INTRUSION DETECTION IN SOLAR ENERGY WIRELESS SENSOR NETWORK USING SUPPORT VECTOR MACHINE AND RANDOM WEIGHT GRASSHOPPER OPTIMIZATION ALGORITHM

Supported by tetfund
TERTIARY EDUCATION TRUST FUND

Ayobami Taiwo Olusesi[1*], Olatilewa Raphael Abolade[2], Abisola Ayomide Olayiwola[3], Ayo Isaac Oyedeji[4], Oluwaseyi Olawale Bello[5]

[1,2,3,4] Department of Computer Engineering, Olabisi Onabanjo University, Ago-Iwoye, Nigeria.
[5] Department of Computer Engineering, Ekiti State University, Ado-Ekiti, Nigeria
*Corresponding E-mail address: olusesi.ayobami@oouagoiwoye.edu.ng

Received: May 15, 2025, Accepted: August 28, 2025

Abstract Wireless Sensor Network (WSN) is made up of sensor and actuator nodes that are widely dispersed within a certain geographic area. Sensing, gathering, processing, and wirelessly transmitting data have successfully been carried out on WSNs. Distributed computing, sensors, computer networks, communication, embedded systems, and other techniques and technologies are all applied in the WSN. Limited communication capacity caused by low energy resources is one of the major challenges facing WSN. However, longer network lifetimes have been made possible by incorporating solar energy with wireless sensor networks (SE-WSN), even if WSN applications are severely limited by battery capacity. Detecting and guiding SE-WSN against sensor nodes from attack is one of the major challenges in SE-WSN. Therefore, this study developed an intrusion detection model for SE-WSN using support vector machine and random weight grasshopper optimization algorithm (SVM-RWGOA). MATLAB environment was used to simulate the developed model. SVM-RWGOA technique showed an improvement in the performance of SE-WSN when it was compared with the existing approach of honeybee optimization algorithm (HBOA) and ensemble particle swarm optimization (ESPSO) using detection accuracy, packet delivery ratio and energy consumption as performance metrics.

Keywords: Solar Energy Wireless Sensor Network, Intusion Detection, Support Vector Machine, Random Weight Grasshopper Optimization Algorithm.

Introduction

Devices are connected as part of a communication system to fulfill user requests. Both "wired" and "wireless" are possible. A system that uses wires to function over a certain area is called a wired system. However, when new trends and developing technology developed, so did wireless communication systems. Compared to wired communication systems, this method of communication revolutionized the way information is transmitted (Simarjeet, 2018). Wireless networks fall into two distinct categories which are the infrastructure-based networks and infrastructure-less networks. Wired access points and extra infrastructure are not required for infrastructure-less systems. They are suitable for use in places where infrastructure is lacking, unreliable, costly, and/or unsuitable for emergency use. They can also be utilized to provide rapid communication. One type of infrastructure-less wireless network is the wireless sensor network (WSN) which is composed of several node devices that can sense their environment and send information about the monitored region (such as a volume or area) over wireless communication.

WSN it is an electronic device that are controlled by a central processing unit (CPU), memory unit, transceiver module, one or more sensing devices, an analog-to-digital converter (ADC), and a power source, usually a battery (Dionisis et al., 2020), Since the transmitting and sensing components rely on the WSN's power capacity, the battery size is the main factor influencing the node size in WSNs. When the battery's usable life is coming to an end, it must be replaced or recharged. The Solar Energy WSN (SE-WSN) was created to enhance the functionality of the sensor nodes in WSN in order to prevent the need for frequent battery changes, which could impair network performance (Rosdiazli et al., 2016). The process of converting solar light energy into electrical energy for use in powering electronics or electrical devices is known as solar energy (Guojiang et al., 2018). Actually, it provides a clean, sustainable, and eco-friendly energy source for humanity. Because of its vast energy reserves, it can provide all the energy required for current human activities. The sensor and battery can be powered by solar cells while the node is in an idle state. The network's lifetime and efficiency have been enhanced by the nodes' ability to run on stored energy when the sun isn't available (Ramzi, 2020).

The wireless sensor network and solar energy are the two main components of SE-WSN. The network protocol, coverage problems, data collection and distribution, time constraints, energy management, fault detection, and security are just a few of the challenges that SE-WSN still faces, despite the advancements it has made to the way WSN operates. As long as a node is within radio range, it can join a SE-WSN at any moment. Information exchange across mobile nodes is facilitated by this. However, wireless nodes are vulnerable to both active and passive attacks, information leaks, service denial, and data integrity change since they do not offer boundary protection to intermediary nodes. Due to their inherent design, which allows nodes to freely enter and exit the network without any restrictions, SE-WSNs are vulnerable to a variety of security threats (Himanshu *et al.,* 2018). Since the nodes act as the network's routing medium, attacking them kills the network (Reza et al., 2020; Dipak and Tarachand, 2020). Also, in order to attract network traffic to itself, a network layer attack in SE-WSN gives its neighbors false routing information. By denying the nodes access to precise sensing data, it presents a serious risk to higher-layer applications. Malicious assaults have been

detected using a variety of trust intrusion detection techniques, however, the present trust model technique still has several shortcomings, such as its incapacity to handle massive amounts of data and constantly shifting trust patterns (Shalini and Syed, 2022).

Numerous efforts have been made to increase the difficulty of protecting SE-WSN from intrusion using SVM and swarm intelligence algorithm. A few instances of swarm intelligence algorithms are cuckoo search (CS), simulated annealing (SA), harmony search (HS), grey wolf optimization (GWO), ant colony optimization (ACO), particle swarm optimization (PSO), whale optimization algorithm (WOA) and Artificial bee colony (ABC) among others. Ting et al. (2021) developed a time varying particle swarm optimization (TV-PSO) for attack detection and trust management in WSN. An energy-conscious security level control technique for solar-powered wireless sensor networks was presented by Jong et al. (2015). The data was encrypted using a public key encryption approach by a node with higher battery power than a preset threshold. Notable outcomes of this procedure include lowering the energy consumption of relaying nodes and enhancing data security. The recommended approach secured the sensory data using either symmetric key or public-key protocols, depending on the energy level. The sender of the data uses the symmetric key to encrypt the plain text in a symmetric-key cryptosystem, and the recipient uses the same key to decrypt the plain text.

A technique that uses a random forest (RF) model for classification and a genetic algorithm (GA) for in intrusion detection system (IDS) intended for Industrial Internet of Things (IIoT) networks was presented by Kasongo (2021). When compared to current IDS frameworks, the GA-RF technique performed better, with an Area Under the Curve (AUC) of 0.98 and a test accuracy of 87.61% for binary classification. The UNSW-NB15 dataset is used to assess the suggested method's efficacy and resilience. By combining the benefits of RF for classification and GA for FS, this methodology improves the security, privacy, and integrity of IIoT networks. Olusesi et al. (2025) developed an efficient routing protocol for SE-WSN using linear function mayfly algorithm, but the work did not consider the detection of intrusion in the network. An efficient IDS that incorporates a Weighted Extreme Gradient Boosting (XgBoost) classifier, a modified wrapper-based approach, and a sine-cosine FS algorithm was presented by Mohiuddin et al. (2023). By expanding the search and efficiently choosing an optimal solution using the sine–cosine function, this strategy aims to improve prediction quality and avoid local optima. Using the UNSW-NB15 and CICIDS datasets, the suggested model successfully categorized binary and multi-class assaults with considerable accuracy, precision, recall, and F1-score metrics. However, there are important limitations regarding the suggested model's scalability, computational efficiency, and suitability for different network scenarios that haven't been covered.

To overcome the shortcomings of conventional intrusion detection technology in a complex and dynamic IoT environment. Liu et al. (2021) proposed a particle swarm optimization-based gradient descent (PSO-GBD) model for intrusion detection in IoT. The model uses PSO- extract features from the data and input them into a one-class SVM for the identification and discovery of malicious data. The model performs well in terms of accuracy and false alarm rate (FAR), and it exhibits good robustness. Nevertheless, no effectiveness comparisons have been made between PSO and other metaheuristic algorithms. Thuan et al. (2024) developed an enhanced IDS in Wireless Sensor Networks using a Genetic Sacrificial Whale Optimization (GSWO) and CatBoost approach. GSWO, which cleverly combines a genetic algorithm (GA) and the modified whale optimization algorithm (WOA) with a conditional inherited choice (CIC), overcomes the drawbacks of traditional methods, including premature convergence, and meets the crucial need for effective feature selection (FS) in WSN security. Support vector machine has been used in recent times as intrusion detection technique in WSN but it is still faced with the challenge of optimal feature selections (Safaldin, et al., 2020). Several swarm intelligence techniques have been employed as optimal feature selection because of their self-organization, scalability, and strength (Hariharam and Sreelekshmi, 2017).

Most of the approaches used in the aforementioned studies made used of algorithms that are faced with the challenge of experiencing a decrease in performance over repetitions, depending on the intensity of the search (Mohammadreza et al., 2019). Furthermore, for increased effectiveness, intrusion detection systems (IDSs) in wireless sensor networks (WSNs), it mostly depends on efficient and optimal feature selection (FS) (Thuan et al., 2024) which requires more focus. Hence, there is a need to develop a model which will be able to perform optimal and effective feature selection on the SVM for better performance of the IDSs in SE-WSN. Therefore, this study developed a more robust intrusion detection in SE-WSN using support vector machines (SVM) and random weight grasshopper optimisation algorithm (SVMRWGOA) for the purpose of improving the SE-WSN performance.

Materials and Methods

Finding simple techniques that facilitate network security is essential to safeguarding SE-WSN against intrusion. These detection techniques will shield in SE-WSN from different security attacks and assist in detecting them (Fatimah et al., 2022). Honey bee optimisation algorithm (HBOA) (RadhaKrishna et al., 2022) and ensemble swarm optimisation (ESPSO) (Shaikh et al., 2025) are both some of the recent existing techniques which been used to improved the performance of WSNs. In ESPSO, PSO was used for feature selection but it has been known for premature convergence when dealing with complex tasks. In HBOA, the authors compared each metrics with simulation time, However, both ESPSO and HBOA did not considered energy consumption of the nodes within the network. Therefor, this study developed a robust support vector machine and random weight grasshopper optimisation algorithm (SVM-RWGOA) model which has been able to addressed the challenges posed by both EPSO and HBOA. SVM was used for malicious detection and a mathematical model using RWGOA was introduced to find optimal feature selection in SVM so as improve the performance of detection mechanism. Simulation of the SVM-RWGOA was carried

out in MATLAB environment using detection accuracy, packet delivery ratio and energy consumption as performance metrics.

Support Vector Machine (SVM)

SVM have been demonstrated to be more effective than other supervised learning techniques. They have been used in a variety of research fields, including text classification, which is applicable in financial institutions to detect frauds, face recognition, medicine, and multiple instance learning, due to their superior performance even in non-linear classification problems. The SVMs are among the most reliable and effective machine learning techniques used to deal with classification, detection and regression (Jair et al., 2020). Finding a suitable partition hyperplane in the sample space where the training sample set is M and separating the samples of various categories is the main goal of the so-called linear separable support vector machine. Two data samples are said to be linearly separable if a linear function can distinguish between them. The hyperplane in the sample space is divided by the linear equation, as shown in Equation 1 (Babacar et al., 2021).

$$W^T x + b = o \quad (1)$$

where W is a normal vector that determines the direction of the hyperplane and b is a displacement that specifies the distance between the hyperplane and the origin. Assume that the hyperplane can classify the training samples properly, in which case the maximum interval hypothesis, as indicated in Equations 2 and 3 is satisfied for the training samples.

$$w^t x_i + b \geq 1, y = 1 \quad (2)$$

$$w^t x_i + b \leq -1, y = -1 \quad (3)$$

Performing linear regression in this space after nonlinear data mapping to a high-dimensional feature space, where the nonlinear difficulty in the low-dimensional domain is equivalent to the large proportional regression problem of dimension feature control is the fundamental concept of nonlinear support vector machine regression. The multi-class classification problem was employed to identify and classify attacks. An issue with multiple classes was divided into two classes. In this work, Kernel Radial Basis Function (KRBF) was used to effectively separate the legitimate and malicious nodes from the shared complex boundaries, as illustrated in Equation 4 (Shalini and Syed 2022).

$$K(x, y) = e^{-\gamma|x-y|^2}, \gamma > 0 \quad (4)$$

The maximum number of samples is shown as $i, y_i \in \{1, -1\}$ and $x_i R_n$ where the positive class Is 1 and negative class is -1 with the subspace of labels conforming to x_i is represented as R_n. Although the SVM model has the benefit of having fewer parameters needed, the requirement for a Gaussian function in the training set for each scenario reduces performance and increases training time when used to large datasets for malicious node classification. As in Equations 5 to 7 (Shalini and Syed 2022), the positive slack variables in soft margin use $\beta_i, i = 1, 2, \ldots \ldots N$ in the restrictions.

$$(\alpha . x_i - p) \geq +1 - \beta_i, \ for\ y_1 = +1 \quad (5)$$

$$(\alpha . x_i - p) \geq -1 + \beta_i, \ for\ y_1 = -1 \quad (6)$$

$$\beta \geq 0 \quad (7)$$

where an error must occur if β_i is less than unity. As a result, the SVM offers information on the malicious attackers, which is then disseminated throughout the network. The neighboring user no longer has access to the ID of malicious attackers.

Algorithm 1: Support Vector Detection Algorithm (Liang et al., *2019)*

Input *sample feature matrix X , sample target value matrix Y , learning rate α, specific kernel function 2: K*

for *v in Y*

v : = log(e) v

Repeat until convergence *{*

a. Using the heuristic method to do the optimization of the two variables α_1, α_1^**, and use them to update the value of b ;*

b. Using one sample per iteration to update θ;

For *i = 1 to m {*

$$\theta_j := \theta_j + \left(y^{(i)} f\left(x^{(i)}\right)\right) x_i^{(i)} \textbf{for every } j$$

}

for *v in* θ

$$v := exp(v)$$

return θ

Grasshopper Optimization Algorithm

The metes-heuristic algorithm has steadily taken over as the primary technology for resolving global optimization problems due to the growing complexity and scope of real-world engineering design optimization problems. However, certain new algorithms have raised a lot of concerns. One of the amazing metes-heuristic algorithms of global optimization is the GOA (Saremi et al., 2017) which merge recently. This is inspired by the natural behaviour of the grasshopper swarm, making utilization of the swarm intelligence to solve optimization problems. GOA has gained increasing interest from academics and researchers; most researchers and practitioners have found success with the unique GOA to solve numerous complicated and real-world problems in many different fields. Phases of exploration and exploitation are both included in the GOA. In the exploration phase, search agents make sudden leaps, while in the exploitation phase, they move more slowly. Figure 1 depicts these stages of the search mechanism in GOA (Lei et al., 2024)

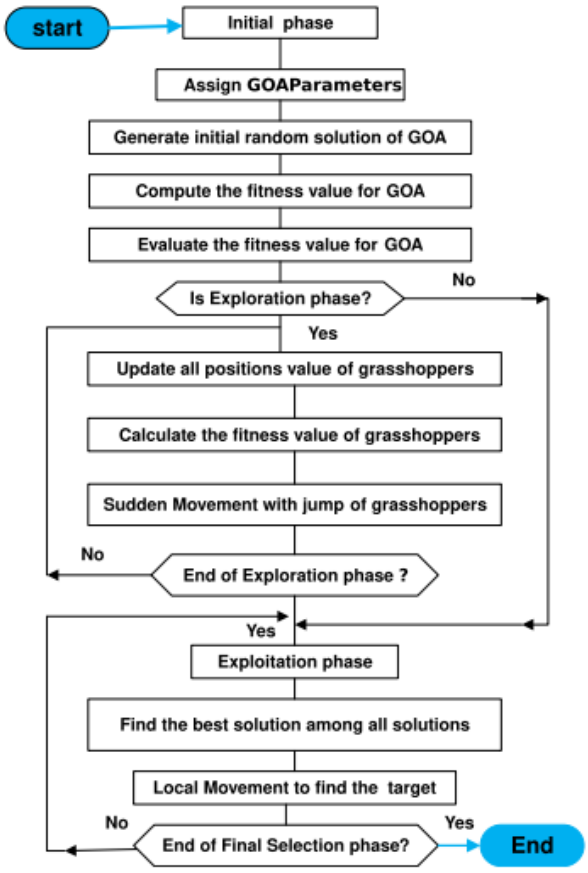

Figure 1: Flow Charts of GOA

GOA Mathematical Model

The social behaviour and hunting technique of grasshoppers in the wild are imitated by the GOA. Each grasshopper in the population represents a solution in this population-based method. The position Xi of each solution is determined by analytically modelling the swarming behaviour of grasshoppers. The grasshopper swarm's behaviour is described by following Equations 7 to 9 (Lei et al., 2024)

$$X_i^d = c_1\left(\sum_{]=1,i\neq j}^{N} c_2 \frac{UB_d - LB_d}{2} s\left(/x_j^d - x_i^d/\right)\frac{/x_j - x_i/}{d_{ij}}\right) + T_d \quad (7)$$

$$s = fe^{\frac{-r}{l}} - e^{-r} \quad (8)$$

$$c = c_{max} - t\frac{c_{max} - c_{min}}{t_{max}} \quad (9)$$

s is the strength of two social forces (repulsion and attraction between grasshopper swarms).

r and $d_{ij}(=/x_j - x_i/)$ are for finding the Euclidean distance, $d_{ij} = \frac{/x_j - x_i/}{d_{ij}}$ represent the unit vector from the ith to the jth grasshopper, f is the strength of attraction while l is the length of attraction

$UB_d - LB_d$ are the upper and lower bounds in the dth search space , c is the non linearity coefficient parameter which gives balance exploration and exploitation got GOA. $c_{max} - c_{min}$ determine the maximum and minimum values of c, t is the current iteration while t_{max} iteration value.

Random Weight Grasshopper Optimization Algorithm

GOA has certain limitations when it comes to complex optimization issues, like a slow rate of convergence and an easier tendency to slip into a local optimum, which hinders the GOA from obtaining better answers.

To make GOA more suitable for this study, Random Weight was combined with GOA techniques to make GOA more capable, to provide a better balance between exploration/exploitation and for the optimal feature selection. The nonlinear adaptive coefficient updating method of Random Weight strategy is developed to replace the linearly declining parameter of c in Equation 9 in order to reduce the inherent weakness of GOA.

Random Weight approach replaced the non-linear coefficient of Equation 9 and it becomes Equation 10.

$$c = \begin{cases} c_{max} - (c_{max} - c_{min}) \times k \times \left(1 + \cos\left(\frac{pixl}{L}\right)\right)^2 \\ c_{max} - (c_{max} - c_{min}) \times k \times \left(1 - \cos\left(\frac{pixl}{L}\right)\right)^2 \end{cases} \quad (10)$$

where k is a constant value between 0 and 1, l is the current iteration and L is the maximum number of iterations

Algorithm 2: SVM Random Weight Grasshopper Optimization Algorithm

Input

Binary Data $\{x_1, x_2, x_3, \ldots\ldots\ldots x_n\}$

Output

Binary ground truth data $\{d_1, d_2, d_3, \ldots\ldots\ldots d_n\}$

Anomaly scores $\{\{f(x_1), f(x_2), f(x_3), \ldots\ldots\ldots f(x_n)\}$

Initialization

Initialize the velocity of each grasshopper randomly

Define position X_i^d *of each grasshopper*

Initialize SVM model

Train SVM model on the binary data

Compute anomaly score of unit cell

While $t < T$

Adjust the position of each grasshopper

Update the velocity and position of grasshopper

If $random < r_1$

Select a location among the best location

Generate new location

Rank the grasshopper and find the current best

Generate output

Results and Discussion

Simulation for the developed SVM-RWGOA intrusion detection model was done using Windows 10 Ultimate 64-bit system, Intel (R) Core ™ i7 with frequency speed of 2.5GHz, 8G RAM , 250GB Solid State Drive (SSD) and the simulation tool of MATLAB environment. The MATLAB simulation tool was suitable for this study because of its high-performance technical computing. Simulation parameters are shown in Table 1 while detection accuracy,

packet delivery ratio and energy consumption are the performance metrics.

Performance Metrics

Detection accuracy, packet delivery ratio and energy consumption are the performance metrics which were used. SVM-RWGOA was compared with HBOA and ESPSO.

i. Detection Accuracy: This is percentage of all attacks that are accurately identified.
ii. Packet Delivery Ratio (PDR): This is calculated by dividing the total number of data packets sent from sources by the total number of data packets that arrive at destinations.
iii. Energy Consumption: Is the total amount of energy needed over time to send, receive, or forward a packet to a network node which is measured in Joules per second. The difference between the sensor's initial and residual energy is its energy consumption.

Table 1: Simulation Parameters

Parameters	Values
Network Area	(200×200) m
Initial Energy of Sensor Node	0.5J
Number of rounds	1000
Energy Coefficient for Free Space Transmission	10pJ/bit/m^2
Energy Coefficient for Multi Path Transmission	0.0013pJ/bit/m^4
Message Size	4Kb/message
Number of Sensor Nodes	100
Receiving Energy per Data bit	50nJ/bit
Transmitting Energy per Data Bit	50nJ/bit

Detection Accuracy

The detection accuracy rate of SVM-RWGOA was assessed for several nodes in the SE-WSN. In Figure 2, setting the number of nodes at 30, SVM-RWGOA detection accuracy rate showed 64.8% while HBOA and ESPSO showed a detection accuracy of 50.2 and 56.3% respectively. Additionally, SVM-RWGOA technique showed a detection accuracy rate of 88.4% at 80 nodes while HBOA and ESPSO showed a detection accuracy of 73.1 and 77.1% respectively. Using the RWGOA for optimal feature selection in SVM for this study as compared to the existing HBOA and ESPSO, SVM-RWGOA has been able to provide a better performance in SE-WSN by improving its detection accuracy.

Energy Consumption

The energy consumption of the sensor in a network, is the difference between its initial and residual energy amount of energy used over time to transmit, receive, or forward a packet to a network. It is measured in joules per second. The SVM-RWGOA energy consumption is contrasted with HBOA and ESPSO as shown in Figure 4. At 70 nodes, the energy consumption of SVM-RWGOA was 23.1J/sec while that of HBOA and ESPSO gave 27.8 and 25.4J/sec respectively

Packet Delivery Ratio

The percentage of total packets received against the total packets transferred among the nodes within the network is the packet delivery ratio (PDR). This is one of the metrics that is used to measure the performance of a network. As shown in Figure 3, at 50 nodes SVM-RWGOA showed a PDR of 75% while HBOA and ESPSO displayed a PDR of 70 and 72% respectively. The PDR of SVM-RWGOA at 100 nodes was 92% while HBOA and ESPSO showed PDR of 85 and 86.9% respectively.

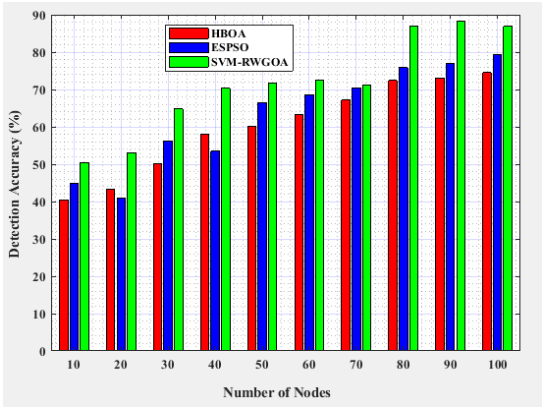

Figure 2: Detection Accuracy

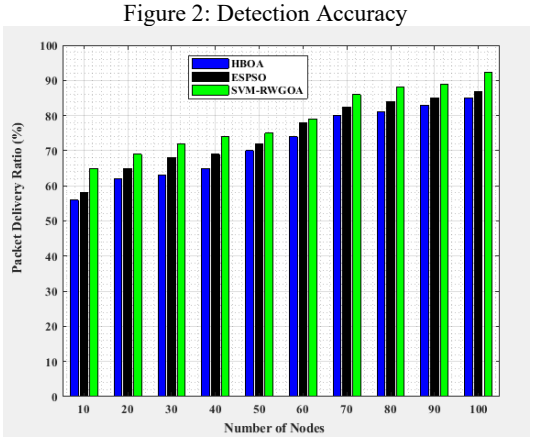

Figure 3: Packet Delivery Ratio

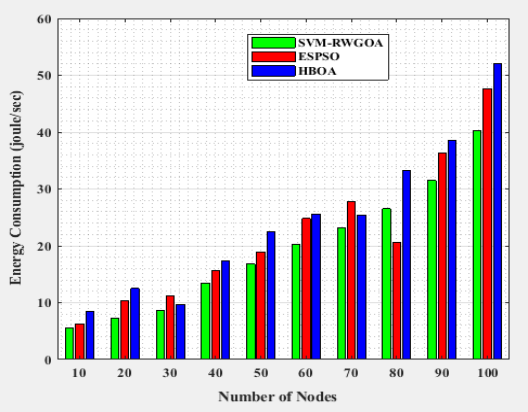

Figure 4: Energy Consumption

Conclusion

The autonomous wireless sensor network (WSN) nodes are linked to tiny solar panels which forms the solar energy wireless sensor network (SE-WSN). Solar energy provides the highest power density and optimum efficiency. This has made it possible to be used as a backup power source for WSNs in order to extend the network lifetime. However, intrusion detection in SE-WSN has become a major challenge facing performance of SE-WSN. Therefore, there is a need for robust intrusion detection model for SE-WSN. This study developed an intrusion detection model using support vector machine (SVM) and random weight grasshopper optimization algorithm (RWGOA). The developed SVM-RWGOA was compared with the existing technique of honey been optimisation algorithm (HBOA) and ensemble particle swarm optimisation (ESPSO) using MATLAB as the simulation tool. In this study, RWGOA performed the optimization strategy for feature selection in SVM which enhanced detection accuracy of SVM. Energy consumption, packet delivery ratio and delivery accuracy were the performance metrics used to contrast SVM-RWGOA with the existing ESPSO and HBOA. It was observed that SVM-RWGOA performed better than the existing technique (HBOA and ESPSO) and has helped in improving the performance of SE-WSN. Future research can look into considering the environmental condition before the deployment of SE-WSN within a specific geographical location. Because it is not an easy task tracking the sensor nodes of SE-WSN placed in a hostile environment or a steep terrain.

References

Lei, W., Jiawei, W., and Tengbin, W. (2022). The improved grasshopper optimization algorithm with Cauchy mutation strategy and random weight operator for solving optimization problems. Springer. *Springer Journal of Evolutionary Intelligence*, 17, Pp. 1751 – 1781

Babacar, G., Dezheng, Z., and Aziguli, W. (2021). Improvement of Support Vector Machine Algorithm in Big Data Background. *Mathematical Problems in Engineering*, Pp.1-9.

Dipak, K., and Tarachand, A. (2020). Renewable Energy Harvesting Schemes in Wireless Sensor Networks: A Survey. *Information Fusion,* Pp. 1-36.

Dionisis, K., Christos, N., Dinitrios, V., and Grigorios, K., (2020). Applications of Wireless Sensor Networks: AN Up-to-Date Survey. *Applied System Innovation*, Volume 3, Issue 14, Pp. 1-24.

Fatimah, K., Hajer, A., and Aseel, A. (2022).Security in Wireless Sensor Networks: Comparative Study. *International Journal of Computer Science & Information Technology,* Volume 14, Issue 3, Pp. 55- 65.

Guojiang, X., Jing, Z., Xufeng, Y., Dongyuan, S., Yu, H., and Gang, Y., (2018). Parameter Extraction of Solar Photovoltaic Models by Means of a Hybrid Differential Evolution with Whale Optimization Algorithm. *Solar Energy,* Volume 176, Pp. 742-761.

Hariharam, N., and Sreelekshmi, S., (2017). A survey on Wireless Sensor Networks. *International Journal of Scientific Engineering and Science,* Volume 1, Issue 11, Pp. 75-81.

Himanshu, S., Ahteshamul, H., and Zainul, A., (2018).Modeling and Optimisation of a Solar Energy Harvesting System for Wireless Sensor Network Nodes. *Journal of Sensor and Actuator Networks,* Volume 7, Issue 40. Pp. 1-19.

Jair, C., Farid, G. L., Lisbeth, R.M., and Asddrubal, L. (2020). A Comprehensive Survey on Support Vector Machine Classification: Applications, Challenges and Trends. *ELSEVIER Journal of Neurocomputing,* Volume 408, Issue 30 , Pp. 189 – 215.

Jong, M., Hong, S., Junmin, Y., and Minho, P., (2016).Power Adaptive Data Encryption for Energy-Efficient and Secure Communication in Solar-Powered Wireless Sensor Networks. *Journal of Sensors,* Volume 2016, Pp. 1 – 9.

Liang, L., Jingxiu, Yang, and Weizhi, M. (2019). Detecting malicious nodes via gradient descent and support vector machine in Internet of Things. *ELSEVIER Journal of Computer and Electrical Engineering,* 77, 339 – 353.

Liu, J.; Yang, D.; Lian, M.; Li, M. Research on intrusion detection based on particle swarm optimization in IoT. IEEE Access 2021, 9, 38254–38268.

Kasongo, S.M. (2021). An advanced intrusion detection system for IIoT based on GA and tree based Algorithms. *IEEE Access*, 9, 113199–113212.

Mohammadreza, E., Esmaeil, S., Milad, M., and Francisco, G. (2019). Parameters Identification of PV Solar Cells Particle Swarm Optimization Algorithm. *Energy* Volume 179, Pp. 358-372.

Mohiuddin, G.; Lin, Z.; Zheng, J.; Wu, J.; Li, W.; Fang, Y.; Wang, S.; Chen, J.; Zeng, X. Intrusion detection using hybridized meta-heuristic techniques with Weighted XGBoost Classifier. Expert Syst. Appl. 2023, 232, 120596.

Oluses, A.T., Adegoke, A.S., Adeboye, S.T., Olatilewa, R.A., and Olayiwola, A.A. (2025). Efficient routing optimization model for solar energy wireless sensor network using linear function mayfly Algorithm, *FUW Trends in Science & Technology Journal*, Volume 10, Issue 1, Pp. 114 – 119.

RadhaKrishna, K., Dudimetla, P., Uzma, N., Ashok, B., and Karthik, K.V. (2022). Optimization of WSN using Honey Bee Algorithm, *Journal of Research in Engineering and Applied Sciences,* Volume 7, Issue 2, Pp. 290 – 294.

Ramzi, B., (2020). Extraction of Uncertain Parameters of Single and Double Diode Model of a Photovoltaic Panel Using Salp Swarm Algorithm, *Measurement,* Volume 154, Pp. 1-10

Reza, F., Somayyeh F.B., and Mehdi, Y. (2020).

Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol, Pp. 1 – 30.

Rosdiazli, I., Tran, D., Sabo, M., Kishore, B., and Khadijah, B., (2017).Solar Energy Harvest for Industrial Wireless Sensor Nodes, *Procedia Computer Science,* Volume 105, Pp. 111-118.

Safaldin, M., Otair, M., & Abualigah, L. (2020). Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks. *Journal of ambient intelligence and humanized computing*, 12(2), 1559-1576.

Saremi S., Mirjalili, S., Lewis, A. (2017) Grasshopper optimisation algorithm: Theory and Application. *Advance Engineering,* Software, 105:30–47

Simarjeet, K., (2018). Wireless Communication Systems: Need, Types and Applications, *International Journal of Research Culture Society*, Volume 2, Issue 1, Pp. 106-107.

Shaikh, A.B., Avijit, P., Fahmida, R., Yamina, I., Tonmoy, R., Mohammad, A.H, Fariha, H. and Muhammad, E.H. (2024). Intrusion Detection for Wireless Sensor Network Using Particle Swarm Optimization Based Explainable Ensemble Machine Learning Approach, *IEEEACCESS*, Volume 13, Pp. 13711 – 13730

Shalini, S., and Syed, Z., (2022). Weighted Coefficient Firefly Optimization Algorithm and Support Vector Machine for Trust Model and Link Reliability, *International Journal of Computer Networks & Communications*, Volume 14, Pp. 117-132.

Ting, Z.,Han, D., Marino, M., Wang, L., and Li, K. (2021) An Evolutionary-Based Approach for Low-Complexity Intrusion Detection in Wireless Sensor Networks. Wireless Personal Communications. ISSN 0929-6212 DOI: https://doi.org/10.1007/s11277-021-08757-w

Thuan, M.N., Han, H.V., Myungsik, Y. (2024). Enhancing Intrusion Detection in Wireless Sensor Networks Using a GSWO-CatBoost Approach, M*DPI Journal of Sensors*, Pp. 1 – 26.