Proceedings of the International Conference on Artificial Intelligence and Smart Systems (ICAIS-2021)
IEEE Xplore Part Number: CFP21OAB-ART; ISBN: 978-1-7281-9537-7

Intrusion Detection System using Optimal Support Vector Machine for Wireless Sensor Networks

Sibi Amaran
Research Scholar,
Department of CSE,
Annamalai University.
sibi.amaran@gmail.com,

Dr. R. Madhan Mohan
Associate Professor,
Department of CSE,
Annamalai University.
madhanmohan_mithu@yahoo.com

2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS) | 978-1-7281-9537-7/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICAIS50930.2021.9395919

***Abstract*—Wireless sensor networks (WSN) hold numerous battery operated, compact sized, and inexpensive sensor nodes, which are commonly employed to observe the physical parameters in the target environment. As the sensor nodes undergo arbitrary placement in the open areas, there is a higher possibility of affected by distinct kinds of attacks. For resolving the issue, intrusion detection system (IDS) is developed. This paper presents a new optimal Support Vector Machine (OSVM) based IDS in WSN. The presented OSVM model involves the proficient selection of optimal kernels in the SVM model using whale optimization algorithm (WOA) for intrusion detection. Since the SVM kernel gets altered using WOA, the application of OSVM model can be used for the detection of intrusions with proficient results. The performance of the OSVM model has been investigated on the benchmark NSL KDDCup 99 dataset. The resultant simulation values portrayed the effectual results of the OSVM model by obtaining a superior accuracy of 94.09% and detection rate of 95.02%.**

Keywords—Intrusion detection, WSN, Machine learning, SVM, Kernel selection

I. INTRODUCTION

Usually, Wireless Sensor Networks (WSNs) are infrastructure-less, distributed, and dynamic [1]. Fog computing is the best example for WSN. In order to meet the objectives like mobility support, geo-distribution, position details, and limited delay requirement for Internet of Things (IoT), while Fog node is served as a user in IoT execution. Due to the susceptible constraints of WSNs, these systems are prone to diverse risk factors and mitigates the system function. Authorized protocols and secured routing protocols imply the usage of cryptographic keys to ensure efficient and effective transmission that is not applicable for securing the intrusions named passive attacks. Hence, valuable data from attackers are considered to be passive attack from a node is inevitable.

According to the survey, [2] have addressed diverse class of feasible intrusions on WSNs like routing attacks, Sybil attacks, and Denial of Service (DoS). To resolve the above defined issues, Intrusion Detection Systems (IDS) is employed in WSNs to predict the abnormal behavior of nodes [3]. Moreover, cluster-based WSNs are capable of reducing the working burden interms processing and energy consumption of nodes [4]. Due to technological development, WSNs are visible and used in various domains of daily lifecycle. Therefore, security of a network is concentrated to make sure the best performance of WSN. Then, IDS-based methods are supreme in detecting irregular movement of internal nodes and limit malicious attacks. The intension of IDS is to collect and analyze the abnormal behavior in short span of time and helps in decision making process. Fig. 1 implies the structure of cluster based WSN (CWSN) model.

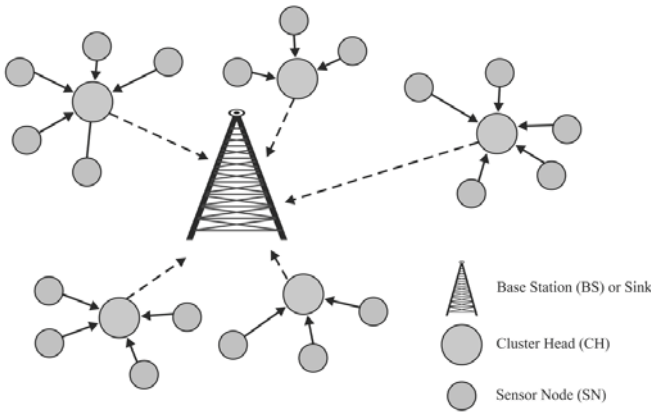

Fig. 1. Structure of WSN

[5] proposed a Deep Learning (DL) model for network intrusion prediction, which is used for reducing the training time of samples and comprised of higher accuracy and prediction measure. [6] deployed the IDS scheme according to the Recurrent Neural Network (RNN) in binary classification and multi-classification, where the effect of greater neurons and learning rate of working function.

[7] established a multi-agent IDS on the basis of immune strategy. The observing agent is used in each node, and decision agent maps the collected data features. If an attack is predicated on Sensor Node (SN), then adjacent Killer agent is active and ready to isolate the anomalous node. Hierarchical detection is applied for non-identical systems as provided by [8] and hierarchical intrusion employs the WSN layer. The SN is the 1st layer, aggregation nodes are 2nd layer, and upper Base Station (BS) is 3rd layer which is suitable to predict the intrusions, data analysis, and decide the intrusion. Due to the random initialization of Extreme Learning Machine (ELM)

model, it is impossible to make a sample-based nonlinear scheme. Kernel ELM (KELM) is used for resolving the problems and shows the optimal function.

[9] introduced online modeling of KELM based on robust leave-one-out cross-validation. The simulation results have depicted that newly presented model improvises the prediction measure of KELM, though the random decision of dataset is supreme in classification process. [10] deployed ELM for Multi-Layer Perceptron (MLP) and tested under the application of KDD CUP dataset where the working function is related to classical schemes to identify the better application. [11] utilized the optimization-based ELM for network intrusion detection and provided the adaptive optimization approach for hidden neurons with higher intrusion prediction value and rapid learning speed.

[12] deployed a standard clustering model termed adaptive chicken swarm optimization framework. By this model, the survival value and scalability of WSN could be maximized and time consumption is limited. Additionally, 2-stage classifier called adaptive support vector machine (SVM) is applied in acknowledgment-based scheme to report the malicious SN. [13] used the extended deep belief network with ELM (DBN-ELM) unified intrusion prediction system, where the model uses feature extraction of DBN to show a learning system, also ELM and final learning is evaluated with the help of majority vote.

This paper presents a new optimal Support Vector Machine (OSVM) based IDS in WSN. The presented OSVM model involves the proficient selection of optimal kernels in the SVM model using whale optimization algorithm (WOA) for intrusion detection. Since the SVM kernel gets altered using WOA, the application of OSVM model can be used for the detection of intrusions with proficient results. The performance of the OSVM model has been investigated on the benchmark NSL KDDCup 99 dataset.

II. Proposed Model

The overall working principle is demonstrated in Fig. 2. The presented OSVM model incorporates intrusion detection using three sub-processes such as pre-processing, classification, and kernel selection. Primarily, the input network data is preprocessed to transform it into a useful format. Followed by, the OSVM model is applied for classification of the intrusions. new OSVM based IDS in WSN. Thirdly, the presented OSVM model involves the proficient selection of optimal kernels in the SVM.

Here, intrusion prediction is carried out using SVM. The Modified Whale Optimization Algorithm (MWOA) has been applied for selecting the best kernel in SVM classification model. A kernel function employed in SVM, $K(x_n, x_i)$, converted the actual data space a novel space with maximum dimension. Hence, the accuracy of WOA models is defined can be improvised by allocating objective function values to random measures.

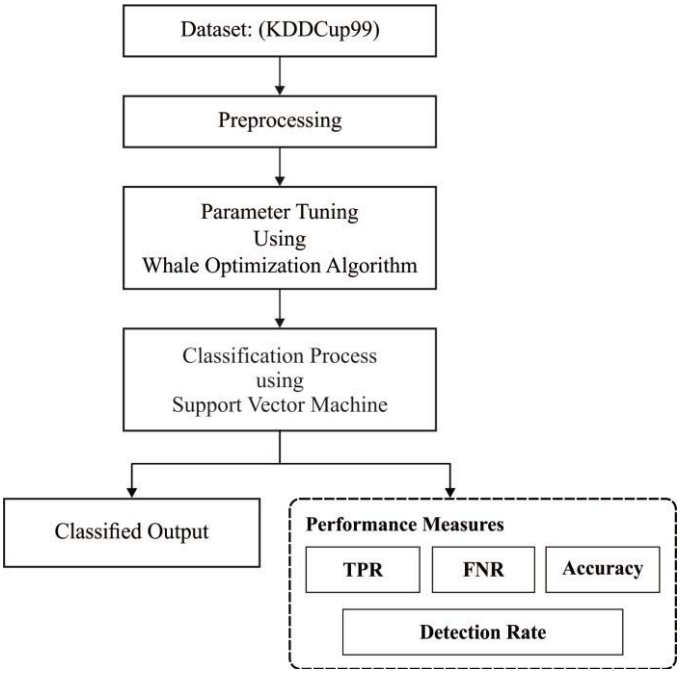

Fig. 2. Working process of OSVM model

It is classified as (i) surrounding the prey, (ii) exploitation (bubble-net attacking) stage, and (ii) exploration of prey. In case of hunting, whales apply the spiral bubble mechanism as demonstrated in WOA.

A. Encircling Prey Phase

Here, the whale explores prey and find the actual location. Followed by, it surrounds the prey as it does not escape from them. This is quantified in the following:

$$D = |C \cdot U^*(z) - U(z)|, \quad (1)$$

$$U(z+1) = U^*(z) - A.D, \quad (2)$$

where A and C defines the coefficient vector, present iteration is saved by z, and U^* implies the optimal position vector attained in recent phase whereas U shows the supreme value of respective position vector. The coefficient vectors are determined by,

$$A = 2a \cdot r_1 - a, \quad (3)$$

$$C = 2 \cdot r_2,$$

where r_1, r_2 implies the random values that reduce linearly in exploitation and exploration states.

B. Exploitation (Bubble-Net Attacking) Phase

It points out the execution of 2 models called shrinking encircling technique and spiral updating position.

Whales enhance the location as defined in the following expression:

$$U(z+1) = De^{bz}\cos(2\pi z) + U^*(z), \quad (4)$$

where $D = |U^*(z) - U(z)|$ refers the distance from present whale's and prey's location and b depicts a constant that illustrates the action of whales in spiral path. This switching is described in numerical format as,

$$U(z+l) = \begin{cases} U^* - AD, p < 0.5 \\ De^{bz}\cos(2\pi z) + U^*(z), p \geq 0.5 \end{cases} \quad (5)$$

where p implies a random value from $[0, 1]$.

C. Exploration (Search for a Prey) Phase

It finds the feature of whales to update the position with reference whale, that is selected in random fashion. Hence, the enhancement to find optimal whale for global search is projected by Eqs. (6) and (7):

$$D = |CU_{rand} - U|, \quad (6)$$

$$U(z+1) = U_{rand} - AD, \quad (7)$$

where U_{rand} denotes the random value that identifies the position of randomly decided whale. This is repeated until reaching the higher iteration.

Furthermore, WOA is improved to MWOA by estimating random measures, r_1 and r_2, applied to encircle the prey as per Eqs. (8) and (9):

$$r_1 = \frac{f_{mx} + f_{mn}}{2}, \quad (8)$$

$$r_2 = \frac{f_{mx} - f_{mn}}{2}, \quad (9)$$

where f_{mx} denotes higher value of Fitness Function (FF) and f_{mn} implies lower value of FF from MBPSO.

D. The Objective Function

The main aim of estimating objective function is to improvise the accuracy of WOA in stress level examination as shown below,

$$Fit = \max_{i=1:n} i = l{:}n\left(\frac{(t_p + t_n)}{(t_p + t_n + f_p + f_n)}\right), \quad (10)$$

where t_p and t_n depicts True Positive (TP) and True Negative (TN); f_p and f_n illustrates the False Positive (FP) and False Negative (FN).

III. Performance Evaluation

The experiment is carried out on an Intel®-core ™ i7-7500 2.70-2.90 GHz CPU processor, 8 GB memory, and running Windows 10 OS (64-bit). The software environment is MATLAB R2014b version. The performance of the proposed OSVM model is validated employing KDDCup99 dataset. Fig. 3 demonstrates the visualization of KDDCup99 dataset.

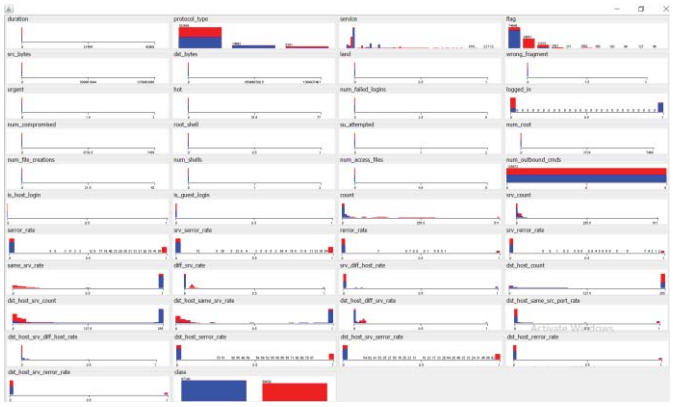

Fig. 3. Visualization of KDDCup99 Dataset

Table 1 and Figs. 4-5 shows the detailed comparative results analysis of the OSVM model with existing methods. The results have demonstrated that the OSVM model has attained a maximum classification outcome over the other techniques. On determining the results with respect to accuracy, it can be evident that the SVM and ELM methodologies have resulted in minimum accuracy values of 88.20% and 87.90% correspondingly. Also, the HIDS and MK-ELM techniques have exhibited moderate outcomes with the accuracy of 91.26% and 92.10% respectively. However, the OSVM model has obtained a maximum accuracy of 94.09%. On estimating the result by means of TPR, it can be clear that the SVM method has resulted in a limited TPR value of 83.73%. Likewise, the ELM model has portrayed reasonable outcomes with a TPR of 83.84%. In line with, the MK-ELM method has reached a competitive TPR of 89.42%. But, the OSVM model has achieved a maximum TPR of 95.53%.

TABLE I

RESULTS ANALYSIS OF PROPOSED OSVM ON KDDCUP99 DATASET

Performance Measures	OSVM	HIDS	SVM	ELM	MK-ELM
Accuracy	94.09	91.26	88.20	87.90	92.10
True Positive Rate	95.53	-	83.73	83.84	89.42
False Negative Rate	4.47	-	16.27	16.16	10.58

Detection Rate	95.02	90.96	74.74	75.53	83.81

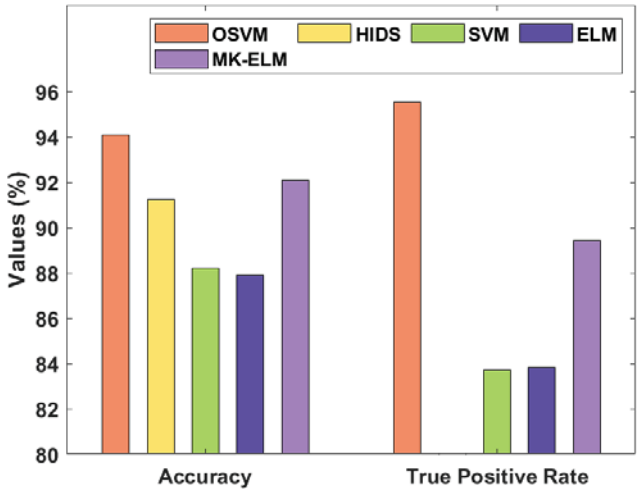

Fig. 4. Accuracy and TPR analysis of OSVM model

On estimating the results interms of FNR, it is evident that the SVM model has resulted in superior FNR value of 16.26%. Also, the ELM model has demonstrated moderate results with an FNR of 16.16%. Likewise, the MK-ELM model has obtained a competitive FNR of 10.58%. However, the OSVM model has reached a minimum FNR of 4.47%. On evaluating the outcomes interms of detection rate, it can be marked that the SVM and ELM models have resulted to lower detection rate values of 74.74% and 75.53% respectively. Besides, the MK-ELM methodology has depicted considerable outcomes with a detection rate of 83.81%. Along with that, the HIDS model has attained a competing detection rate of 90.96%. However, the OSVM model has obtained a maximum detection rate of 95.02%.

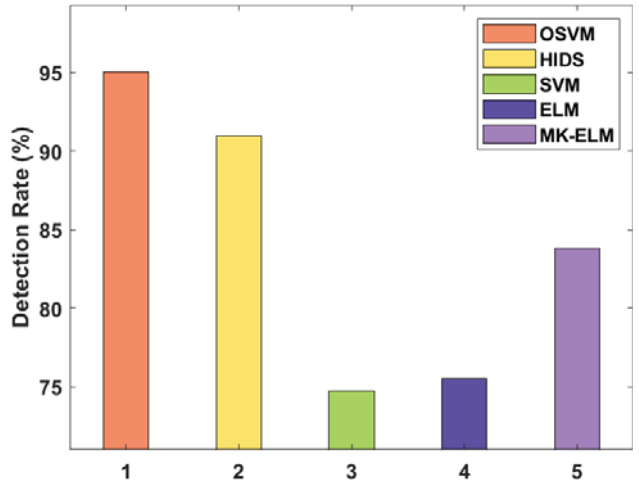

Fig. 5. Detection Rate analysis of OSVM model

IV. Conclusion

This paper has developed an effective OSVM based IDS model in WSN. The presented OSVM model incorporates intrusion detection using three sub-processes such as pre-processing, classification, and kernel selection. Primarily, the input network data is prepocessed to transform it into a useful format. Followed by, the OSVM model is applied for classification of the intrusions. new optimal Support Vector Machine (OSVM) based IDS in WSN. Thirdly, the presented OSVM model involves the proficient selection of optimal kernels in the SVM model using WOA for intrusion detection the performance of the OSVM model is investigated on the benchmark NSLKDDCup 99 dataset. The resultant simulation values portrayed the effectual results of the OSVM model by obtaining a superior accuracy of 94.09% and detection rate of 95.02%. As a part of future improvement, the WOA can be replaced by hybrid metaheuristic algorithms.

References

[1] Baraneetharan, E. "Role of Machine Learning Algorithms Intrusion Detection in WSNs: A Survey." Journal of Information Technology 2, no. 03 (2020): 161-173.

[2] Smys, S., Abul Basar, and Haoxiang Wang. "Hybrid Intrusion Detection System for Internet of Things (IoT)." Journal of ISMAC 2, no. 04 (2020): 190-199.

[3] A. Mehmood, M.M. Umar, H. Song, 'ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks, Ad Hoc Netw. 55 (2017) 97–106.

[4] V. Patel, J. Gheewala, An efficient session key management scheme for cluster based wireless sensor networks, in: Proc. IEEE Int. Adv. Comput. Conf. (IACC), 2015, pp. 963–967.

[5] Shone N, Ngoc TN, Phai VD et al (2018) A deep learning approach to network intrusion detection. IEEE Trans Emerg Top Comput Intell 2(1):41–50

[6] Yin C, Zhu Y, Fei J et al (2017) A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access 5(2):21954–21961

[7] Zhang, F., Guo, S., Zhang, C. and Guo, P., 2019. An interval multiobjective approach considering irrigation canal system conditions for managing irrigation water. Journal of Cleaner Production, 211, pp.293-302.

[8] Rani TP, Jayakumar C (2017) Unique identity and localization based replica node detection in hierarchical wireless sensor networks. Comput Electr Eng 64:148–162

[9] Zhang YT, Ma C, Li ZN et al (2014) Online modeling of kernel extreme learning machine based on fast leave-one-out crossvalidation. Shanghai Jiaotong Univ (Sci) 48:641–646

[10] Tang J, Deng C, Huang GB (2016) Extreme learning machine for multilayer perceptron. IEEE Trans Neural Netw Learn Syst 27(4):809–821

[11] Wang CR, Xu RF, Lee SJ et al (2018) Network intrusion detection using equality constrained-

optimization-based extreme learning machines. Knowl Based Syst 147:68–80

[12] Borkar GM, Patil LH, Dalgade D et al (2019) A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: a data mining concept. Sustain Comput Inform Syst 23:120–135

[13] Liang, D. and Pan, P., 2019, July. Research on intrusion detection based on improved DBN-ELM. In 2019 International Conference on Communications, Information System and Computer Engineering (CISCE) (pp. 495-499). IEEE.