International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhanced SVM-Based Novel Detection of Intrusions for Wireless Sensor Networks (WSNS)

[1]Namit Gupta, [2]Sandeep Kumar Jain, [3]Vikas Sagar, [4]Sonali Gowardhan Karale

Submitted:21/04/2023 **Revised:**11/06/2023 **Accepted:**24/06/2023

Abstract: The use of wireless sensor networks (WSNs) is expanding rapidly due to the quick advancement of wireless sensor technology. WSNs have significant military significance as well as a wide range of potential commercial applications. However, it has significant security issues because of factors such as the lack of resources available for terminal equipment and the nature of the wireless communication environment. Wireless sensor networks (WSNs) are susceptible to a variety of assaults because of their dispersed architecture and limited resources, making intrusion detection for WSNs an essential part of network security. The purpose of intrusion detection systems (IDS) in WSNs is to detect and react to intrusion attempts and other harmful activity. It takes a long time to perform a conventional intrusion detection algorithm. As a result, we have developed a novel intrusion detection framework for the wireless sensor network to help prevent this issue. This paper's major contribution is the proposal of an enhanced support vector machine (ESVM)-based intrusion detection algorithm and the construction of an intrusion detection system (IDS) for WSN's DoS attacks. Additionally, the suggested method's performance is enhanced by chaotic levy grasshopper optimization (CLGO). From the perspectives of detection rate, packet delivery rate, transmission delay, and energy consumption analysis, the proposed IDS can significantly improve network performance by identifying and removing malicious nodes in the network. It has the features of a simple structure, a short computation time, and a high detection rate.

Keywords: *Wireless sensor network (WSN), intrusion detection (ID), DoS attacks, enhanced support vector machine (ESVM), chaotic levy grasshopper optimization (CLGO)*

1. Introduction

The diverse WSN system includes sensors and tiny actuators in addition to multipurpose compute units. In a WSN, hundreds or thousands of autonomous, low-power, affordable wireless nodes can be utilized for overseeing and tracking the appropriate surroundings. Building a WSN requires attention to safety, durability, scaling, dependability, and self-healing.WSNs are used for a wide variety of purposes, including the armed forces, earthquakes, industrial machine, ocean, and environmental monitoring [1].The rapid advancement in innovation that has resulted in the manufacturing of intelligent sensors in recent years has sparked widespread interest in WSNs. Since these sensors are often smaller and have fewer computational units and computational assets, they are cheaper. Information from smart sensor nodes may be sensed, measured, and collected, and then sent to a central location where decisions are made [2].One or more base stations are used to serve as the coordinating hub for most WSNs. A base station acts as an entry point for a different network, houses valuable data, and facilitates communication between machines and humans. Each base station serves as the trunk of a tree in the routing forest created by all of the node sensors [3].

Both wired and wireless networks may benefit from the use of an IDS to identify intrusion attempts. The system immediately alerts its controller if an intruder is detected. There has been a flurry of recent research on IDSs for the Internet of Things (IoT). For instance, many strategies have been suggested for implementation in wireless sensor networks. In addition to their connection to the cloud, WSNs are also a part of cyber-physical systems. Wire-based network intrusion detection systems are more challenging to build because of the network's unique architecture and less-reliable infrastructure. The authors also contend that the answers to questions about the nature of an intrusion in wireless networks depend on factors such as network procedure, confidentiality, implementation, and diversity [4]. There are two categories of sensor nodes based on their sensing capabilities: homogenous nodes and

1Assistant Professor, College of Computing Science and Information Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India, Email id: namit.k.gupta@gmail.com

2Assistant Professor, Department of Electrical Engineeing, Vivekananda Global University, Jaipur, India, Email Id: sandeep_jain@vgu.ac.in

3Assistant Professor & Dy. HoD, Department of Artificial Intelligence (AI), Noida Institute of Engineering and Technology, Greater Noida, Uttar Pradesh, India, Email id: drvikas.sagar@niet.co.in

4Assistant Professor, Department of Computer Science and IT, Jain(Deemed-to-be University), Bangalore-27, India, Email Id: gk.sonali@jainuniversity.ac.in

heterogeneity nodes. Similarly, there are two kinds of wireless sensor networks: homogeneous WSNs and heterogeneous WSNs.

Because these nodes are battery-powered, their useful lifespan is limited, making it much more important to discover methods of increasing energy output. Wireless sensor networks may be used in a many different contexts, such as medical care, transportation, safety, and even the military[5]. In each of these contexts, nodes in networks primarily serve as information collectors. Different forms of assaults on WSNs put its communication in danger, but security is the biggest concern [6]. WSN is an internal component of the IoT that facilitates the exchange of large amounts of data to improve ecological user control. First, to see and communicate with the outside world, WSN uses a large number of sensor nodes grouped in Ad hoc On-Demand Distance Vector (AODV) fashion. While modeling a WSN system, power use, connectivity, and space for storage is among the most important constraints to take into account [7]. To enhance the SVM-based detection of intrusions for WSNs.

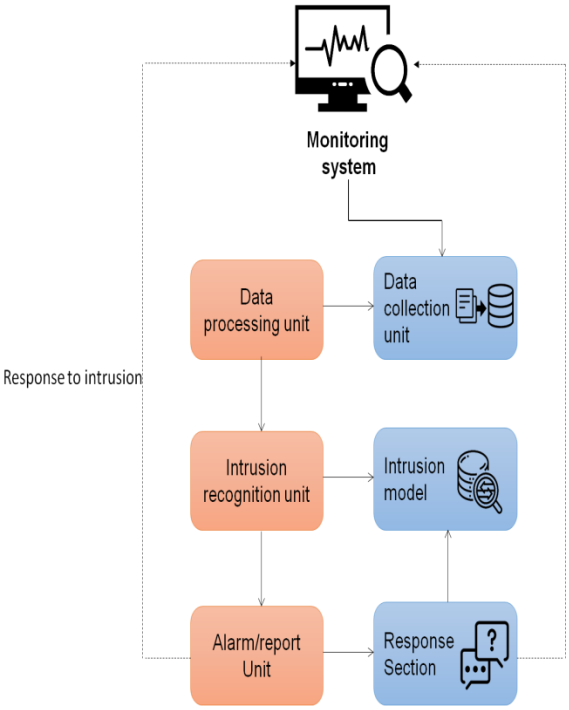

Fig.1. Architecture of IDS

2. Related Work

While developing and setting up WSNs, security, dependability, and conservation of energy are naturally at the forefront. Therefore, the increased vulnerability of WSNs might be attributed to the inaccessibility of features and the difficulty of powering the nodes. Networks of sensors periodically put nodes to sleep to make effective use of electrical resources. They become alert whenever they detect motion [8]. Effective, accurate, and careless detection technique that can detect the presence of jamming devices and duplicated nodes in WSN is essential. Due to their limited capabilities and characteristics, Many different types of security breaches may affect devices in the Internet of Things. In Internet of Things, wireless connections between nodes with limited battery life are often sporadic. For example, IoT devices might be stolen and used in an individual node repeat assault [9].The most common applications are in fields like defense, smart city development, and agricultural surveillance. The WSN has to function at a premium for these uses. However, several potential security concerns might compromise a WSN's performance. Threats to the integrity of the WSN may cause catastrophic failure. Therefore, effective and rapid protection against incursion is very desirable [10]. WSNs are employed in the armed forces for a variety of purposes, including area monitoring, healthcare for troops, smart transportation and logistics, and more. In order to monitor the whereabouts of people and vehicles for safety purposes, sensor nodes are dispersed randomly across the region. The camera module in these sensor networks is responsible for taking pictures or recording video. The acquired picture could not be sufficient to appropriately identify the incursion or aberrant behavior in the field owing to factors such as the environment, lighting, and other factors [11]. WSN nodes are susceptible to attack, and the ability to identify range of existing intrusion detection systems is limited. Detection preprocessing is a methodology for reducing the power consumption of nodes in WSNs that organizes nodes into groups based on their individual responsibilities. To further improve accuracy in identifying unusual measures by the WSN detection system for intrusions while decreasing the occurrence of false alarms rate, by making the technique for categorized kernel extreme acquiring device, following to Mercer Property to generate multi-kernel activities is under consideration [12]. It cooperates to identify, gather, evaluate, and transmit information on objects seen inside the network's viewing area, and then sends that information on to the network's proprietor. Typical attacks on WSNs include blackholes, grayholes, floods, and planning assaults, all of which have the potential to do substantial damage quickly. In addition, detection methods for WSN run into issues with a low recognition rate, high calculation costs, and numerous false alerts because of the restricted number of sensor nodes and the enormous quantity of superfluous as well as significant connection of network information [13].While the adoption of free standards and COTS hardware has started in WSN networks for safety-critical, the environment and applications, the issues of hostile infiltration and frequency cohabitation remain. Threats such as matching technique interference and complex, collaborative intrusion assaults are investigated [14].This rapid intrusion detection and prevention in border regions using WSNs is made possible by the exponential growth of computer capacities coupled with

explainable machine-learning methods. Through Monte Carlo simulation, the researchers were able to derive four characteristics: the RoI's surface area, the sensors' detecting range, the sensors' transmission range, and the quantity of sensors [15].

3. Energy Consumption Model

Due to resource constraint, lowering energy use and increasing WSN lifetimes are of crucial significance. Energy usage in WSNs is often analyzed using the conventional threshold, c0, which is based on the Radio Energy Dissipation Model (REDM) assumption of a constant distance c between the transmitting and receiving nodes. The energy used in transmitting a single bit:

$$F_{SV}(l,c) = \begin{cases} F_{elec} \times l + \xi_{et} \times l \times c^2, c < c_0 \\ F_{elec} \times l + \xi_{bno} \times l \times c^2, c \geq c_0 \end{cases} \quad (1)$$

The amount of power needed to receive a single bit:

$$F_{QV}(l) = F_{elec} \times l \quad (2)$$

Where l is the size of the data packet and F_{elec} is the amount of energy needed to send or receive 1 bit of data. When $c<c_0$,

the signal is sent across a short distance utilizing the free space model fs. When $c>c_0$, long-distance transmission is indicated by the multiple pathways transmitting attenuation model amp.

4. Data Collection Module

The parameters used by the data-gathering module are inferred from real-world observations of the effects of distributed denial-of-service (DDoS) attacks, gained via the modeling of nodes both before and after an attack, accounting for a variety of factors that affect network behavior. In the event of a breach by malicious nodes, the amount of packets received or sent by the targeted node and its neighbors in a given period will rise dramatically, causing them to exceed the available bandwidth limit and cause recurrent packet loss. Using the AODV routing protocol as an experimental foundation, we can identify the following characteristics of a DoS assault.

Quantity of packets acquired by node n in a given time interval (QO) is equal to the sum of the packets lost (OK) during that time interval.

$$Q_{CQ}(m,\tau) = \sum_\tau QO - \sum_\tau OK \quad (3)$$

The packet delivery rate (PDR) is calculated by dividing the number of packets obtained by all nodes in a network during a particular period of time by the number of packets lost over the same time period.

$$D_{QV}(m,\tau) = \sum_\tau QO - \sum_\tau OK \quad (4)$$

The loss of energy (KF) $E_{KF}(m,\tau)$ is equal to the amount of consumed energy per unit time for node n. Given formulae 1 and 2, we may write $E_{KF}(m,\tau)$ as follows. The amount of energy In Use per Second (Eidle) of a Node.

$$E_{KF}(m,\tau) = \sum_\tau G_{DV} + \sum_\tau F_{QV} + \tau F_{idle} \quad (5)$$

Time Delay In Whole (TTL) The median amount of period in units of time for the node n took to send packets to the destination node is denoted by S_{FFC} (m,τ), while the total amount of packets that were accepted is denoted by CO(Receive, Packets).

$$S_{FFC}(m,\tau) = \sum_\tau FFC / \sum_\tau CO \quad (6)$$

$Q_{cache}(m,\tau)$ is the use of a node's cache, where n is the number of nodes, K is the packet length, and CT is the cache size.

$$Q_{cache}(m,\tau) = \sum_\tau K / \left(CT \times D_{QV}(m,\tau)\right) \quad (7)$$

5. Support Vector Machine (SVM)

The basic concept is shown to function. Using preliminary processing, categorization, and kernel selection, the described SVM model combines intrusion detection. The first step is preprocessing the network data inputs into a more usable format. The next step is to classify the attacks using the SVM model. Finally, the ESVM model provided here entails the careful choice of the best kernels for the SVM and is used for incursion detection. Support vector machines (SVM), a kernel function called is used to transform the original data space into a higher-dimensional, completely new space.

One common artificial intelligence algorithm that serves for regression as well as classification is the Support Vector Machine (SVM). Machine Learning, on the other hand, use it for Classification issues. The purpose of a support vector machine (SVM) calculation is to locate the best line or decision limit that can partition the space with n dimensions into classes, making it simple to subsequently assign the fresh data point to the appropriate category. This optimum threshold is shown as a hyperplane. In order to build the hyper plane, a support vector machine (SVM) is employed to choose the wacky foci/vectors. The computer is known as a Support Vector Machine because support vectors are utilized to characterize the most severe cases.

SVMs may be either linear or non-linear. In cases when a dataset can be partitioned into two groups through a straight line, we refer to this kind of data as "linearly separable," and the classifier in question is known as a Linear Support Vector Machine (SVM). Non-Linear Support Vector Machines (SVMs) are used to classify data that cannot be organized linearly. Face recognition, image classification, text labeling, stock market predictions, and many other applications all benefit greatly from the use of

SVM Algorithms. SVM is a kind of supervised learning. In Rn x R, there is a set of training data denoted by (x1, y1) through (xn, yn) predicted using f(x) instead of y, which is sampled from a distribution O(y,x) whose shape is uncertain and whose slope is used to compute the error. Finding the function f that minimizes the error as presented is equivalent to finding the function that reduces the expected level of error on the new data.

$$\int U(z, e(w) O(y, x)\, cw\, cy \quad (8)$$

$$g_\theta(w) \geq 0.5 \rightarrow z = 1 \quad \text{(i)}$$

$$g_\theta(w) < 0.5 \rightarrow z = 0 \quad \text{(ii)}$$

0.5 is the decision boundary , and it is used in regression analysis,

$$I(\theta_0, \theta_1) = \frac{1}{2n} \sum_{j=1}^{n} (h_\theta(w_j) - Z_j)^2 \quad (9)$$

Where I= squared error cost function on Θ0 and Θ1, m= number of training examples, i= , Θ0 = parameters for the hypothesis *h*Θ , Θ1 = parameters for the hypothesis *h*Θ , *h*Θ = predicted value of the hypothesis, w_j = independent feature, Z_j= actual value to find the minimized error function.

6. Chaotic Levy Grasshopper Optimization Algorithm (CLGOA)

The chaotic Levy Grasshopper Optimization Algorithm is a metaheuristic method for optimizing a function by fusing ideas from chaotic dynamics and Levy flights. It takes its cue from the way grasshoppers move and their propensity for irrational leaps of discovery.

Ten different kinds of improved CLGOAs may be used to estimate the parameters of frequency-modulated sound synthesis or to construct three-bar trusses. The bridging mechanism of GOA was improved using ten chaotic maps, and the findings revealed that CLGOA with the Singer map was superior.

The Multi-Area Economic Dispatching (MAED) issue may be addressed with the use of a Logistic Map GOA (LMGOA) based on, one of the other 9 variations of CLGOA. Using Differential Evolution (DE), Evolutionary Programming (EP), Particle Swarm Optimization (PSO), and Artificial Bee Colony (ABC) as comparisons, LMGOA was shown to be superior in all three case studies. The results of the tests showed that LMGOA is better than both CLGOA and state-of-the-art methods.

It was suggested that the automated voltage regulator system use a PID controller based on an improved chaotic GOA (ECGOA). The error, robustness, stability, and transient responsiveness of ECGOA were all verified as satisfactory. Thirteen of the most common benchmark functions were used to test CLGOA's performance.The results of the studies showed that CLGOA provided superior solutions than those obtained using the traditional GOA.

Mathematical models of grasshopper swarming behavior look like this:

$$W_j = T_j + H_j + B_j \quad (10)$$

W_j stands for ith grasshopper, T_j represents the social interaction, $H_j$shows the gravity force on the ith grasshopper, and B_j represents the wind advection.

$$T_j = \sum_{i=1, i\neq j}^{M} t(c_{ji})\, \widehat{c_{ji}} \quad (11)$$

The t function is define social forces, is computed as:

$$t(q) = ef^{\frac{q}{k}} - f^{-r} \quad (12)$$

where f is the attractive force and l is the attractive distance scale.

The H component in Eq. (10)

$$H_j = -h\widehat{f_g} \quad (13)$$

The B component in Eq. (10)

$$B_j = v\widehat{f_x} \quad (14)$$

After substituting T. H and B in Eq. (10), the equation becomes

$$W_j = \sum_{i=1, i\neq j}^{M} t(|w_i - w_j|) \frac{w_i - w_j}{c_{ji}} - h\widehat{f_h} + v\widehat{f_x} \quad (15)$$

$$W_j^c = d_1 \left(\sum_{i=1, i\neq j}^{M} d_2 \frac{va_c - ka_c}{2} t(|w_i^c - w_j^c|) \frac{w_i - w_j}{c_{ji}} \right) + \widehat{S_c} \quad (16)$$

upper and lower bounds are represented by v_{ac} and k_{ac}. $\widehat{S_c}$represents the target value, d1 and d2 are the coefficients to shrink the comfort zone, repulsion zone and attraction zone

$$d = dmax - J \frac{dmax - dmin}{M} \quad (17)$$

J represents the number of current iteration and M represent the maximum number of iterations. Here dmax and dmin represents the maximum and minimum value of d.

7. Result and Discussion

In this research, we present an ESVM+CLGO-based intrusion detection system (IDS) that can protect a network against DDoS assaults. The experimental findings demonstrate that the network performance may be enhanced and brought closer to the ideal with the suggested ESVM+CLGO implemented into the system.

The suggested ESVM+CLGO method is effective in a large number of simulations to quickly identify network assaults and remove rogue nodes from the system. Other network assaults need to be the subject of future research. The analysis has a 97% degree of accuracy. After carefully comparing its performance to that of competing fuzzy logic-based method to avert intrusions (FzMAI) systems, researchers have determined that is the best option. The technology does not address the issue of detecting and preventing intrusions in WSNs.In addition, the data memory size and time-series forecasting are taken into account to assess the local outlier detection algorithm (LODA's) effectiveness, with the latter's ultimate goal being to anticipate the true worth of outlier data. The impact of noisy data as a proportion of the whole is another important but difficult area that needs further research. To better identify outliers in WSNs, we might consider combining uncertainty modeling with LODA.

7.1 Accuracy

To make reliable predictions in ESVM+CLGOA, it is necessary to consider both optimistic and pessimistic outcomes. The term accuracy is used to describe how close a forecast comes to the actual outcome, as well as how confidently it may be made. The detection efficiency was determined by comparing the predicted and observed values. The success rate of detecting the instrusions with our method is greater than using more conventional methods. The figure 2 stands for an assessment of the precision.

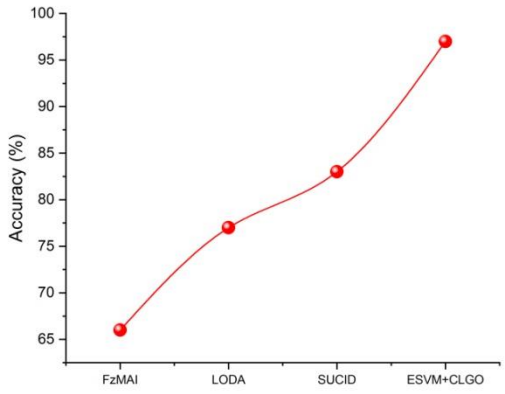

Fig.2. Accuracy

Table 1. Accuracy between existing and proposed

	Accuracy (%)
FzMAI	66
LODA	77
SUCID	83
ESVM+CLGO	97

7.2 Detection rate

It has been shown that when model complexity grows, the total detection rate falls. In a WSN-based IDS setting, fewer features are needed to detect threats. The proposed solution also improves upon existing execution times that are depicted in figure 3.

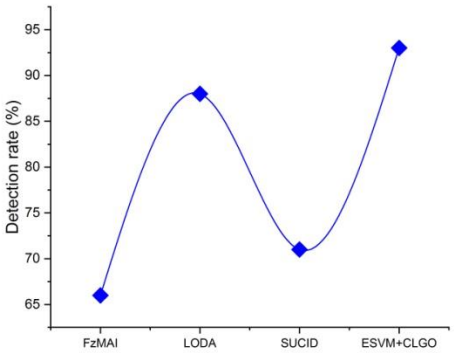

Fig.3. Detection rate

Table 2. Outcomes of Detection rate

	Detection rate (%)
FzMAI	66
LODA	88
SUCID	71
ESVM+CLGO	93

7.3 End to end delay (EED)

Each packet's time of arrival plus the total number of correctly intercepted packets equals the end-to-end delay (EED). Fig. 5 (a) shows the IDS in different situations with the increase of malicious nodes in the network, the network topology more complex, the network suffered more DoS attacks, the IDS average DR decreased; Malicious nodes have an impact on latency as a whole in Fig. 4 (b). The median network EED rises dramatically with the number of malicious nodes in the system. Figure 4 (b) demonstrates that as the end-to-end delay is increased from 49 ms to 1631 ms, the amount of unauthorized nodes in the system also increases from 0 to 10, but IDS is still able to effectively detect and remove those nodes from the entire network. Figure 4 (b) demonstrates that ESVM+CLGO outperforms other IDS in terms of its influence on EED, and hence is more suited to the

transmission job of wireless sensor networks.

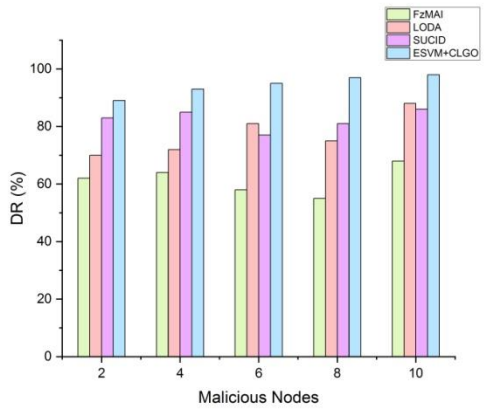

Fig.4(a). The relationship between the number of malicious nodes and the detection rate of IDS under DoS attack

Table 4(a). Malicious node detection in existing and proposed techniques

Malicious Nodes	**DR (%)**			
	FzMAI [16]	**LODA [6]**	**SUCID [2]**	**ESVM+CLGO**
2	62	70	83	89
4	64	72	85	93
6	58	81	77	95
8	55	75	81	97
10	68	88	86	98

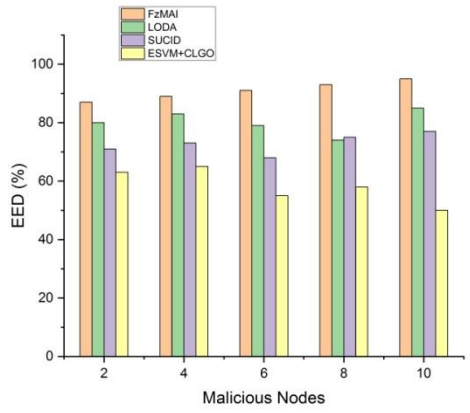

Fig.4(b). The relationship between the number of malicious nodes and network delay under DoS

Table 4 (b).Malicious node detection and delay in existing and proposed techniques

Malicious Nodes	**EED (%)**			
	FzMAI [16]	**LODA [6]**	**SUCID [2]**	**ESVM+CLGO**
2	87	80	71	63
4	89	83	73	65
6	91	79	68	55
8	93	74	75	58
10	95	85	77	50

8. Conclusion

The widely used and reliable ESVM feature selection technique is widely used in IDS and other applications. By prioritizing the most important characteristics, the CLGO algorithm may increase the efficiency with which intrusions are detected and the precision with which they are classified. Several authors have offered methods to boost the ESVM-based IDS scheme's performance. However, several issues reduce the algorithm's efficacy, including execution time, total features picked, and accuracy. The study improves the performance of an ESVM+CLGOA based IDS system in a WSN. A multi-objective function is used to improve the prediction system's overall performance. function is used to improve overall performance.As its effectiveness in predicting unknown classes increases, so do its speed of execution, the number of characteristics it chooses, and its accuracy. The proposed model is trained and tested, with the results compared to those of previously developed IDS methods based on ESVM and CLGO. Implementation time, total features chosen, false alarm rate, detection rate, and accuracy are all areas where the suggested model was shown to excel above the state-of-the-art models. Alternate deep-learning methodologies to enhance accuracy in classification will be the focus in subsequent studies.

References

[1] Shakya, S., 2021. Modified gray wolf feature selection and machine learning classification for wireless sensor network intrusion detection. IRO Journal on Sustainable Wireless Systems, 3(2), pp.118-127.

[2] Safaei, M., Ismail, A.S., Chizari, H., Driss, M., Boulila, W., Asadi, S. and Safaei, M., 2020. Standalone noise and anomaly detection in wireless sensor networks: a novel time-series and adaptive

Bayesian-network-based approach. Software: Practice and Experience, 50(4), pp.428-446.

[3] Singh, A., Amutha, J., Nagar, J., Sharma, S. and Lee, C.C., 2022. AutoML-ID: Automated machine learning model for intrusion detection using a wireless sensor network. Scientific Reports, 12(1), p.9074.

[4] Safaldin, M., Otair, M. and Abualigah, L., 2021. Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks. Journal of ambient intelligence and humanized computing, 12, pp.1559-1576.

[5] Alqahtani, M., Gumaei, A., Mathkour, H. and Maher Ben Ismail, M., 2019. A genetic-based extreme gradient boosting model for detecting intrusions in wireless sensor networks. Sensors, 19(20), p.4383.

[6] Singh, N., Virmani, D. and Gao, X.Z., 2020. A fuzzy logic-based method to avert intrusions in wireless sensor networks using WSN-DS dataset. International Journal of Computational Intelligence and Applications, 19(03), p.2050018.

[7] Maheswari, M. and Karthika, R.A., 2021. A novel QoS based secure unequal clustering protocol with intrusion detection system in wireless sensor networks. Wireless Personal Communications, 118, pp.1535-1557.

[8] Jhade, S. ., Kumar, V. S. ., Kuntavai, T. ., Shekhar Pandey, P. ., Sundaram, A. ., & Parasa, G. . (2023). An Energy Efficient and Cost Reduction based Hybridization Scheme for Mobile Ad-hoc Networks (MANET) over the Internet of Things (IoT). International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 157–166. https://doi.org/10.17762/ijritcc.v11i2s.6038

[9] Mohd, N., Singh, A. and Bhadauria, H.S., 2020. A novel SVM based IDS for distributed denial of sleep strike in wireless sensor networks. Wireless Personal Communications, 111(3), pp.1999-2022.

[10] Jeyaselvi, M., Sathya, M., Suchitra, S., Jafar Ali Ibrahim, S. and Kalyan Chakravarthy, N.S., 2022. SVM-Based Cloning and Jamming Attack Detection in IoT Sensor Networks. In Advances in Information Communication Technology and Computing: Proceedings of AICTC 2021 (pp. 461-471). Singapore: Springer Nature Singapore.

[11] Singh, A., Nagar, J., Sharma, S. and Kotiyal, V., 2021. A Gaussian process regression approach to predict the k-barrier coverage probability for intrusion detection in wireless sensor networks. Expert Systems with Applications, 172, p.114603.

[12] Mahamuni, C.V. and Jalauddin, Z.M., 2021, December. Intrusion monitoring in military surveillance applications using wireless sensor networks (WSNs) with deep learning for multiple object detection and tracking. In 2021 International Conference on Control, Automation, Power and Signal Processing (CAPS) (pp. 1-6). IEEE.

[13] Zhang, W., Han, D., Li, K.C. and Massetto, F.I., 2020. Wireless sensor network intrusion detection system based on MK-ELM. Soft Computing, 24, pp.12361-12374.

[14] Sharma, M. K. (2021). An Automated Ensemble-Based Classification Model for The Early Diagnosis of The Cancer Using a Machine Learning Approach. Machine Learning Applications in Engineering Education and Management, 1(1), 01–06. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/1

[15] Jiang, S., Zhao, J. and Xu, X., 2020. SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments. IEEE Access, 8, pp.169548-169558.

[16] O'Mahony, G.D., Curran, J.T., Harris, P.J. and Murphy, C.C., 2020. Interference and intrusion in wireless sensor networks. IEEE Aerospace and Electronic Systems Magazine, 35(2), pp.4-16.

[17] 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.

[18] Jianjian, D., Yang, T. and Feiyue, Y., 2018. A novel intrusion detection system based on IABRBFSVM for wireless sensor networks. Procedia computer science, 131, pp.1113-112.