Prediction of Network Attacks using Bio-Inspired Machine Learning Algorithm

Ananya Aggarwal, Priyam Agrawal, Kanmani Sivagar

***Abstract:** Most of the times, data is created for the Intrusion Detection System (IDS) only when the set of all real working environments are explored under all the possibilities of attacks, which is an expensive task. Network Intrusion Detection software shields a system and computer network from staff and non-authorized users. The detector's ultimate task is to build a foreboding classifier (i.e. a model) which would help in distinguishing between friendly and non-friendly connections, known as attacks or intrusions.This problem in network sectors is prevented by predicting whether the connection is attacked or not attacked from the dataset. We are using i.e. KDDCup99 using bio inspired machine learning techniques (like Artificial Neural Network). Bio inspired algorithm is a game changer in computer science. The extent of this field is really magnificent as compared to nature around it, complications of computer science are only a subset of it, opening a new era in next generation computing, modelling and algorithm engineering. The aim is to investigate bio inspired machine learning based techniques for better packet connection transfers forecasting by prediction results in best accuracy and to propose this machine learning-based method to accurately predict the DOS, R2L, U2R, Probe and overall attacks by predicting results in the form of best accuracy from comparing supervised classification machine learning algorithms. Furthermore, to compare and discuss the performance of various ML algorithms from the provided dataset with classification and evaluation report, finding and analysing the confusion matrix and for classifying data from the priority and result shows that the effectiveness of the proposed system i.e. bio inspired machine learning algorithm technique can be put on test with best accuracy along with precision, specificity, sensitivity, F1 Score and Recall.*

***Keywords** : Bio-inspired, Intrusions, KDDCup99, Machine Learning*

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author

Ms. Ananya Aggarwal, Student, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India. Email: ananya1398@gmail.com

Mr. Priyam Agrawal, Student, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India. Email: priyam1712cse@gmail.com

Mrs. Kanmani Sivagar, Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India. Email: kanmanis@srmist.edu.in

I. INTRODUCTION

Bio-inspired computing, also known as biologically inspired computing, is a field that combines all subfields related to the topics of connectionism, emergence and social behaviour. It is most of the time related to the field of AI(artificial intelligence), as many of its pursuits can be linked to machine learning. It relies majorly on the fields of mathematics , computer science and biology. Bio-inspired computing comes under natural computation. The concept of bio computing can be defined as the biological usage or its

processes in forming new computational techniques and new fields of computer science.

Genetic algorithm (GA) is often homogenous with respect to the existing used learning algorithms. Also, new physiological observations says that in biological neurons, synapses changes themselves with the local learning rules and it presents a biophysically motivational learning rule which adhers by the shape of the correlated signals resulting in learning properties which depends on the dendritic site. We examine this rule in a biophysical model and in an equivalent artificial neural network model. For this, it requires association of scientists and researchers from different communities like artificial intelligence , computer science, ecology, biology, social science etc. in order to have a wider and detailed analysis of each micro level interactions there by having much more significant and remarkable results.

II. RELATED WORK

Zhang et al.[1] introduced a clustered intruding system which takes in consideration the Sybil attack to ameliorate the rate of likelihood of double spending happening in the network of Bitcoin. They combined a Sybil attack and a double-spend attack in their new study. On the negative side , the model lacks in providing information about the intruder making distinct profiles. Therefore , the rate of happening the above is not on a higher end.

Ma et al.[2] showcased the forth put generalship would boost the discovery utility to a good extent than generalships like discovery which is uniform in nature and the effective detection. A discovery which is consistent in nature tells us the each possible path which is consistent. However as the levelling of intrusion technology with proper coordination is taking place at a high rate , the intruders are migrating from the stone age DDoS intrusions to newly advanced DDoS intrusions. The only problem with this is that the intrusions are not being completely eradicated against distinct connections through internet.

Sun et al.[3] put forward a newly developed technique including ways to decide path for multi-AUVs cooperative full coverage using Glasius Bio Neural Network (GBNN) algorithm. In the GBNN and the AUV method, the information about the environment is given by the AUV itself. Each one of the AUV senses other AUVs as a hurdle which are mobile. AUV in water area gets a green light to move around freely. This multi-AUV model does not inculcate NN(Neural Network) and grid map in it. Zhang et al.[4] stated a method called Physarum Solver. It was used to solve the counterbalance issue of traffic network assignment. This method results in the most advantageous result by automatically modifying each link's worth. It reaches the counterbalance assignment by dividing the demand among OD pairs present in the chain. Many numerical instances were taken to help in portraying this algorithm. It has not found accurate mathematical model to solve the traffic equilibrium assignment problem. Yuan et al.[5] proposed a taxonomy of adversial example. This paper tried to emphasize on the studies of inhospitable instances of DL domain. Correlating it with current other work, it demonstrated various threats and their results in the instances. It did not make large-scale applications, which resulted in difficulty in testing the tenacity of DNN architecture. Villain et al.[6] presented the puzzling scenario with the discovery of intersperse manifold-category intrusions penetrating through a system network connection and enlightened about the misleading analysis by interspersing and thievery intrusions. Hidden Markov Model (HMM) is given importance as it inculcates two of its unifying structure(architecture) coming from ML strategy resulting in evaluation power and its acting consequences. Shawly et al.[7] presented an interesting discovery plan of Neural Network intrusion by closely analyzing the irregularity in the act of exchanging information link. The intended intrusion discovery plan is swift than the old and typical objects wherein a pause has to be dealt with until the physical nodes are destroyed and vanished. Apart from this, a known group of intrusions contributing to adjourning and ruining of packets is also discovered using intended intrusion discovery plan. Intrusions which are wordly or refined are not discovered through this method. Yang et al.[8] introduced Honeypot strategies for finding solution to DDoS attacks in IIoT world using SDN. Dynamic protection for SDN is provided by honeypot. It offers a strategy for most advantageous protection while going through DDoS attacks. It demonstrates an anti-honeypot related attack for assisting intruders. A pseudo-honeypot game method is also proposed for studying the interaction between intruders and defenders.

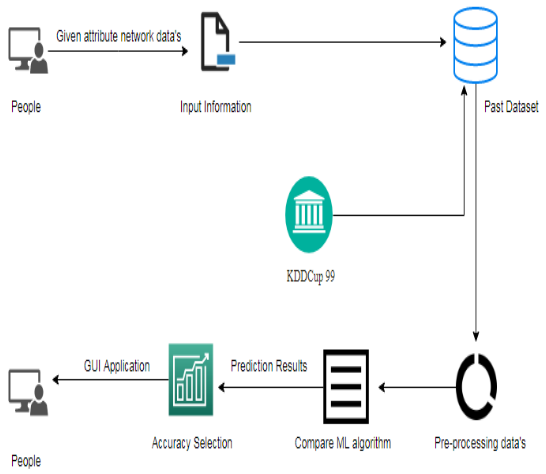
Zhang et al.[9] presented that a spontaneous opinion of intrusion basis coming from the core depth of network stage has proven to be a safe spot for applications from acquiring the standard and countable force of reasoning of the initial intrusion ground metric. Also, actions were developed and carved to contradict ZD intrusions i.e. zero day intrusions for quantitating connection's deformity keeping safety and security in consideration from the upper visible level to the network stage. Two strategies were developed showing conversion from intrusion ground of every encoded computer instructions to an intrusion likelihood and ultimately piling those combined similar likelihoods to a unified quantity of intrusions in network . On top of this , a successful attempt was made in designing a heuristic approach contributing to evaluation of intrusion in connection , minimizing the work of computing the intrusion surface for a single software encompassing inside a compressed expenditure. Hu et al.[10] researched the viewer-based ETC for a range of interlinked machines connected to each other via a linear topology under recurring Denial of Service confined intrusions. An advanced pliant action occurring transmission technique was put forward to improve the competency of interlinked materials whilst not hindering the denial of service intrusions. Taking innovatory notes from the spasmodic characteristics of the denial of service intrusions, a fresh viewer fault detector machine model was laid down helping in analyzing consequences of the pliant action inspired tool and containing in a binding well defined boundary. Li et al.[11] devised and suggested a positive thinking about the cloud environment created by the micro service architecture as well as container technology for overpowering less rate defined denial of service intusions with increased alarmity. To achieve this , mathematical system was created to formulate the above situation around cloud container surrounding. This opened gates for defending defined DOS intrusions in the above mentioned surrounding with the help of minimal materials. This in turn gave scholars a technique to alleviate low damaging defined DOS intrusions. The above may actively distribute the resources and can amend the count of packets(containers) to counter-attack DDoS type of intrusion.

III. PROPOSED METHODOLOGY

The methodology aims in observing the most important features that help to predict the type of attacks, i.e, DoS, R2L, U2R and Probe and combination of attacks and to identify the trends that will help us in hyper parameter selection and selection of model. We use bio-inspired machine learning classification methods to aid in predicting the class of new input. To investigate the network connection and identify whether it is attacked or not based on the data set. Finally, to evaluate and analyze statistical and visualized results, which find the standard patterns for all regiments.

Attacks are classified into the following mail classes:

1. Denial of Service(DoS)
2. User to Root(U2R)
3. Remote to User(R2L)
4. Probing



A. Denial of Service

DOS or denial of service is a sub category of intrusions wherein an intruder plays and jumbles with the storage and evaluating assests and make them appear as too cluttered and overblown to grasp sanctioned requisitions , rejecting permissible people to gain control of the system.

B. User to Root

In User to Root intrusion, the intruder begins with admittance to an authenticated end user account and gains root access on the system. Everyday faults in programming and the environment presumptions give the attacker a chance to modify the susceptibility of root access.

C. Remote to User

In this intrusion, an attacker transfers packets to the system through a chain which takes advantage of the system's susceptibility to gain an illegal access as an owner. There are various classes of R2L intrusions and the most familiar intrusion done that belongs to this is social engineering.

D. Probe

Probe is a class of attack wherein an attacker collects information about a network in a way that helps in finding the possible loopholes. An intruder has a design of services and system which are present on a chain that helps to play with the data in order to look for vulnerabilities and ruins. There are various types of these: some misconduct the system's built-in features and some using techniques like. This class requires very minimal specialised and professsional knowledge.

IV. RESULTS

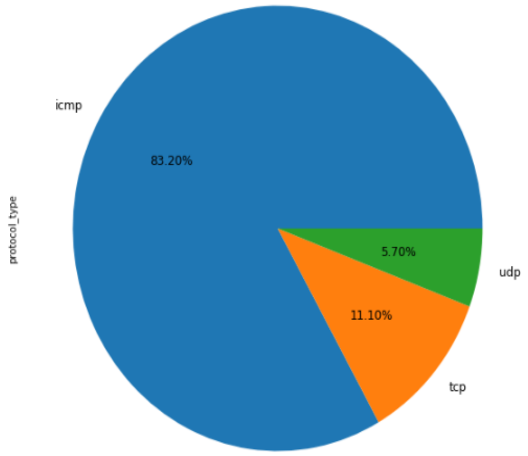


Fig. 1.Percentage count of protocol type

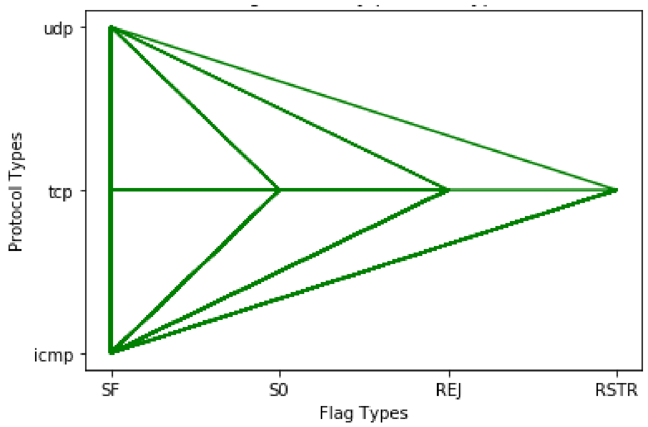


Fig. 2.Flag details by each protocol type

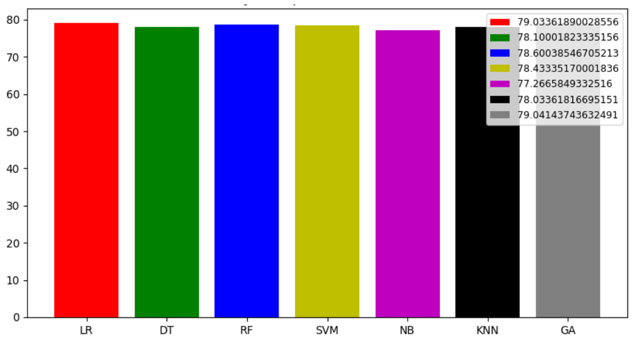


Fig. 3.Accuracy calculation of DoS attack

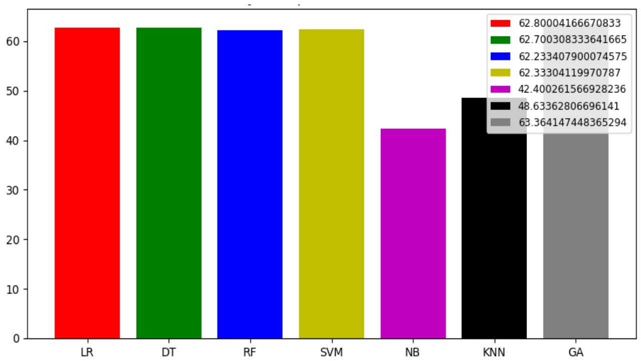


Fig. 4.Accuracy calculation of R2L attack

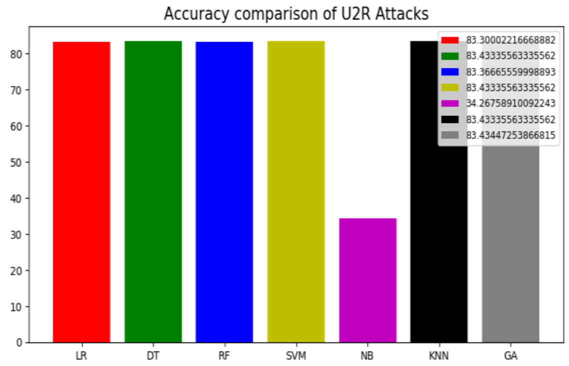


Fig. 5.Accuracy calculation of U2R attack

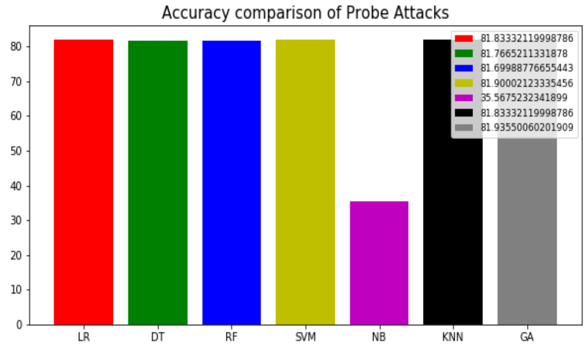


Fig. 6.Accuracy calculation of Probe attack

Retrieval Number: F1138038620/2020©BEIESP
DOI:10.35940/ijrte.F1138.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

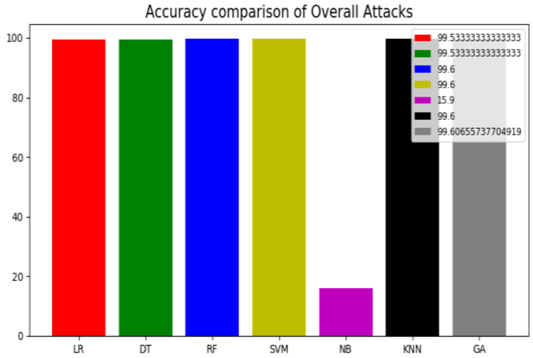


Fig. 7.Accuracy calculation of overall attack

V. CONCLUSION

In this paper, Bio inspired Algorithm along with other Machine learning algorithms is carried out on KDD Cup 99 dataset. First, separate analysis of different algorithms along with bio inspired is performed by applying it to U2R , R2L , DOS and probe attacks. It analyses the involvement of each network attacks to classification and their properties are selected as relevant features. Then comparative analysis is applied on and classification summary for each category is presented. As compared to the existing algorithms and techniques, our proposed work fairly improves the classification accuracy for R2L , DOS , Probe and U2R attacks. Hence we can conclude that the Bio-Inspired Algorithm proves to be an efficient classifier for all the above mentioned network attacks.

REFERENCES

1. Zhang, S., & Lee, J. H. (2019). Double-spending with a Sybil Attack in the Bitcoin Decentralized Network. *IEEE Transactions on Industrial Informatics*.
2. Ma, X., An, B., Zhao, M., Luo, X., Xue, L., Li, Z., ... Guan, X. (2019). Randomized Security Patrolling for Link Flooding Attack Detection. IEEE Transactions on Dependable and Secure Computing.
3. Sun, B., Zhu, D., Tian, C., Luo, C. (2018). Complete coverage autonomous underwater vehicles path planning based on glasius bio-inspired neural network algorithm for discrete and centralized programming. IEEE Transactions on Cognitive and Developmental Systems, 11(1), 73-84.
4. Zhang, X., Mahadevan, S. (2017). A bio-inspired approach to trafc network equilibrium assignment problem. IEEE transactions on cybernetics, 48(4), 1304-1315.
5. Yuan, X., He, P., Zhu, Q., Li, X. (2019). Adversarial examples: Attacks and defenses for deep learning.IEEE transactions on neural networks and learning systems.
6. Villain,J.,Deniau,V.,Fleury,A.,Simon,E.P.,Gransart, C., Kousri,R.(2019).EM Monitoring and classication of IEMI and protocol-based attacks on IEEE 802.11 n communication networks. IEEE Transactions on Electromagnetic Compatibility.
7. Shawly, T., Elghariani, A., Kobes, J., Ghafoor, A. (2019). Architectures for Detecting Interleaved Multistage Network Attacks Using Hidden Markov Models.IEEE Transactions on Dependable and Secure Computing.
8. Yang, H., Ju, S., Xia, Y., Zhang, J. (2019). Predictive Cloud Control for Networked Multiagent Systems With Quantized Signals Under DoS Attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems.
9. Zhang, M., Wang, L., Jajodia, S., Singhal, A. (2018). Network Attack Surface: Lifting the Concept of Attack Surface to the Network Level for Evaluating Networks' Resilience against Zero-Day Attacks.IEEE Transactions on Dependable and Secure Computing.
10. Hu, S., Yue, D., Han, Q. L., Xie, X., Chen, X., Dou, C. (2019). Observer-Based Event-Triggered Control for Networked Linear Systems Subject to Denial-of-Service Attacks. IEEE transactions on cybernetics.
11. Li, Z., Jin, H., Zou, D., Yuan, B. (2019). Exploring New Opportunities to Defeat Low-rate DDoS Attack in Container-based Cloud Environment .IEEE Transactions on Parallel and Distributed Systems.

AUTHORS PROFILE

Ms. Ananya Aggarwal, Student, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India. Email: ananya1398@gmail.com

Mr. Priyam Agrawal, Student, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India. Email: priyam1712cse@gmail.com

Mrs. Kanmani Sivagar, Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India. Email: kanmanis@srmist.edu.in