IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007077|

Decentralized Intrusion Prevention (DIP) Against Co-ordinated Cyber Attacks On Distribution Automation Systems

Dr. R. Vijayanand[1] , B. Pravallika[2], B. Bhargavi [3], N. Eshwitha[4], Ritika Kalyani [5]

Assistant Professor, Department of Computer Science Engineering, J. B. Institute of Engineering and Technology, Moinabad, Hyderabad, Telangana, India [1]

B. Tech Student , Department of Computer Science Engineering, J. B. Institute of Engineering and Technology, Moinabad, Hyderabad, Telangana, India [2,3,4,5]

ABSTRACT: Nowadays, every digital network and communication technology are integrated into distributed systems which makes today's digital network more remotely monitored. Thus, the distribution grid or smart grid is more vulnerable. Though there are various anti-virus software packages and firewalls are unable to prevent vulnerabilities. That is the main reason why the intrusion detection and prevention play major role in today's network security. In this project we proposed, DIP (Decentralized intrusion prevention) with Whale Optimization Algorithm with K-NN Classifier. The main reason for choosing whale optimization algorithm with K-NN classifier is, it gives more accurate results.

KEYWORDS: Intrusion detection, Intrusion prevention, K-NN classifier, Network security

I. INTRODUCTION

In this paper, I want to let you know what an intrusion means. An intrusion is an unauthorized activity on a digital network. This intrusion involves activities like unauthorized activity, denial of service, and various types of exploits.
Intrusion Detection System (IDS): Intrusion Detection System is a software security application that monitors network's traffic and system activities for any malicious activity.
Intrusion Prevention System (IPS): Intrusion Prevention System is a form of network security that works to detect and prevent identified threats. Like IDS, it also monitors our network for any possible malicious events and captures information about those events and also reports activities of these events to the system administrator. Furthermore, it prevents the succession of the threat.

Intrusion prevention systems are of mainly two types. They are:

1. Network-based intrusion prevention system (NIPS)
2. Host-based intrusion prevention system (HIPS)

Network-based intrusion prevention system (NIPS): Network-based intrusion prevention system mainly monitors the network traffic to know the occurrence of threat. The main goal of the NIPS is to prevent the network from threats such as cyber-attacks, unauthorized activity.
Host-based intrusion prevention system (HIPS): Host-based intrusion prevention system is similar to network-based intrusion prevention system but monitors the internal system activities.

II. RELATED WORK

Nilesh kunhare, Ritutiwari and Joydipdhar introduced an intrusion detection system using machine learning techniques where they have used particle swarm optimization algorithm for feature selection [1]. It is derived from the bird flocking behaviour. It involves the adaption of rapidly changing movements and interactions of social animals like birds and fishes. They used SVM classifier.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007077|

Zaman, S.; El-Abed, M.; Karray, F. proposed a model to select features for IDSs[2]. Those features were selected through using evolutionary algorithms: GA, PSO and differential evolution. They conducted a comparison between these algorithms in terms of efficiency. But the accuracy rate by using these algorithms got very less. So we proposed whale optimization algorithm for feature selection using a classifier called KNN (K- nearest neighbor). By using whale optimization algorithm with K-NN classifier we got the accurate results with the accuracy of 98.42%.

III. METHODOLOGY

The Methodology consists of six stages. They are Collection of Datasets, Pre-processing, Applying WOA algorithm, Training and Testing data, Validation of the model, Attack prevention.

Step 1 – Collection of datasets: In this paper, the data is collected from a dataset called CICIDS2017 dataset which contains up-to-date common attacks and real-world data analysis using CICFlowmeter with labelled flows. The collected data is converted into .csv file so that it can be read easily by the machine.

Step 2 – Pre-processing: Data pre-processing is converted with the collection of data from the dataset provided and converting it into a format that is understandable by the intrusion detector. The dataset is passed through several pre-processing steps such as removal of labels, removing features, label encoding and data binarization.

Step 3 – Applying whale optimization algorithm: After cleaning the data, it is passed through the feature selection algorithm i.e., whale optimization algorithm. Now, the dataset is split into two datasets that one dataset can be used to create the model by training an algorithm and other dataset to test the model. In this paper, the data is split in the ratio of 7:3, 70% of training data and 30% of testing data. In the testing data, we separate actual values from the dataset. Feature selection algorithm WOA is applied to the data .It helps us in getting the informative features i.e., whether the attack has occurred or not. Now the data is given to the classification machine learning algorithm for training as well as testing. In this paper, we are using KNN classifier.

Step 4 – Training and Testing: As the next step, KNN classifier is used for training and testing. The performance of the KNN classifier algorithm depends on the value of k, the number of nearest neighbors of the test process we applied the k value as '5'.

Step 5 –Validation of model: After completing all the above mentioned steps and the classifier is trained using optimal subset of features. The test data is then directed to saved trained model to detect intrusions. Records matching to the normal class are considered as normal data and the other records are reported as attacks.

Step 6 – Attack prevention: If there is any attack encountered then the system is blocked and the same information is shared to the other system which ensures that only good traffic of network passes through the system.

IV. PSEUDOCODE

Step 1: Collect the data from the dataset CICIDS2017.
Step 2: Perform data pre-processing such as removing labels, encoding data, removing features and data binarization.
Step 3: Values in each feature must be standardized. Thus, least value in each feature should be 0 and maximum value should be 1.
Step 4: Split the data into two parts. In this paper, the data is split in the ratio of 7:3, 70% of training data and 30% of testing data. In the testing data, we separate actual values from the dataset.
Step 5: Apply WOA algorithm to the training dataset to perform feature selection.
Step 6: The output that we get from the WOA algorithm is given as input to the machine learning algorithms for training. Here we use KNN classifier for classification of model
Step 7: From step 4, the testing data is given to the model for prediction and validation. We compare the predicted values and the actual values for finding the accuracy of the model.
Step 8: A graph with fitness value on Y-axis and number of iterations on X-axis is created to analyse the performance.

V. EXPIREMENTAL RESULTS

In figure 1 where the Genetic algorithms(GA) and K-NN classifier are used, the accuracy of 96.6% is achieved, whereas, in figure 2 where Particle swarm optimization(PSO) and K-NN classifier is used, the accuracy of 96% is achieved.

In figure 3, Whale optimization algorithm and K-NN classifier techniques are used and we got the highest accuracy i.e. 98.42% which is greater than the existing models. Whale optimization algorithm finds the informative features from the given dataset and then it is given as input to the Machine learning algorithm K-NN classifier for prediction.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007077|

This algorithm is mostly used for classification and regression models as it gives efficient and accurate results compared to other algorithms and is easy to implement. So, this is the reason we got the highest accuracy for this model. This model also handles a large amount of data and it doesn't crash even it is overloaded. In this paper, we trained and tested this model with 9920 set of features so that it can handle the overload.

The below figures show the accuracy of different models which are built using different algorithms

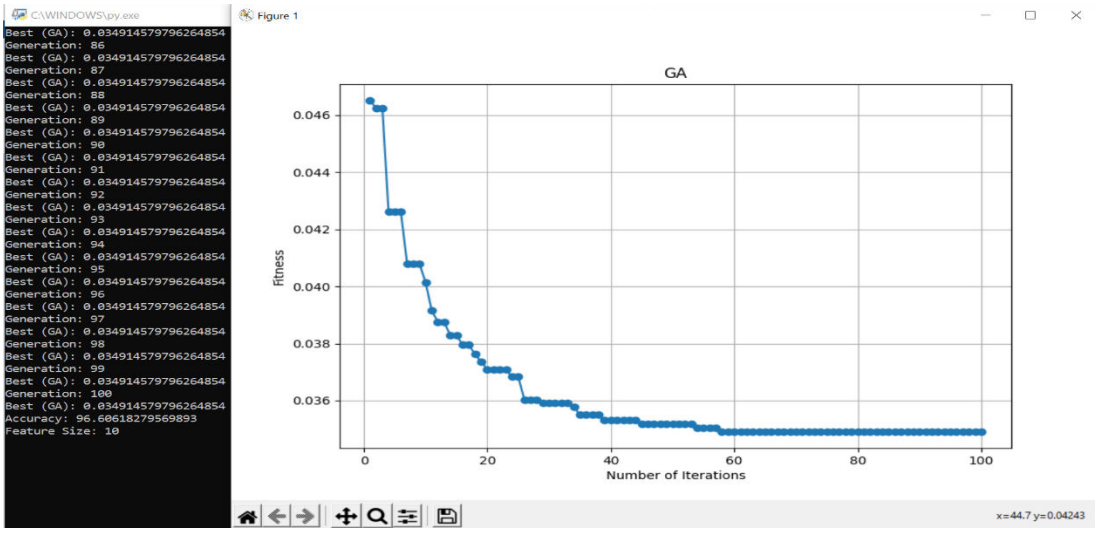

Fig 1: Model built using GA and K-NN classifier

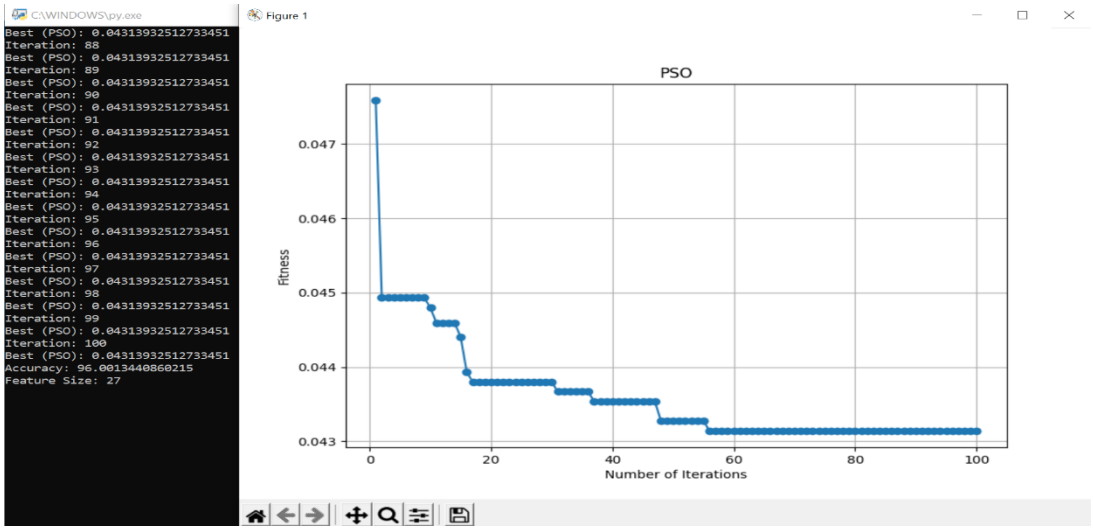

Fig 2: Model built using PSO and K-NN classifier

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007077|

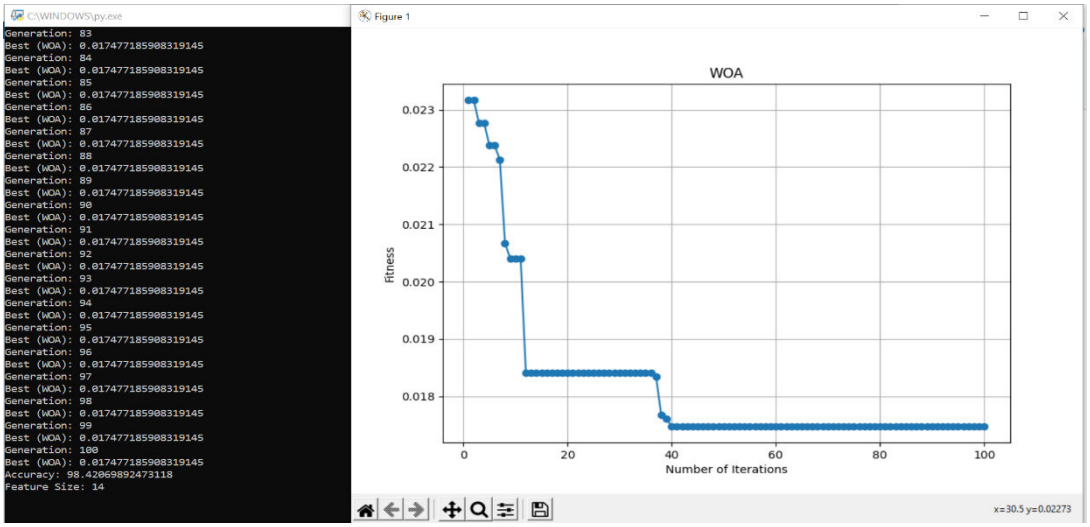

Fig 3: Model built using WOA and K-NN classifier

VI. CONCLUSION

In this paper, we proposed a novel feature method using whale optimization algorithm and KNN classifier for improving the performance of intrusion detection system. This method selects the most informative features from the existing network data which helps us to improve the accuracy of KNN based intrusion detection system. We made comparison of proposed method with the other feature selection algorithm like dragon fly algorithm and pigeon inspired optimization algorithm on the basis of detection rate, execution time, computational complexities provided the efficiency of the proposed method.

As we look towards the future, as the threats are increasing in scale, more security vendors are focusing on various machine learning algorithms in order to take action over various intrusion that are taking place in a network. There are also various techniques like white box testing, black box testing that pay way for the intrusion detection and prevention system. Additionally, we also have accessed latest technology and security professionals to discover, analyse and suppress latest threats. More and more human analysis, incident-response team and forensic team need to be involved in every company to build modern intrusion detection and prevention systems. Automotive industry needs to incorporate defensive intrusion detection and prevention into the latest path as the impact of attacks could be disastrous.

REFERENCES

[1] Nilesh Kunhare , Ritu Tiwari And Joydip Dhar, "Particle swarm optimization and feature selection for intrusion detection system", Sadhana (2020) 45:109 , https://doi.org/10.1007/s12046-020-1308-5Sadhana(0123456789).

[2] Zaman, S.; El-Abed, M.; Karray, F. Features selection approaches for intrusion detection systems based on evolution algorithms. In Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, Kota Kinabalu, Malaysia, 17–19 January 2013; pp. 1–5

[3] Syarif, I. Feature selection of network intrusion data using genetic algorithm and particle swarm optimization. EMITTER Int. J. Eng. Technol. 2016, 4, 277–290.

[4] S. Mirjalili and A. Lewis, "The whale optimization algorithm", *Adv. Eng. Softw.*, vol. 95, pp. 51-67, May 2016.

[5] D. E. Goldberg, Genetic algorithms in Search Optimization and Machine Learning, Reading, MA, USA:Addison-Wesley, 1989.

[6] B. Mukherjee, L. T. Heberlein and K. N. Levitt, "Network intrusion detection", *IEEE Netw.*, vol. 8, no. 3, pp. 26-41, May 1994.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details