Detection of DDoS using Artificial Neural Network

Aryan Sharma
Department of Networking and Communications
SRM Institute of Science and Technology
Chennai, India

Nitin Tekchandani
Department of Networking and Communications
SRM Institute of Science and Technology
Chennai, India

Dr. K. Venkatesh
Designation: Assistant Professor
Department of Networking and Communications
SRM Institute of Science and Technology
Chennai, India

Abstract: Cyber attacks are one of the most deadliest and lethal attacks in today's world. One of these attacks being the Distributed Denial of Service attack. A DDoS attack is a malicious way to disturb the ongoing traffic of the server. It overflows the victim or its assets by flooding the internet traffic. DDoS attacks attain effectiveness by using compromised computers or IoT devices as sources of internet traffic. In a DDoS attack, a malicious actor attempts to cause troubles in the normal functioning of a network or server by buffer overflowing it with a flood of internet requests. In simple words Distributed Denial of Service attacks can be defined as a traffic stop in which cars are stopped on the highway due to unknown circumstances and are prevented from reaching their destination. In this attack the incoming logs of the network traffic suffer from many incoming network logs which takes the server down and causes the loss of time and resources to the organization. The intruders use the bots to buffer the traffic to the victim or organization, overwhelming its infrastructure and causing it to crash or become inaccessible. In this paper we have presented a way to detect the Denial of Service attacks using neural networks. We compared our model with the other models in the field and got a higher accuracy rate and consistency of

the model. It has been trained on over 5000 sites which are malicious and brought out an accuracy of about 98.

I. Introduction

Distributed Denial of Service (DDoS) attacks are causing great problems for business and organizations of all sizes. These attacks can have a devastating as well as lethal on the avail- ability and reliability of critical services, causing significant financial losses and damage to brand reputation. To mitigate the risks associated with DDoS attacks, various techniques have been developed over the years, including network-based solutions, such as firewalls and intrusion detection systems. However, these solutions are often inadequate against more sophisticated attacks that can evade detection. Denial of ser- vice (DoS) attacks can have a number of disadvantages for individuals and organizations, ranging from lost productivity to reputational damage, financial costs and time. One of the most immediate effects of a DoS attack is downtime. Websites or online services can become unavailable or extremely slow, which can be costly for businesses that rely on their online presence to generate revenue. In some cases, downtime can last for hours or even days, resulting in lost sales, missed opportunities, and frustrated customers. DoS attacks can also have a significant impact on productivity. If employees are unable to access important systems or applications due to a DoS attack, their ability to work can suffer. This can result in delays or missed deadlines, which can be costly for businesses. In addition, IT teams may be forced to spend valuable time and resources responding to the attack, which can further impact productivity. This leads to the loss of valuable time and money to the organization and also impacts the reliability of the organization among its competitors and the market. Another disadvantage of DoS attacks is reputational damage. If customers or users are unable to access an organization's services, it can cause loss of reliability and confidence in an organization. This can cause severe trouble for businesses that are dependent on their reputation to gain customers. Other disadvantages include server disruption, legal consequences ,since it can lead to data leakage of the users and difficulty in mitigation since DDOS attacks are complex and sometimes can take up to 10 to 12 hours to mitigate. Artificial Neural Network is a type of deep learning artificial intelligence algorithm that clones the behavior of the human neural or nervous system and could be taught to recognize patterns in data. By analyzing network traffic patterns, ANNs can identify anomalous activity that may be indicative of a DDoS attack. Moreover, ANNs can adapt to changing attack patterns and learn from past experiences, making them an effective solution against both known and unknown attacks. In this research paper, we will implement the use of ANNs for finding and detecting DDoS attacks. We will discuss the principles of ANNs and how they can be applied to DDoS detection. We will also examine some of the challenges associated with implementing ANNs in a DDoS detection system and discuss some best practices for achieving effective results.

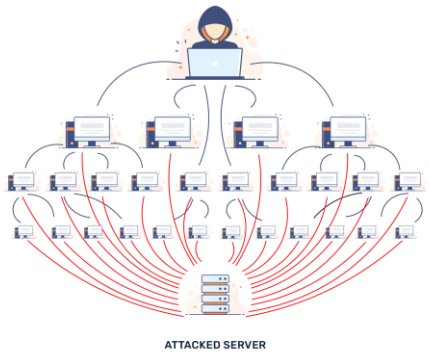

Figure 1

II. Scope

The scope of this project is to develop a DDoS detection system using artificial neural networks (ANNs) as the primary approach. The project aims to explore the principles of ANNs and their application to DDoS detection, including the selec- tion of appropriate network architecture, training data, and algorithms. The project will also investigate the challenges associated with implementing ANNs in a DDoS detection system, such as optimizing performance, mitigating false positives and negatives, and adapting to changing attack patterns. The project's scope includes the development of a proof-of- concept implementation of the DDoS detection system using ANNs.The project will also consider the scalability and per- formance of the system, as well as its integration with existing network infrastructure. One further scope is that Another direction is to focus on developing more proactive solutions for DDoS mitigation. The model is trained to detect the malicious websites and set an alarm and has the ability to learn new approaches, so when there is any new form of DoS attack it can learn the approach and whenever any attack happens with the same approach it can detect it. DDoS is one of the most dangerous attacks in today's world, DDoS detection technique can be used in banking sectors which are mostly targeted by the attackers, the other aspect can be of the National security, since a country's most top secret intel can be most profitable to the attackers. The ultimate goal of this project is to demonstrate the effectiveness and reliability of ANNs as a solution for detecting DDoS attacks and to provide recommendations for the design and implementation of such systems. The project's scope will be limited to the use of ANNs for DDoS detection and will not cover other aspects of network security or broader cyber security issues.

III. Motivation

The motivation behind using artificial neural networks (ANNs) for the detection of DDoS attacks stems from the increasing frequency and complexity of these attacks in the cyber world. As cyber security is an advanced field, it requires staying up-to-date with the latest trends and developments in cyber attacks. In the past, DoS attacks were common, but DDoS attacks have now become more prevalent and can cause significant financial losses and reputational damage to businesses and organizations. Traditional methods of detecting and mitigating DDoS attacks, such as network-based solutions, are often inadequate against more sophisticated attacks that can evade detection. ANNs can be trained on large datasets of network traffic to identify patterns and anomalies associated with DDoS attacks. This allows for more

accurate and efficient detection of DDoS attacks, as well as the ability to identify new and previously unknown types of attacks.ANNs have several advantages over traditional methods of detecting DDoS attacks. Artificial Neural Network has the ability to identify patterns in connection with DDoS attacks that could not be analyzed or detected by older systems or softwares. In addition, ANNs have the ability to learn from the information provided to them and make alterations in future if it is needed this makes them effective against DDoS attacks. In recent years, the use of ANNs for DDoS detection is gaining attention as it is an effective way against DDoS and other cyber attacks and possess the ability to modify themselves according to the need.

IV. Literature Review

The use of artificial neural networks (ANN) for DDoS detection is being researched as it possesses a great power against cyber attacks. In recent years, machine learning is being updated to include it in anti cyber attack softwares. One of the earliest studies on the use of Artificial Neural Networks for DDoS detection was conducted by Professor Phuoc and Lee in the year 2007. The researchers used deep learning to differentiate network traffic into normal traffic and DDoS traffic. Their conclusion showed that deep learning was able to get a high detection rate but the false alarm rates were unpredicted as it showed false negatives many times which made it unreliable. In a more modern study, Chen in 2016 proposed a deep learning based technique for DDoS detection using stacked autoencoders. His results showed that his framework was able to achieve high accuracy in detecting DDoS attacks. Another study in 2018 by Alzahrani shows that he used a convolutional neural network (CNN) for DDoS detection. He compared the performance of his CNN with other machine learning algorithms and found that their CNN outperformed the other detecting techniques in terms of accuracy and detection rate but his technique got high false positives on the sites which were not under attack. In a similar study by Reddy in 2019, he used multiple classifiers, including a CNN, for DDoS detection. His results showed that his approach was able to achieve high detection rates with low false alarm rates. Other researchers like Singh in 2021 proposed an ANN based detection technique in which he used a a combination of selection and extraction techniques. His work showed that their system was able to detect DDoS attacks with high accuracy and low false alarm rates but caused heavy load on the system which made the system overheated due to over processing of the model. Similarly, in a study by Hussain in 2020 , he proposed a hybrid detection method that combined both the use of ANN and support vector machine (SVM) classificators. The system was trained on a large dataset of network traffic. Their are advancements being done everyday to counter the cyber attacks, since this is a field of computer science in which people with bad intentions always find a way to counter computer softwares,

V. Architecture

DDoS attacks impose significant ultimatum to the availability of the online facilities. To address this problem, Artificial Neural Networks are being suggested as a potential way for detecting and mitigating DDoS attacks. ANNs are arithmetic models motivated by the functioning of the human nervous system that can learn from data and recognize patterns. The architecture for detecting DDoS attacks using ANNs typically involves several layers of interconnected processing units. The input layer receives data from various sources, such as network traffic or system logs. The data is then preprocessed to extract relevant features, such as packet headers, packet size, or traffic volume. These features are fed into the hidden layers, where they are processed by the neurons to extract higher-level representations of the data. The hidden layers are where the most complex computations take place. The neurons in these layers use activation functions to transform the inputs into outputs, which are then passed to the next layer. The hidden layers in each layer can be different depending on the difficult level of the problem and the amount of information provided for the model's training. The layer that provides the result produces the final solution of the network's operation. In the case of DDoS detection, the output layer may have two neurons, one for normal traffic and one for attack traffic. The output neuron with the highest activation level is the one that determines the network's prediction for the input data. To train the network, a dataset of labeled data is required. The dataset consists of examples of normal traffic and DDoS attacks, and the corresponding output labels for each example. The network is trained using a supervised learning technique which includes techniques like propagation through back, to modify the weights and biases of the neural mind in the network to decrease the bugs between the predicted result and the results we get. We have introduced a column that collects normal values as numeral 0 and any other value that has a sight of being suspicious as 1. We will implement this system as our detector for a model that identifies any attack possible. The detecting plan of action will use some networking protocols that will be able to learn the difference between an attack and an ethical working program. Popular information feeded to the machine learning model classifies DDOS and other attacks . It will help us to identify continuous patterns of DDoS attacks and will help us to locate the long-term traffic chain. Once the network has been trained, it can be used to classify new data as either normal traffic or attack traffic. The network's accuracy depends on the quality and quantity of the training data, as well as the complexity of the network architecture. In conclusion, the architecture for detecting DDoS attacks using ANNs is a complex and powerful approach that leverages the ability of neural networks to learn from data and recognize patterns.

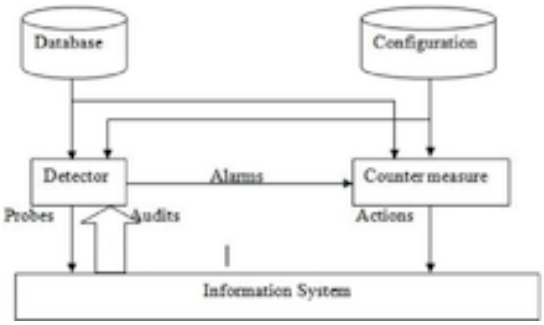

Figure 2

VI. Methodology

In this project, we developed a binary classifier for DDoS attack detection using a simple methodology. We have added a column that encodes ethical values as 0 and any malicious attack values as 1. We then used it as a differentiator for a model that identified a DDoS attack. The observing tactic uses network protocols that were able to learn the difference between an attack and legal work. Popular information feeded to the machine learning model classifies DDOS and other attacks . It will help us to identify continuous patterns of DDoS attacks and will help us to locate the long-term traffic chain. The data collected in the study showed that a large proportion of normal incoming traffic was related to HTTP(Hypertext Transfer Protocol) , while the attack traffic was spread across multiple network protocols. The DDOS attacks observed in the project were located many different ways into the MCS system, out of which a small group were complex, and some were unable to cause an impact. The project helped to differentiate recurring patterns of DDoS and identify them in the l traffic log. DDoS is a type of attack that wishes to interrupt the normal traffic of a network of an organization, system or facilities by overflowing it with a buffer of traffic from multiple sources. By monitoring network traffic and analyzing historical data, we were able to identify and classify various types of attacks, providing valuable insights into the nature and patterns of these attacks.There are several methodologies used in Distributed Denial of Service attacks, which include volume attacks, protocol based attacks, and application layer attacks which is a layer of the famous OSI model. This approach could be used to improve the security of network systems and protect against DDoS attacks in the future.

VII. RESULT AND ANALYSIS

Artificial Neural Networks have given effective results in detecting DDoS attacks, they have provided fast and accurate results than other traditional and old methods. Artificial Neural Networks have the ability to learn from provided data and recognize patterns, loopholes that may not be visible through manual testing. It makes it a powerful weapon against DDoS attacks. The advantages of using Artificial Neural Networks for DDoS detection is that it possesses the ability to change to new attack recognizing patterns. Traditional methods were based on detecting on a predefined dataset of attack techniques, which might not have been detected. In addition, Artificial Neural Networks can remember patterns in a dataset and learn from it, making them able to detect new and unknown attack patterns. This makes Artificial Neural Networks a powerful tool for detecting malicious attacks, which are attacks that exploit vulnerabilities that are unknown to the user. The success of using Artificial Neural Networks for DDoS

detection is highly dependent on the quality and quantity of the training dataset. Artificial Neural Networks require large amounts of training data to learn and improve accuracy. Artificial Neural Networks have the ability to adapt to new patterns and detect zero day attacks, which give them a significant advantage over traditional signature based detection methods.

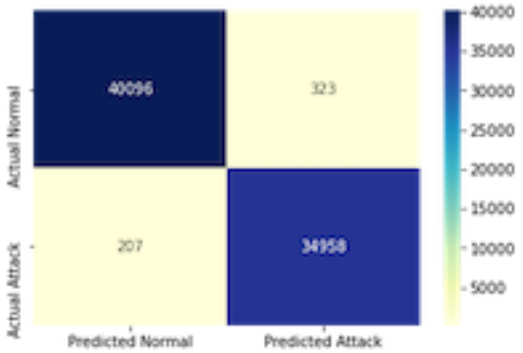

Figure 3

The above graph shows the precision of the model by telling how many false positives were there, how many false negatives and how many times the model actually predicted the attack. We tested our project and got a success ratio of 98 percent. This percentage was irrespective of the false positives and false negatives.

VIII. REFERENCES

[1] Sood, S.K. ”DDoS attacks and defense mechanisms: a classification.” International Journal of Computer Science and Network Security.

[2]Al-Qershi, O.M, ”Review of DDoS Attack Detection Techniques.”A Comprehensive Study of DDoS Attacks and Defense Mechanisms.” Journal of Network and Computer Applications.

[3]Mirkovic, Jetal. ”Taxonomy of DDoS Attacks and Defense Mechanisms.” ACM SIGCOMM Computer Communication Review.

[4]”A Survey of DDoS Attack and Its Detection Techniques.” Journal of Internet Services and Applications, 2019.

[5]”A Survey of DDoS Attack and Defense Mechanisms” by Dheeraj Kumar Singh and Balamurugan Balusamy (2019).

[6]Mohammed, R. A., Al-Jumeily, D., Hussain, A. J. (2019). Anomaly detection for DDoS attacks. Journal of ambient intelligence and humanized computing.

[7]Gao, H., Liu, Y., Dai, W., Wang, Y., Zhao, Y. (2020). A comprehensive review of DDoS attacks and defense mechanisms in cloud computing. Future Generation Computer Systems.

[8]Razak, R. A., Khan, S. U. (2019). A comprehensive survey of DDoS attacks and their mitigation techniques. Com- puters Security.

[9]Alshammari, R., Alshammari, N., Alshammari, T. (2021). Distributed Denial of Service (DDoS) Attacks: An Overview. In Cybersecurity and Secure Information Systems.

[10]Ye, Y., Zhu, M., Xu, B. (2020). A survey on DDoS attack detection and defense techniques. Journal of Network and Computer Applications.

[11]Saeed, S, Abbas, H., Chen, D. (2020). An adaptive deep learning-based detection and mitigation framework for DDoS attacks in the cloud environment. Future Generation Computer Systems.

[12]Jia, X., Wang, T., Zhang, M., Yang, L. (2021). A lightweight and accurate DDoS attack detection model using PCA based feature extraction and random forest. Journal of Ambient Intelligence and Humanized Computing.

[13]A survey of DDoS attacks and defense mechanisms in cloud computing" by L. Jyoti and S. K. Dhurandher.

[14]"A hybrid approach for detecting and mitigating DDoS attacks in cloud computing environments" by H. B. K. Al- Mistarihi et al.

[15]Mitigating DDoS attacks using software-defined networking: A survey" by F. Gao et al.

[16]Zhang, Y., Yang, X., Luo, X., Li,Y. (2020). A hybrid model based on LSTM and CNN for DDoS attack detection.

[17]Alsanea, M., Almazaydeh, L., El-Abd, M. (2020). DDoS attack detection and mitigation in SDN-based cloud networks using machine learning algorithms.

[18]Al-Quraishi, Y. M., Bensaber, A. S. (2020). A DDoS attack detection and prevention system based on an ensemble of machine learning classifiers. Journal of Network and Computer Applications.

[19]Zhang, Y., Yang, X., Luo, X., Li, J., Li, Y. (2020). A hybrid model based on LSTM and CNN for DDoS attack detection.

[20]Alizadeh, H., Karami, M. (2019). Detection and prevention of DDoS attacks using machine learning techniques: A review. International Journal of Information Security and Privacy.

[21]Yaseen, M. A., Al-Jumeily, D. (2021). A comprehensive survey of distributed denial of service (DDoS) attacks and detection techniques. Journal of Ambient Intelligence and Humanized Computing.

[22]S. S. Rawat and V. P. Singh, "A Comprehensive Study on the Detection and Mitigation Techniques of Distributed Denial of Service (DDoS) Attacks.

[23]K. Imani, M. H. Anisi, A. Abdullah and A. Gani, "A Review of DDoS Attack and Defense Mechanisms in Cloud Computing".

[24]Rishi, O., Bhatia, R. (2016). A review on detection and prevention techniques of DDoS attack.