colony algorithm by Al Tashi et al. (2019) in attempt to balance exploration and exploitation, with authors concluding in both cases that the GWO is still prone to get stuck into local optimum.

As we can see from all mentioned approaches, although the hybridization and ensembles approaches can address some of the shortcomings of the individual metaheuristic algorithms, they generally added complexity in their operation and increased the computational resource requirements. Existing GWO based feature selection methods for intrusion detection predominantly employed traditional sigmoid function for binarization which gives very limited exploration ability and also a limited convergence speed especially in highly dynamic environments such as Mobile Adhoc NET (MANET) traffic. Few researchers employed improved transfer function combined with information theory based initialisation which directly bias search toward good feature subsets in the initial stage of the feature search process, and therefore motivated the need to developing an XTF-GWO algorithm described herein, that combines an X shaped transfer function with information Gain seeded initialization to enhance the exploration/exploitation performance balance for binary feature selection on MANET intrusions, this approach will be illustrated in section 3, section 4 and section 5.

3. METHODOLOGY

3.1 Data Acquisition and Pre-processing

From the ITU-ML5G-PS-006 (2025), the large scale intrusion detection data set containing about 2.3 million records in seventy eight features based on flows and that describe network traffic flows with, regarding the data, some packet features, some traffic characteristics, the protocol information and even behavioural measures were used as data sets; every record is marked as normal flow and as a certain kind of attack and allows binary as well as multiclass evaluation to the proposed intrusion detection methods; to the pre processing phase only dynamic non deterministic values like source/destination IPs/ports, Record time were eliminated, so properties no deeply related to an attack are taken 15. In order to include values about the categorical features like PROTOCOL TYPE or SERVICE TYPE, the value was transformed in the corresponding integer number, all the features are also scaled to be included within the range [0, 1] thanks to the min-max normalization that let every feature contributes the same amount to the optimization task

3.2 Information Gain Guided Population Initialisation

Instead of completely random initialisation for the wolf population, XTF-GWO calculates the Information Gain of all the candidate feature attributes to select those that have the greater discrimination power. The information gain (IG) of attribute t is defined as

$$IG(t) = -\sum P(ci) \log P(ci) + P(t) \sum P(ci|t) \log P(ci|t) + P(t') \sum P(ci|t') \log P(ci|t') \qquad (1)$$

where ci represents the class labels, P(ci) is the probability of class i, and P(ci|t) and P(ci|t′) denotes the conditional probabilities of the class given the presence or absence of feature t. The population is then divided into two parts. A proportion of the population, governed by an injection ratio, is seeded using features with high Information Gain values according to

$$P(i) = 1, \text{ if rnd} < \text{Normalized IG}(i);\ \ 0, \text{ otherwise} \tag{2}$$

while the remaining wolves are initialised at random following

$$P(i) = 1, \text{ if rnd} > 0.5;\ \ 0, \text{ otherwise} \tag{3}$$

Where rnd is a uniform random number on zero-to-one range. This hybrid initialisation introduces a bias toward potentially promising regions of the search space without compromising the level of diversity necessary to ensure effective global exploration.

3.3 X Shaped Transfer Function for Binary Conversion

Since the Gray Wolf Optimization update equations produce continuous positional values, a transfer function is necessary to translate these continuous values into discrete decisions of feature selection. XTF-GWO is proposed to use a X-shape transfer function as shown in

$$XTF(X_{ij}) = \left| 1 / (1 + e^{(-X_{ij})}) - 0.5 \right| \times 2 \tag{4}$$

where Xij denotes the continuous position of wolf i along feature dimension j. The resulting probability governs the binary conversion rule

$$X_{i,t+1} = 1, \text{ if rand} < XTF(X_{i,t});\ \ 0, \text{ otherwise} \tag{5}$$

Here, rand represents the uniformly distributed random number and Xi,t+1 represents the update of the binary status for the feature. Different from the typically applied sigmoid transfer function, the X shaped equation results in a sharper symmetric probability curve near the zero points for the features, driving the wolves to make more certain decision of inclusion or exclusion of any particular feature, providing an equilibrium between the exploration and exploration search approaches.

3.4 Algorithm Design

The XTF-GWO scheme is made of 9 basic stages: first the population size, pop\size, and the maximum number of iteration, max\iter are initialized; then the wolf positions are constructed following the information gain guided scheme above; each wolf is mapped onto binary feature subset using X shaped transfer function; its fitness value obtained when passing it as a feature subset to Support Vector Machine is evaluated using classification accuracy measure. The three best fitted wolves are called Alpha, Beta,Delta,and other Omegas update their position around them as per standard Grey Wolf update equations. The transfer function is repeatedly applied in order to guarantee a binary feasibility during each stage, finally this process is iterated until the maximum iteration count, then the Alpha position becomes the best feature subset.

Table 1 Summarises The Algorithm In Pseudocode Form.

Step	Operation
1	Initialise population size N, maximum iterations MaxIter and injection ratio R
2	Compute Information Gain for every candidate feature

Step	Operation
3	Generate the initial wolf population using the hybrid initialisation scheme
4	Apply the X shaped transfer function to obtain binary feature subsets
5	Evaluate fitness of each wolf via Support Vector Machine classification accuracy
6	Identify Alpha, Beta and Delta wolves based on fitness ranking
7	Update wolf positions using the modified Grey Wolf equations
8	Reapply the X shaped transfer function for binary conversion
9	Repeat steps four to eight until MaxIter is reached, then return the Alpha position as the optimal feature subset

Table 1. Pseudocode for the XTF-GWO Feature Selection Algorithm

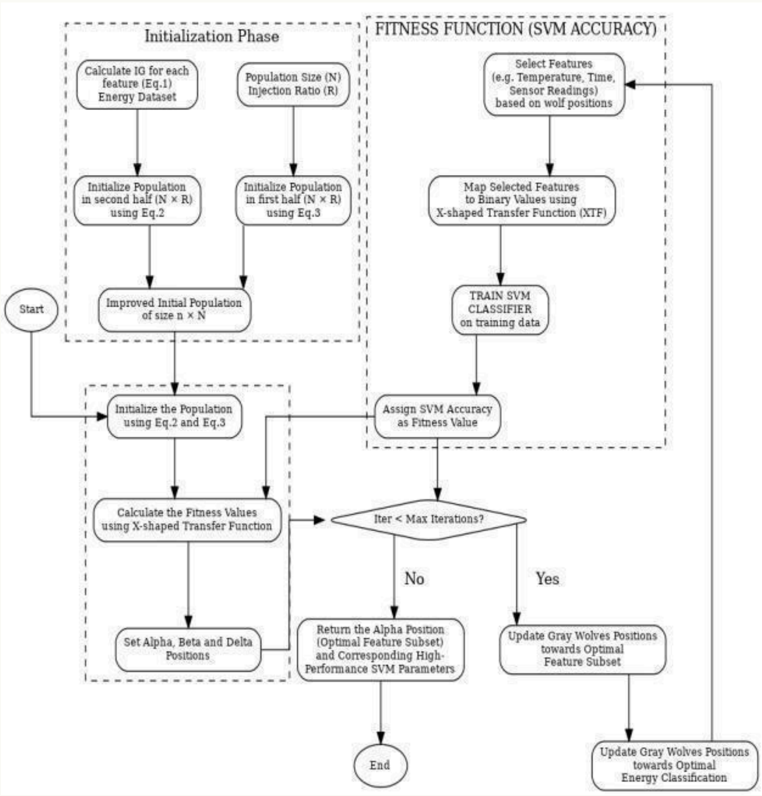

Figure 1. Flowchart of the XTF-GWO Feature Selection Procedure

3.5 Performance Evaluation Metrics

The quality of feature subsets generated by XTF-GWO was evaluated indirectly based on the classifier's (Support Vector Machine in this case) performance in terms of accuracy, precision, recall and F1 score. Accuracy represents the ratio of correct prediction among the total predicted value; precision represents the ratio of actual attack number correctly identified; recall represents the ratio of actual attack number among all of the predictions that it should contain actual attack; F1 represents the harmonic mean of precision and recall. The values are calculated based on those four components (True Positives (TP), True Negative (TN), False Positives (FP), and False Negatives (FN)) in a confusion matrix in four attack ratios 25%, 50%, 75% and 100%.

4. RESULTS

Table 2 summarizes the classification results with a feature subset extracted through the standard Grey Wolf Optimization and used as classifier in the Support Vector Machine algorithm. Table 2 shows that the performance gradually and progressively increases with an injection ratio that grows from 82.10 % of accuracy at 25% injection level, till 89.15% accuracy level at 100% injection level, in the same manner as precision, recall, and F1 score are concerned.

Injection Ratio	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
25%	82.10	81.50	80.80	81.15
50%	84.45	83.20	82.50	82.85
75%	87.30	85.90	85.10	85.50
100%	89.15	88.40	87.60	88.00

Table 2. Classification Performance Using Standard GWO Feature Selection

Table 3 shows the corresponding outcomes acquired through using these feature subsets selected by the proposed XTF-GWO algorithm. At an injection ratio of 25%, the developed algorithm attained the accuracy of 88.42 percent, which is still significantly greater than the best outcome acquired utilizing the standard algorithm at any injection ratio. Its overall performance achieved improvement as the injection ratio increased and obtained accuracy of 91.15 percent at an injection ratio of 50 percent and 75 percent. Moreover, accuracy improved to 96.82 percent, precision improved to 96.18 percent, recall increased to 95.93 percent, and F1-score improved to 96.05 percent at 100 percent injection ratio.

Injection Ratio	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
25%	88.42	87.54	86.91	87.22
50%	91.15	90.08	89.47	89.77
75%	91.15	90.08	89.47	89.77
100%	96.82	96.18	95.93	96.05

Table 3. Classification Performance Using XTF-GWO Feature Selection

For all injection ratios tested, the feature subsets generated by XTF-GWO returned a greater accuracy, precision, recall and F1 score than the equivalent subsets generated by the generic algorithm. For both scenarios, this difference in results grew in step with increase of the injection ratio. As noted previously, a levelling-off occurs in between fifty percent and seventy five percent: the feature set had likely already stabilized at what could be considered an optimum feature set and new samples did not produce an increase in accuracy due to the algorithm's convergence rather than stagnation.

5. DISCUSSION

The relative success of XTF-GWO over the standard method is likely to be due to the combined influence of the IG guided initialisation with the X shaped transfer function. The strategy of "seeding" several wolves with a subset of features previously identified as having significant discriminatory power helps the optimisation of the algorithm to begin more effectively in an area close to an ideal solution within the solution space; less time will be spent searching the remaining space to converge on a promising subset of features. This initial advantage of the algorithm is made significantly greater by the 'X' transfer function, the probability of choosing, or excluding, a specific feature rapidly approaching one or zero around a decision boundary, unlike the sigmoid function which will struggle and force the wolves into a "standoff". This behaviour enhances the exploration versus exploitation, allowing the algorithm to search wide areas of the feature space and then to refine promising solutions; it has the effect of preventing premature convergence into a local optimum which has been previously demonstrated in previous GWO based feature selection studies (Liu et al., 2023; Alzubi et al., 2020).

This advantage became most apparent at the highest injection ratio, where the richer depiction of the attack traffic enabled the optimisation algorithm to distinguish greater between the features that were useful to the prediction of attack traffic versus those that were redundant. Even at the lowest injection ratios, where the number of attack records is substantially smaller than either the overall network records or the benign records, there was still a large advantage over the standard approach, suggesting that our custom initialization strategy performs especially well under data limited circumstances such as those which exist in typical MANETs where attack records account for only a tiny fraction of overall network traffic. The similarities in performance between fifty and seventy five percent suggest that the selected features generalize well once sufficient relevant examples have been utilized, and do not rely upon a continuously increasing pool of attack examples.

The present results are consistent with the general findings of many authors, and suggest that the effective use of optimised transfer functions along with the initialisation strategy has the potential to enhance wrapper based feature selection significantly (Alharbi et al., 2021; Alamiedy et al., 2020). What is encouraging is that the method developed is fully self-sufficient and does not create additional architectural overhead when compared with, for instance, fully hybrid metaheuristic approaches that attempt to blend, say, GWO and theParticle Swarm Optimisation, or the Harris Hawks Optimisation algorithm(Al Wajih et al., 2021; Al Tashi et al., 2019), yet still achieve more or less equivalent gains. This demonstrates the effectiveness of single algorithm modification over large-scale hybridisation efforts which can increase both implementation and computational requirements significantly, an issue that should not be disregarded in the constrained MANET environment.

6. CONCLUSION AND RECOMMENDATION

This paper describes the implementation and assessment of a Modified Grey Wolf Optimization algorithm called XTF-GWO, which mitigates the unsuitability of the standard GWO for binary feature selection by employing an X shaped transfer function and Information Gain based population initialisation technique. The algorithm is tested in conjunction with a Support Vector Machine classifier using four attack injection ratios and the assessment proves XTF-GWO generates more discriminative features subsets than the standard counterpart across all conditions; obtaining improvements between 5 and 8 percentage points and reaching 96.82 percent accuracy when using full injection. These results suggest a simple to implement and efficient approach using a sharper, data informed, transfer function and a focused initialisation method is available to enhance feature selection techniques used within intrusion detection systems for Mobile Ad Hoc Networks.

The proposed XTF-GWO is recommended to be considered by network security researchers and practitioners to apply as a pre-processing step into a wrapper-based intrusion detection pipeline, especially where limitations of computational and energy exist. Future works will verify the performance of the transfer function combined with other meta-heuristic optimisers besides WOA and classifiers other than SVM classifiers. The proposed work will also assess the proposed approach in terms of other benchmark datasets and network environments, such as vehicular Adhoc Network and wireless sensor networks, in order to identify the generality.

References

Acharya, N. and Singh, S. (2018) An IWD based feature selection method for intrusion detection system. *Soft Computing*, *22*, 4407 to 4416.

Al Tashi, Q. et al. (2019) Binary optimization using hybrid grey wolf optimization for feature selection. *IEEE Access*, *7*, 39496 to 39508.

Al Wajih, R. et al. (2021) Hybrid binary grey wolf with harrishawks optimizer for feature selection. *IEEE Access*, *9*, 31662 to 31677.

Alamiedy, T.A. et al. (2020) A hybrid feature selection approach for intrusion detection based on grey wolf optimizer. Journal of Ambient Intelligence and Humanized Computing.

Alazzam, H., Sharieh, A. and Sabri, K.E. (2020) A feature selection algorithm for intrusion detection system based on Pigeon Inspired Optimizer. *Expert Systems with Applications*, *148*, 113249.

Alharbi, A. et al. (2021) Local global best bat algorithm for neural network based botnet detection. *Electronics*, *10*(11), 1341.

Alzubi, Q.M. et al. (2020) Modified binary grey wolf optimizer for feature selection in intrusion detection. IEEE Access.

Baird, C. et al. (2024) Security threats and detection in Mobile Ad Hoc Networks. Conference proceedings.

Devika, R. et al. (2022) A review of Mobile Ad Hoc Network characteristics and applications.

Hota, H.S. and Shrivas, A.K. (2014) Decision tree techniques applied on NSL KDD data and its comparison with various feature selection techniques. Advanced Computing, Networking and Informatics, 1, 205 to 211.

Hussain, S. and Fathimah, F. (2024) Intrusion detection systems for Mobile Ad Hoc Networks: a review.

Kasongo, S.M. and Sun, Y. (2020) Performance analysis of intrusion detection systems using a feature selection method on the UNSW NB15 dataset. *Journal of Big Data*, *7*, 105.

Khammassi, C. and Krichen, S. (2017) A GA LR wrapper approach for feature selection in network intrusion detection. *Computers and Security*, *70*, 255 to 277.

Khare, N. et al. (2020) SMO DNN: spider monkey optimization and deep neural network hybrid classifier model for intrusion detection. *Electronics*, *9*(4), 692.

Liu, Z. et al. (2023) Anomaly detection on IoT network intrusion using machine learning.

Mirjalili, S., Lewis, A. and Mirjalili, S.M. (2014) Grey Wolf Optimizer. *Advances in Engineering Software*, *69*, 46 to 61.

Natesan, P. et al. (2017) Hadoop based parallel binary bat algorithm for network intrusion detection. *International Journal of Parallel Programming*, *45*, 1194 to 1213.

Nimbalkar, P. and Kshirsagar, D. (2021) Feature selection for intrusion detection system in Internet of Things environment using information gain and gain ratio. *ICT Express*, *7*(2), 177 to 181.

Sharafaldin, I., Lashkari, A.H. and Ghorbani, A.A. (2018) Toward generating a new intrusion detection dataset and intrusion traffic characterization. Proceedings of ICISSP.

Theng, D. and Bhoyar, K.K. (2024) Feature selection techniques for machine learning: a survey of more than two decades of research. Knowledge and Information Systems.

Xiao xue, Y. et al. (2024) Bio inspired metaheuristic algorithms for engineering optimization problems.