ISSN: 2249-7196
IJMRR/April. 2025/ Volume 15/Issue 2s/393-398
Nukarapu Devendra Ashok/ International Journal of Management Research & Review

Distributed Denial of Service: Attack techniques and mitigation

Nukarapu Devendra Ashok
PG scholar, Department of MCA, CDNR collage, Bhimavaram, Andhra Pradesh.
K.Suparna
(Assistant Professor), Master Of Computer Applications, Dnr collage, Bhimavaram, Andhra Pradesh.

ABSTRACT: A Distributed Denial of Service (DDoS) attack is an attempt to make a service unavailable by overwhelming the server with malicious traffic. DDoS attacks have become the most tedious and cumbersome issue in recent past. The number and magnitude of attacks have increased from few megabytes of data to 100s of terabytes of data these days. Due to the differences in the attack patterns or new types of attack, it is hard to detect these attacks effectively. In this paper, we devise new techniques for causing DDoS attacks and mitigation which are clearly shown to perform much better than the existing techniques. We also categorize DDoS attack techniques as well as the techniques used in their detection and thus attempt an extensive scoping of the DDoS problem. We also compare our attack module with a couple of tools available.

I. INTRODUCTION

Distributed denial of service (DDoS) attacks is a subclass of denial of

service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic. An example of this type of attack is a domain name system amplification attack, which makes requests to a DNS server using the target's Internet Protocol (IP) address. The server then overwhelms the target with responses.

In a DDoS attack, cybercriminals take advantage of normal behavior that occurs between network devices and servers, often targeting the networking devices that establish a connection to the internet. Therefore, attackers focus on the edge network devices (e.g., routers, switches), rather than individual servers. A distributed denial-of-

service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

The exponential growth of DDoS attacks is mostly due to the total lack of regulatory control over IoT devices, which makes them excellent recruits for the botnets. A hijacked group of IoT devices with unique IP addresses can be redirected to make malicious requests against websites, causing a DDoS attack.

Three broad types of DDoS attacks

- Application layer attacks. The application layer is where the server generates the response to an incoming client request.
- Protocol attacks.
- Volumetric attacks.

LITEARTURE SURVEY

[1] **S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046- 2069, Fourth Quarter 2013**

Distributed Denial of Service (DDoS) flooding attacks are one of the biggest concerns for security professionals. DDoS flooding attacks are typically explicit attempts to disrupt legitimate users' access to services. Attackers usually gain access to a large number of computers by exploiting their vulnerabilities to set up attack armies (i.e., Botnets). Once an attack army has been set up, an attacker can invoke a coordinated, large-scale attack against one or more targets. Developing a comprehensive defense mechanism

against identified and anticipated DDoS flooding attacks is a desired goal of the intrusion detection and prevention research community.

[2] S. S. Kolahi, A. A. Alghalbi, A. F. Alotaibi, S. S. Ahmed and D. Lad, "Performance comparison of defense mechanisms against TCP SYN flood DDoS attack," 2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), St. Petersburg, 2014, pp. 143-147.

Distributed Denial of Service (DoS) attacks is one of the major threats and among the hardest security problems in the Internet world. In this paper, we study the impact of a UDP flood attack on TCP throughputs, round trip time, and CPU utilization on the latest version of Windows and Linux platforms, namely, Windows Server 2012 and Linux Ubuntu 13. This paper also evaluates several defense mechanisms including Access Control Lists (ACLs), Threshold Limit, Reverse Path Forwarding (IP Verify), and Network Load Balancing. Threshold Limit defense gave better results than the other solutions.

[3] B. Nagpal, P. Sharma, N. Chauhan and A. Panesar, "DDoS tools: Classification, analysis and comparison," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 342-346.

Distributed Denial of Service (DDoS) attacks are the major concern for the security experts. DDoS attack presents a serious risk to the internet. In this type of attack a huge number of accommodated targets send a request at the victim's site simultaneously, to exhaust the resources (whether computing or communication resources) within very less time. In the last few years, it is recognised that DDoS attack tools and techniques are emerging as effective, refined, and complex to indicate the actual attackers.

[4] Mahadev, V. Kumar and K. Kumar, "Classification of DDoS attack tools and its handling techniques and strategy at application layer," 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall), Bareilly, 2016, pp. 1- 6.

Computer networks basically consist of seven layers in all at different levels. The seventh layer i.e. application layer is responsible to ful fill the user's requests. Distributed Denial of Service Attack (DDoS) is a condition in which upper three layers of any computer network generally stop their jobs to ful fill the request of clients. DDoS attacks at seventh layer have become highly complex to solve. Various companies hire attack developers or purchase attacking tools to pull down the business of their competitors. DDoS attack's developers are continuously adding new features in this weapon which makes application detector unable to identify.

[5] Python bindings for Qt application framework. [Online]. Available: https://riverbankcomputing.com/software/pyqt/intro [8] Hping security testing tool. [Online]. Available: http://hping.org/

A Distributed Denial of Service (DDoS) attack involves flooding a server with malicious traffic in order to make it unavailable. In the recent past, DDoS attacks have become the most tedious and inconvenient issue. The number and size of attacks has grown in recent years, from a few megabytes to hundreds of terabytes. It is difficult to detect these attacks effectively due to differences in attack patterns or new types of attacks. We devise new techniques for causing DDoS attacks and mitigation in this paper, which are shown to perform significantly better than existing techniques.

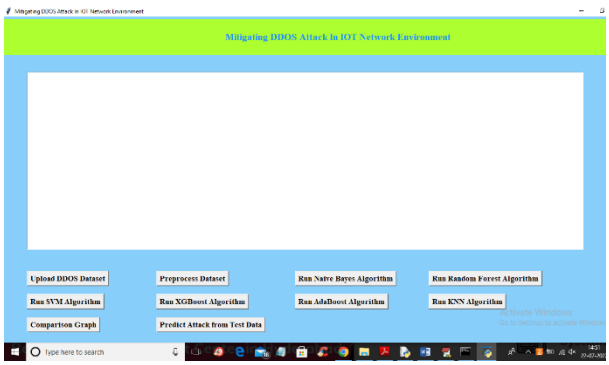
RESULTS

A. Attack results and analysis

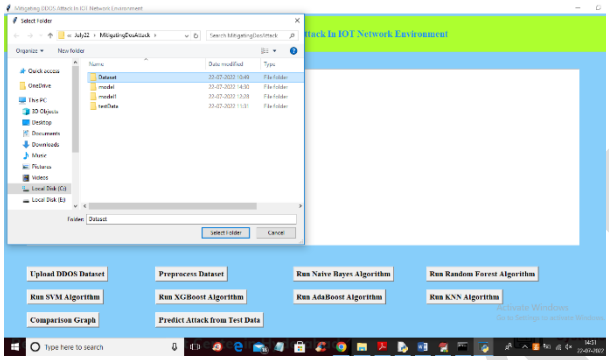
ISSN: 2249-7196

IJMRR/April. 2025/ Volume 15/Issue 2s/393-398

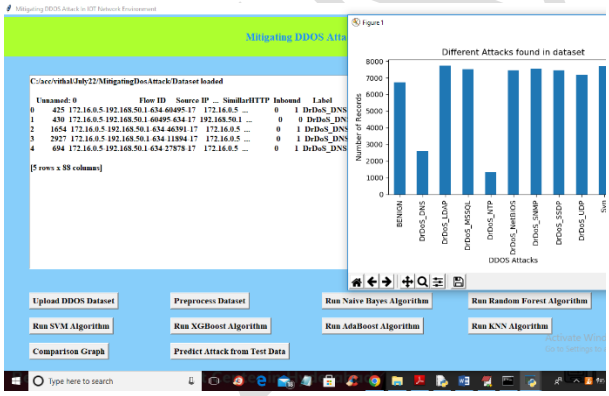
Nukarapu Devendra Ashok/ International Journal of Management Research & Review



In above screen click on 'Upload DDOS Dataset' button tto upload dataset and get below output

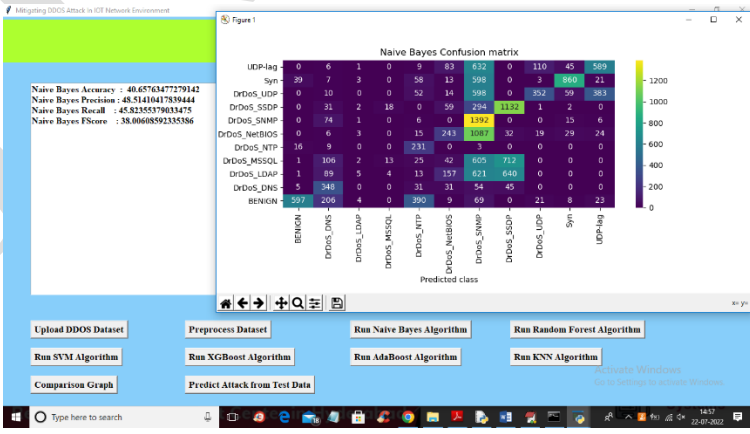


In above screen selecting and uploading 'Dataset' folder and then click on 'Select Folder' button to load dataset and get below output



In above screen dataset loaded and we can see dataset contains both numeric and non-numeric data and in above graph x-axis represents attack names and y-axis represents count of those records. Now close above graph and then click on 'Preprocess Dataset' button to process dataset and get below screen

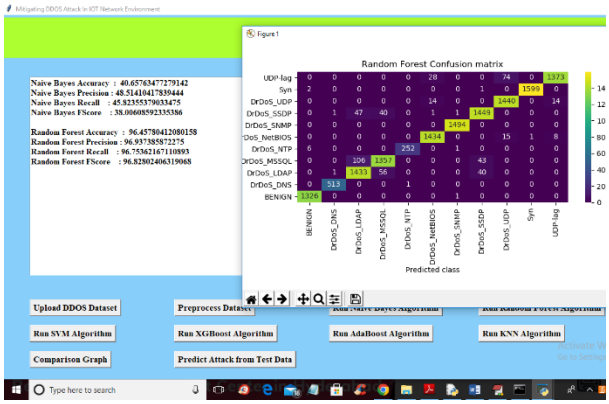
In above screen we can see all dataset values converted to numeric format and dataset contains more than 70000 records and each record contains 87 features and then we have split dataset into train and test and for training application using 56685 records for training and 14172 for testing. Now train and test data is ready and now click on 'Run Naïve Bayes Algorithm' button to train Naïve Bayes and get below output



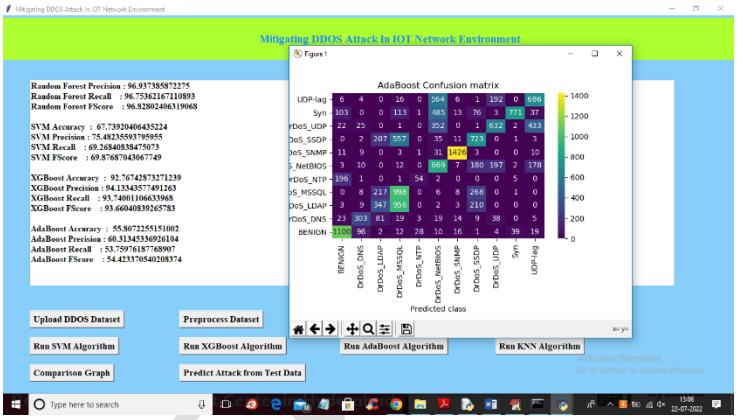
In above screen with Naïve Bayes we got 40% accuracy and in confusion matrix graph x-axis represents PREDICTED classes and y-axis represents TRUE classes and prediction count in same row and column names are the correct prediction and count in different row and column names are the incorrect prediction and we can see Naïve Bayes predicted so many wrong prediction and close above graph and then click on 'Run Random Forest Algorithm' button to get below output

ISSN: 2249-7196

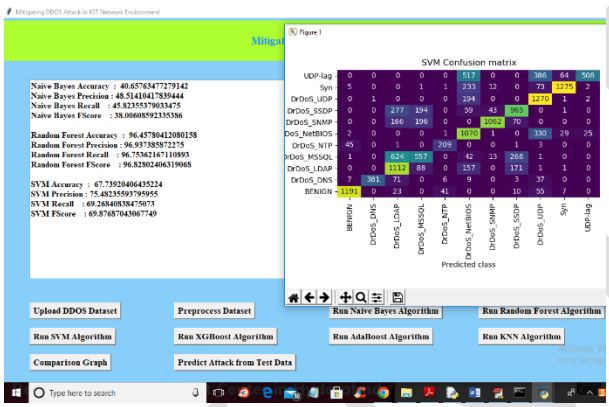
IJMRR/April. 2025/ Volume 15/Issue 2s/393-398



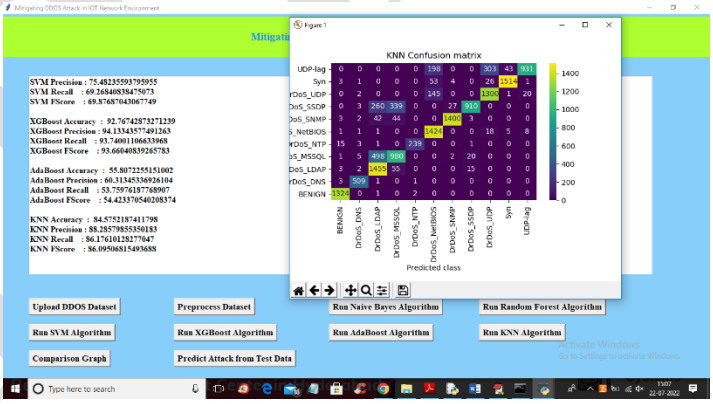
In above screen with Random Forest we got more than 96% accuracy and in graph also we can see lots of predictions are correct. Now close above graph and then click on 'Run SVM Algorithm' button to get below output



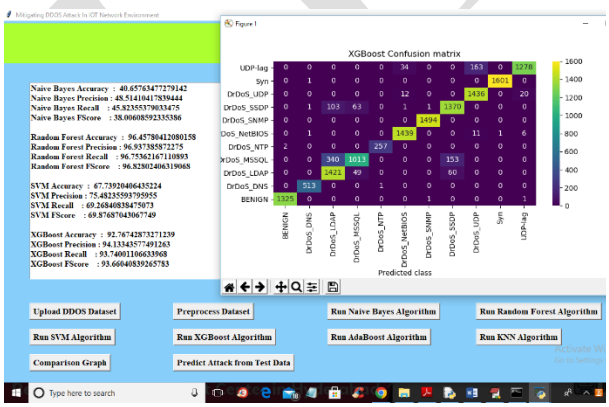
In above screen with ADABOOST we got 55% accuracy and now close above graph and then click on 'Run KNN Algorithm' button to get below output



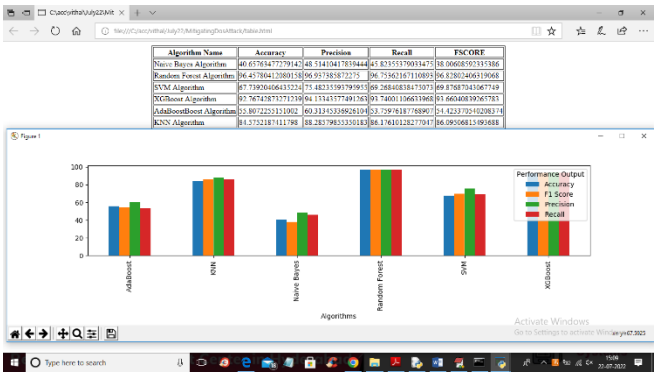
In above screen with SVM we got 67% accuracy and now close above graph and then click on 'Run XGBOOST Algorithm' button to get below output



In above screen with KNN we got 84% accuracy and now close above graph and then click on 'Comparison Graph' button to get below graph

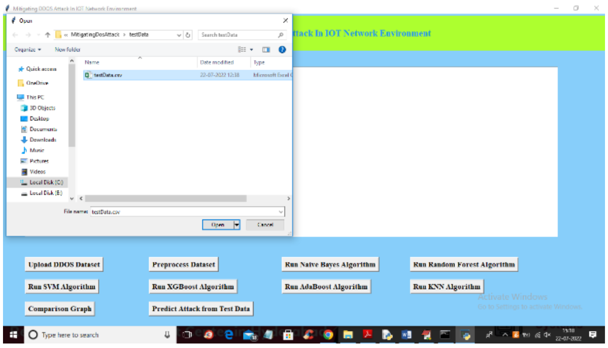


In above screen with XGBOOST we got 92% accuracy and now close above graph and then click on 'Run ADA BOOST Algorithm' button to get below output

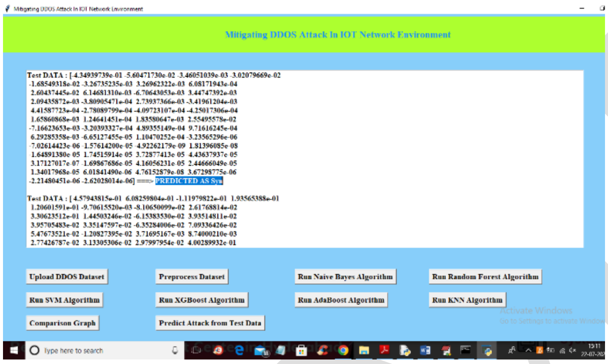


In above graph and comparison table we can see Random Forest got high accuracy and in above graph different colour bar represents different metrics such as accuracy, precision, recall and FSCORE. Now click on 'Predict Attack from Test

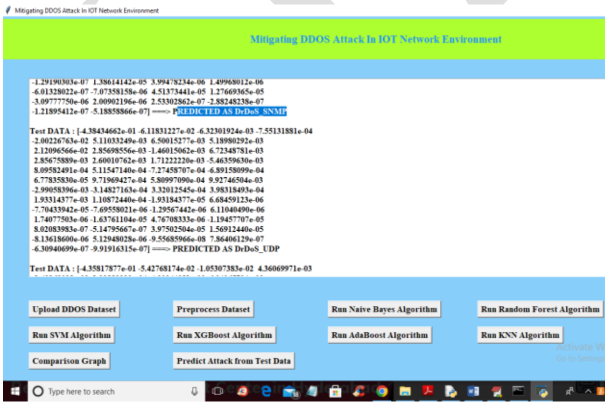
Data' button to upload test data and get below output

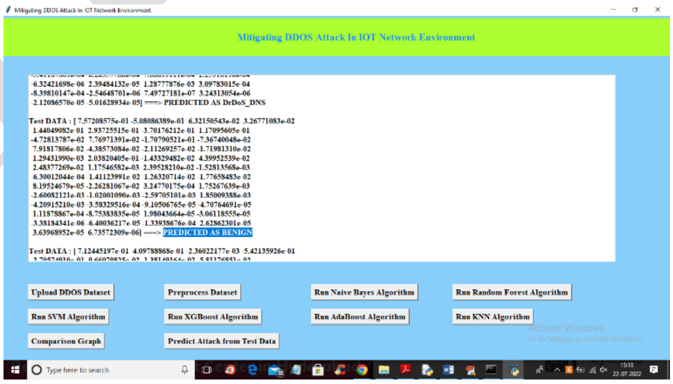


In above screen selecting and uploading TEST DATA file and then click on 'Open' button to get below output



In above screen in square bracket we can see TEST DATA features and after arrow symbol =➔ we can see predicted ATTACK as 'SYN' and scroll down above screen to view different predicted output





In above screens with each different test records different attacks and benign (normal) classes are predicted

CONCLUSION

This paper gives an adequate knowledge to implement Denial of Service attacks. It highlights various DDoS attack methodologies, attack tools as well as provides information on developing a DoS attack tool from scratch. It also suggests basic mitigation strategies and their implementation that could be adopted to defend the

attacks. This paper shows the destructive effects that can be caused to the network with intermediate programming and networking skills and thus tries to highlight the importance of such knowledge to mitigate those effects.

REFERENCES

[1] S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046- 2069, Fourth Quarter 2013

[2] S. S. Kolahi, A. A. Alghalbi, A. F. Alotaibi, S. S. Ahmed and D. Lad, "Performance comparison of defense mechanisms against TCP SYN flood DDoS attack," 2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), St. Petersburg, 2014, pp. 143-147.

[3] B. Nagpal, P. Sharma, N. Chauhan and A. Panesar, "DDoS tools: Classification, analysis and comparison," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 342-346.

[4] Mahadev, V. Kumar and K. Kumar, "Classification of DDoS attack tools and its handling techniques and strategy at application layer," 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall), Bareilly, 2016, pp. 1- 6.

[5] Kali Linux Operating System - Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments. [Online]. Available : https://www.kali.org/

library. It employs common syntax for Python, NumPy, and dictionary arrays.