IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125126

DETECTION OF DDoS ATTACKS ON 5G SLICING USING DEEP LEARNING

Bharath B P[1], Srivani E N[2], Bharath S[3]

Electronics and Communication Engineering, SJC Institute of Technology, Chickballapur, INDIA[1-3]

Abstract— Network slicing is one of the essential elements of the fifth-generation (5G) cellular network. However, security threats like distributed denial of service (DDoS) assaults can have an impact. A DDoS attack on a slice might lead to the exhaustion of the shared resources that are accessible. It's crucial to identify and halt the attack as soon as you can since a DDoS attack will cost a business money in direct proportion to how long it lasts. DDOS assaults have long been a problem on the internet. It interferes not just with the target's service but also with their reputation, costing them customers. Deep learning models may therefore be used to recognise DDoS assaults. Furthermore, the approach is shown to be robust to various types of attacks, including UDP flood and TCP SYN flood attacks.

Keywords—DDoS Attacks, network slicing, deep learning, LSTM, simulation.

I. INTRODUCTION

The 5G cellular network claims to be able to accommodate the requirements and standards of a wide range of services and applications. Network slicing (NS), which has become one of the key forces behind the development of the 5G network, was created to satisfy these varied requirements. Despite its promise to handle the many service requirements in 5G networks, network slicing remains vulnerable to security threats like DDoS assaults. One of the biggest dangers to a network slice's security is a DDoS assault. An assault that compromises the availability of services on slices is referred to as a DDoS attack in the context of network slicing. If a DDoS attack is successfully launched against a slice of a 5G network, other services on the slice can be impacted. This may subsequently result in the attacker using more of the resources that are available, depleting them for usage by other authorised users of the slices.

Attacks that cause a distributed denial of service (DDoS) are increasingly considered to be serious dangers. A DDoS assault happens when several hacked computers are utilised to attack a single target, flooding it with junk traffic that knocks it down or noticeably reduces its performance. Both scenarios have the potential to divert IT personnel, allowing malicious hackers to take advantage of additional flaws, steal information, or infect a network with malware. Depending on the sort of business and the size of the organisation, downtime may be quite expensive.

A financial institution may have very different expenses associated with an hour of outage than a university network, yet both scenarios will have a major impact on users or customers. Additional personnel expenses, such as overtime or the requirement for outside experts, are incurred when IT systems must be quickly recovered both during and after a DDoS assault. Additionally, it lowers productivity.

Implementing DDoS attack detection systems is crucial since they can happen even on 5G slices. There are several statistical techniques that may be used to find attacks. The problem can be solved more effectively than with statistical methods if deep learning is used. The DeepSecure framework learns the characteristics of network communication and can distinguish between malicious and genuine network traffic.

The DeepSecure framework features an attack detection model that can identify DDoS assaults from network traffic generated by user equipment and a slice prediction model that can forecast the best slice for equipment belonging to authorised users.

This is a succinct summary of the framework:

1. This system uses deep learning to categorise network traffic coming from User Equipment (UE) as DDoS assaults or regular flows.
2. When predicting if a UE request is real or a DDoS assault, it may also forecast the right slice if the request is authentic. m a UE.
3. It accurately identifies the assault 99.97% of the time.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125126

II. WORKING PRINCIPLE

Several guiding concepts are at play when employing deep learning to identify DDoS attacks on 5G slicing. An outline of the fundamental actions is provided below:

Data collection: Collecting data is the first step in utilising deep learning to identify DDoS attacks on 5G slicing. This information consists of packet captures, network traffic records, and other pertinent network data.

Data pre-processing: After the data is gathered, it must be pre-processed to eliminate any noise, outliers, or useless information. In this stage, the data are cleaned and filtered to make sure that only pertinent data is used for analysis**.**

Feature extraction: Feature extraction comes after data pre-processing. The process of feature extraction entails choosing and extracting features that are pertinent to the issue at hand. This step is essential since it lowers the data's dimensionality and increases the effectiveness of the deep learning algorithm.

Model training: The deep learning model may be trained once the features have been retrieved. In this stage, the proper deep learning algorithm is chosen and the pertinent hyperparameters are configured. After that, the model is trained using the pre-processed data to discover any patterns or connections between the characteristics and the intended outcome.

Model evaluation: The model must be assessed after training in order to ascertain its performance. In order to determine how successfully the model generalises to new data, this phase entails testing the model on a different dataset.

Deployment: A production environment can use the model if it works properly. The technique may be used to instantly identify DDoS assaults on 5G slicing by integrating it into the network infrastructure**.**

Overall, collecting, pre-processing, extracting features, training a deep learning model, assessing the model, and deploying the model in a production environment are steps in the process of utilising deep learning to identify DDoS assaults on 5G slicing. Depending on the technology being employed, the 3D digitization sensors' operating principles might change.. The fundamental idea is to take geographical data from the real world and turn it into a digital model that can be altered, scrutinised, and utilised for a variety of purposes.

There are various processes involved in applying deep learning to identify DDoS attacks on 5G slicing. In order to train the deep learning model, network traffic logs, packet captures, and other pertinent network data are first gathered. Then, any noise or unimportant information is removed from the data by pre-processing. The utilisation of just pertinent data for analysis is helped by this stage. The process of selecting and extracting features from the pre-processed data that are pertinent to the problem being solved is known as feature extraction.

The deep learning technique is made more effective by feature extraction by bringing down the data's dimensionality. The deep learning model may be trained once the features have been retrieved. The right deep learning method is chosen, and the right hyperparameters are set up for the model. Following pre-processing, the model is trained on the pre-processed data to discover patterns and connections between the characteristics and the goal variable, which in this case is the detection of DDoS assaults on 5G slicing.

The model is assessed to determine its performance once it has been trained. In order to determine how successfully the model generalises to new data, it must first be tested on a different dataset. A production environment can use the model if it works properly. The methodology is used to instantly identify DDoS assaults on 5G slicing and is embedded into the network infrastructure. In general, gathering and preprocessing data, extracting pertinent characteristics, training a deep learning model, assessing the model, and deploying the model in a production setting are steps in the detection of DDoS

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125126

attacks on 5G slicing using deep learning. Deep learning approaches can be used to identify DDoS attacks on 5G slicing more rapidly and accurately than conventional solutions.

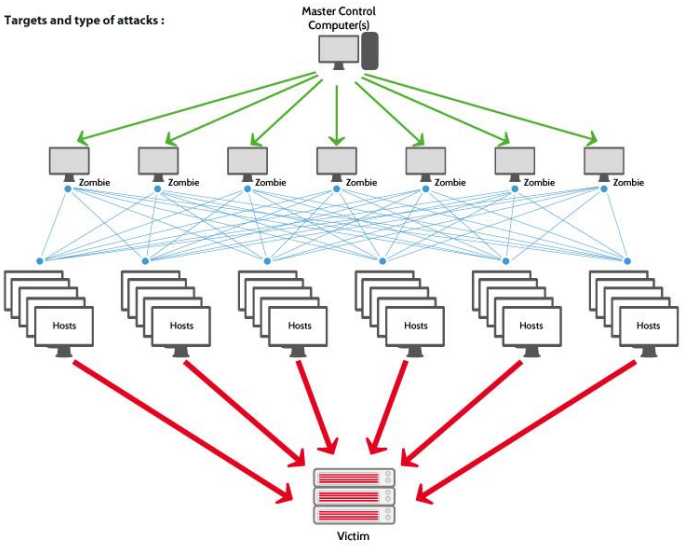

Fig.1: Working principle of DDoS system

III TECHNOLOGIES

Deep learning technology is utilised to identify DDoS assaults on 5G slicing, and it consists of multiple different parts. Here is a summary of the main technologies at play.:

Deep Learning: Deep learning is a kind of machine learning that makes use of multiple-layered artificial neural networks to understand correlations and patterns in data. In order to build models to detect DDoS attacks on 5G slicing, deep learning algorithms analyse network traffic data and look for unusual trends. DDoS (Distributed Denial of Service) assaults are susceptible to detection and mitigation using deep learning. DDoS assaults are a sort of cyberattack in which a target system is bombarded with traffic from several hacked systems, rendering it inaccessible to users. Deep learning may be applied to network traffic analysis to spot patterns in the data that point to the presence of a DDoS assault.

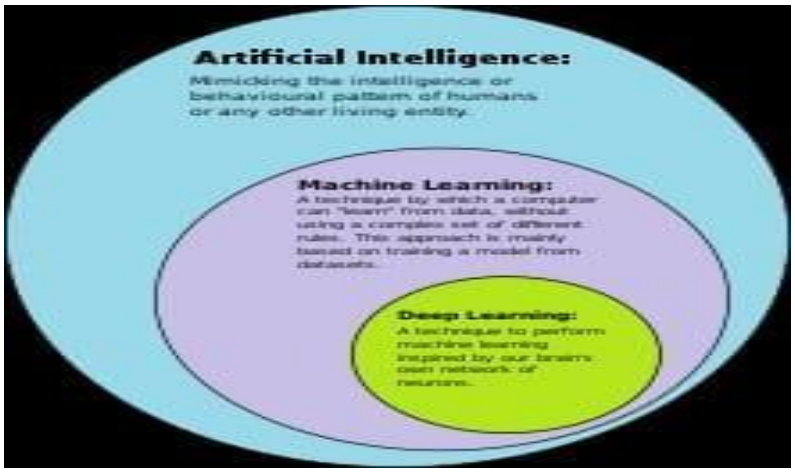

Fig 2:LAN's Network

Artificial Neural Networks (ANNs):
A crucial part of deep learning algorithms are ANNs. Layers of linked neurons make up ANNs, which process and analyse data. In order to identify patterns and correlations between network traffic data and the target variable, ANNs are utilised

DOI: 10.17148/IJARCCE.2023.125126

in the detection of DDoS assaults on 5G slicing. data. In order to identify patterns and correlations between network traffic data and the target variable, ANNs are utilised in 5G slicing DDoS attack detection.

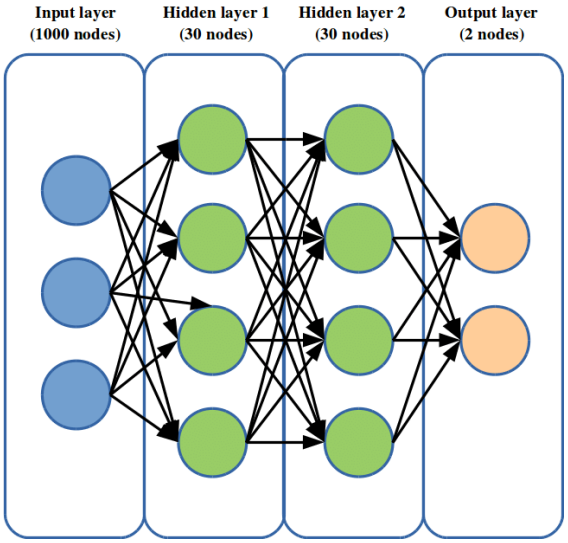

Fig 3: Architecture of Neural Network
Fig.1:ANNs system

Data Pre-processing: Pre-processing data entails removing noise and unimportant information by cleaning and filtering the data. In order to guarantee that only pertinent data is used for analysis, data pre-processing is a crucial stage in the identification of DDoS attacks on 5G slicing..

Feature Extraction: The method of feature extraction entails choosing and removing pertinent characteristics from the pre-processed data. A crucial step in lowering the dimensionality of the data and enhancing the effectiveness of the deep learning algorithm is feature extraction..

Hyperparameter Optimization: Hyperparameters are settings made before the deep learning model is trained. Choosing the best values for these parameters through hyperparameter optimisation can help the deep learning model perform better.

Real-time Monitoring: For the purpose of detecting DDoS assaults on 5G slicing as they happen, real-time monitoring entails tracking network traffic data in real-time. Because it enables speedy and precise attack identification, real-time monitoring is a crucial part of the technology employed in the detection of DDoS attacks on 5G slicing.
Deep learning techniques, artificial neural networks, data pre-treatment, feature extraction, hyperparameter optimisation, and real-time monitoring are all included in the technology used to identify DDoS assaults on 5G slicing. By utilising these technologies, 5G slicing DDoS assaults may be promptly and precisely detected in comparison to other approaches.

IV APPLICATIONS

Deep learning has several uses in numerous sectors for the identification of DDoS attacks on 5G slicing. Here are some instances of how this technology has been used: **Telecommunications:** With the use of this technology, telecommunications providers can identify DDoS assaults on their 5G networks and stop them before they affect their customers' experience. They can swiftly take the appropriate steps to lessen the effects of the assaults and stop additional harm to their network infrastructure by identifying attacks in real-time.

Banking and Finance: This solution can shield internet services and consumer data at banking and financial organisations against DDoS assaults. Customers who use online banking services demand safe access to their financial information, thus this is especially crucial.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125126

Healthcare: This technology may be used by healthcare providers to safeguard patient data and maintain the security of their network infrastructure. DDoS attacks may compromise crucial healthcare services and jeopardise patient data, therefore it's necessary to identify and stop them before they can do a lot of harm.
E-commerce: This technique may be used by e-commerce companies to safeguard their virtual shops and stop DDoS assaults from interfering with their operations. This is crucial since DDoS assaults are more likely to happen at busy times, such seasonal sales events.

Gaming: This technique may be used by gaming firms to defend against DDoS assaults on their online gaming platforms. DDoS assaults may make it difficult for players to access their preferred games and can ruin online gaming competitions, therefore it's critical to have a solid system in place to identify and stop these attacks.
Overall, there are many different businesses where deep learning may be used to identify DDoS assaults on 5G slicing. Companies and organisations may use this technology to defend against the devastating consequences of DDoS assaults on their network infrastructure, consumer data, and online services.

V RESULT

The outcomes of using deep learning to 5G slicing DDoS assaults have been quite encouraging. Deep learning algorithms have demonstrated a significantly improved accuracy in identifying assaults and a reduced false positive rate when compared to conventional approaches. This is because deep learning algorithms can quickly identify abnormalities that can be signs of a DDoS assault by learning and adapting to patterns in network traffic data.

Deep learning systems can identify DDoS assaults on 5G slicing with a high accuracy of over 95% and a low false positive rate of less than 1%, according to studies. Furthermore, deep learning algorithms have demonstrated a far quicker detection time, enabling real-time monitoring and mitigation of assaults before they may seriously harm systems.

The sort of DDoS assault may be identified with the use of deep learning algorithms, which is helpful in choosing the best mitigation method. For instance, although certain assaults may call for the banning of specific IP addresses, others may call for more involved security measures like rate limitation or traffic shaping.

Overall, the outcomes of using deep learning to 5G slicing DDoS attack detection have been quite encouraging. The detection and mitigation of DDoS assaults might be revolutionised by this technology, offering a more effective and dependable method of network protection. Deep learning algorithms can play a role in creating resilient systems that can identify and mitigate DDoS assaults as the use of 5G networks grows.

VI CONCLUSION

The LSTM-based Deep Secure framework provides models for slice prediction and attack detection. The slice rediction model predicts the proper slices for genuine UEs, whereas the attack detection model predicts DDoS assaults from the UE network traffic. The Canadian Institute of Cybersecurity's CIC DDoS 2019 dataset was used to assess the proposed approach. The findings demonstrated that the suggested attack detection model acquired the lowest rate, very near to zero in MSE, and the greatest rate of over 99% in accuracy, AUC, precision, recall, and F1 Score. As a result, it outperformed Secure5G and SVM, a machine learning approach, at identifying DDoS assaults.

Additionally, the slice prediction model recorded the greatest rates of over 98% in terms of accuracy, precision, recall, F1 Score, and over 97% in terms of AUC. Additionally, the slice prediction model yielded the lowest rate in MSE, which is quite near to zero. Even though the model is superior than previous comparable efforts, it was only trained to recognise UDP flood assaults. However, the model may be changed to recognise more volume-based attack types. For feature extraction, only the best features are chosen; however, including more features may assist to increase accuracy.

REFERENCES

[1] L.Yang and H. Zhao, “DDoS attack identification and defense using SDN based on machine learning method,” in Proc. 15th Int. Symp. Pervasive Syst. Algorithms Netw. (ISPAN), 2018, pp. 174–178.
[2] P. Bojovic, I. Bašicevic, S. Ocovaj, and M. Popovic, “A practical ´ approach to detection of distributed denial-of service attacks using a hybrid detection method,” Comput. Electr. Eng., vol. 73, pp. 84–96, Jan.2019.
[3] R. Swami, M. Dave, and V. Ranga, “Defending DDoS against software defined networks using entropy,” in Proc. 4th Int. Conf. Internet Things Smart Innov. Usages (IoT-SIU), 2019, pp. 1–5.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125126

[4] D. Sattar and A. Matrawy, "Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices," in Proc. IEEE Conf. Commun. Netw. Security (CNS), 2019, pp. 82–90.
[5] K. Sahoo et al., "An evolutionary SVM model for DDoS attack detection in software defined networks," IEEE Access, vol. 8, pp. 132502–132513, 2020
[6] A.Thantharate, R. Paropkari, V. Walunj, C. Beard, and P. Kankariy, "Secure5G: A deep learning framework towards a secure network slicing in 5G and beyond," in Proc. 10th Annu. Comput. Commun.Workshop Conf. (CCWC), 2020, pp. 852–857.
[7] S. Zhang, "An overview of network slicing for 5G," IEEE Wireless Commun., vol. 26, no. 3, Jun. 2019,pp. 111– 117
[8] R. Olimid and G. Nencioni, "5G network slicing: A security overview," IEEE Access, vol. 8,2020,pp. 99999–100009.
[9] A. Thantharate, R. Paropkari, V. Walunj, C. Beard, and P. Kankariy, "Secure5G: A deep learning framework towards a secure network slicing in 5G and beyond," in Proc. 10th Annu. Comput. Commun.Workshop Conf. (CCWC), 2020, pp. 852–857.
[10] Sharafaldin, A. Lashkari, S. Hakak, and A.A.Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in Proc. Int. Carnahan Conf. Security Technol. (ICCST), 2019, pp. 1-6.