DDoS Attack Detection and Mitigation System

Anu Jose
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology
Palai,Kottayam,Kerala

Jone Abraham
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology
Palai,Kottayam,Kerala

Lisha Chacko
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology
Palai,Kottayam,Kerala

Reethu Joseph
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology
Palai,Kottayam,Kerala

Dr.Sruthy S
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology
Palai,Kottayam,Kerala

***Abstract*—This paper serves as a model and set of instructions for a machine learning-based system for detecting and mitigating DDoS attacks.Cyberattacks of the type known as DDoS attempts to block.By flooding it with traffic from numerous sources, you can prevent a network or website from being accessed. One tactic for thwarting DDoS assaults is the use of DDoS detection and mitigation software.This programme uses a variety of techniques, including as source-based traffic filtering, rate limitations, and the blocking of malicious traffic, to identify and mitigate DDoS attacks. The DDoS detection and mitigation software provides a number of features, including real-time network monitoring, alerting, and reporting, that enable businesses to stay informed about the condition of their networks and react swiftly to attacks.These attacks are recognised and stopped by software for DDoS detection and mitigation, preventing network and website overload. Typically, the programme analyses network data in real-time in order to spot trends that might point to a DDoS attack. Here, we make decisions on whether to allow or deny traffic by using machine learning algorithms to detect these patterns. The software may also have capabilities like traffic scrubbing, which helps filter out harmful traffic while letting genuine traffic pass, and rate restriction, which helps prevent assaults by restricting the amount of traffic that can be delivered to a website or network.Software for DDoS detection and mitigation is a crucial tool for defending networks and websites against DDoS attacks, helping to ensure that they remain available and accessible to legitimate users.**

***Index Terms*—DDoS, Machine Learning**

I. Introduction

A distributed denial- of- service (DDoS) attack is a cunning attempt to stop a targeted company from conducting its regular business.By flooding the target or its supporting structure with Internet traffic, a service or network can be attacked.These assaults have the potential to do serious harm and interfere with crucial web services. DDoS attacks are made successful by using numerous compromised computer systems as attack sources. DDoS assaults are a popular type of cyber attack in which hackers attempt to saturate a network or website with traffic in order to render it inaccessible to authorized users.DDoS detection and mitigation software is, in general, an essential tool for defending networks and websites from DDoS attacks and reducing the unavailability of online services.

Software for DDoS detection and mitigation detects and stops these attacks, reducing network and website overload. The programme often examines network data in real-time to look for patterns that could indicate a DDoS attack. Here, we use machine learning techniques to identify these patterns and then decide whether to accept or prohibit traffic. The software may also contain features like rate restriction, which helps prevent attacks by capping the amount of traffic that can be transmitted to a website or network, and traffic scrubbing, which helps filter out malicious traffic while letting legitimate traffic pass.An essential tool for protecting networks and websites against DDoS attacks is software for DDoS detection and mitigation.

II. Objective and Scope

The main goal of this DDoS attack discovery and mitigation solution is to protect a targeted computer or network against DDoS attacks. A targeted victim might lessen the incoming threat by using a network outfit that has been expressly developed for them or a pall-Grounded protection service. DDoS Protection Services assist businesses to prevent distributed denial of service attacks and keep their operational websites accessible round-the-clock. Attack mitigation, also known as DDoS protection, aids organizations in being well-prepared for the looming threat of DDoS by lowering the event's rigidity or soberness. When conducting a Distributed Denial of Service (DDoS) assault, the bushwhacker employs numerous hacked or controlled sources. Due to the distinctive nature of these assaults, it should be possible to quickly create tailored mitigations against illegitimate requests that may assume the appearance of being legitimate business demands or emanating from problematic IPs, unexpected topographies, etc. Occasionally, getting knowledgeable support to research company patterns and create tailored defenses may also be effective in calming attacks as they are. By protecting operations and preventing distributed denial of service assaults, DDoS Protection Services help organizations maintain the continuous availability of their Operations websites. Associations benefit from DDoS Protection by being properly prepared for the looming threat of DDoS attacks. The technique of successfully defending a targeted network from a distributed denial of service (DDoS) assault is known as DDoS mitigation. A targeted victim is qualified to lessen the impending issue by using a pall grounded protection service or a specifically created network equipment.

III. Literature Survey

We had fixed a time window during which we had recorded Internet activity at the router in order to detect an assault.Using the same programme that was used to generate training sets from the sample files, we converted the collected flow into a detection set. When a router discovers an attack, it can either decide to stop all packets from reaching the target or to warn the target about the assault. Region name and packet count may be included in the attack information.The destination may also be given authority to restrict traffic at a router.The destination can then do its own analysis to determine the nature of the attack and determine whether or not to block incoming packets from the reporting router. The destination server may choose to stop traffic in response to a variety of factors. The router may offer such characteristics as additional details. A Decoy, Bait, and Real Web server, as well as a unique intrusion protection mechanism, make up the network.

A. The significance of DDoS attacks Detection

DDoS attack detection is crucial for a number of reasons: Early notice: Organizations may be able to take measures to reduce the impact of DDoS attacks on their operations by early detection of these attacks. Resource planning: Detection of DDoS attacks can help organizations to plan their resources and allocate budget to prevent or mitigate future attacks. Risk assessment: Detection of DDoS attacks can help organizations to assess the risks they face and take appropriate measures to protect themselves. Legal issues: Detection of DDoS attacks can be important for legal purposes, as it can provide evidence of the attack and help organizations to pursue legal action against the attackers. Reputation management: Detection of DDoS attacks can help organizations to manage their reputation by taking timely action to mitigate the attack and communicate with stakeholders about the situation.

1) DDoS Attacks Detection and Mitigation in SDN using Machine Learning: One major attack that plagues the SDN network is the distributed denial-of-service (DDoS) attack. There are several approaches to prevent the DDoS attack in an SDN network.[1] We have evaluated a few machine learning techniques, i.e., J48, Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (K-NN), to detect and block the DDoS attack in an SDN network. The evaluation process involved training and selecting the best model for the proposed network and applying it in a mitigation and prevention script to detect and mitigate attacks. The results showed that J48 performs better than the other evaluated algorithms, especially in terms of training and testing time.

2) Real time DDoS attack detection and mitigation using machine learning: DDoS cyber weapons are heavily driven by a variety of factors, such as hacktivism, personal vengeance, anti-government force, angry employers/customers, ideological and political cause, computer espionage, and so forth.[20] Attackers can affect the availability of services on the internet network by mimicking a reliable source by using the potent method known as IP spoofing. Because faked traffic uses the same resources as regular traffic, detecting and filtering it becomes crucial. The online monitoring system (OMS), faked traffic detection module, and interface-based rate limitation (IBRL) algorithm make up the suggested paradigm. OMS provides DDoS impact measurements in real time by monitoring the degradation in host and network performance metrics. The spoofed traffic detection module incorporates hop count inspection algorithm (HCF) to check the authenticity of incoming packet by means of source IP address and its corresponding hops to destined victim. HCF coupled with support vector machine (SVM) provides 98.99 percentage accuracy with reduced false positive.

B. Methods of Mitigation

To reduce DDoS attacks, a variety of techniques can be used: Cleaning up the traffic By recognising and separating harmful traffic from genuine traffic, traffic scrubbing ensures that only valid traffic reaches the intended network or service. Several methods, including rate limitation, filtering based on IP address or other factors, and challenge-response mechanisms, can be used to accomplish this. Network-level protection: Implementing defenses against DDoS attacks at the network level is known as network-level defense. This can involve filtering unwanted traffic and preventing it from accessing the target network or service using firewalls, intrusion prevention systems (IPS), and other security measures.Increased capacity for handling more traffic is achieved by bandwidth expansion, which enables a network or service to withstand a DDoS attack without being overburdened. The bandwidth of current servers can be increased or more servers can be added to accomplish this.

Redirection: Redirection includes sending traffic to a different network or service that can handle the extra traffic instead of the intended network or service. Load balancers or other traffic control tools can be used for this. Blackholing is the practice of routing all traffic from a certain source to a ”black hole,” or more accurately, a ”dead end,” which absorbs the traffic and keeps it from reaching the desired network or service. Overall, the organization’s unique circumstances and resources will determine the most effective strategy for minimizing DDoS attacks. To effectively protect against DDoS attacks, a mix of these techniques could be required.

1) Mechanism to mitigate real time DDoS attack: Computer networks are subject to an unprecedented number and variety of attack, the majority of which are distributed denial of service (DDoS). The nature and mechanisms employed in these DDoS attacks continually change, creating a significant challenge for detection and management. To address this evolving nature of attacks, approaches are required that can effectively detect and mitigate emerging attacks. In this paper, a mechanism that not only detects the presence of a DDoS attacks but also identifies the route of attack and commences a process of mitigation at the initial stage of identification.[1] The proposed research involves an optimized SVM classification algorithm integrated with SNORT IPS to provide prevention mechanisms for the entire network when subject to DDoS attack. The proposed IPS method allows traffic identified as legitimate to pass through the network, whereas suspect traffic is flagged and has to go through an identification system. We present the algorithm with experimental results that show better performance than simple Snort IPS, Probabilistic Neural Network (PNN), Back Propagation (BP), Chi-square, and PSO-SVM in terms of accuracy, exposure and specificity.[11] These results show that the average accuracy rate of the method is 97 percent.

IV. Proposed System

The suggested method uses machine learning to detect and mitigate DDoS attacks.Network security and defence against external threats are considered to be effectively solved by the proposed smart DDoS Attack detection and Mitigation system. Machine learning techniques have been widely used in intrusion detection because conventional systems frequently have a lower detection rate under new attacks and a significant overhead when working with audit data.The suggested system functions as a sensor that can be put anywhere on the network, classifying online traffic using an MLA-based approach that draws conclusions from random traffic samples collected on network devices using stream protocol. The suggested method is hardware and software upgrade-free, and it is compatible with the Internet infrastructure.

A. *Technique*

Gather and prepare data: Gathering and preparing data that may be used to train a machine learning model is the first stage in utilizing machine learning to detect DDoS attacks. Examples of both typical network traffic and traffic from DDoS attacks should be included in this data. To make the data acceptable for training the model, it might be required to clean and alter it.

Develop the model: After the data has been gathered and prepared, a machine learning model can be trained using it. In most cases, this entails dividing the data into a training set and a validation set, then training the model on the training set using the right machine learning method.

Model evaluation: After the model has been trained, its accuracy and performance should be assessed using the validation set. This can assist in finding any flaws or problems with the model and help with any necessary model adjustments. The model can be used to detect DDoS attacks in real time once it has been trained and assessed. In most cases, this entails putting in place a system that can monitor and analyse network traffic in real-time, then classifying it as normal or suspicious using the trained machine learning model. Once a malicious flow has been verified by the anomaly detection module, the Anomaly Mitigation module is in charge of implementing mitigation measures to prevent network disruption or performance degradation. In the framework, attack at its source is stopped. The preventing attacks caused by IP spoofing does not necessarily involve banning the attackers' IP addresses. For proof-of-concept purposes, in this case, attacker's Ethernet address

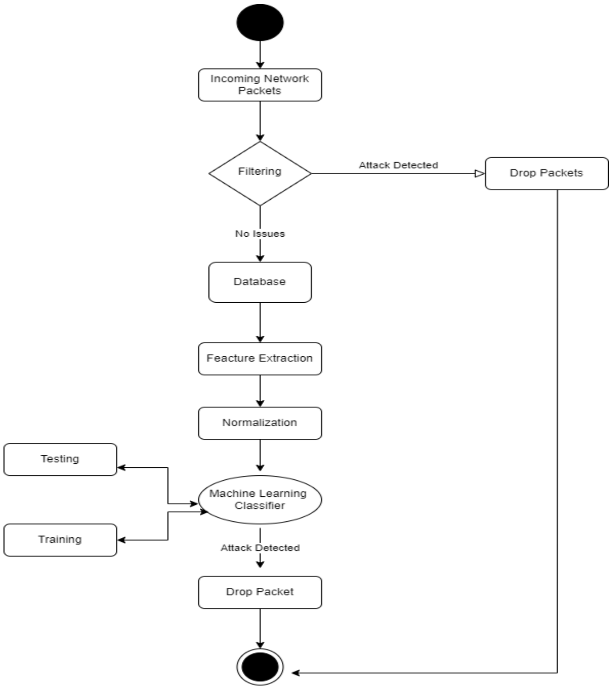

Fig. 1. Activity diagram: DDoS Detection

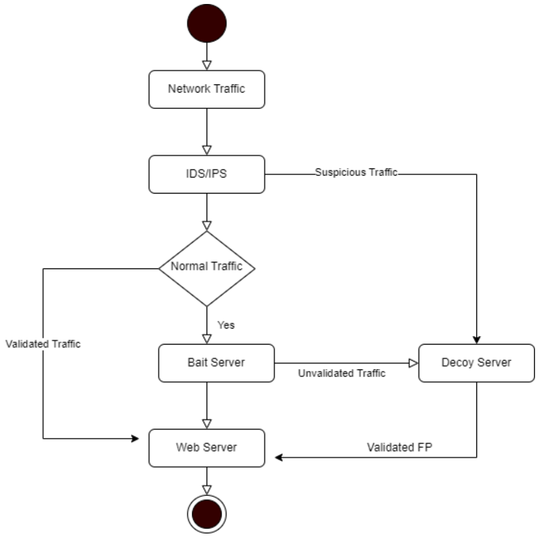

Fig. 2. Activity diagram: DDoS Mitigation

is blocked.

V. Conclusion

The availability and dependability of websites and other online resources are seriously threatened by DDoS (Distributed Denial of Service) assaults. They are increasingly being used as a tool for cyber espionage and sabotage, and they can result in serious disruptions and financial losses for targeted organisations.Technical and non-technical techniques must be used in conjunction for effective DDoS mitigation and prevention. In addition to incident response planning, stakeholder engagement, and legal action against the attackers, technological measures include traffic filtering, traffic scrubbing, load balancing, and network design. By examining traffic patterns and seeing unexpected spikes or patterns that would suggest an assault, machine learning algorithms can also be used to detect and mitigate DDoS attacks in real-time.To lessen the effects of these attacks and guarantee the availability and dependability of their online resources, organisations must have a strong DDoS security strategy in place. Implementing both technical and nontechnical measures, such as stakeholder communication and incident response planning, may be necessary to achieve this. It's crucial to regularly test and train DDoS prevention systems to make sure they are efficient in fending off assaults.

References

[1] Rahman, O., Quraishi, M. A. G., Lung, C.-H. (2019). DDoS Attacks Detection and Mitigation in SDN Using Machine Learning. 2019 IEEE World Congress on Services (SERVICES). doi:10.1109/services.2019.00051

[2] Yi Zhang, Qiang Liu, Guofeng Zhao. (2010). A real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis. 2010 3rd International Conference on Computer Science and Information Technology. doi:10.1109/iccsit.2010.5563549

[3] Ndibwile, J. D., Govardhan, A., Okada, K., Kadobayashi, Y. (2015). Web Server Protection against Application Layer DDoS Attacks Using Machine Learning and Traffic Authentication. 2015 IEEE 39th Annual Computer Software and Applications Conference. doi:10.1109/compsac.2015.240

[4] Li, S., Cui, Y., Ni, Y., Yan, L. (2019). An Effective SDN Controller Scheduling Method to Defence DDoS Attacks. Chinese Journal of Electronics, 28(2), 404–407. doi:10.1049/cje.2019.01.017

[5] Vanitha, K. S., UMA, S. V., Mahidhar, S. K. (2017). Distributed denial of service: Attack techniques and mitigation. 2017 International Conference on Circuits, Controls, and Communications (CCUBE). doi:10.1109/ccube.2017.8394146

[6] Yan, Q., Yu, F. R., Gong, Q., Li, J. (2016). Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. IEEE Communications Surveys Tutorials, 18(1), 602–622. doi:10.1109/comst.2015.2487361

[7] Chin, T., Mountrouidou, X., Li, X., Xiong, K. (2015). Selective Packet Inspection to Detect DoS Flooding Using Software Defined Networking (SDN). 2015 IEEE 35th International Conference on Distributed Computing Systems Workshops. doi:10.1109/icdcsw.2015.27

[8] Dharma, N. I. G., Muthohar, M. F., Prayuda, J. D. A., Priagung, K., Choi, D. (2015). Time-based DDoS detection and mitigation for SDN controller. 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS). doi:10.1109/apnoms.2015.7275389

[9] Jun, J.-H., Oh, H., Kim, S.-H. (2011). DDoS flooding attack detection through a step-by-step investigation. 2011 IEEE 2nd International Conference on Networked Embedded Systems for Enterprise Applications. doi:10.1109/nesea.2011.6144944

[10] Shameli-Sendi, A., Pourzandi, M., Fekih-Ahmed, M., Cheriet, M. (2015). Taxonomy of Distributed Denial of Service mitigation approaches for cloud computing. Journal of Network and Computer Applications, 58, 165–179. doi:10.1016/j.jnca.2015.09.005

[11] Daffu, P., Kaur, A. (2016). Mitigation of DDoS attacks in cloud computing. 2016 5th International Conference on Wireless Networks and Embedded Systems (WECON). doi:10.1109/wecon.2016.7993478