IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DISTRIBUTED DENIAL OF SERVICE ATTACK DETECTION USING MACHINE LEARNING ALGORITHM

Prof. Girisha Bombale[1], Dhananjay Tangtode[2], Shayan Sayyad[3], Omkar Gelye[4], Sarthak Sawant[5]

[1]Professor at Department of Artificial Intelligence & Data Science, Shree Ramchandra College of Engineering, Pune.

[2]Student at Department of Artificial Intelligence & Data Science, Shree Ramchandra College of Engineering, Pune.

[3]Student at Department of Artificial Intelligence & Data Science, Shree Ramchandra College of Engineering, Pune.

[4]Student at Department of Artificial Intelligence & Data Science, Shree Ramchandra College of Engineering, Pune.

Abstract— "A Distributed Denial of Service (DDoS) attack is an endeavor to render a service inaccessible by inundating the server with malevolent traffic. DDoS attacks have emerged as one of the most formidable and burdensome challenges in recent times. Both the frequency and scale of these attacks have escalated from mere megabytes to hundreds of terabytes of data today. Detecting these attacks effectively has become increasingly challenging due to variations in attack patterns and the emergence of new attack types. In this study, we propose novel techniques for executing DDoS attacks and for their mitigation, demonstrating significant improvements over existing methods. Additionally, we classify DDoS attack techniques and the methodologies employed in their detection, providing a comprehensive overview of the DDoS issue. Furthermore, we conduct a comparative analysis of our attack module with several available tools."

Keyword: DDOS Attack, Support Vector Machine algorithm, Random forest algorithm

I. INTRODUCTION

"The industrial sector is experiencing a significant transformation due to the information era.". In this context, the notion of smart grid arose as the times demanded, and it has since gained widespread recognition on a global scale, becoming a common development trend in the global power business. However, there have been instances of smart grid intrusion in the past. On January 6, 2016, for example, hackers attacked the Ukrainian electricity grid infrastructure, forcing hundreds of houses to turn off their lights. This is the first time in history that a cyber-attack has resulted in power interruptions. This cyber-attack on industrial control systems is unquestionably a watershed moment.

DDoS attacks aim to disrupt normal service operation by flooding a target system with overwhelming traffic, often originating from multiple compromised devices. These attacks can lead to severe consequences, including financial losses, reputational damage, and service outages for businesses and individuals.

II. DETECTION TECHNIQUES

Signature Based Detection-This approach identifies known attack patterns (signatures) and compares them with real-time traffic. While effective for known attacks, it struggles to detect novel or zero-day attacks.

Anamoly Based Detection- This method analyzes traffic patterns and identifies deviations from established baselines. It can detect novel attacks but faces challenges in setting accurate thresholds and handling dynamic traffic patterns.

Hybrid Detection- This combines signature-based and anomaly-based approaches, leveraging the strengths of both. It offers comprehensive protection but requires careful integration and configuration to avoid false positives.

III. METHODOLOGY

Following methods were used to develop the DDOS Attack Detection Model:

A. Data Preprocessing

- Acquire a DDoS attack dataset: We are using KD-99 dataset for training and testing the model. Ensure the dataset contains labelled data with features like packet size, flow duration, source IP address, and attack type.
- Preprocess the data: This involves handling missing values, scaling numerical features, and encoding categorical features.
- Split the data: Divide the dataset into training, validation, and testing sets. Use the training set to build the model, the validation set to fine-tune hyperparameters, and the testing set to evaluate the final model's performance.

B. SVM Training

- Import necessary libraries: Use libraries like Scikit-learn in Python for model building and evaluation.
- Initialize the SVM model: Choose an appropriate kernel function (e.g., linear, radial basis function). You might need to experiment with different kernels to find the best performing one.
- Train the model: Fit the model to the training data.
- Hyperparameter tuning: Use techniques like GridSearchCV to find the optimal hyperparameters for the SVM model (e.g., regularization parameter, kernel coefficient).
- Evaluate the model: Use metrics like accuracy, precision, recall, and F1-score to assess the model's performance on the validation set.

C. Random Forest Training

- Initialize the Random Forest model: Specify the number of trees in the forest and other hyperparameters like maximum depth and minimum number of samples per leaf.
- Train the model: Similar to SVM, fit the model to the training data.
- Hyperparameter tuning: Use techniques like RandomizedSearchCV to optimize hyperparameters for the Random Forest model.
- Evaluate the model: Evaluate the model's performance using the same metrics as for SVM on the validation set.

D. Comparison and Selection:

- Compare the performance of both models on the validation set. Consider factors like accuracy, precision, recall, and computational cost while choosing the best model.

E. Testing:

- Evaluate the chosen model on the held-out testing set to assess its generalizability on unseen data.

IV. RESULT

The paper aimed to provide a concise overview of DDoS attack detection techniques and methodologies for mitigating them. Here are the key findings and results

A. Detection Techniques:

- Strengths and limitations of signature-based, anomaly-based, and hybrid approaches are discussed.

B. Emerging trend: Increased adoption of machine learning and deep learning for improved detection accuracy and efficiency.

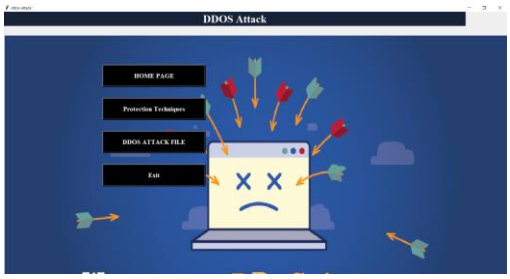
C. Scientific Methodologies:

- Statistical analysis: Effectiveness in identifying deviations from normal traffic patterns, using methods like CUSUM and MAD.

- Machine learning and deep learning: Potential for learning complex attack patterns and adapting to evolving threats, with algorithms like SVM, KNN, and DNN gaining traction.

D. Mitigation Strategies:

- Traffic filtering: Effectiveness in reducing attack load through blacklisting and rate limiting.
- Resource scaling: Ability to dynamically adjust resources like bandwidth and processing power to handle increased traffic volume.
- Collaboration: Importance of information sharing among network operators for coordinated defence and improved detection capabilities.



V. CONCLUSION

Overall, the paper emphasizes the evolving nature of DDoS attacks and the need for continuous development of detection and mitigation techniques. It highlights the effectiveness of combining traditional methods with advanced scientific methodologies and ongoing research efforts for building a more secure and resilient internet ecosystem.
This work provides a smart grid Dos attack detection methodology based on machine learning to address the challenge of smart grid intrusion detection. In real time, the approach gathers network communication data between the smart meter and the data server.
1) Training the data using SVM algorithm.
2) The Convolutional Neural network is used to classification.
3) KDD99 dataset is used to train data.

ACKNOWLEDGMENT

The research team acknowledges the invaluable support and help provided by Prof. Girisha Bombale in carrying out the project.

REFERENCES

Reference Papers

[1] S. RoselinMary, M. Maheshwari, M. Thamaraiselvan
Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)
[2] Faisal Hussain,Syed Ghazanfar Abbas, Muhammad Husnain,Ubaid U. Fayyaz, Farrukh Shahzad,Ghalib A. Shah.
Iot Dos and DDOS attack detection using ResNet.
[3] Faisal Mochamad Teguh Kurniawan, Setiadi Yazid Abdelrhman Mohammed, Iman Abuel Maaly Abdelrahman.
Mitigation and Detection Strategy of DoS Attack on Wireless Sen_x0002_sor Network Using Blocking Approach and Intrusion Detection System.
[4] Xiang-Gui Guo, Xiao Fan, Jian-Liang Wang, and Ju H. Park.
"Event-triggered switching-type fault detection and isolation for fuzzy control systems under Denial-of-Service (DoS) attacks."
[5]Mohiuddi Ahmed

"Mitigating DoS Attacks: A Framework for Detection Based on Collective Anomalies and Clustering"