International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
OPEN ACCESS
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST25121154

Advancing Cybersecurity: A Machine Learning Framework for Detecting Distributed Denial of Service (DDoS) Attacks

[1]Aman Anand, [2]Prof. Manish Kumar Singhal
[1]M.tech Scholar, [2]Associate Professor & H.O.D
[1,2]Department of Information Technology (IT)
[1,2] NRI Institute of Information Science and Technology, Bhopal, Madhya Pradesh, India
[1]amananand3797@gmail.com, [2]manishsinghal.nirt@gmail.com

ARTICLEINFO

Article History:

Accepted : 04 Jan 2025
Published: 07 Jan 2025

Publication Issue :
Volume 12, Issue 1
January-February-2025

Page Number :
37-45

ABSTRACT

This paper explores the nature of threats posed by Distributed Denial of Service (DDoS) attacks on large networks, such as the Internet, emphasizing the need for effective detection and response mechanisms. These mechanisms must be implemented not only at the network edge but also within its core. The paper introduces methods to detect DDoS attacks by analyzing entropy and frequency-sorted distributions of specific packet attributes. Anomalies in these attributes' characteristics serve as indicators of potential DDoS attacks. The proposed methods are evaluated for detection accuracy and performance using live traffic traces collected from diverse network environments, including core Internet nodes and edge networks. Results demonstrate the effectiveness of these methods against current DDoS attacks and provide insights into improving detection capabilities for more sophisticated, stealthier threats. Additionally, the paper describes a detection-response prototype and discusses how the detection system can be extended to support effective response decision-making.

Keywords : Distributed denial of service (DDoS), Attack Detection, Machine Learning, Neural Network, ANN Approach, MATLAB, 5G Network.

INTRODUCTION

The introduction of 5G networks and IoT infrastructure is anticipated to enable more stable and reliable connections and communications. The advanced radio access technology of 5G offers features like low latency, high availability, and exceptional efficiency, which significantly benefit various IoT applications. However, 5G-enabled IoT technologies must go beyond merely enhancing network speed;

they should also prioritize security and improve service reliability.

A study commissioned by the European Union highlights concerns over the increased dependence on software to manage 5G networks, which could expose vulnerabilities that are likely to become more pronounced. A successful attack on a 5G network could have severe repercussions, as cybercriminals exploit these vulnerabilities to gain access to sensitive data, demand ransom, or disrupt network availability. Consequently, 5G networks are particularly susceptible to security threats, both internal and external. Internal threats, such as those posed by individuals working within the network, can lead to data breaches and service manipulation, further emphasizing the need for robust security measures.

A. An Attack-Resistant 5G IOT Infrastructure

A layered system is proposed to enhance the security of 5G networks in the context of the Internet of Things (IoT). This architecture integrates security mechanisms to detect and respond to potential attacks in 5G-enabled IoT networks.

Overview of a Secure 5G-Enabled IoT Architecture

Figure 1 illustrates a hierarchical security architecture for 5G-enabled IoT networks, leveraging distributed multi-access edge computing (MEC). This architecture is divided into three primary layers: the access layer, the MEC layer, and the cloud layer.

- **Access Layer**: Devices in this layer send data to the MEC layer for processing.
- **MEC Layer**: The MEC layer serves as an intermediary, receiving data from devices in the access layer. It relies on computing hardware such as servers, connection devices, or communication routers. This layer processes and forwards information in real-time to gateways connected to the 5G network.
- **Cloud Layer**: High-priority IoT applications, which require instantaneous data transmission, benefit from the rapid communication capabilities of the 5G network.

Gateways within the architecture manage device-to-device communication and ensure command signals are relayed accurately to their destinations, enabling efficient and secure operation of IoT systems.

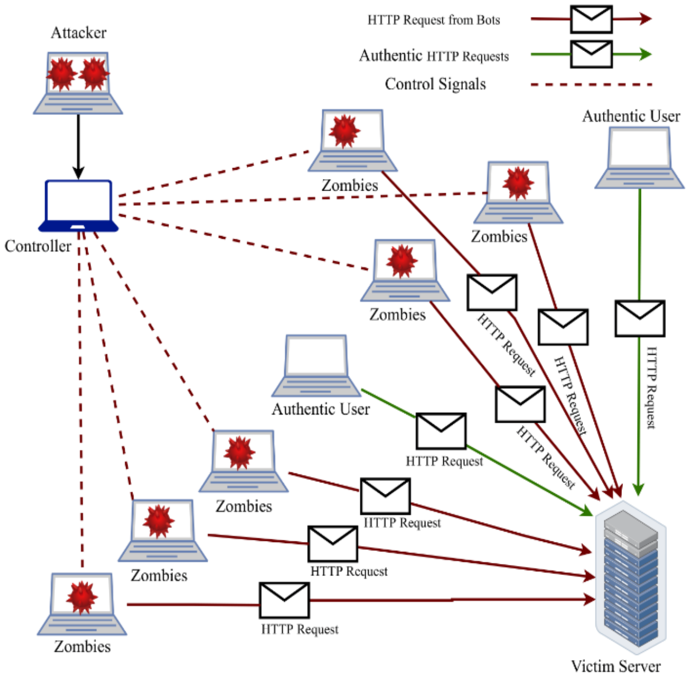

Figure -1 Schematic diagram of a DDoS attack.

B. Types of DDoS attacks

- Volumetric
- Protocol
- Application

LITERATURE SURVEY

The literature survey discusses the user wants faster data transmission speed and secures services. 5G NR promise to deliver all the basic as well as advanced facilities in contrast to prior. This technology allows users to high-definition and volume data within a second. 5G Technology 5G can handle larger traffic to cover the massive demand of the devices.

P. Arun Raj Kumar et.al (2024) - The widespread adoption of the Communication (TCP/IP) protocol stack, coupled with the increasing availability of advanced attack tools, has led to a rise in network hackers who intentionally or unintentionally target networks, resulting in Distributed Denial of Service (DDoS) attacks. Existing machine learning techniques, such as neural classifiers, have been employed to detect these attacks. However, these classifiers often suffer from limited generalization capabilities, leading to reduced performance and a high rate of false positives.

This paper examines the performance of various machine learning algorithms to identify an optimal base classifier, using the publicly available KDD Cup dataset for evaluation. Based on experimental results, the Resilient Back Propagation (RBP) algorithm was selected as the base classifier for further research. The primary focus of this study is to enhance the performance of the RBP classifier [01].

Sura Abdulmunem Mohammed Al-Juboori et.al. (2023) Man-in-the-Middle (MITM) and Denial-of-Service (DoS) attacks are two prevalent types of network intrusions that allow attackers to compromise connected devices and steal sensitive information. In this study, datasets related to MITM and DoS attacks were sourced from the Kaggle platform. Various machine learning algorithms were employed to mitigate these attacks and enhance device security. The acquired dataset underwent preprocessing steps, including handling missing values, as it contained a significant amount of null entries. [02].

Mustafa S. Ibrahim Alsumaidaie et.al. (2023) - Distributed Denial of Service (DDoS) attacks have become increasingly prevalent and advanced, driven by the rapid growth of 5G networks, smart devices, and the Internet of Things (IoT). These developments pose significant challenges to cybersecurity. This study aims to propose an effective method for detecting and preventing DDoS attacks to safeguard communication networks against such threats. The proposed method, referred to as the "Intelligent Distributed Denial of Service Attacks Detection (IDDOSAD) Approach," leverages ensemble learning combined with supervised machine learning techniques. These include Random Forests, Decision Trees, K-Nearest Neighbors (KNN), XGBoost, and Support Vector Machines (SVM). The methodology involves key steps such as data collection, preprocessing, dataset splitting into training and testing subsets, selecting predictive models, and evaluating their performance to enhance detection accuracy [03].

Marian Gusatuet.al. (2022):- Multi-access Edge Computing (MEC), a key enabler of 5G technology, aims to bring cloud computing resources closer to end users. This article addresses the challenge of mitigating Distributed Denial-of-Service (DDoS) attacks within the 5G MEC framework. It proposes solutions that integrate virtualized environments with the management components of the MEC architecture. Building on previous research, the proposed measures are designed to reduce the risk of DDoS attacks disrupting legitimate traffic [04].

Yea-Sul Kim et.al. (2022):- The primary objective of next-generation 5G cellular networks is to create larger, low-latency Internet of Things (IoT) ecosystems. However, vulnerable IoT devices could potentially be exploited for distributed denial of service (DDoS) attacks targeting 5G mobile carriers at terabit-per-second (Tbps) scales. As a result, integrating machine learning (ML) for autonomous network intrusion detection is gaining traction in 5G networks. It is anticipated that ML-driven DDoS attack monitoring will significantly enhance the speed and efficiency of threat detection in these advanced networks [05].

Nashid Shahriar et.al(2021):- A key technology that enables 5G networks is network slicing, which allocates dedicated logical resources for different applications on a single physical network. However, denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks pose a significant threat, potentially disrupting the performance and functionality of network slices. Moreover, current methods for detecting DoS/DDoS attacks often rely on datasets from 5G network simulations rather than real-world 5G network slices. This study first explores how DDoS attacks can negatively affect performance metrics, such as latency and bandwidth, for users within network slices [06].

Vijey Thayananthan. et.al (2021):- The fifth-generation (5G) network facilitates a wide range of systems, including reliable communication for applications that demand the highest levels of security. Numerous servers are leveraging different Cloud Technology (DC) architectures to explore new network topologies, which in turn accelerates the development of Software-Defined Networking (SDN). Distributed Denial of Service (DDoS) attacks, launched by malicious users, present significant security challenges to SDN-based 5G networks. While several approaches exist to mitigate DDoS attacks in SDN environments, safeguarding the SDN controller remains one of the most complex and critical issues in the field [07].

Amit V Kachavimath et.al. (2020) - The successful implementation and operation of the Internet of Things (IoT) relies heavily on the adoption of effective data transmission protocols. Among these, the widely used publish/subscribe Message Queuing Telemetry Transport (MQTT) protocol plays a key role in IoT applications. As the adoption of MQTT grows, especially among IoT manufacturers, the cybersecurity threats targeting the protocol are expected to rise. In particular, Application Layer Denial of Service (DoS) attacks, which have been known to cause major disruptions in traditional systems, pose a significant threat to IoT devices. This study presents a framework for detecting DoS attacks at the application layer for the MQTT protocol and evaluates its effectiveness in real-world DoS attack scenarios that align with the protocol's structure. We propose an MQTT-specific machine learning-based detection system designed to protect message brokers from such threats. Our analysis tests the impact of these attacks on various MQTT brokers and assesses the framework's efficiency in identifying malicious activity. The results show that even when MQTT brokers experience denial of legitimate access and limited resources, attackers can still overwhelm the server. Additionally, our investigation into MQTT properties revealed a high level of accuracy in detecting attacks, with length- and field-based characteristics being especially effective in identifying IoT-specific threats, which in turn reduced the false positive rate [08].

Ferhat Ozgur Catak et.al. (2019) - Due to the increasing use of botnets, fuzziers, shellcode, and other network-related vulnerabilities, many organizations are facing overwhelming amounts of network traffic, much of which consists of network attacks. These attacks disrupt daily operations, negatively impacting the business. Utilizing classification models can help identify and distinguish these attacks more quickly. Distributed denial of service (DDoS) attacks aim to disrupt or reduce the availability of services for legitimate users. The primary objective of this project was to classify network traffic using deep learning techniques and network flow models. A deep neural network-based approach was employed to enhance the classification performance of the system. The classification performance of network traffic, as evaluated by the model used in this study, is depicted in figures and tables, along with relevant metrics. The results indicate that the proposed model is capable of identifying DDoS attacks with a high level of accuracy using deep learning methods [09].

METHOD

Advancing cybersecurity to address Distributed Denial of Service (DDoS) attacks involves leveraging machine learning frameworks that enhance the ability to detect and mitigate such threats effectively. A machine learning-based framework operates by analyzing network traffic patterns, identifying anomalies, and distinguishing between legitimate traffic and malicious activity. This process begins with the collection of extensive datasets, including normal traffic and DDoS attack data, which are preprocessed to remove noise and extract relevant features. Advanced algorithms, such as supervised or unsupervised learning models, are then trained to recognize attack patterns. Techniques like Support Vector Machines (SVM), Neural Networks, and Decision Trees are commonly employed for classification tasks. Additionally, real-time detection is facilitated by integrating the machine learning model with network monitoring tools, enabling swift responses to mitigate attacks.

A machine learning framework for detecting DDoS attacks can be amplified through feature selection and dimensionality reduction techniques, such as Principal Component Analysis (PCA) or Recursive Feature Elimination (RFE). These methods help focus on the most significant attributes, improving model accuracy and reducing computational overhead. Furthermore, ensemble learning techniques, such as Random Forests and Gradient Boosting Machines, combine the predictions of multiple models to enhance detection performance.

To further bolster the framework, real-time streaming analytics and cloud-based solutions can be employed. By deploying the framework in a distributed architecture, organizations can monitor and analyze vast volumes of traffic across multiple nodes, ensuring scalability and responsiveness. Collaboration with threat intelligence platforms also aids in enriching the model with real-time updates on emerging DDoS patterns and attack vectors.

The application of machine learning in DDoS detection is not without challenges. False positives, model drift due to changes in network behavior, and adversarial attacks aimed at deceiving the model are some common issues. Addressing these challenges requires regular retraining of models, robust validation techniques, and the integration of adversarial learning mechanisms.

a. Proposed Work

An Artificial Neuron Network (ANN) is a computer model designed to mimic the structure and functions of biological neural networks. In the field of Computer Science, it operates similarly to the human nervous system, receiving, processing, and transmitting data. ANNs typically consist of three main layers:

- **Input Layer**: This is where all input data is introduced into the model.
- **Hidden Layers**: These layers, which may include multiple stages, process the data received from the input layer.
- **Output Layer**: After processing, the results are provided through the output layer.

b. Applications Should Neural Networks Be Used

They serve as universal approximates and are most effective when applied to systems that can tolerate some level of error. Neural networks are an example of such systems. For tasks like balancing a checkbook, using a neural network would not be ideal! However, they excel in the following areas:

- Identifying relationships or uncovering patterns within a dataset;
- Handling large datasets with significant size, variety, or complexity;
- Situations where the relationships between factors are not well understood;
- When it is challenging to describe the connections using traditional methods.

CONCLUSION

The conclusion of the integration of machine learning into cybersecurity has proven to be a transformative approach for mitigating Distributed Denial of Service (DDoS) attacks. By leveraging advanced algorithms, such frameworks can identify attack patterns in real time, enabling proactive responses that minimize disruption. This study demonstrates that machine learning not only enhances detection accuracy but also adapts to evolving attack vectors, ensuring robust defense mechanisms. As cyber threats become increasingly sophisticated, the continuous refinement of such frameworks will be critical to safeguarding digital infrastructures. This multidisciplinary approach can address challenges such as data privacy, model interpretability, and the scalability of detection systems. Future research should focus on improving the resilience of these frameworks against adversarial attacks and exploring hybrid solutions that combine machine learning with traditional cybersecurity measures. Ultimately, advancing machine learning frameworks will play a pivotal role in creating a safer and more resilient cyberspace for individuals, organizations, and critical infrastructure worldwide.

REFERENCES

[1]. P. Arun Raj Kumar, S. Selvakumar "Distributed denial of service attack detection using an ensemble of neural classifier" Volume 34, Issue 11, 15 July 2011, Pages 1328-1341.

[2]. Sura Abdulmunem Mohammed Al-Juboori, Firas Hazzaa1 , Zinah Sattar Jabbar, Sinan Salih2 , Hassan Muwafaq Gheni ―Man-in-the-middle and denial of service attacks detection using machine learning algorithms‖ Vol. 12, No. 1, February 2023, pp. 418~426.

[3]. Mustafa S. Ibrahim Alsumaidaie Khattab M. Ali Alheeti 1 , Abdul Kareem Alaloosy ―Intelligent Detection of Distributed Denial of Service Attacks: A Supervised Machine Learning and Ensemble Approach‖ March 2023.

[4]. Guşatu, Marian, and Ruxandra F. Olimid. "Improved security solutions for DDoS mitigation in 5G Multi-access Edge Computing." In International Conference on Information Technology and Communications Security, pp. 286-295. Springer, Cham, 2022.

[5]. Kim, Ye-Eun, Yea-Sul Kim, and Hwankuk Kim. "Effective Feature Selection Methods to Detect IoT DDoS Attack in 5G Core Network." Sensors 22, no. 10 (2022): 3819.

[6]. Al-Shareeda, Mahmood A., and Selvakumar Manickam. "MSR-DoS: Modular Square Root-based Scheme to Resist Denial of Service (DoS) Attacks in 5G-enabled Vehicular Networks." IEEE Access (2022).

[7]. Gao, Qinghang, Hao Wang, Liyong Wan, Jianmao Xiao, and Long Wang. "G/M/1- Based DDoS Attack Mitigation in 5G Ultradense Cellular Networks." Wireless Communications and Mobile Computing 2022 (2022).

[8]. Dr. D.Ganesh, Dr.K.Suresh, Dr.M.Sunil Kumar ―Improving Security in Edge Computing by using Cognitive Trust Management Model‖ 2022.

[9]. Ling Hou , Mark A. Gregory And Shuo Li ―Multi-Access Edge Computing and Vehicular Networking‖ 21 November 2022.

[10]. Khan, Md Sajid, Behnam Farzaneh, Nashid Shahriar, NiloySaha, and Raouf Boutaba. "SliceSecure: Impact and Detection of DoS/DDoS Attacks on 5G Network Slices.(2021)".

[11]. Alamri, Hassan A., VijeyThayananthan, and Javad Yazdani. "Machine Learning for Securing SDN based 5G network." Int. J. Comput. Appl 174, no. 14 (2021): 9-16.

[12]. Sakib Shahriar Shafin, Sakir Adnan Prottoy , Saif Abbas , Safayat Bin Hakim, Abdullahi Chowdhury , and Md. Mamunur Rashid ―Distributed Denial of Service Attack Detectionusing Machine Learning and Class Oversampling‖ 2021. 60

[13]. Amit V Kachavimath, Shubhangeni Vijay Nazare and Sheetal S Akki ―Distributed Denial of Service Attack Detection using Naïve Bayes and K-Nearest Neighbor for Network Forensics‖ 2020.

[14]. Kim, Youngsoo, Jong Geun Park, and Jong-Hoon Lee. "Security threats in 5G edge computing environments." In 2020 International Conference on Information and Communication Technology Convergence (ICTC), pp. 905-907. IEEE, 2020.

[15]. Ferhat Ozgur Cataka, and Ahmet Fatih Mustacoglub ―Distributed denial of service attack detection using autoencoder and deep neural networks‖ 2019.

[16]. Animesh Gupta ―Distributed Denial of Service Attack Detection Using a Machine Learning Approach‖ 2018.

[17]. Moudoud, Hajar, Lyes Khoukhi, and Soumaya Cherkaoui. "Prediction and detection of fdia and ddos attacks in 5g enabled iot." IEEE Network 35, no. 2 (2020): 194-201.

[18]. Sharafaldin, Iman, Arash Habibi Lashkari, Saqib Hakak, and Ali A. Ghorbani. "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy." In 2019 International Carnahan Conference on Security Technology (ICCST), pp. 1-8. IEEE, 2019.

[19]. Ni, Jianbing, Xiaodong Lin, and Xuemin Sherman Shen. "Efficient and secure serviceoriented authentication supporting network slicing for 5G-enabled IoT." IEEE Journal on Selected Areas in Communications 36, no. 3 (2018): 644-657.

[20]. Li, Dong, Chang Yu, Qizhao Zhou, and Junqing Yu. "Using SVM to detect DDoS attack in SDN network." In IOP Conference Series: Materials Science and Engineering, vol. 466, no. 1, p. 012003. IOP Publishing, 2018.

[21]. Larijani, Hadi, Jawad Ahmad, and Nhamoinesu Mtetwa. "A novel random neural network based

approach for intrusion detection systems." In 2018 10th Computer Science and Electronic Engineering (CEEC), pp. 50-55. IEEE, 2018.

[22]. Adrien Bonguet and Martine Bellaiche ―A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing‖ 5 August 2017.

[23]. Zhao, S., Li, W., Zia, T., & Zomaya, A. Y. (2017, November). A dimension reduction model and classifier for anomaly-based intrusion detection in internet of things. In 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (pp. 836-843). IEEE.

[24]. Boro, Debojit, and Dhruba K. Bhattacharyya. "DyProSD: a dynamic protocol specific defense for high-rate DDoS flooding attacks." Microsystem Technologies 23 (2017): 593-611.

[25]. Azhagiri, M. "HIDDEN CONDITIONAL RANDOM FIELDS FOR INTRUSION DETECTION SYSTEM USING LAYERED APPROACH."

[26]. Mangaleswaran, M. "Layered Approach for Intrusion Detection System Using Hidden Conditional Random Fields." (2017).

[27]. Zantedeschi, Valentina, Maria-Irina Nicolae, and Ambrish Rawat. "Efficient defenses against adversarial attacks." In Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, pp. 39-49. 2017.

[28]. Boro, Debojit, Himant Basumatary, Tribeni Goswami, and Dhruba K. Bhattacharyya. "UDP flooding attack detection using information metric measure." In Proceedings of International Conference on ICT for Sustainable Development: ICT4SD 2015 Volume 1, pp. 143-153. Springer Singapore, 2016.

[29]. Timotheou, Stelios. "Fast Non-Negative Least-Squares Learning in the Random Neural Network." Probability in the Engineering and Informational Sciences 30, no. 3 (2016): 379-402.

[30]. Papernot, Nicolas, Patrick McDaniel, Arunesh Sinha, and Michael Wellman. "Towards the science of security and privacy in machine learning." arXiv preprint arXiv:1611.03814 (2016).