International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

# Intrusion Detection in Wireless Sensor Networks using Support Vector Machine with Grasshopper Optimization Algorithm

**C. Murugesh[1], Dr. S. Murugan[2]**

[1]Assistant Professor, Programmer,Department of Computer and Information ScienceAnnamalai University, Annamalai Nagar
Email: *78murugesh[at]gmail.com*

[2]Assistant Professor, Dr. M.G.R. Government Arts and Science College for Women, Villupuram.
Email: *smuruganmpt79[at]gmail.com*

**Abstract:** ***Wireless Sensor Networks (WSNs) serve as the backbone for numerous critical applications, including environmental monitoring, industrial automation, and healthcare. However, the inherent vulnerabilities of these networks to security threats necessitate robust Intrusion Detection Systems (IDS). Traditional rule-based IDSs often fall short of addressing the evolving nature of attacks in WSNs. This research presents an innovative approach that combines the power of Support Vector Machine (SVM) classifiers with the Grasshopper Optimization Algorithm (GOA) for effective intrusion detection (SVMGOA-ID) technique in WSNs.The SVMGOA-ID approach harnesses SVM, a well-established machine learning technique known for its proficiency in binary classification tasks. SVMs are trained to distinguish between normal network behavior and intrusion attempts, learning intricate patterns from a labeled dataset. However, the success of SVMs is highly dependent on appropriate parameter settings, and suboptimal choices can lead to reduced detection accuracy.To address this challenge, the Grasshopper Optimization Algorithm (GOA) simulated by the natural behavior of grasshoppers in search of optimal foraging spots, is introduced for parameter optimization. The GOA efficiently explores the parameter space of SVM models, seeking the ideal configuration that maximizes intrusion detection accuracy. Comprehensive experiments are conducted using benchmark datasets, evaluating the efficiency of the SVMGOA-IDmethodology in detecting various intrusion types.***

**Keywords:** Wireless Sensor Networks;Support Vector Machine; Intrusion Detection Systems; Grasshopper Optimization Algorithm

## 1. Introduction

Wireless sensor networks (WSNs) are not same as the standard computer network, however, it interconnects sensor networks through wireless connections without a centralized control network [1]. This can be similar to distributed transmission that adjacent nodes that arecontrolled by each node in a system. It has developed and is vulnerable to any attacks in a suitable atmosphere [2]. It is owing to extensive Internet use and numerous security difficulties that arise in different DoS forms. It is the major problem of every network security problem as it produces larger amount of data traffic to utilize entire allocated system sources and deactivates the transmission connection by stopping server from processing authorized requisitions for clients to perform transactions [3]. The DDOS practicable computational sources are the processing part and network bandwidth of memory and computers. Its capacity is compressed by the transmission channels [4]. If DDOS can be initiated, a massive quantity of unacceptable traffic data overflowed the allocated channel into a transmission link. Occasionally, attack targets to the network nodes protect a massive quantity of undesirable requests with all communication channels to the node [5]. Fig. 1 portrays the architecture of IDS.

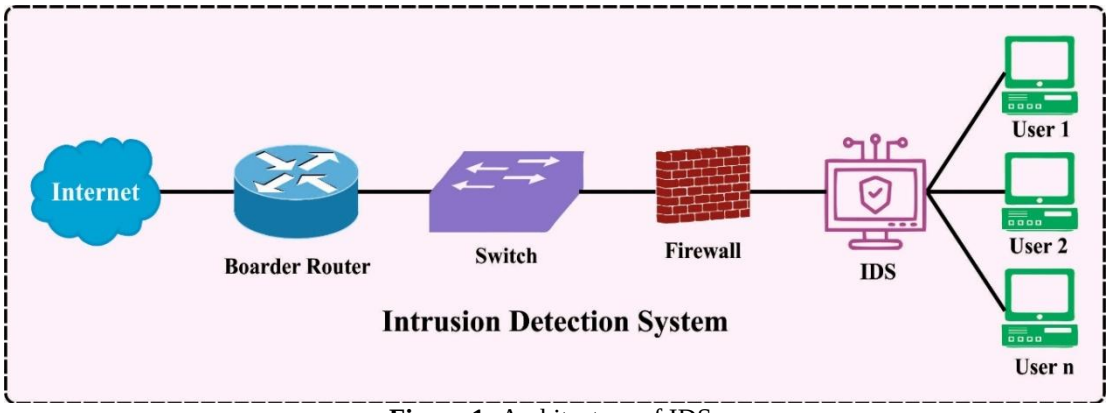


**Figure 1:** Architecture of IDS

The Intrusion Detection System (IDS) is presented by Denning in 1987 then, with numerous enhanced methods and developments imposed on it [6], IDS was demonstrated as an efficient technology to face cyber-attacks. IDS is categorized into two categories namely host- and network-based on position of IDS system in the networks [7]. A host

based IDS monitors and detects application tasks for devices processing on system and network configurations. An advantage of a host based IDS has been analyzed in previous databases for detecting savvy intruders, which can be utilized in advanced methods and appears hard to detect in actualtime [8]. Nevertheless, it contains a few drawbacks which are processing time, storage on the hosts, other resources, and memory consumption. It can detect a large network with minimum use, simultaneously, it is an optimum-grained identification ability [9]. DL methods for ID are recently analyzed by several researchers. The huge volume of network data produced ID problems likable to DL approaches [10].

Fu et al. [11] developed a DDQN technique for arrangement position depending on Geography Position Information (GPI). GPI can prevent the complex computational procedure of channel state data. The DDQN technique could be presented for attaining the functional relation among GPI and the optimum UAV deployment position. Also, the incorporation of CNN-LSTM methods.In [12], the authors presented a hybrid method in that the nodes have been collectively clustered to create the CDS thus, the data transmission is increased. Packet distribution is executed depending on the CDS of nodes and unsuitable network failure to maintain similar node waking as frequently can be prevented.

Devi et al. [13] recommended novel rule-based IDS, which contains a count of security methods. This technique uses a set of rules produced by the RF method. These created rules are dependent upon features extraction from WSNs data comprising hop count, energy consumption, and packet size. Integrated rule-based methods and ML techniques could be employed for enhancing the accuracy and effectiveness of intrusion detection approaches.Hemanand et al. [14] designed an intelligent IDS technique through the Cuckoo Search Greedy Optimization (CSGO) and Likelihood-SVM (LSVM) approaches. Firstly, the database pre-processing is carried out for normalizing the features. The optimum feature sets were chosen and provided to the input of CSGO method. Secondly, the LSVM-based ML classification method was employed to predict the classified label.

Umamaheshwari et al. [15] introduced efficient IDS for classification of attacks in a WSN employing ML approach. A baseline technique has been designed by features extraction from WSN-DS database applied a DT method. For minimizing the time for attack identification, an FS employing Statistical Analysis, Fisher Score, and d Correlation Score by Kruskal-Wallis (KW) test, Relief, and MRMR techniques are analyzed.Srivastava and Bharti [16] recommended a Hybrid Model of One-class SVM and Isolation forest (HMOI) technique that is a 'Classification + Classification' framework. It can be 2 important stages. The first stage overcomes the problem of unlabelled data that has major popularity in real-time database of WSNs and transforms it into labelled data. The second stage has been determined for performing anomaly detection.

This research presents an innovative approach that combines the power of Support Vector Machine (SVM) classifiers with the Grasshopper Optimization Algorithm (GOA) for effective intrusion detection (SVMGOA-ID) technique in WSNs. The SVMGOA-ID approach harnesses SVM, a well-established ML technique known for its proficiency in binary classification tasks. SVMs are trained to distinguish between normal network behavior and intrusion attempts, learning intricate patterns from a labeled dataset. However, the success of SVMs is highly dependent on appropriate parameter settings, and suboptimal choices can lead to reduced detection accuracy. To address this challenge, the GOA simulated by the natural behavior of grasshoppers in search of optimal foraging spots, is introduced for parameter optimization. The GOA efficiently explores the parameter space of SVM models, seeking the ideal configuration that maximizes intrusion detection accuracy.

## 2. The Proposed Model

In this study, we have focused and development of the SVMGOA-ID technique in WSNs. The main purpose of SVMGOA-ID technique contains two phases namely SVM-based feature selection and hyperparameter tuning using GOA.

### 2.1 Feature selection-based SVM

In this stage, the SVMs are highly dependent on appropriate parameter settings, and suboptimal choices can lead to reduced detection accuracy. During the labeled database$D$ with $N$instances, the labels (y) are binary, taking a value of both 1 and$-1$ [17]. The feature vector $(x_i)$ is a $n$-dimension vector that signifies the amount of accessible features and is determined by Eq. (1).

$$D = \{(x_i, y_i) | x_i \in R^n, y_i \in \{-1,1\}\}_{i=1}^{N} \quad (1)$$

The optimum hyperplane is defined by formula$f(x) = w \cdot x + b$, with $x$ as input, $w$ the feature co-efficient, and $b$implies the bias. The purpose is to minimalize$\|w\|^2$butadequatelimitations (Eq. (2)), purpose for maximizing the margin among the hyperplane as well asneighboringinstances in 2-classes data. The SVM approach balances decreasing misclassifications and determining a hyperplane with important margin, dependent upon the elected kernel function (for instance, polynomial, linear, or RBF).

$$\min\left(\frac{1}{2}\|w\|^2 + C\sum_{i=1}^{N}\xi_i\right)$$
$$Subject\ to: \begin{cases} y_i(w \cdot x + b) \geq 1 - \xi_i i = 1, \ldots, N \\ \xi_i \geq 0 \end{cases} \quad (2)$$

whereas $\xi_i$refers to the slack variable to evaluate the distance amount of the misclassified and hyperplane instances with penalty co-efficient (C). The KuhnTucker statehas beenchangedas a dual Lagrangian problem by establishing Lagrangian multipliers for limitations of the problems(Eq. (2)). The purpose is to evaluate the difference $(\xi_i)$among the hyperplane as well as incorrectly locatedinstances, and resolve the problem utilizing the transformed Lagrangian dual formulation:

$$\min \sum_{i=1}^{N}\alpha_i - \frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N} y_i\, y_j\, \alpha_i \alpha_j x_i x_j$$

$$Subject\ to: \begin{cases} \sum_{i=1}^{N} \alpha_i\, y_i = 0 \\ 0 \le \alpha_i \le C \end{cases} \quad (3)$$

By resolving the optimizer problem in Eq. (3), the Lagrange co-efficient $\alpha_i$ (Lagrange co-efficient of $i^{th}$instance) is defined. This optimum$\alpha$ value is utilized for calculating the hyperplane parameters ($b$ and $w$), leading to the subsequent classification function:

$$f(x) = sign\left(\sum_{i=1}^{N} \alpha_i\, y_i(x_i \cdot x_j) + b\right) \quad (4)$$

If linear separation is difficult, nonlinear classifier approach such as SVM is employed. By deploying a mapping function represented in Eq. (5), the SVM transmissions data in low- to high-dimensional spaces, permittingsimple separation among class borders. Eq. (6) presents the utilization of a non-linear function, $(x)$, for mapping input feature vectors (x) in an $n$-dimension space to 1D feature space, increasing classification. This problem needs to determinethe kernel function $(x_i, x_i)$ , as expressed in Eq. (7).

$$\forall i, x_i \to \varphi(x_i) \quad (5)$$

$$\phi(x) = \left(\varphi_1(x), \ldots, \varphi_l(x)\right) \quad (6)$$

$$K(x_i \mathrm{x_j}) = \left(\phi(x_i) \cdot \phi(x_j)\right) \quad (7)$$

Next, the optimizer problem is changed as the formula written as:

$$\min \sum_{i=1}^{N} a_i - \frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N} y_i\, y_j\, \alpha_i \alpha_j K(x_i, x_i)$$

$$Subject\ to: \begin{cases} \sum_{i=1}^{N} \alpha_i\, y_i = 0 \\ 0 \le \alpha_i \le C \end{cases} \quad (8)$$

If the non-linear kernel canbe employed, Eq. (4) for the decision function canalter and change into Eq. (9).

$$f(x) = sign\left(\sum_{i,j=1}^{N} \alpha_i\, y_i K(x_i, x_i) + b\right) \quad (9)$$

The RBF is a generally employed kernel in SVM applications. It is determined as Eq. (10):

$$K(x_i.x_j) = \exp\left(-\frac{\|x_i - x_j\|^2}{\sigma^2}\right) \quad (10)$$

SVMs are prominent for their computational efficacy and efficiencyincontrolling high-dimension data without being dependent on difficult methods.

### 2.2 Parameter tuning using GOA

To address this challenge, the GOA simulated by the natural behavior of grasshoppers in search of optimal foraging spots, is introduced for parameter optimization.GOA is a novel algorithm simulated by the swarming behaviors of grasshoppers [18]. All the grasshoppers in the swarm havetheir own location is the feasible solution to the optimization problems. GOA comprises three subcomponents, $S\_i$ the social interaction, $G\_i$ the gravitation force on $i^{th}$ grasshoppers, and $A\_i$ the wind advection.

$$X\_i = S\_i + G\_i + A\_i \quad (11)$$

In Eq. (11) $Xi$ shows the location of $i^{th}$ grasshoppers.

$$S_i = \sum_{i=1}^{N} s\left(d_{ij}\right)\widehat{d_{ij}} \quad (12)$$

In Eq. (12), $s$ shows the function to determine the strength of social force, $d\_ij = |\mathrm{X\_j} - X\_i|$ the distance among $i^{th}$ and $j^{th}$ grasshoppers, and $(d\_ij =)(X\_j - X\_i)/d\_ij$ indicates a unit vector from $i^{th}$ to $j^{th}$ grasshoppers.

$$s(r) = fe^{\wedge}((-r))/1 - e^{\wedge}(-r) \quad (13)$$

In Eq. (13), $f$ refers to the intensity of attraction, 1 shows the attractive length scale, within [0,4] control attraction or repulsion among individual grasshoppers, and $r$ denotes the force of repulsion. The distance should be standardized within [1,4] since $s$ function could not manage stronger forces with longer distance.

The $G$ element consists of two different parts, $g$ denotes the gravitational constant and $(e\_g)^{\wedge}$ indicates a unity vector nearby the center of earth.

$$G_i = -g\widehat{e_g} \quad (14)$$

The wind advection $A$ is evaluated by Eq. (14):

$$A_i = u\widehat{e_w} \quad (15)$$

In Eq. (15),$\widehat{e_w}$ shows the unity vector in the wind direction and $u$ denotes the constant drift:

$$X_i = \sum_{\substack{j=1 \\ j \ne i}}^{N} s\left|x_j - j_i\right| \frac{\left|x_j - j_i\right|}{d_{ij}} - g\widehat{e_g} + u\widehat{e_w} \quad (16)$$

The balance among exploitation as well as exploration in a stochastic algorithm assistsin searching for global optima. Any special parameters are added to show exploitation and exploration in dissimilar phases of optimizer:

$$X_i^d = c\left(\sum_{\substack{j=1 \\ j \ne i}}^{N} c\frac{ub_d - lb_d}{2} s\left|x_j - j_i\right| \frac{\left|x_j - j_i\right|}{d_{ij}}\right) + T_d \quad (17)$$

In Eq. (17), the component of $G$ is ignored assuming no wind direction and gravitational force is often towards a target. $[\![ub]\!]\_d$ and $[\![lb]\!]\_d$ shows the upper and lower bounds at the $d$ dimensional space and $T_d$ refers to the values of $d^{th}$dimension in the target. The inner 'c' decreases attraction or repulsion forces among grasshoppers relative to the amount of iterations, whereas outer 'c' maintain the balance between exploitation and exploration. The reducing coefficient '$c$' is applied twice in Eq. (17) to control forces between grasshoppers and is updated using Eq. (18).

$$c = cmax - l\frac{\mathrm{cmax} - \mathrm{cmin}}{L} \quad (18)$$

Where $L$ represents the maximal iteration counter, $cmax = 1$ denotes the maximal value, $cmin = 0.00001$ indicates the minimal value, and 1 shows the existing iteration.

## 3. Experimental Validation

The ID results of the SVMGOA-ID approach are studied here. Fig. 2 exhibits the confusion matrices produced by the SVMGOA-ID methodology at 80:20 and 70:30 of TRP/TSP. The resultspoint out the effective recognition and classification of 5 classes accurately.

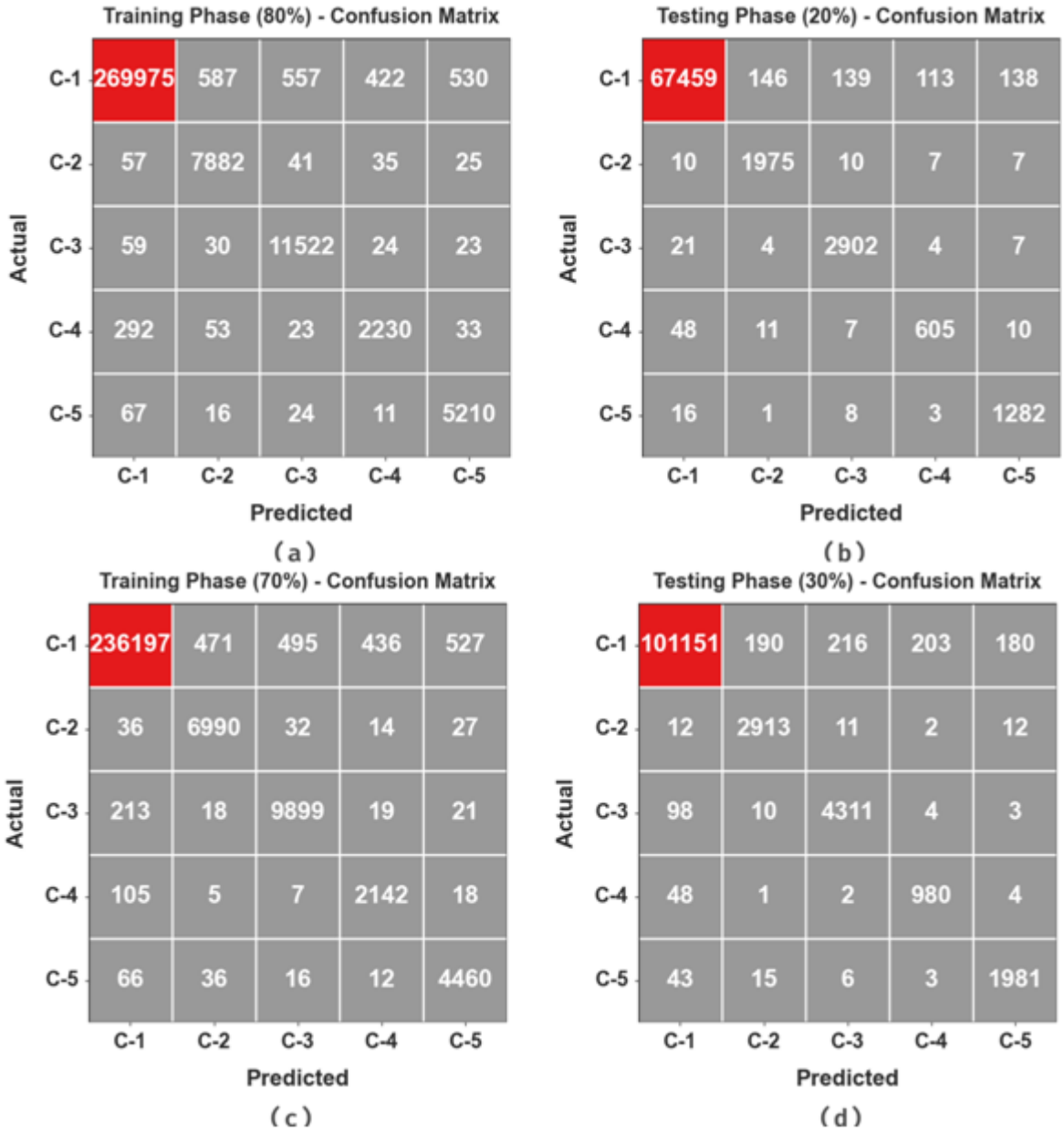


**Figure 2:** Confusion matrices of (a-b) 80:20-TRP/TSP and (c-d) 70:30-TRP/TSP

The ID results of the SVMGOA-ID approach with 80:20-TRP/TSP are studied in Table 1 and Fig. 3. The results imply the effectual recognition of five classes. On 80%-TRP, the SVMGOA-ID approach accomplishes average $accu_y$, $sens_y$, $spec_y$, $F_{score}$, and MCC of 99.61%, 95.73%, 99.49%, 93.59%, and 92.62% correspondingly. Then, on 20%-TSP, the SVMGOA-ID methodologyrealizes average $accu_y$, $sens_y$, $spec_y$, $F_{score}$, and MCC of 99.62%, 96.60%, 99.56%, 94.04%, and 93.11% correspondingly.

**Table 1:** ID outcome of SVMGOA-ID approach with 80:20-TRP/TSP

| Class | $Accu_y$ | $Sens_y$ | $Spec_y$ | $F_{Score}$ | MCC |
|---|---|---|---|---|---|
| **TRP (80%)** | | | | | |
| C1 | 99.14 | 99.23 | 98.28 | 99.53 | 95.06 |
| C2 | 99.72 | 98.03 | 99.76 | 94.92 | 94.82 |
| C3 | 99.74 | 98.83 | 99.78 | 96.72 | 96.61 |
| C4 | 99.70 | 84.76 | 99.83 | 83.32 | 83.18 |
| C5 | 99.76 | 97.79 | 99.79 | 93.46 | 93.43 |
| **Average** | **99.61** | **95.73** | **99.49** | **93.59** | **92.62** |
| **TSP (20%)** | | | | | |
| C1 | 99.16 | 99.21 | 98.63 | 99.53 | 95.18 |
| C2 | 99.74 | 98.31 | 99.78 | 95.27 | 95.19 |
| C3 | 99.73 | 98.77 | 99.77 | 96.67 | 96.55 |
| C4 | 99.73 | 88.84 | 99.83 | 85.63 | 85.55 |
| C5 | 99.75 | 97.86 | 99.78 | 93.10 | 93.09 |
| **Average** | **99.62** | **96.60** | **99.56** | **94.04** | **93.11** |

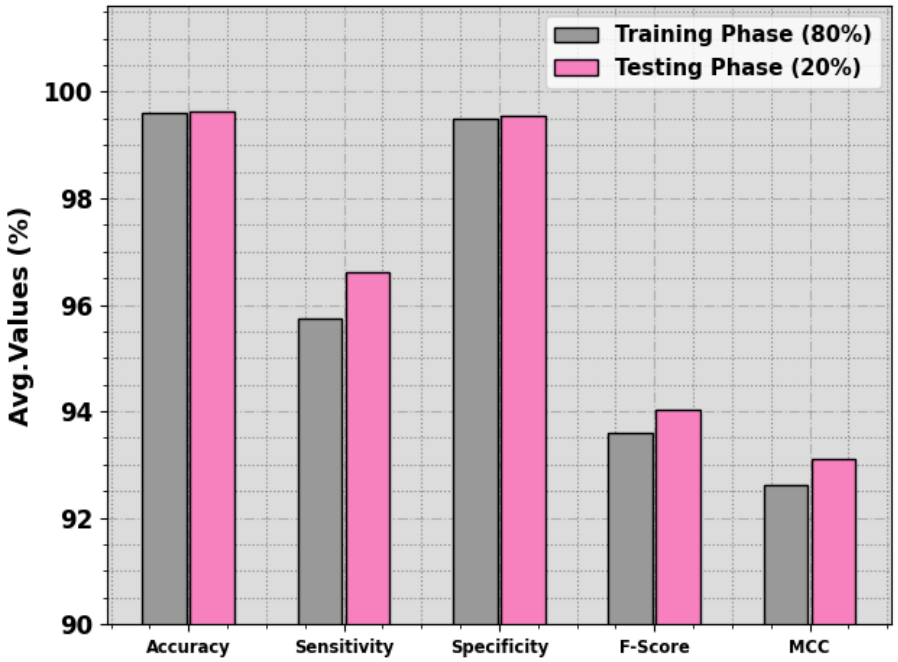


**Figure 3:** Average of SVMGOA-ID methodology with 80:20-TRP/TSP

The ID result of the SVMGOA-ID methodology with 70:30-TRP/TSP is studied in Table 2 and Fig. 4. The outcome value referred the effective recognition of five classes. On 70%-TRP, the SVMGOA-ID methodrealizes average $accu_y$, $sens_y$, $spec_y$, $F_{score}$, and MCC of 99.61%, 97.25%, 99.48%, 94.22%, and 93.25% correspondingly. Next, on 30%-TSP, the SVMGOA-ID systemachieves average $accu_y$, $sens_y$, $spec_y$, $F_{score}$, and MCC of 99.62%, 97.36%, 99.46%, 94.63%, and 93.68% correspondingly.

**Table 2:** ID outcome of SVMGOA-ID methodology with 70:30-TRP/TSP

| Class | $Accu_y$ | $Sens_y$ | $Spec_y$ | $F_{Score}$ | MCC |
|---|---|---|---|---|---|
| **TRP (70%)** | | | | | |
| C1 | 99.10 | 99.19 | 98.26 | 99.51 | 94.84 |
| C2 | 99.76 | 98.46 | 99.79 | 95.63 | 95.55 |
| C3 | 99.69 | 97.34 | 99.78 | 96.02 | 95.86 |
| C4 | 99.77 | 94.07 | 99.81 | 87.43 | 87.53 |
| C5 | 99.72 | 97.17 | 99.77 | 92.50 | 92.47 |
| **Average** | **99.61** | **97.25** | **99.48** | **94.22** | **93.25** |
| **TSP (30%)** | | | | | |
| C1 | 99.12 | 99.23 | 98.08 | 99.51 | 94.95 |
| C2 | 99.77 | 98.75 | 99.80 | 95.84 | 95.77 |
| C3 | 99.69 | 97.40 | 99.78 | 96.10 | 95.95 |
| C4 | 99.76 | 94.69 | 99.81 | 88.01 | 88.12 |
| C5 | 99.76 | 96.73 | 99.82 | 93.71 | 93.64 |
| **Average** | **99.62** | **97.36** | **99.46** | **94.63** | **93.68** |

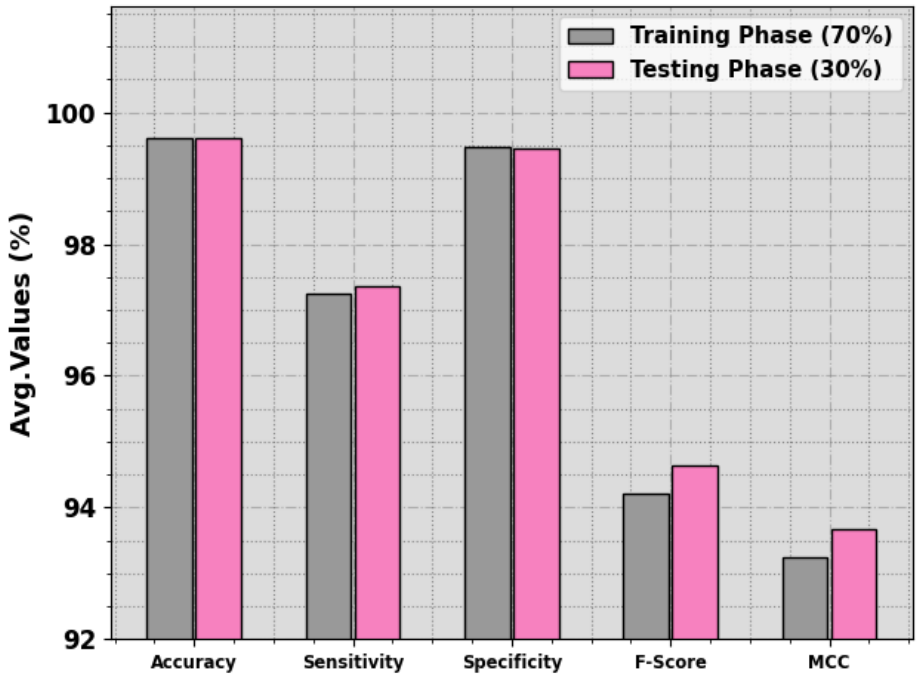


**Figure 4:** Average of SVMGOA-ID approach with 70:30-TRP/TSP

The SVMGOA-ID approach is compared with other ML classifiers in Table 3.In Fig. 5, the ID outcomes of the SVMGOA-ID approach are examined in terms of $accu_y$ and $F_{score}$. The results exhibited the effectual performance of the SVMGOA-ID approach. Based on $accu_y$, the SVMGOA-ID approach reaches improving $accu_y$ of 99.62% while the Adaboost, GB, XGBoost, KNN, and KNN-PSO methodologies attain decreasing $accu_y$ of 96.30%, 94.23%, 95.91%, 96.40%, and 96.47% respectively. In addition, based on $F_{score}$, the SVMGOA-ID systemachieves enhance $F_{score}$ of 94.63% while the Adaboost, GB, XGBoost, KNN, and KNN-PSO methods reach lesser $F_{score}$ of 91.09%, 92.43%, 90.70%, 90.79%, and 92.59% correspondingly.

In Fig. 6, the ID analysis of the SVMGOA-ID approach is examined interms of $sens_y$ and $spec_y$. The outcome values depicted the effectual performance of the SVMGOA-ID approach. Based on $sens_y$, the SVMGOA-ID methodology reaches improving $sens_y$ of 97.36% while the Adaboost, GB, XGBoost, KNN, and KNN-PSO methods attain lower$sens_y$ of 94.96%, 96.95%, 94.75%, 96.99%, and 94.10% correspondingly. Moreover, based on $spec_y$, the SVMGOA-ID approach reaches greater$spec_y$ of 99.46% while the Adaboost, GB, XGBoost, KNN, and KNN-PSO methodologies gainminimal$spec_y$of 94.47%, 94.55%, 94.14%, 96.20%, and 94.21% correspondingly.

**Table 3:** Comparative outcome of SVMGOA-ID methodology with ML systems

| Methods | $Accu_y$ | $Sens_y$ | $Spec_y$ | $F_{Score}$ |
|---|---|---|---|---|
| The Proposed Model | 99.62 | 97.36 | 99.46 | 94.63 |
| AdaBoost | 96.30 | 94.96 | 94.47 | 91.09 |
| GB | 94.23 | 96.95 | 94.55 | 92.43 |
| XGBoost | 95.91 | 94.75 | 94.14 | 90.70 |
| KNN | 96.40 | 96.99 | 96.20 | 90.79 |
| KNN-PSO | 96.47 | 94.10 | 94.21 | 92.59 |

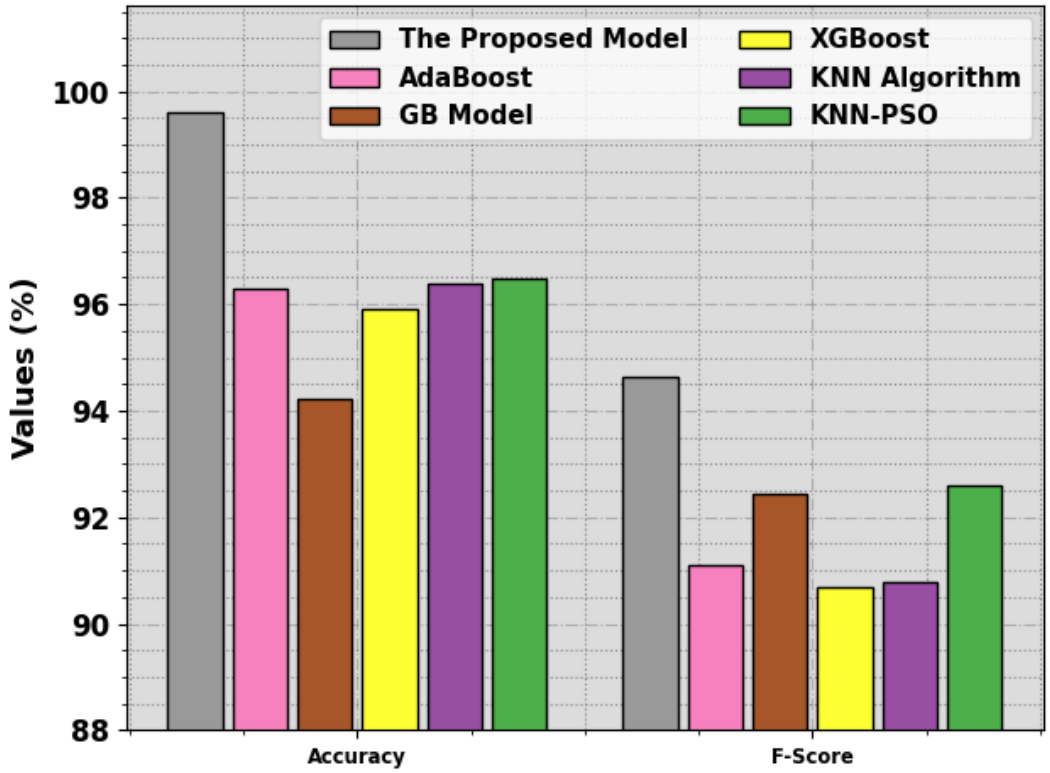


**Figure 5:** $Accu_y$ and $F_{score}$ outcome of SVMGOA-ID approach with ML systems

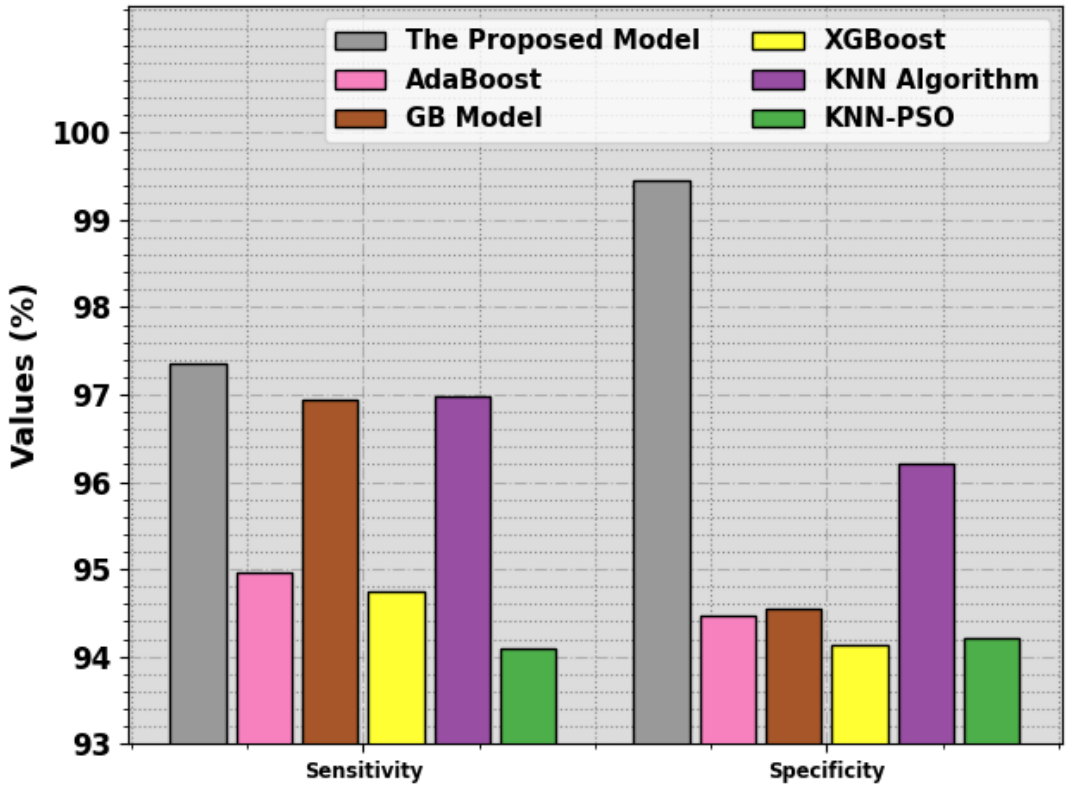


**Figure 6:** $Sens_y$ and $Spec_y$ outcome of SVMGOA-ID methodology with ML systems

## 4. Conclusion

In this study, we have focused and development of the SVMGOA-ID technique in WSNs. The SVMGOA-ID approach harnesses SVM, a well-established ML technique known for its proficiency in binary classification tasks. SVMs are trained to distinguish between normal network behavior and intrusion attempts, learning intricate patterns from a labeled dataset. However, the success of SVMs is highly dependent on appropriate parameter settings, and suboptimal choices can lead to reduced detection accuracy. To address this challenge, the GOA simulated by the natural

behavior of grasshoppers in search of optimal foraging spots, is introduced for parameter optimization. The GOA efficiently explores the parameter space of SVM models, seeking the ideal configuration that maximizes intrusion detection accuracy.

## References

[1] Borkar, G.M., Patil, L.H., Dalgade, D. and Hutke, A., 2019. A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept. *Sustainable Computing: Informatics and Systems*, *23*, pp.120-135.

[2] Baraneetharan, E., 2020. Role of machine learning algorithms intrusion detection in WSNs: a survey. *Journal of Information Technology*, *2*(03), pp.161-173.

[3] Alsahli, M.S., Almasri, M.M., Al-Akhras, M., Al-Issa, A.I. and Alawairdhi, M., 2021. Evaluation of machine learning algorithms for intrusion detection system in WSN. *International Journal of Advanced Computer Science and Applications*, *12*(5).

[4] Deshpande, S., Gujarathi, J., Chandre, P. and Nerkar, P., 2021. A Comparative Analysis of Machine Deep Learning Algorithms for Intrusion Detection in WSN. In *Security Issues and Privacy Threats in Smart Ubiquitous Computing* (pp. 173-193). Springer, Singapore.

[5] Singh, A., Amutha, J., Nagar, J., Sharma, S. and Lee, C.C., 2022. AutoML-ID: automated machine learning model for intrusion detection using wireless sensor network. *Scientific Reports*, *12*(1), pp.1-14.

[6] Singh, A., Amutha, J., Nagar, J., Sharma, S. and Lee, C.C., 2022. Lt-fs-id: Log-transformed feature learning and feature-scaling-based machine learning algorithms to predict the k-barriers for intrusion detection using wireless sensor network. *Sensors*, *22*(3), p.1070.

[7] Singh, G. and Khare, N., 2021. A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. *International Journal of Computers and Applications*, pp.1-11.

[8] Elbahadır, H. and Erdem, E., 2021, September. Modeling Intrusion Detection System Using Machine Learning Algorithms in Wireless Sensor Networks. In *2021 6th International Conference on Computer Science and Engineering (UBMK)* (pp. 401-406). IEEE.

[9] Amaran, S., Mohan, R.M. and Jebakumar, R., 2023. Optimal Machine Learning Based Intrusion Detection System in Wireless Sensor Networks for Surveillance Applications. *Journal of Mobile Multimedia*, pp.437-450.

[10] Chandre, P., Mahalle, P. and Shinde, G., 2022. Intrusion prevention system using convolutional neural network for wireless sensor network. *Int J Artif Intell ISSN*, *2252*(8938), p.8938.

[11] Fu, R., Ren, X., Li, Y., Wu, Y., Sun, H. and Al-Absi, M.A., 2023. Machine Learning-Based UAV Assisted Agricultural Information Security Architecture and Intrusion Detection. *IEEE Internet of Things Journal*.

[12] Saravana Kumar, N.M., Suryaprabha, E. and Hariprasath, K., 2022. Machine learning based hybrid model for energy efficient secured transmission in wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-16.

[13] Devi, M., Nandal, P. and Sehrawat, H., 2023. A novel rule-based intrusion detection framework for secure Wireless Sensor Networks.

[14] Hemanand, D., Reddy, G.V., Babu, S.S., Balmuri, K.R., Chitra, T. and Gopalakrishnan, S., 2022. An intelligent intrusion detection and classification system using CSGO-LSVM model for wireless sensor networks (WSNs). *International Journal of Intelligent Systems and Applications in Engineering*, *10*(3), pp.285-293.

[15] Umamaheshwari, S., Kumar, S.A. and Sasikala, S., 2021, October. Towards building robust intrusion detection system in wireless sensor networks using machine learning and feature selection. In *2021 international conference on advancements in electrical, electronics, communication, computing and automation (ICAECA)* (pp. 1-6). IEEE.

[16] Srivastava, A. and Bharti, M.R., 2023. Hybrid Machine Learning Model for Anomaly Detection in Unlabelled Data of Wireless Sensor Networks. *Wireless Personal Communications*, *129*(4), pp.2693-2710.

[17] Rahmani, A., Hojati, F., Hadad, M. and Azarhoushang, B., 2023. A Hybrid Approach for Predicting Critical Machining Conditions in Titanium Alloy Slot Milling Using Feature Selection and Binary Whale Optimization Algorithm. *Machines*, *11*(8), p.835.

[18] Sajjad, F., Rashid, M., Zafar, A., Zafar, K., Fida, B., Arshad, A., Riaz, S., Dutta, A.K. and Rodrigues, J.J., 2023. An efficient hybrid approach for optimization using simulated annealing and grasshopper algorithm for IoT applications. *Discover Internet of Things*, *3*(1), p.7.