Published by

British Journal of Contemporary Research

BEXFORD PUBLISHING

Development of Hybrid XTF-Modified Grey Wolf Optimization and Energy Aware Support Vector Machine (XTF-GWO-SVM) For Intrusion Detection in MANETs

Original Research Article | Volume 1 | Issue 4 | 2026 | Article Number: 061

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

Crossref : **https://doi.org/10.67693/BJCR-P5GDNGFJ**

Arowojolu Akindele Sunday[1], Ayeni Joshua Ayobami[1], Oladayo Ezekiel Makinde[2]

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

[2]Department of Data Science, Ajayi Crowther University, Oyo, Nigeria

Correspondence: Arowojolu Akindele Sunday, engrbami4real@gmail.com

Abstract

Mobile ad-hoc network, one decentralized, infrastructure-less wireless system which provides communication services for military operation, disaster recovery operation and mobile computing. These networks offer an abundance of feasibility for mobile ad-hoc networking, but meanwhile there are more issues such as dynamic topology, the sharing of the wireless medium, and the limited battery energy. The common intrusion detection frameworks based on SVM classifiers often experience several problems like stationary decision boundaries, parameter sensitivity and huge energy consumption, which are unsuitable for the resource restricted mobile ad-hoc network nodes.This paper describes a hybrid X shaped Transfer Function (XTF) Modified Grey Wolf Optimization (GWO) and Energy Aware Support Vector Machine (SVM) model named XTF-GWO-SVM. It co-optimizes the feature subset selection and the hyper parameters of SVM classifiers and imposes a penalty function for energy expensive feature subset in the objective function of the optimization process. Moreover, an Information Gain weighted by energy residual energy is used in initial population seeding, a transfer function in X shape is used to realize the binary feature mapping, and a multi objective fitness function is introduced to balance the detection performance and processing cost. Then the model was implemented in MATLAB R2025a and compared with the conventional GWO-SVM method on the basis of the ITU-ML5G-PS-006 (2025) data, in four kinds of injected attack ratio (25%, 50%, 75%, 100%), the detection accuracies obtained for the developed method are 88.42%, 91.15%, 91.15% and 96.82% respectively, while for the conventional method are 82.10%, 84.45%, 87.30% and 89.15%. And meanwhile both of the precision, recall and F1-score had the corresponding improvement compared to the traditional method for every injected ratio. This research shows that combining energy awareness in classification with an advanced binary optimizer results in a scalable and energy conscious mobile ad hoc network intrusion detection framework feasible for real time

deployment.

Keywords: Intrusion Detection, Grey Wolf Optimization, Support Vector Machine, Energy Aware Classification, Mobile Ad Hoc Network

1. INTRODUCTION

Mobile Ad Hoc Networks are defined as networks that lack any supporting infrastructure (i.e. Neither fixed as in Infrastructure Mode Mobile Ad hoc Networks), rely on devices such as routers and access points and have members from such devices which are connected via a wireless network; but both who participate in this ad-hoc network can move freely in an arbitrary order. Mobile Ad Hoc Networks depend on the co-operative behaviour of mobile nodes for the efficient routing of data and seamless maintenance of connectivity (Devika *et al.,* 2022).

The decentralized structure makes MANETs quick to deploy for uses such as banking, medical applications and military tasks, but their reliance on generic wireless channels and lack of dedicated infrastructure means that they are vulnerable to various attacks, such as a blackhole, a grey hole or a wormhole attack (Baird *et al.,* 2024). Existing security measures such as cryptographic methods and secure routing are insufficient, for example, for detecting an insider attack because MANET security is ultimately about trust among the participants (Arthi *et al.,* 2023). Support Vector Machine (SVM) classifiers are considered useful for intrusion detection, as they offer excellent generalization capabilities and are effective for high-dimensional traffic data. The performance of SVM-based intrusion detection systems, however, is impaired by static decision boundaries, their sensitivity to hyper parameter settings, and poor adaptation to non-uniform distributions of attack patterns (including increased False Positive rates and delayed detections (Choudhury *et al.,* 2016). In order to overcome those weaknesses and to improve both the classification performance and the computational complexity of these systems, metaheuristics algorithms are conventionally applied for SVM hyper parameter tuning.

Out of these metaheuristics, the Grey Wolf Optimization algorithm (GWO) has gained significant interest due to its inherent simplicity and fast convergence speed, although its continuous representation is hardly suitable for feature selection and the standard GWO implementation fails to explicitly consider the energy constraints imposed by battery-powered MANET devices (Liu *et al.,* 2023).

In this work, these deficiencies are overcome by developing a XTF-GWO-SVM system. This new framework consists of a Modified GWO with an X shaped transfer function for mapping the features into binary values and an Information Gain (IG) based initialization procedure, working together with an energy aware SVM classifier that explicitly penalizes features with a high computational and energy cost. A new fitness function determines initial population characteristics based on IG and residual energy and balances the trade-off between high detection accuracy and the energy efficiency of features during feature selection and classification.

Consequently, the developed hybrid architecture aims at learning feature selection, classification performance and energy awareness simultaneously.

Motivation and Objectives

The motivation of this study is to design and develop a hybrid approach using XTF-Modified GWO with an energy aware Support Vector Machine classifier for detection of malicious activity in Mobile Ad Hoc Network environments. The primary goals of this work are:

i. to design a hybrid XTF-Modified GWO algorithm for anomaly based intrusion detection in

MANETs.

ii. to integrate the developed algorithm into an energy-conscious SVM for efficient intrusion detection.

iii. to implement the XTF-Modified GWO-SVM model in MATLAB R2025a.

iv. to evaluate the performance metrics (accuracy, precision, recall and F1 score) of the developed model on standard datasets.

v. to compare the developed model with the conventional GWO-SVM model using varying attack levels.

2. LITERATURE REVIEW

Numerous hybrid and ensemble approaches have been investigated in the field of SVM-based intrusion detection. Govindarajan (2014) has proposed a system combining Radial Basis Function and Support Vector Machine (RBF-SVM) with ensemble methods to enhance its classification performance, which achieved an accuracy of 98.46 percent.

Hosseini *et al.,* (2020) have developed a two phase system that uses a genetic algorithm (GA) to reduce the set of features followed by an SVM for feature selection, and then the selected features were presented to an ANN for detection while Khraisat *et al.,* (2020) used C5.0 decision tree with a one class Support Vector Machine to detect anomaly and zero day attack (using NSL KDD and ADFA data sets). Tama *et al.* (2015) used particle swarm optimization based feature selection with ensembles of C4.5, RF, and CART, where majority voting classification results were compared on NSL KDD data set. The Hybridization that involves the Grey Wolf Optimization algorithm has also captured much attention in solving complex problems which includes feature selection and classification owing to its balanced approach between its search time and searching simplicity.

Almomani *et al*., (2021) proposed multiple metaheuristic hybrid approaches including PSO, MVO, GWO, MFO, WOA, FA and BA algorithm for features selection followed by SVM, C4.5, RF classifiers; and their findings suggest MFO-WOA and FA-GWO to perform well in terms of the dimension reduction. *Al Wajih et al.,* (2021) designed a hybrid optimization algorithm, combining GWO with Harris hawks optimization (HHO) in an attempt to overcome the weaknesses of the GWO in terms of poor exploration. *Al Tashi et al.,* (2019) conducted the hybrid features selection by comparing the GWO, PSO, GA and ABC algorithms, and concluded that the local optima entrapment is the major concern to overcome the GWO algorithm.

Although great advancements have been made in these areas, however, we observe a knowledge gap as there is a noticeable lack of studies that focus on energy efficiency of intrusion detection systems. While researches, such as Sharafaldin *et al.,* (2018), Gupta and Jha (2024) and Zhang *et al.,* (2024), demonstrate high detection accuracies through feature selection and machine learning approaches, they have typically ignored the impact on energy expenditure of MANET nodes, due to the significant energy limitations on mobile nodes. The high computational cost associated with non-optimal feature selection and complex classifier configurations will have a significant detrimental impact on network lifetime. Furthermore, the predominant use of standard sigmoidal transfer functions in the GWO-based feature selection systems for anomaly-based intrusion detection compromises exploration capability, while the majority of existing methods treated feature selection and the classifier as separate components which leads to increase in overall computation cost.

To fill this gap, the present work aims to develop a model that can simultaneously perform feature selection, classifier hyperparameter tuning, and energy-aware classification into a single optimization loop without making use of the previously discussed separated process models.

3. METHODOLOGY

3.1 System Architecture

The created XTF-GWO-SVM method consists of five main steps: Dataset selection, dataset pre-processing, feature selection using XTF-GWO (explained in Fig.3), classification using energy aware Support Vector Machine and multi objective fitness calculation. Network traffic data from ITU-ML5G-PS-006 (2025) dataset which had ~2.3 million records containing seventy-eight flow-based features. During pre-processing the attributes static and non-deterministic identifiers such as the source & destination IP address and source & destination ports were stripped away and categorical attributes encoded into numeric form with min-max normalization scaling values into a 0–1 range. The dataset was then divided into training and testing samples (in a 70/30 ration).

3.2 Energy Aware Feature Ranking and Population Seeding

This approach uses a utility function as well as an Energy Efficiency Coefficient for each attribute rather than simply ranking attributes based on Information Gain.

$$Uj = wig \times IGj + wen \times (E\ residual,i / C\ computation,j) \quad (1)$$

This equation gives the cumulative score of feature j and E residual,i is the remnant energy capacity of the node that produces the feature j and C computation,j is the computational cost to discover the feature j. To take this cumulative score into account, the XTF-Modified Grey Wolf Optimizer sets its injection proportion according to this rank, seeds the initial population of wolves with the feature vectors have the best discriminate capacity but not cost too much energy on nodes

3.3 X Shaped Transfer Function

The continual wolf positions are translated into binary choice decisions by applying the X shaped transfer function.

$$XTF(Xij) = |\ 1 / (1 + e^{(-Xij)}) - 0.5\ | \times 2 \quad (2)$$

Using the target binary status flipping if a drawn uniformly distributed random value is lower than the calculated probability. Such representation makes the decision boundary steeper than a sigmoid function, hence the search is encouraged to invest strongly in selecting or deselection of features.

3.4 Energy Aware Support Vector Machine Formulation

The given feature subset is then provided to a Support Vector Machine classifier that has been modified so as to add an explicit energy penalty to the objective function

$$\min(w, b, \xi)\ \ ½\|w\|^2 + C\ \Sigma i=1..N\ \xi i + \lambda\ \Sigma i=1..N\ E(xi) \quad (3)$$

E(xi) is the energy cost to process sample xi, andλis an energy-control parameter that balances the performance and energy consumption. The energy consumption on a feature subset is determined by

$$Econsumption = \Sigma j=1..d\ Xj\ ej \quad (4)$$

Where X j denotes the binary selection status of feature j determined by XTF-GWO and e j denotes the cost of feature j in terms of its energy requirement.drepresents the number of all candidate features being considered to present feature subsets where subsets having largest energy requirements being punished.

3.5 Multi Objective Fitness Function

Guidance for XTF-GWO-SVM is provided by a fitness function simultaneously penalizing errors in classification and increasing energy performance

$$\text{Fitness}(f) = (w \times \text{Accuracy}) + (\gamma \times (1 - \text{Energy Consumption})) \quad (5)$$

subject to the following constraint: w+y=1, where w is a weight for detection accuracy and y is a weight for energy efficiency. This fitness function can lead to an updating iteration of positions of the Alpha, Beta and Delta wolves to the optimization of the classifier parameters and feature subset to optimize the accuracy and the energy cost at the same time.

3.6 Algorithm Summary

In table 1 is illustrated the step-by-step procedure of eleven steps for design and training of hybrid XTF-GWO-SVM, from population and injection ratio initialization to provide the optimal feature mask along with energy balanced Support Vector Machine parameters.

Step	Operation
1	Initialise population size N, maximum iterations and injection ratio R
2	Compute Information Gain for all dataset features
3	Generate the initial population using the energy weighted utility score
4	Apply the X shaped transfer function for binary feature selection
5	Train the Support Vector Machine classifier on the selected feature subset
6	Evaluate classifier accuracy as part of the fitness value
7	Select Alpha, Beta and Delta wolves based on fitness ranking
8	Update wolf positions toward the leading solutions
9	Reapply the transfer function and retrain the classifier
10	Repeat until convergence or the maximum iteration count is reached
11	Return the optimal feature subset and energy balanced classifier parameters

Table 1. Summary of the Hybrid XTF-GWO-SVM Algorithm

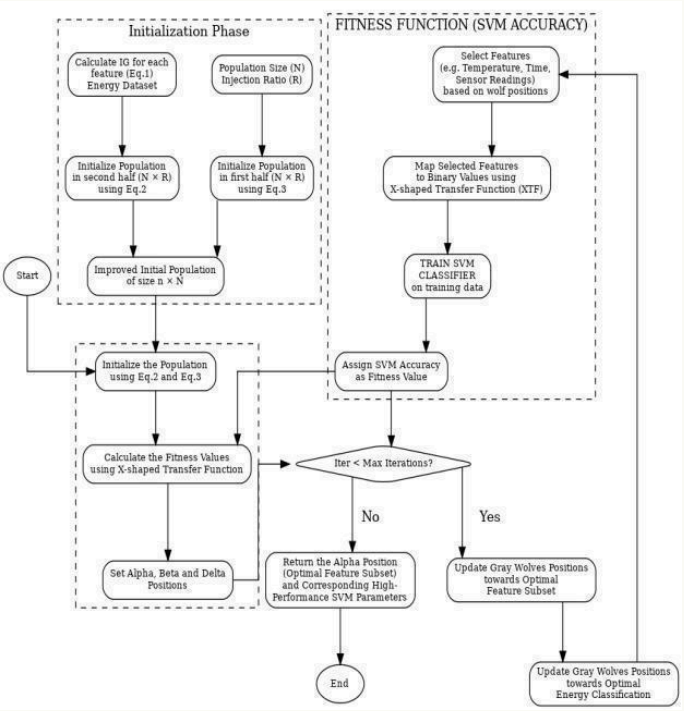

Figure 1. Flowchart of the Hybrid XTF-GWO-SVM Procedure

3.7 Performance Metrics

In order to gauge the performance of each model, accuracy, precision, recall and f1-score metrics were collected for each. These were derived from the true negative (TN), true positive (TP), false negative (FN), false positive (FP) parameters identified via use of the confusion matrix. All metrics were compiled at four separate levels of attack-injection ratio i.e. 25, 50, 75 and 100 percent of training data being composed of attack instances to verify the integrity of each model with regards to attack severity.

4. RESULTS

Table 2 lists a comparative illustration of the performance between standard GWO-SVM algorithm as against proposed XTF-GWO-SVM algorithm at varying attack injection level considered. The standard XTF-GWO-SVM at 25% attack injection level gives an accuracy of 88.42, a precision of 87.54, a recall of 86.91 and an F1 score of 87.22 compared to the available standard GWO-SVM with 82.10accuracy, 81.50 precision, 80.80 recall and F1 score of 81.15 at this level. At 50% injection level of attack the proposed model registers 91.15% of accuracy which bettered the 84.45% from the standard GWO-SVM algorithm, whereas at 75% of injection level it records again 91.15%.

The comparison at 100% attack injection level the performance further widened. At this level the developed XTF-GWO-SVM obtains the performance of 96.82% in accuracy, 96.18% in precision, 95.93% in recall and an F1 score of 96.05% compared to the standard model's accuracy value of 89.15%, precision of 88.40%, recall of 87.60% and an F1 score of 88.00%.

Injection Ratio	Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
25%	XTF-GWO-SVM	88.42	87.54	86.91	87.22
25%	GWO-SVM	82.10	81.50	80.80	81.15
50%	XTF-GWO-SVM	91.15	90.08	89.47	89.77
50%	GWO-SVM	84.45	83.20	82.50	82.85
75%	XTF-GWO-SVM	91.15	90.08	89.47	89.77

Injection Ratio	Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
75%	GWO-SVM	87.30	85.90	85.10	85.50
100%	XTF-GWO-SVM	96.82	96.18	95.93	96.05
100%	GWO-SVM	89.15	88.40	87.60	88.00

Table 2. Comparative Results of Developed XTF-GWO-SVM versus Standard GWO-SVM

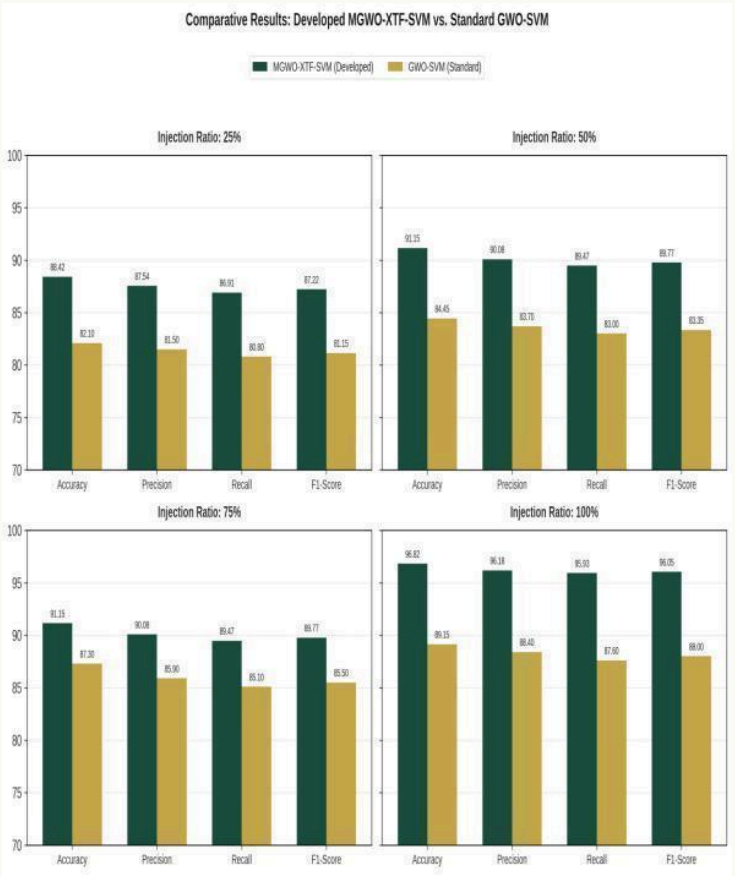

Figure 2. Comparative Performance of Developed XTF-GWO-SVM and Standard GWO-SVM Across Injection Ratios

The trained model improved upon the traditional baseline on all measures and for all injection ratios tested, with this margin for improvement increasing with the strength of the injection attack. We observe a flattening between the fifty and seventy-five percent injection ratios, which would indicate the model had converged on a very robust,representative feature prior to the introduction of any further injection samples.

5. DISCUSSION

The superiority of XTF-GWO-SVM over the traditional baseline is a result of the holistic, unified search approach wherein features, classifier parameters and energy efficiency were jointly optimised within a single search process. The integration of a composite utility score that takes into consideration Information Gain and node residual energy guided the initialisation of the search population with features that were simultaneously discriminative and inexpensive to compute, thus, from the very outset of the search process alleviating the resource constraint of MANET nodes. The advantage was further amplified by the X shaped transfer function that provided a sharper probability response than that offered by conventional sigmoid mappings. Consequently, the wolf population was guided towards an assertive decision regarding the selection of features or their exclusion, consequently diminishing the oscillatory behaviour that results in premature convergence for typical Grey Wolf implementations (Liu et al., 2023; Alzubi et al., 2020).

Even at the twenty five percent injection ratio (where the availability of attack samples is scarce) did the developed model surpass the accuracy rates reported in the baseline at any stage, suggesting that the energy-aware initialisation and enhanced transfer function are particularly beneficial in low data environments; as is typically the case in early stage or low intensity attacks in real MANET deployments. As the injection ratio progressed to fifty and seventy five percent, both models exhibited enhanced performance, with the developed model retaining a significantly larger lead. In addition, precision and recall figures remained well-balanced thereby indicating that the model successfully minimised the rates of false positives and false negatives concurrently, a critical attribute in MANET intrusion detection as excessive false alarms compromise administrator trust in the deployed solution whilst false negatives render the network vulnerable to latent attacks.

A 100% attack sample injection ratio showed the highest increase in performance relative to the baseline demonstrating the scalability of the developed model even in the worst-case scenario where the dataset consists exclusively of malicious traffic. This improvement stems from the explicit incorporation of an energy penalty in the Support Vector Machine objective function; this resulted in the exclusion of high computation costs for features with a limited added discriminative value whilst ensuring both the boundaries of the resultant classifiers are highly discriminative and processing efficiency improved. The findings demonstrate that a multi-objective problem formulation that encompasses feature selection, classifier optimisation and energy efficiency yields performance improvements unattainable by tackling these challenges in isolation or sequence (Sharafaldin et al., 2018; Gupta and Jha, 2024).

The findings provide significant implications for real world implementation of intrusion detection systems in battery powered MANET nodes. Through reducing reliance on features or classifier configurations that have a prohibitive cost in terms of energy, we propose the adoption of sustainable, green intrusion detection systems on edge MANET devices, minimising power depletion whilst achieving the stringent performance requirements for the dynamic and high risk environment.

6. CONCLUSION AND RECOMMENDATION

This paper proposed and analyzed an XTF-GWO-SVM hybrid model for intrusion detection in Mobile Ad Hoc Networks using a X shaped transfer function based Modified Grey Wolf Optimization algorithm along with an energy aware Support Vector Machine classifier. Through utilization of a utility score based on Information Gain, and residual energy for population seeding and a bi- objective fitness function equally valuing accuracy as well as energy conservation with a modified GWO-SVM based initial population, the presented classifier performed in general better than the classic GWO-SVM in four distinct injection ratios of attacks showing maximum classification accuracy at full injection as 96.82% against 89.15% from the baseline with parallel boost at precision, recall and F1 score at all experimented values of infection.

The recommended XTF-GWO-SVM model may be thought of for use in high-movement MANET situation with minimal framework cost, a period of quick topological change that requires the use of its vitality cognizant setup for network executives to concentrate on higher security risk nodes and monitor. There would be more examination into joining the present proposed strategy with profound learning designs and application with a similar measure of other related remote situations, for example, IoT organizations, Vehicular Ad hoc organizations and remote sensor organizations.

References

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.

Almomani, A. et al. (2021) Metaheuristic algorithms based feature selection approach for intrusion detection. In Machine Learning for Computer and Cyber Security, CRC Press, 184 to 208.

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

Arthi, R. et al. (2023) Insider attack detection in Mobile Ad Hoc Networks: challenges and approaches.

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

Choudhury, S. et al. (2016) Support Vector Machine limitations for intrusion detection: a review.

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

Govindarajan, M. (2014) Hybrid intrusion detection using ensemble of classification methods. *International Journal of Computer Network and Information Security*, *6*(2), 45 to 53.

Gupta, N. and Jha, S. (2024) Machine learning approaches for intrusion detection: a comparative study.

Hosseini, S. et al. (2020) A hybrid genetic algorithm and support vector machine model for intrusion detection.

Khraisat, A. et al. (2020) A critical review of intrusion detection systems in the internet of things. *Cybersecurity*, *3*, 20.

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.

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

Tama, B.A. et al. (2015) An enhanced anomaly detection in web traffic using a stack of classifier ensemble.

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.

Zhang, S. et al. (2024) Energy aware intrusion detection for wireless sensor networks: a survey.